Introduction to Quantum Algorithms

K.C. Kong

Physics and Astronomy
University of Kansas

Department of Physics
Oklahoma State University
August 7-9, 2024

Classical Computing

- “Efficient” computation time scales polynomially with the problem size.
  - Search ~ n^4
  - $n = 1000$, $t = 1$ sec
  - $n = 1050$, $t = 1.2$ sec
- “Inefficient” computation times scales exponentially.
  - Factoring ~ 2^n
  - $n = 1000$, $t = 1$ sec
  - $n = 1001$, $t = 2$ sec
  - $n = 1012$, $t = 1$ hour
  - $n = 1050$, $t = 3.3$ million years

1	3	5	7	9	11	13	15
17	19	21	23	25	27	29	31
33	35	37	39	41	43	45	47
49	51	53	55	57	59	61	63

2	3	6	7	10	11	14	15
18	19	22	23	26	27	30	31
34	35	38	39	42	43	46	47
50	51	54	55	58	59	62	63

4	5	6	7	12	13	14	15
20	21	22	23	28	29	30	31
36	37	38	39	44	45	46	47
52	53	54	55	60	61	62	63

8	9	10	11	12	13	14	15
24	25	26	27	28	29	30	31
40	41	42	43	44	45	46	47
56	57	58	59	60	61	62	63

16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

Example: Inner product

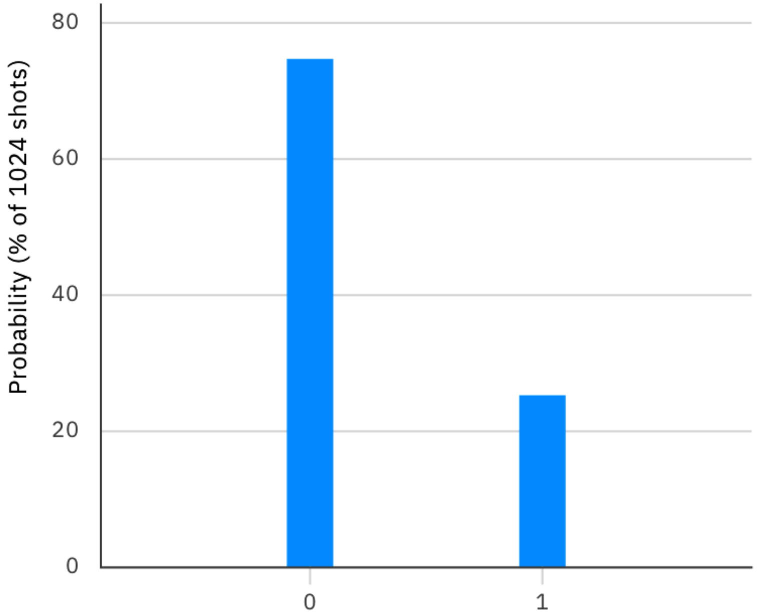
- Let $|\psi\rangle, |\phi\rangle \in \mathbb{C}^{2^n}$ be two $N = 2^n$ dimensional vectors. How to compute the magnitude of the inner product $|\langle\phi|\psi\rangle|^2$?

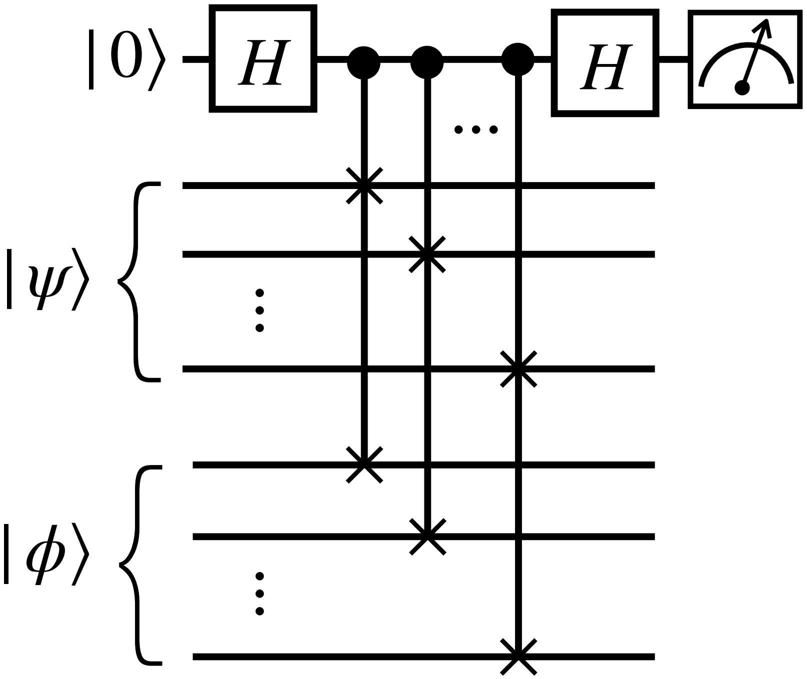
$$|\psi\rangle = (\psi_1, \cdots, \psi_N)$$

$$|\phi\rangle = (\phi_1, \cdots, \phi_N)$$

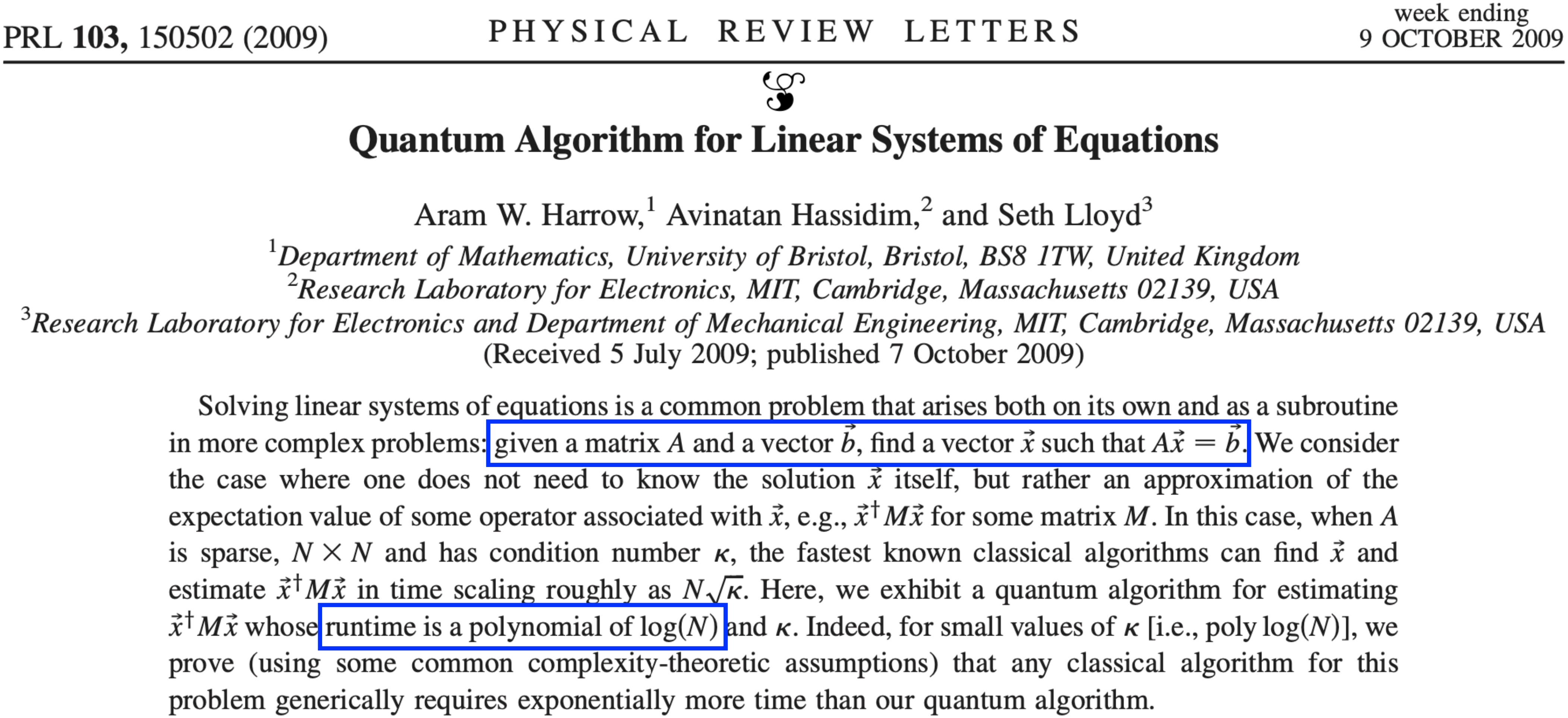
$$\langle\phi|\psi\rangle = \sum_{i=1}^{N} \phi_i^* \psi_i$$

- Digital
  - $N = 2^n$ multiplications and additions
  - Decompose multiplications and additions as NAND gates
- Quantum
  - Run the following circuits with $2n + 1$ qubits and $n + 2$ gates
  - $\mathrm{Prob}(0) - \mathrm{Prob}(1) = |\langle\phi|\psi\rangle|^2$





The First Wave of Quantum Machine Learning?



PRL **103,** 150502 (2009) PHYSICAL REVIEW LETTERS week ending 9 OCTOBER 2009

Quantum Algorithm for Linear Systems of Equations

Aram W. Harrow,[1] Avinatan Hassidim,[2] and Seth Lloyd[3]

[1] *Department of Mathematics, University of Bristol, Bristol, BS8 1TW, United Kingdom*
[2] *Research Laboratory for Electronics, MIT, Cambridge, Massachusetts 02139, USA*
[3] *Research Laboratory for Electronics and Department of Mechanical Engineering, MIT, Cambridge, Massachusetts 02139, USA*

(Received 5 July 2009; published 7 October 2009)

Solving linear systems of equations is a common problem that arises both on its own and as a subroutine in more complex problems: given a matrix A and a vector $\vec{b}$, find a vector $\vec{x}$ such that $A\vec{x} = \vec{b}$. We consider the case where one does not need to know the solution $\vec{x}$ itself, but rather an approximation of the expectation value of some operator associated with $\vec{x}$, e.g., $\vec{x}^\dagger M\vec{x}$ for some matrix M. In this case, when A is sparse, $N \times N$ and has condition number κ, the fastest known classical algorithms can find $\vec{x}$ and estimate $\vec{x}^\dagger M\vec{x}$ in time scaling roughly as $N\sqrt{\kappa}$. Here, we exhibit a quantum algorithm for estimating $\vec{x}^\dagger M\vec{x}$ whose runtime is a polynomial of $\log(N)$ and κ. Indeed, for small values of κ [i.e., poly $\log(N)$], we prove (using some common complexity-theoretic assumptions) that any classical algorithm for this problem generically requires exponentially more time than our quantum algorithm.

$$Ax = b$$

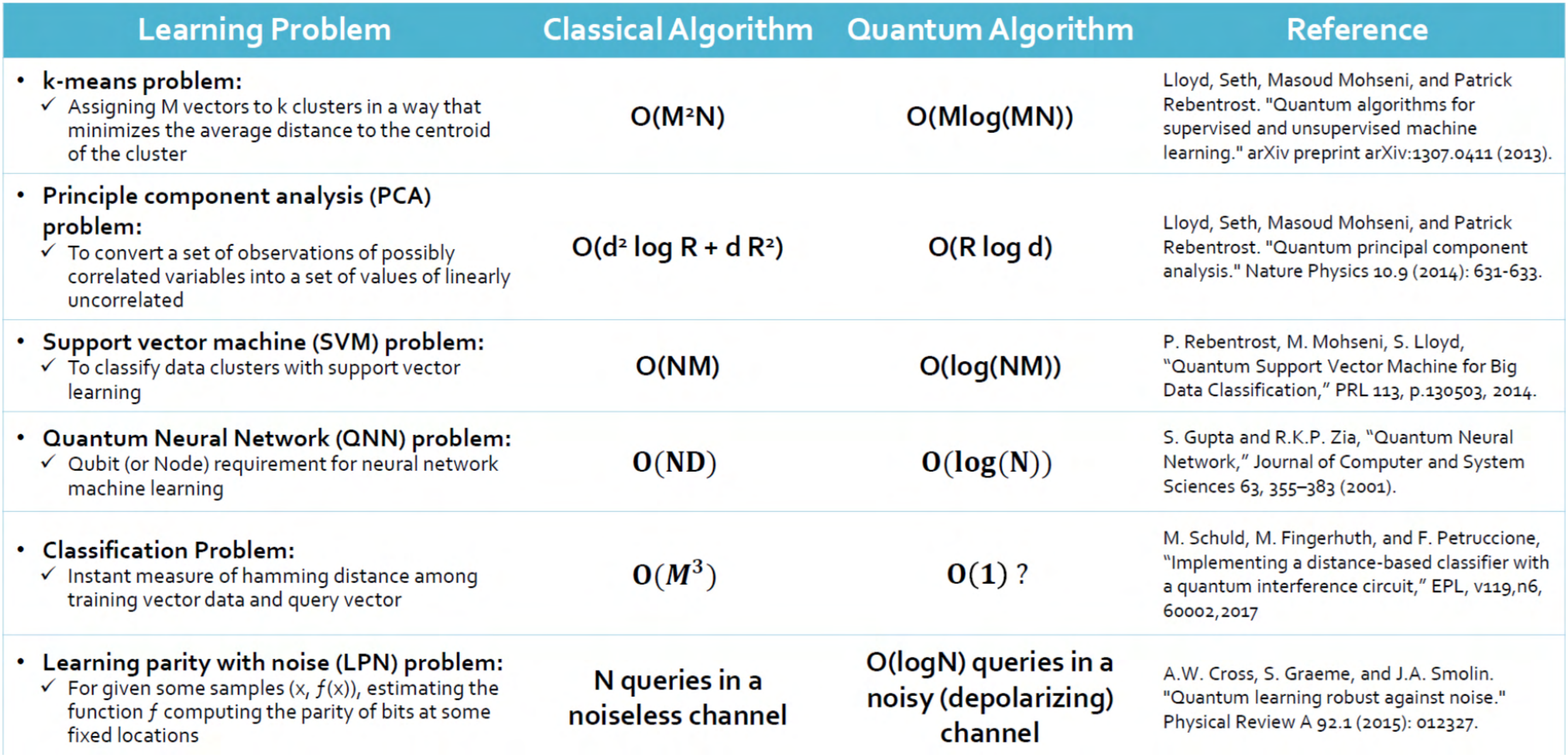
Complexity of inversion of a regular matrix=$O(N^3)$

Complexity of inversion of a sparse matrix=$O(N)$

The exponential Speed-Up

Description	Classical Algorithm	Quantum Algorithm	Reference
• **Grover's algorithm:** ✓ searches an unstructured database (or an unordered list) with N entries	$O(N)$	$O(\sqrt{N})$	L.K. Grover, "A fast quantum mechanical algorithm for database search." Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM (1996).
• **Shor's algorithm:** ✓ Integer factorization	$O\left(e^{1.9(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}\right)$	$O\left((\log N)^2(\log\log N)(\log\log\log N)\right)$	D. Beckman, et al. "Efficient networks for quantum factoring." Physical Review A 54.2 (1996).
• **Quantum Fourier Transform:** ✓ Discrete Fourier transform of size *N*	$O(N\log N)$	$O(\log N\ \log\log N)$	P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proc. 35th Annual Symp. on Foundations of Comp. Sci., pp.124-134(1994)
• **Eigenvalue solver:** ✓ To find eigenvalues and eigenvectors of a local Hamiltonian	$O(N^{2\sim 2.236})$	$O\left((\log N)^4\right)$	Abrams and S. Lloyd, "Quantum Algorithm Providing Exponential Speed Increase for Finding Eigenvalues and Eigenvectorsg." Phys. Rev. Lett. 83, 24, p.5162 (1999).
• **Matrix inversion:** ✓ Finding inverse matrix. This can be applied to find a vector x satisfying Ax=b, where A and b are Hermitian N × N matrix and a unit vector, respectively	$O(Ns\kappa(\log 1/\epsilon))$	$\tilde{O}\left(\frac{\log N\, s^2\kappa^2}{\epsilon}\right)$	A.W. Harrow, Avinatan Hassidim, and S. Lloyd. "Quantum algorithm for linear systems of equations." Physical review letters 103.15 (2009): 150502.
• **Distance (inner product) evaluation:** ✓ Calculating inner product between a given N dimensional vector and each N dimensional vector of M samples	$O(MN)$	$O(\log NM\ )$	S. Lloyd, Masoud Mohseni, and Patrick Rebentrost. "Quantum algorithms for supervised and unsupervised machine learning." arXiv preprint arXiv:1307.0411 (2013).

The exponential Speed-Up



Learning Problem	Classical Algorithm	Quantum Algorithm	Reference
• **k-means problem:** ✓ Assigning M vectors to k clusters in a way that minimizes the average distance to the centroid of the cluster	$O(M^2N)$	$O(M\log(MN))$	Lloyd, Seth, Masoud Mohseni, and Patrick Rebentrost. "Quantum algorithms for supervised and unsupervised machine learning." arXiv preprint arXiv:1307.0411 (2013).
• **Principle component analysis (PCA) problem:** ✓ To convert a set of observations of possibly correlated variables into a set of values of linearly uncorrelated	$O(d^2 \log R + d R^2)$	$O(R \log d)$	Lloyd, Seth, Masoud Mohseni, and Patrick Rebentrost. "Quantum principal component analysis." Nature Physics 10.9 (2014): 631-633.
• **Support vector machine (SVM) problem:** ✓ To classify data clusters with support vector learning	$O(NM)$	$O(\log(NM))$	P. Rebentrost, M. Mohseni, S. Lloyd, "Quantum Support Vector Machine for Big Data Classification," PRL 113, p.130503, 2014.
• **Quantum Neural Network (QNN) problem:** ✓ Qubit (or Node) requirement for neural network machine learning	$O(ND)$	$O(\log(N))$	S. Gupta and R.K.P. Zia, "Quantum Neural Network," Journal of Computer and System Sciences 63, 355–383 (2001).
• **Classification Problem:** ✓ Instant measure of hamming distance among training vector data and query vector	$O(M^3)$	$O(1)$?	M. Schuld, M. Fingerhuth, and F. Petruccione, "Implementing a distance-based classifier with a quantum interference circuit," EPL, v119,n6, 60002,2017
• **Learning parity with noise (LPN) problem:** ✓ For given some samples (x, f(x)), estimating the function f computing the parity of bits at some fixed locations	N queries in a noiseless channel	O(logN) queries in a noisy (depolarizing) channel	A.W. Cross, S. Graeme, and J.A. Smolin. "Quantum learning robust against noise." Physical Review A 92.1 (2015): 012327.

Different Quantum Advantages/Speedups

1. **A provable quantum speedup**: (gold standard)
requires a proof that there can be no classical algorithm that performs as well or better than the quantum algorithm. (grover's algorithm)

2. **A strong quantum speedup**:
compares the quantum algorithm with the best known classical algorithm. (shore's algorithm)

3. **Common quantum speedup**:
relaxes the 'best classical algorithm' to the 'best available classical algorithm'

4. **Potential quantum speedup:**
compares two specific algorithms and relating the speedup to this instance only

5. **Limited quantum speedup:**
compares conceptually equivalent algorithms

References

- Qiskit Textbook, examples and PennyLane codebook and examples
- Quantum Computing: A Gentle Introduction by E. Rieffel and W. Polak
- Machine Learning with Quantum Computers by M. Schuld and F. Petruccione
- Quantum Computation and Quantum Information by M. Nielsen and I. Chuang

- Introduction to Classical and Quantum Computing by T. Wong
- An Introduction to Quantum Machine Learning for Engineers
- A Short Introduction to Quantum Computing for Physicists by Oswaldo Zapata

HW

- Check out the following webpage
  - https://kckong.ku.edu/PHSX600-801/

- Install Qiskit / PennyLane in your laptop or Google colab.

- Create your IBM Quantum account (for IBMQ Lab and IBMQ Composer).

- Try simple Qiskit examples
  - Example 1 with single gates on colab
  - Example 2 with single qubit circuit on colab
  - Example 3 with multiple qubits and measurements

Topics to discuss

- Introduction to QM, Single qubit, and system with two or more qubits
- Quantum algorithms
- Quantum Machine Learning
  - QAOA and feedback based algorithm
  - Two applications: collider and dark matter

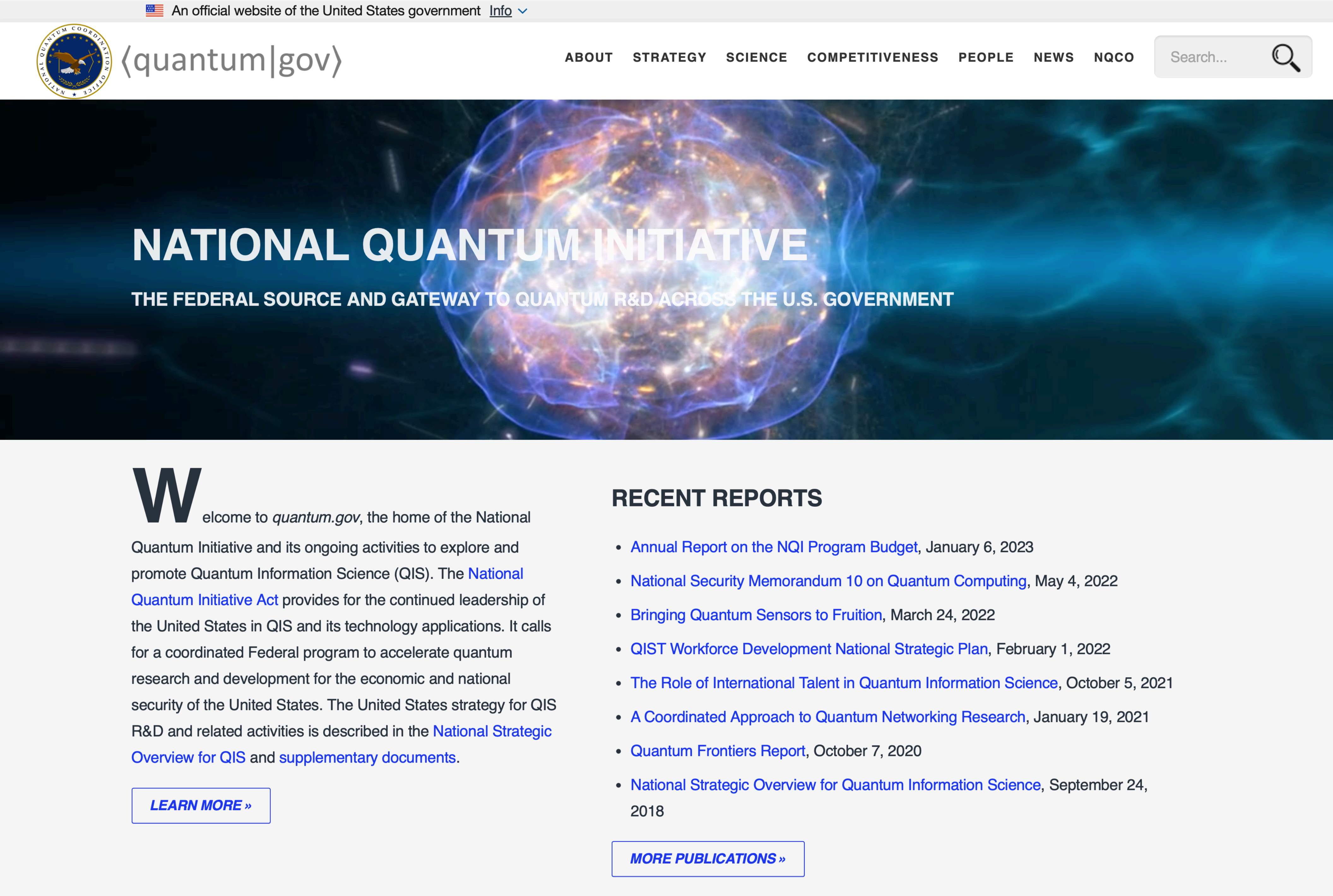
- We will not discuss
  - Hardware/experimental aspect of quantum computer
  - Computational complexity theory
  - How to use Qiskit/PennyLane
  - QRAM, quantum tomography, quantum sensing
  - Quantum communication, quantum information theory
  - Quantum cryptography, traversable wormhole
  - ……

Topics to discuss

1. Single qubit, Dirac notation, Bloch sphere and measurements
2. Quantum circuits, singlet qubit gate, two qubit gates, three qubit gates, no cloning, superdense coding, teleportation
3. Quantum algorithms, data embedding, Deutsch algorithm, Deutsch-Jozsa, Bernstein-Vazirani algorithm, Simon’s algorithm
4. Quantum Fourier Transformation and quantum phase estimation
5. Shor's algorithm and Grover’s algorithm
6. Quantum machine learning, distance-based classifier
7. Quantum optimization, QUBO, Adiabatic theorem, variational quantum algorithms
8. QAOA, FALQON, ADAPT-QAOA
9. Single qubit-classifier using data re-uploading
10. Harrow-Hassidim-Lloyd Algorithm (Ax=b)
11. Quantum error correction, bit flip error correction, stabilizer formalism, phase flip error correction

Very brief history of quantum computing

- 1924 The term “quantum mechanics” used by M. Born
- 1925 Formulation of matrix mechanics by Heisenberg, Born, Jordan
- 1925-1927: Copenhagen interpretation
- 1930 “The principles of quantum mechanics” by Dirac
- 1935 Einstein, Podolsky and Rosen
- 1935 “Quantum entanglement” and Schrödinger’s cat by Schrodinger and Einstein
- 1947 “Spooky action at a distance” in a letter to M. Born by A. Einstein
- 1976 Attempt to create quantum information theory
- 1980 Quantum mechanical model of Turing machine by Benioff (ANL)
- 1981 “Simulating Physics with Computers" by Feynman
- 1985 Quantum Turing machine by Deutsch
- 1992 Deutsch-Jozsa algorithm
- 1993 First paper on quantum teleportation
- 1994 Shor’s factoring algorithm (cf RSA encryption)
- 1996 Grover search algorithm (Bell)
- 2004 First five photon entanglement by China
- 2011 First commercially available quantum computer (D-Wave)
- 2017 First quantum teleportation of independent single-photon qubit (14km) by China
- 2018 US National Quantum Initiative Act
- 2019 Google quantum supremacy
- 2022 Nobel prize (Aspect, Clauser , Zeilinger) for violation of Bell’s inequality
- 2022 433 qubits by IBM
- 2023 Breakthrough Prize (Bennet, Brassard, Shor, Deutsch)



NATIONAL QUANTUM INITIATIVE

THE FEDERAL SOURCE AND GATEWAY TO QUANTUM R&D ACROSS THE U.S. GOVERNMENT

Welcome to *quantum.gov*, the home of the National Quantum Initiative and its ongoing activities to explore and promote Quantum Information Science (QIS). The National Quantum Initiative Act provides for the continued leadership of the United States in QIS and its technology applications. It calls for a coordinated Federal program to accelerate quantum research and development for the economic and national security of the United States. The United States strategy for QIS R&D and related activities is described in the National Strategic Overview for QIS and supplementary documents.

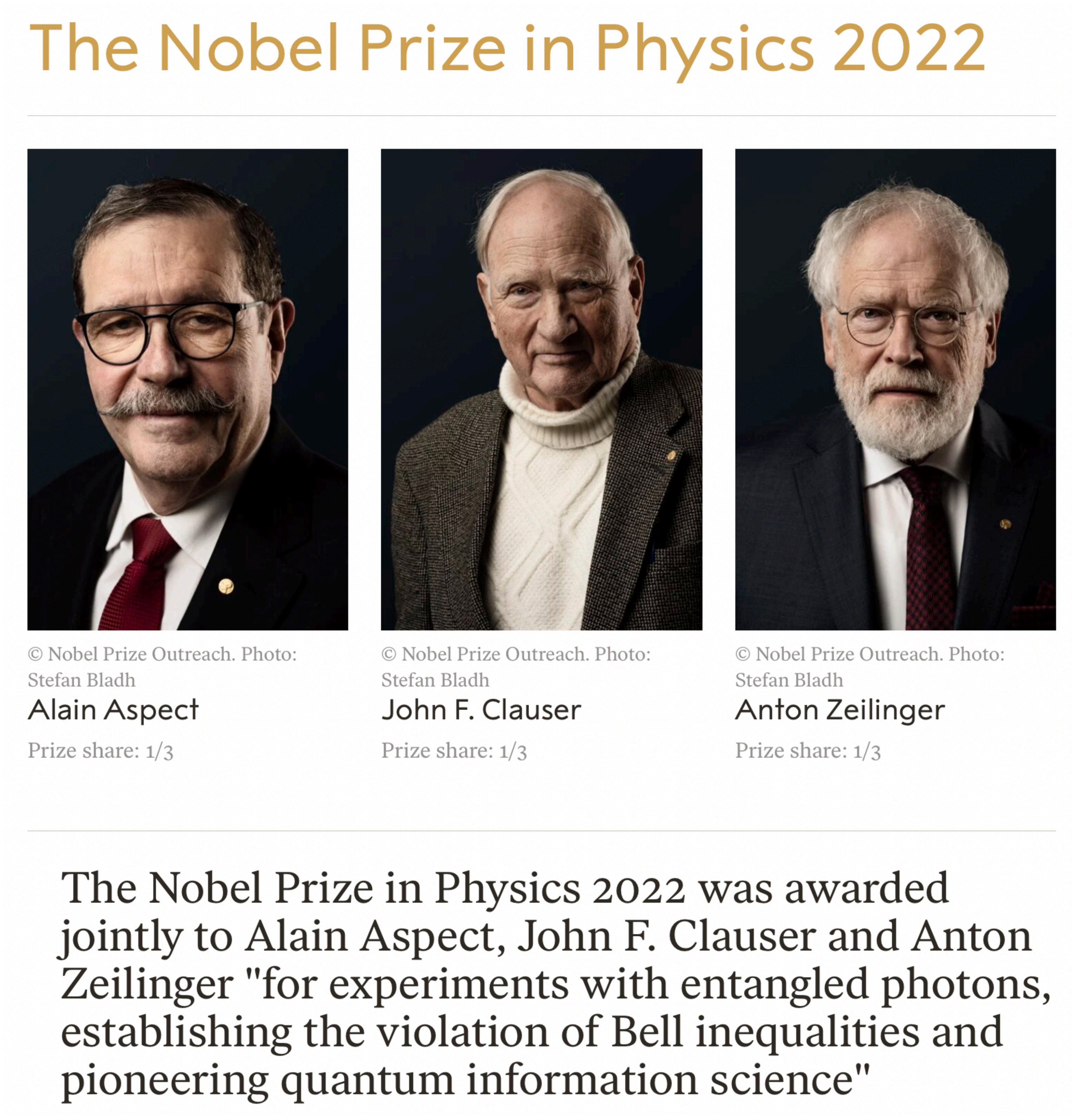
LEARN MORE »

RECENT REPORTS

- Annual Report on the NQI Program Budget, January 6, 2023
- National Security Memorandum 10 on Quantum Computing, May 4, 2022
- Bringing Quantum Sensors to Fruition, March 24, 2022
- QIST Workforce Development National Strategic Plan, February 1, 2022
- The Role of International Talent in Quantum Information Science, October 5, 2021
- A Coordinated Approach to Quantum Networking Research, January 19, 2021
- Quantum Frontiers Report, October 7, 2020
- National Strategic Overview for Quantum Information Science, September 24, 2018

MORE PUBLICATIONS »

NATIONAL QUANTUM INITIATIVE



The Nobel Prize in Physics 2022

© Nobel Prize Outreach. Photo: Stefan Bladh

Alain Aspect

Prize share: 1/3

© Nobel Prize Outreach. Photo: Stefan Bladh

John F. Clauser

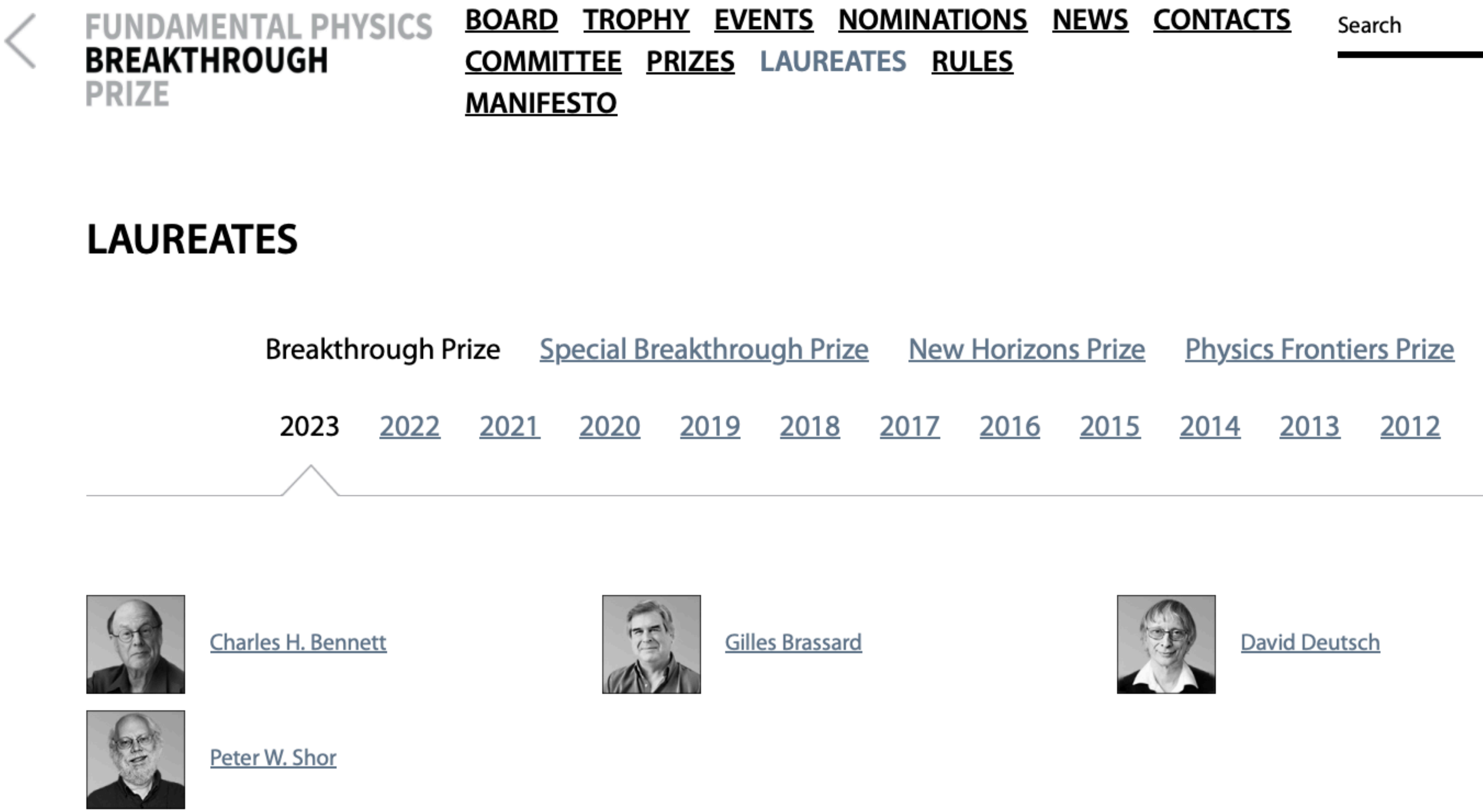
Prize share: 1/3

© Nobel Prize Outreach. Photo: Stefan Bladh

Anton Zeilinger

Prize share: 1/3

The Nobel Prize in Physics 2022 was awarded jointly to Alain Aspect, John F. Clauser and Anton Zeilinger "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science"



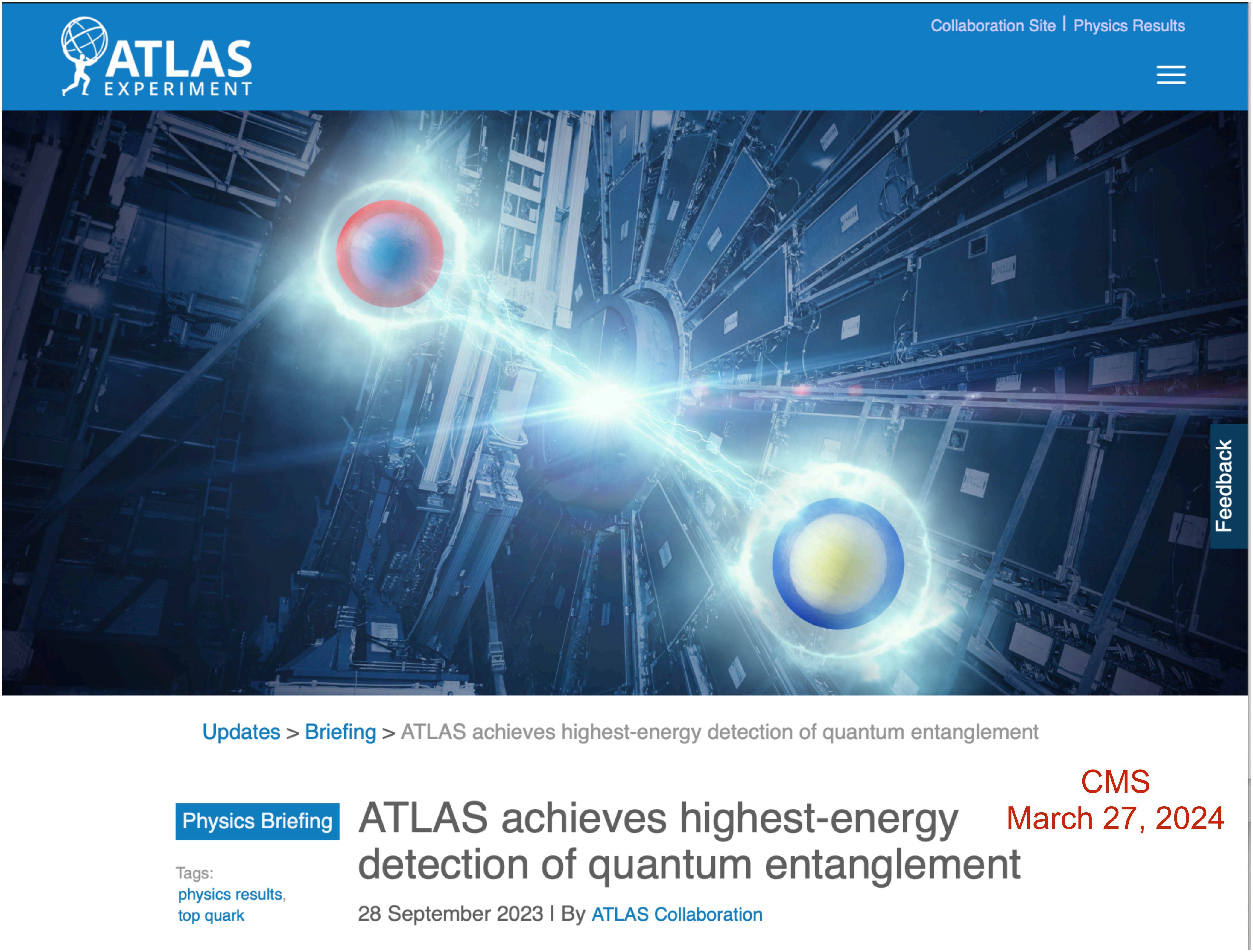
LAUREATES

Charles H. Bennett

Gilles Brassard

David Deutsch

Peter W. Shor



Updates > Briefing > ATLAS achieves highest-energy detection of quantum entanglement

Physics Briefing

ATLAS achieves highest-energy detection of quantum entanglement

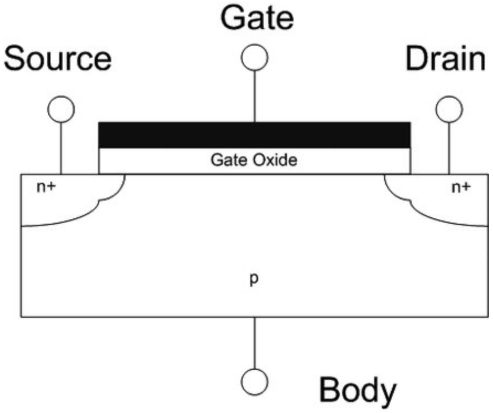
Tags:
physics results,
top quark

28 September 2023 | By ATLAS Collaboration

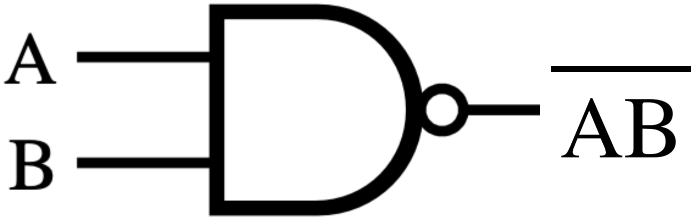
CMS
March 27, 2024

Digital Computing

Digital computation with n bits: $\{0,1\}^n \longrightarrow \{0,1\}^m, \quad m \leq n$



$+$



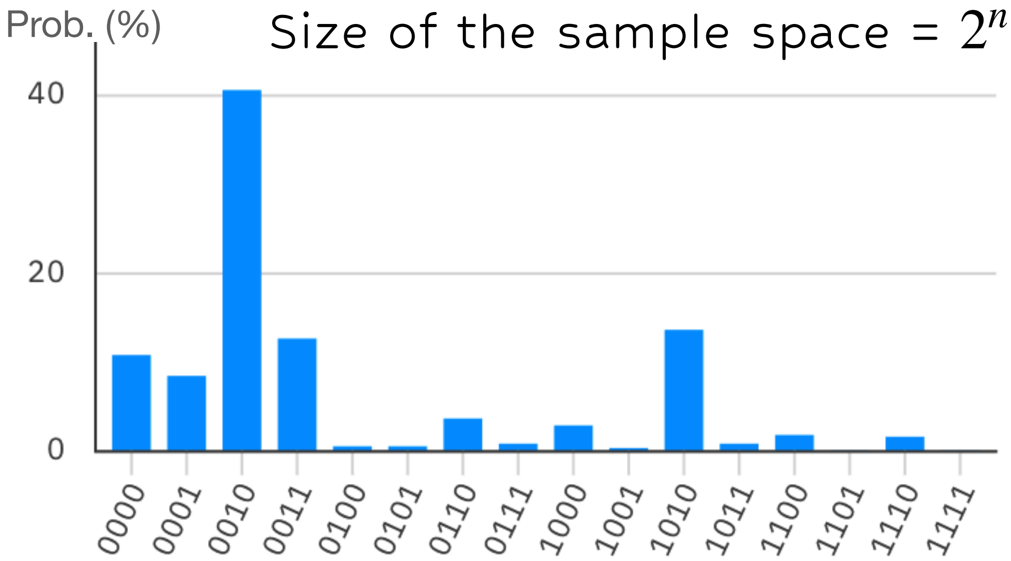
A	B	$\overline{AB}$
0	0	1
0	1	1
1	0	1
1	1	0

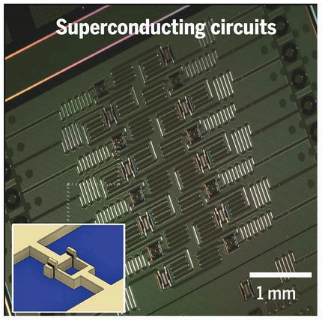
Quantum computing?

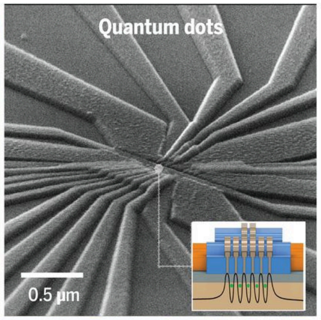
Quantum computation with n qubits:

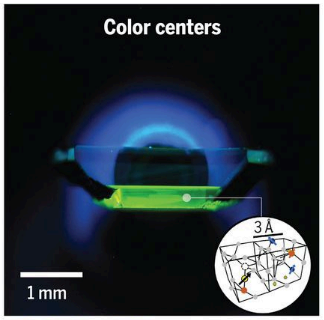
$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{2^n} \end{pmatrix} \in \mathbb{C}^{2^n}$$

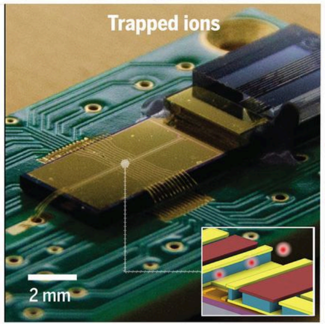
Size of the sample space = 2^n

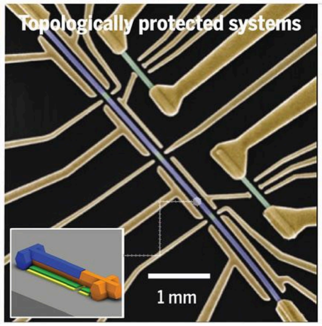






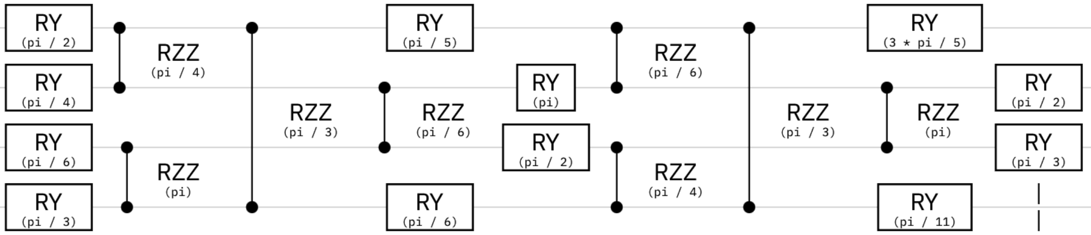






+

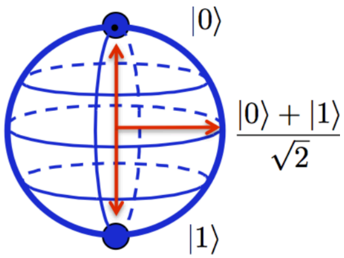
Unitary transformation



Need transition form classical to quantum:

Classical Bit

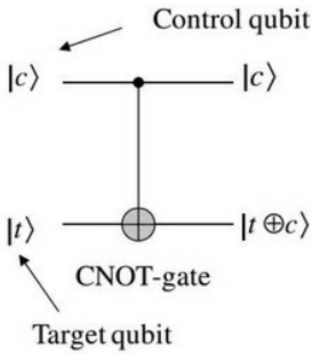
Classical Quantum



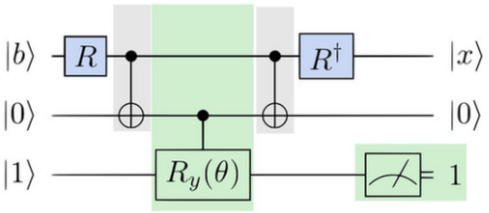
Qubit

bits ⟷ qubits

gates ⟷ quantum gates



algorithms ⟷ quantum algorithms



Example: Inner product

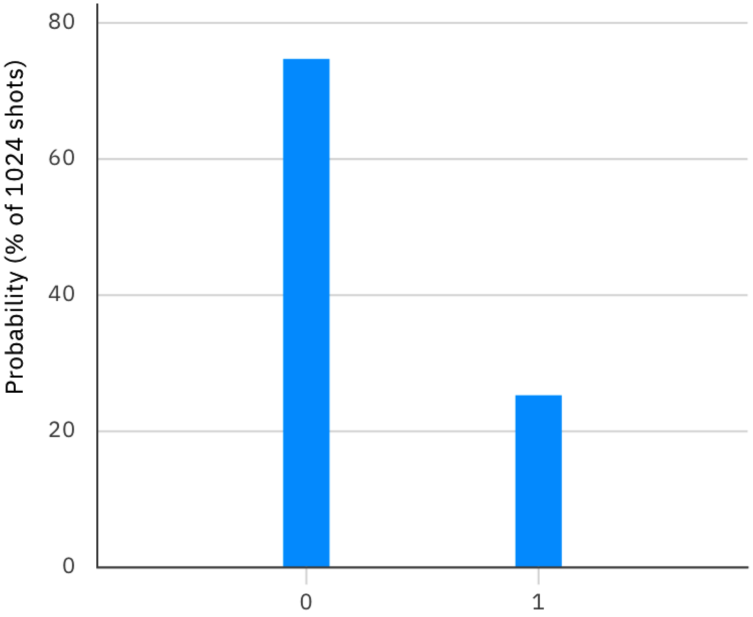
- Let $|\psi\rangle, |\phi\rangle \in \mathbb{C}^{2^n}$ be two $N = 2^n$ dimensional vectors. How to compute the magnitude of the inner product $|\langle\phi|\psi\rangle|^2$?

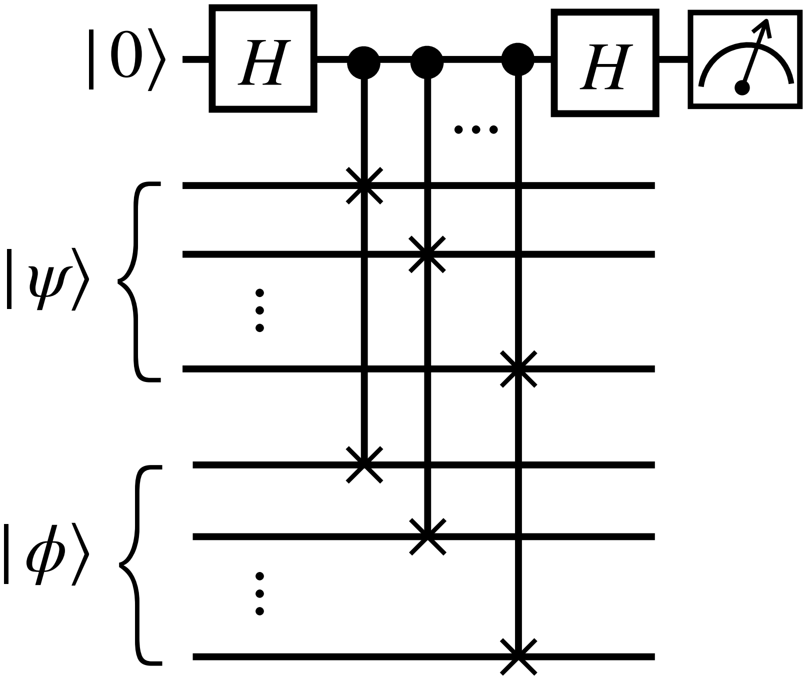
$$|\psi\rangle = (\psi_1, \cdots, \psi_N)$$

$$|\phi\rangle = (\phi_1, \cdots, \phi_N)$$

$$\langle\phi|\psi\rangle = \sum_{i=1}^{N} \phi_i^* \psi_i$$

- Digital
  - $N = 2^n$ multiplications and additions
  - Decompose multiplications and additions as NAND gates
- Quantum
  - Run the following circuits with $2n + 1$ qubits and $n + 2$ gates
  - $\mathrm{Prob}(0) - \mathrm{Prob}(1) = |\langle\phi|\psi\rangle|^2$

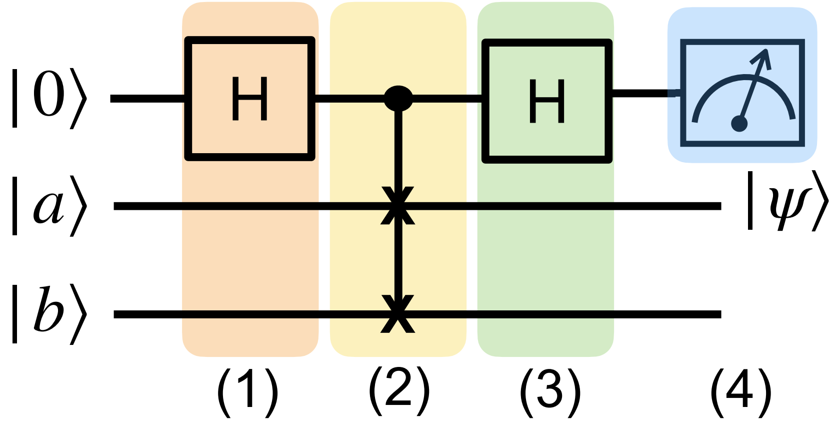




Proof: Inner product

$$|a\rangle \otimes |b\rangle = |a\rangle |b\rangle$$

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



(1) $$H\left(|0\rangle|a\rangle|b\rangle\right) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|a\rangle|b\rangle$$

(2) $$SWAP\,H\left(|0\rangle|a\rangle|b\rangle\right) = \frac{1}{\sqrt{2}}SWAP(|0\rangle + |1\rangle)|a\rangle|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle|a\rangle|b\rangle + |1\rangle|b\rangle|a\rangle)$$

(3) $$|\psi\rangle = H\,SWAP\,H\left(|0\rangle|a\rangle|b\rangle\right) = \frac{1}{\sqrt{2}}H(|0\rangle|a\rangle|b\rangle + |1\rangle|b\rangle|a\rangle)$$

$$= \frac{1}{2}|0\rangle\left(|a\rangle|b\rangle + |b\rangle|a\rangle\right) + \frac{1}{2}|1\rangle\left(|a\rangle|b\rangle - |b\rangle|a\rangle\right)$$

sum of the “unswapped” and the “swapped”

difference

(4) $$P(0) = |(\langle 0 \otimes I)|\psi\rangle|^2 = \frac{1}{2} - \frac{1}{2}|\langle a|b\rangle|^2$$

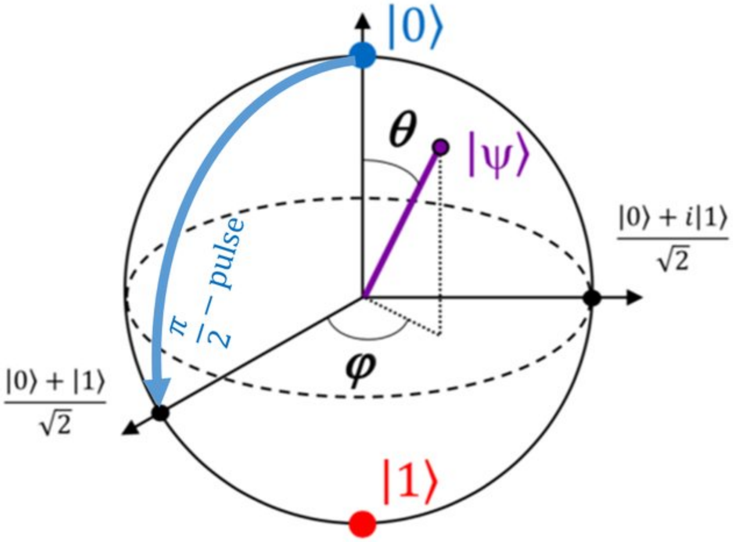
$$P(1) = |(\langle 0 \otimes I)|\psi\rangle|^2 = \frac{1}{2} + \frac{1}{2}|\langle a|b\rangle|^2$$

$\Rightarrow$

$$P(1) - P(0) = |\langle a|b\rangle|^2$$

Why Quantum Computing?

- Quantum simulation
- Cryptography
  - Mathematics: factoring, hidden subgroup program, discrete logarithm problem
- Optimization
- Search algorithm
- Quantum Machine Learning
  - Quantum Advantages?
    - Learns better with small # of data
    - Faster convergence
    - Less # of parameters
- What are the interesting problems?


$|0\rangle$
θ
$|\psi\rangle$
$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
$\frac{\pi}{2}$ – pulse
φ
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$|1\rangle$

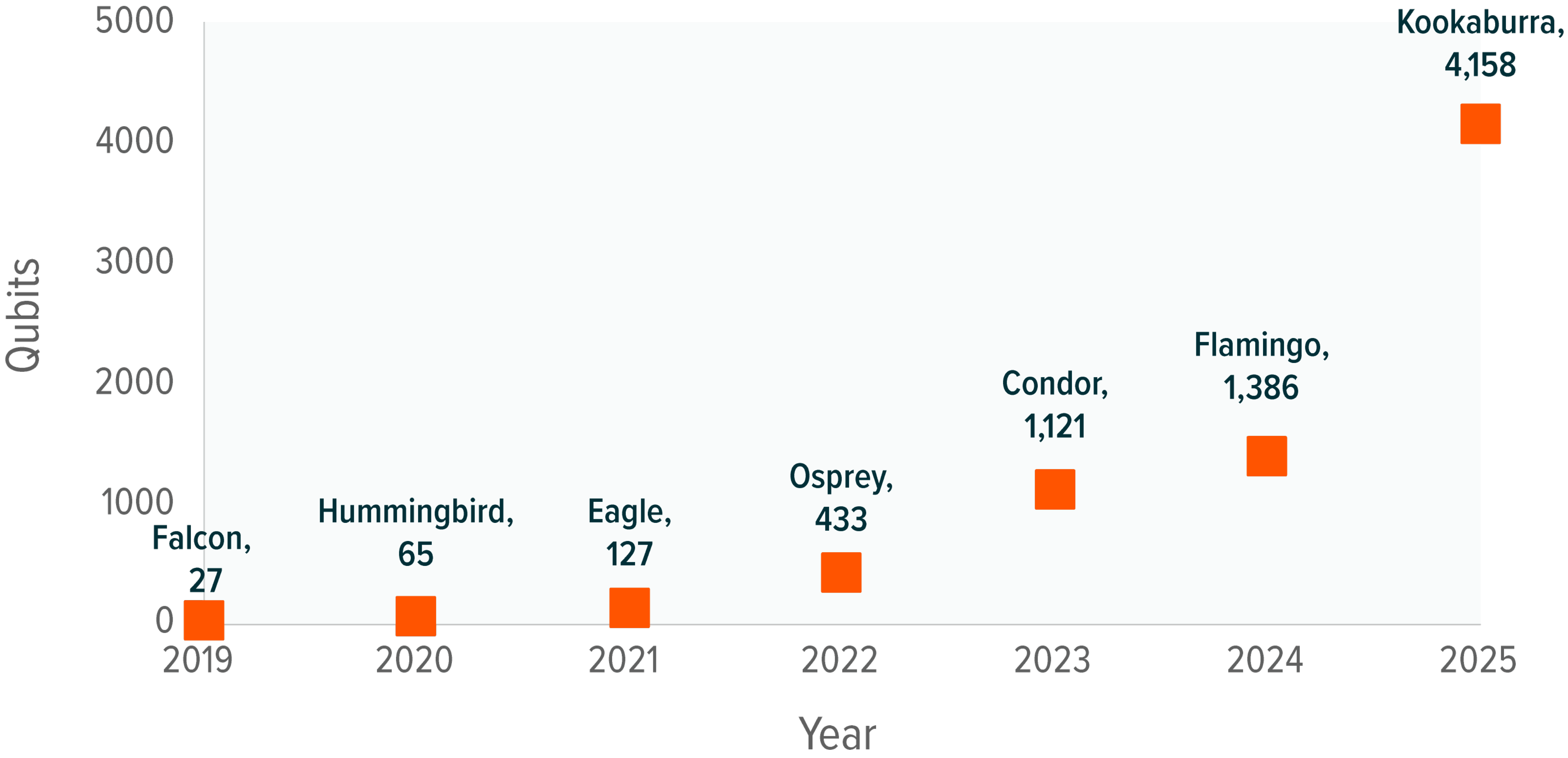
$$|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\varphi}sin\frac{\theta}{2}|1\rangle$$

A few popular tools for quantum simulation

- Qiskit (IBM)
    - IBM Quantum Composer
    - IBM Quantum Platform
- PennyLane and Strawberry Fields (Xanadu)
- TensorFlowQuantum (google)
- CUDA Quantum (NVIDIA)
- TensorCircuit

IBM QUANTUM PROCESSORS ROADMAP

Sources: Global X analysis of information derived from: IBM. (2022). Our new 2022 development roadmap.



Note: 2022 onwards includes planned processor launches.

A quantum computing partnership with the University of Chicago and the University of Tokyo

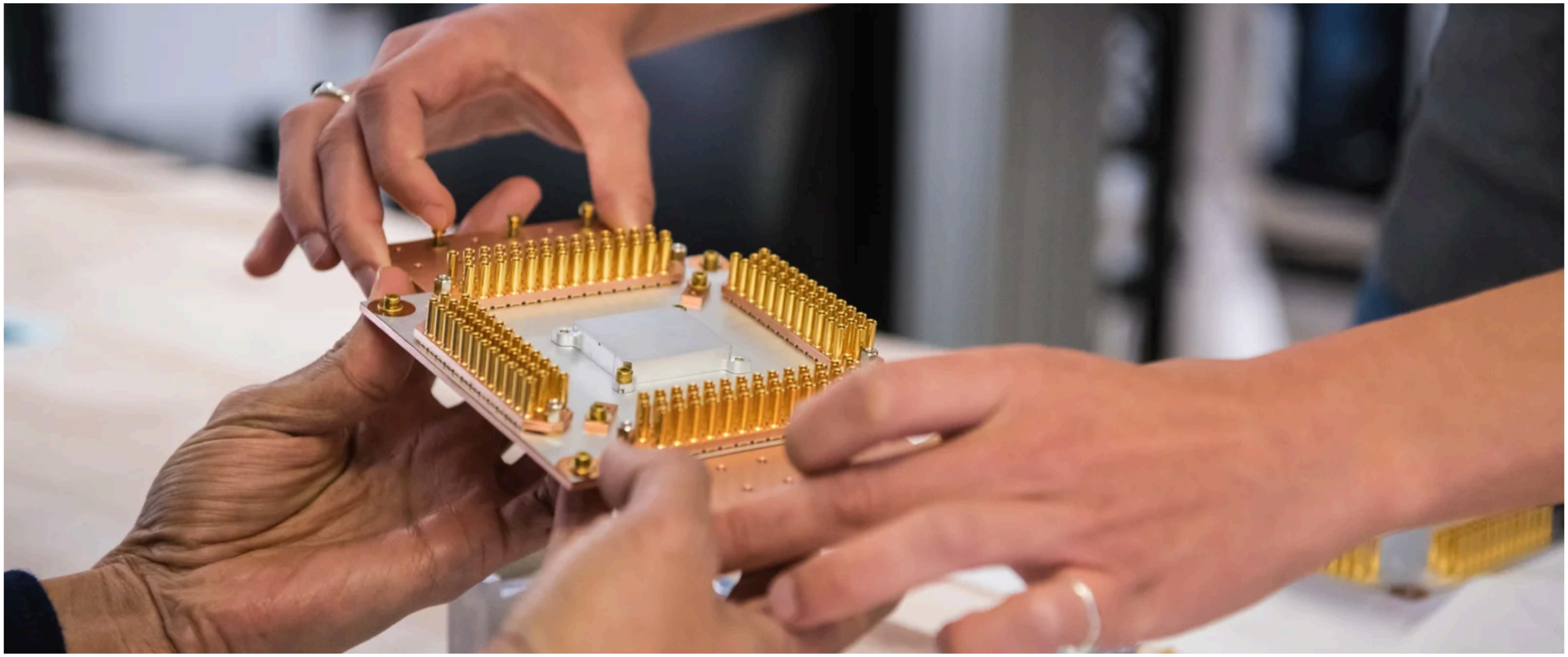
The commitment, to be signed May 21 on the sidelines of the G7 and U.S.-Japan Leaders' Meeting, aims to advance development of a fault-tolerant quantum computer by supporting research, entrepreneurship and workforce training.

May 17, 2023 · 2 min read

Charina Chou
Director and COO,
Google Quantum AI

Hartmut Neven
VP, Google Quantum AI

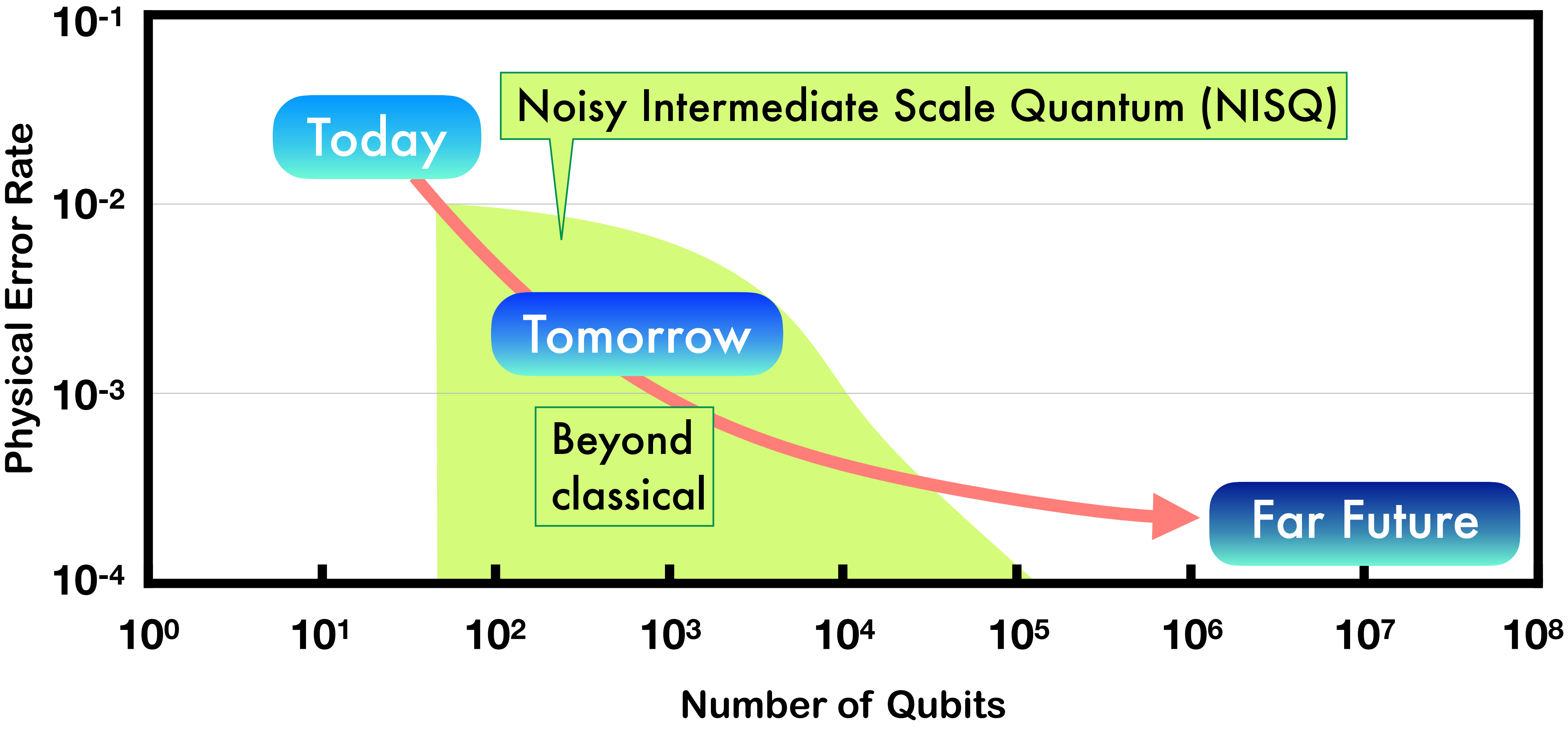
Share



Quantum computers are hard to build

- Qubits, unlike classical bits, need to interact strongly among themselves to form entangled states, which in turn form the basis for computation in quantum computers. But to achieve this experimentally is incredibly hard.

Quantum Hardware Roadmap



Is there a “Moore's law” for quantum computing?

- https://arxiv.org/pdf/2303.15547

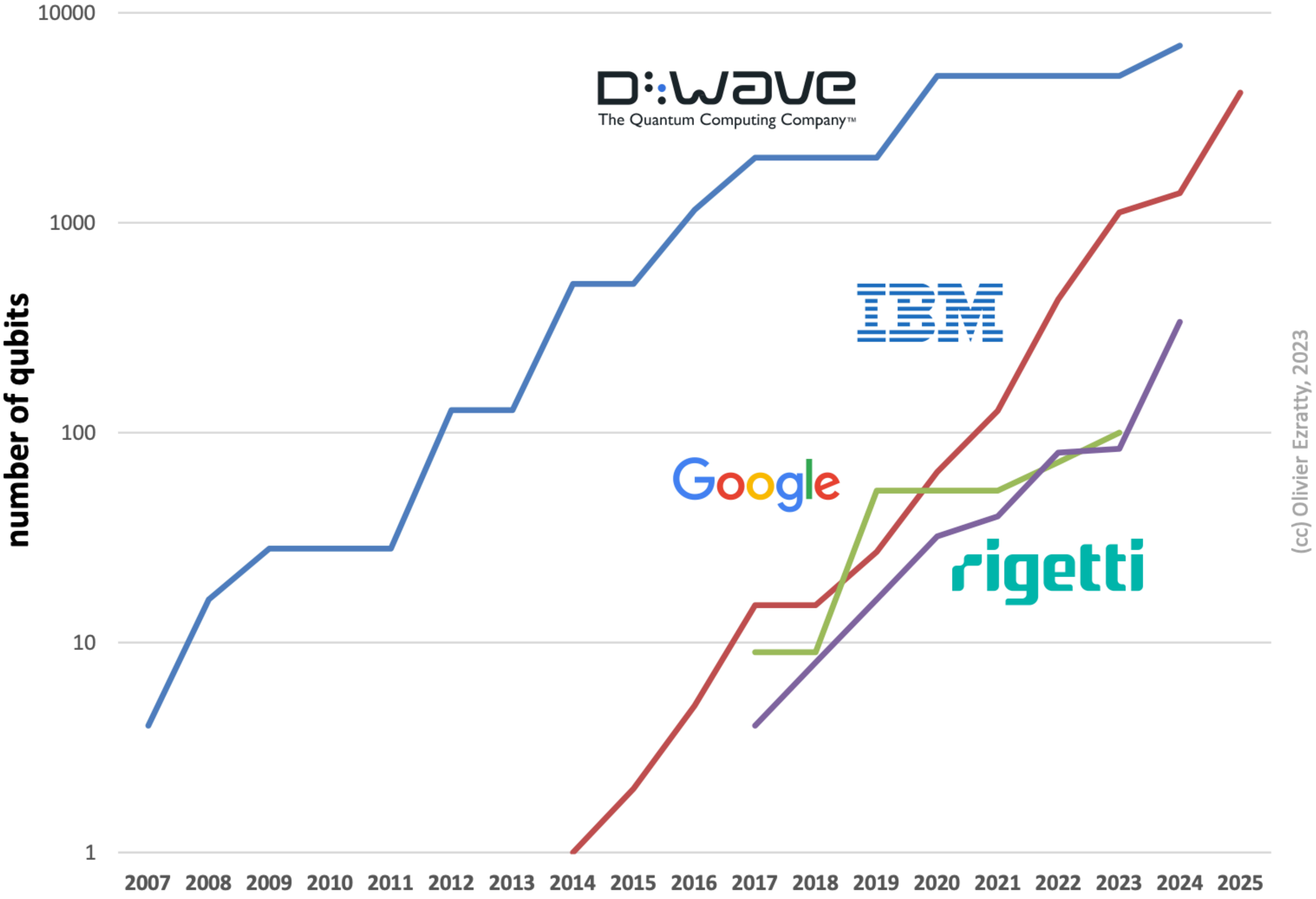


Figure 6: evolution of the number of physical qubits with D-Wave, IBM, Google and Rigetti. Compilation: Olivier Ezratty.

Is there a “Moore's law” for quantum computing?

- https://arxiv.org/pdf/2303.15547

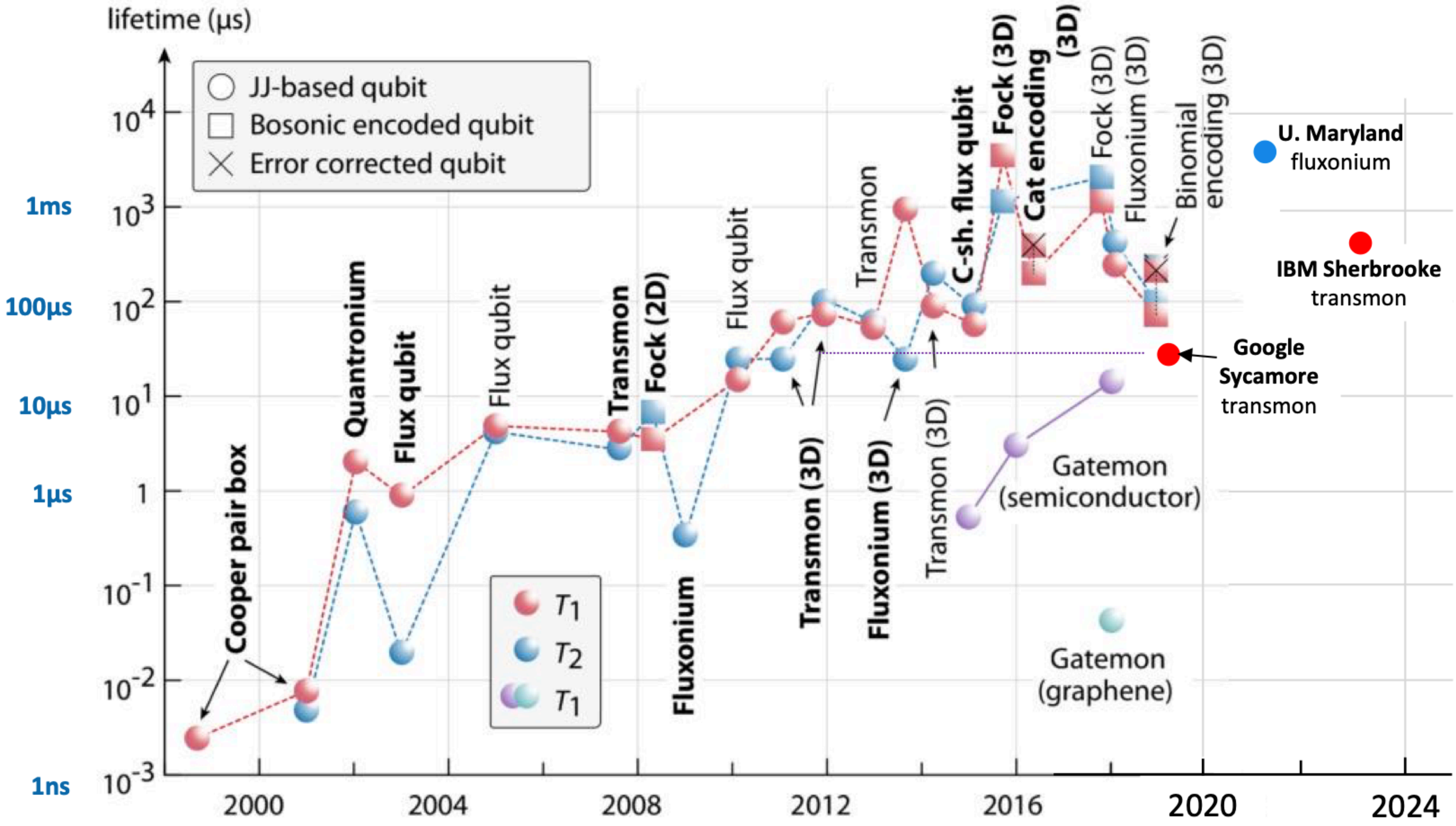


Figure 7: evolution of superconducting lifetime over time. Source: Morten Kjaergaard et al[50].

Is there a “Moore's law” for quantum computing?

- https://arxiv.org/pdf/2303.15547

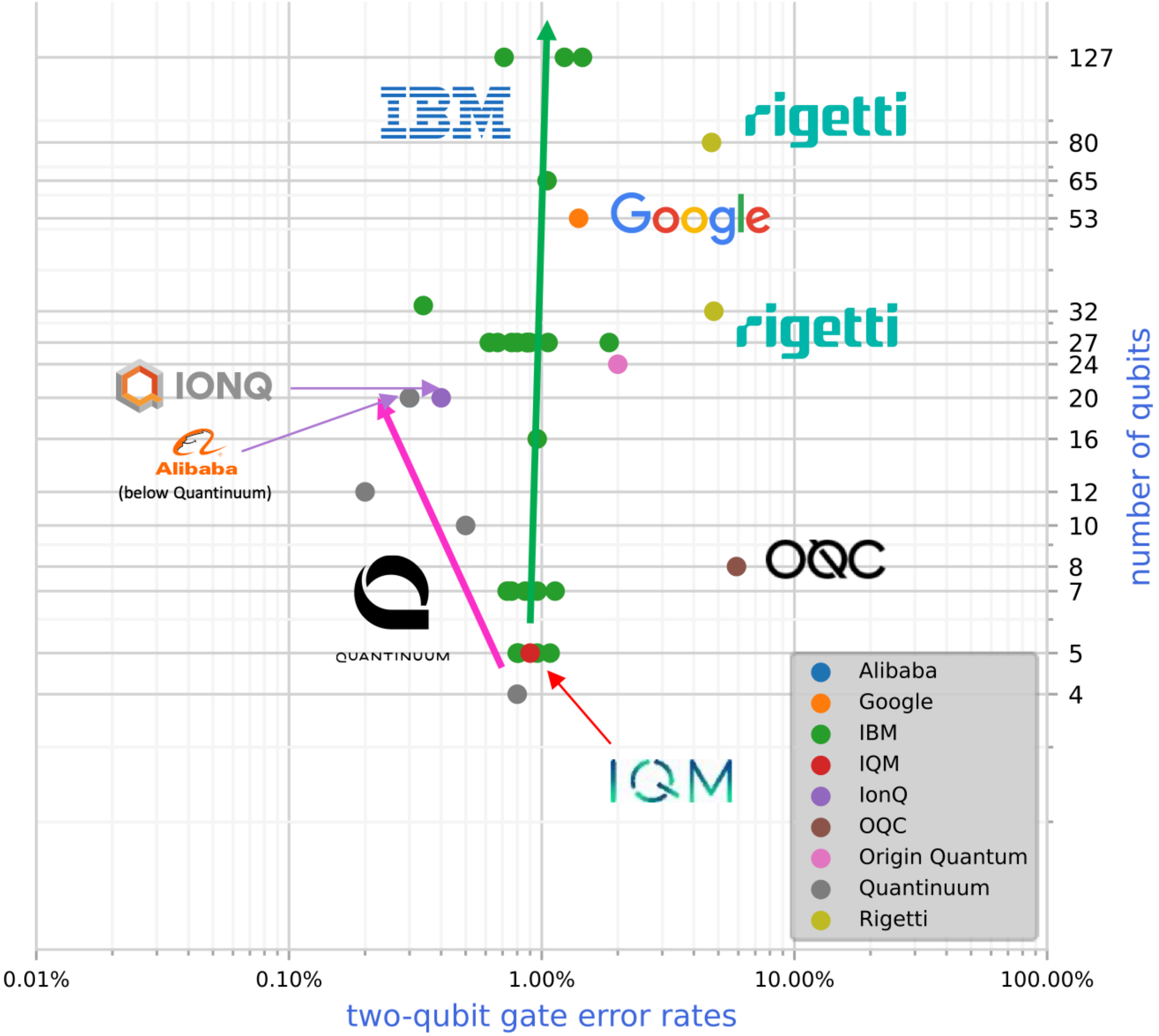


Figure 9: scatter plot of qubit numbers and two-qubit gate error rates for commercial vendors. Source: vendor fidelities numbers compiled by Olivier Ezratty as of March 2023.

Is there a “Moore's law” for quantum computing?

- https://arxiv.org/pdf/2303.15547

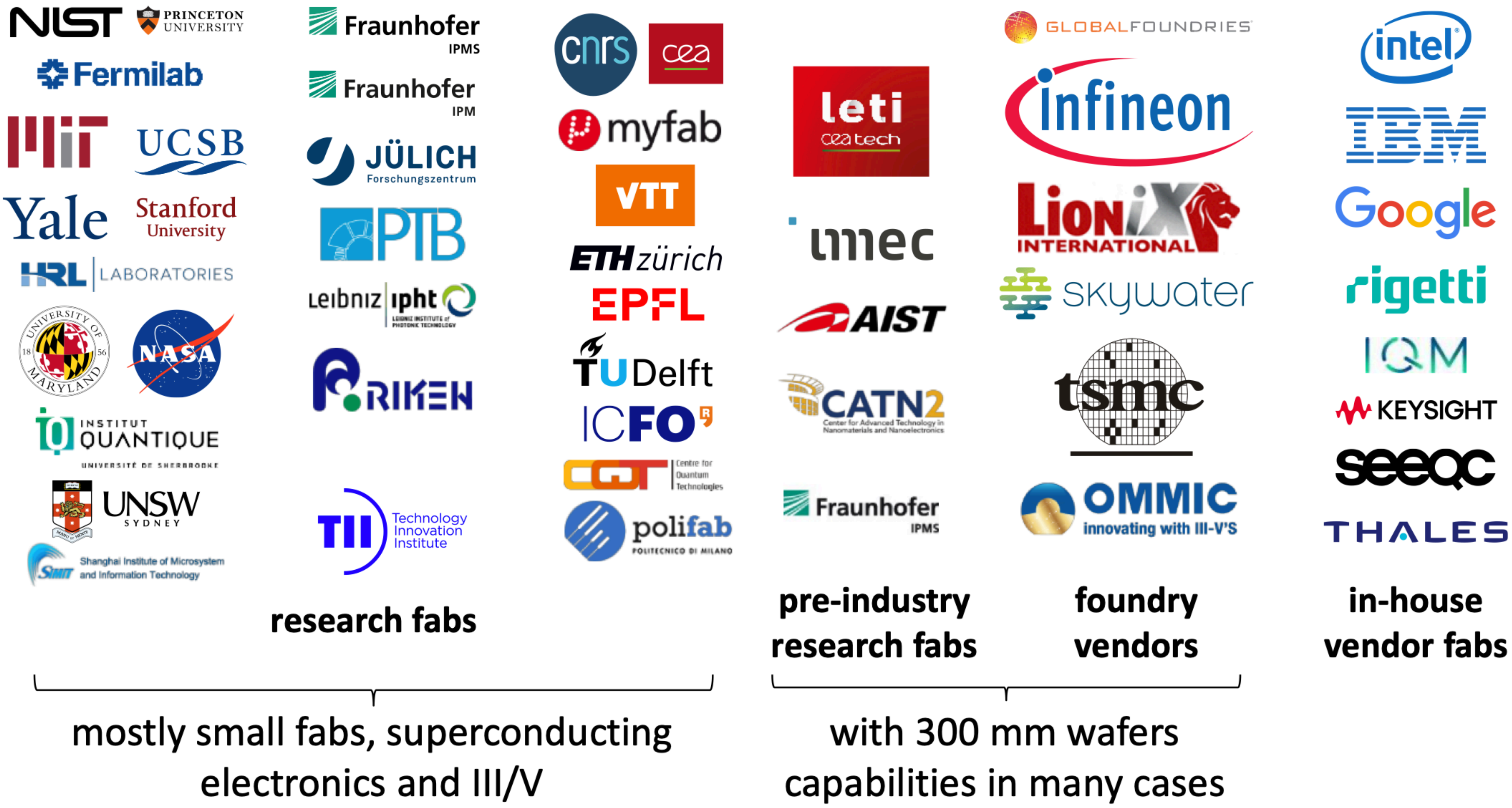
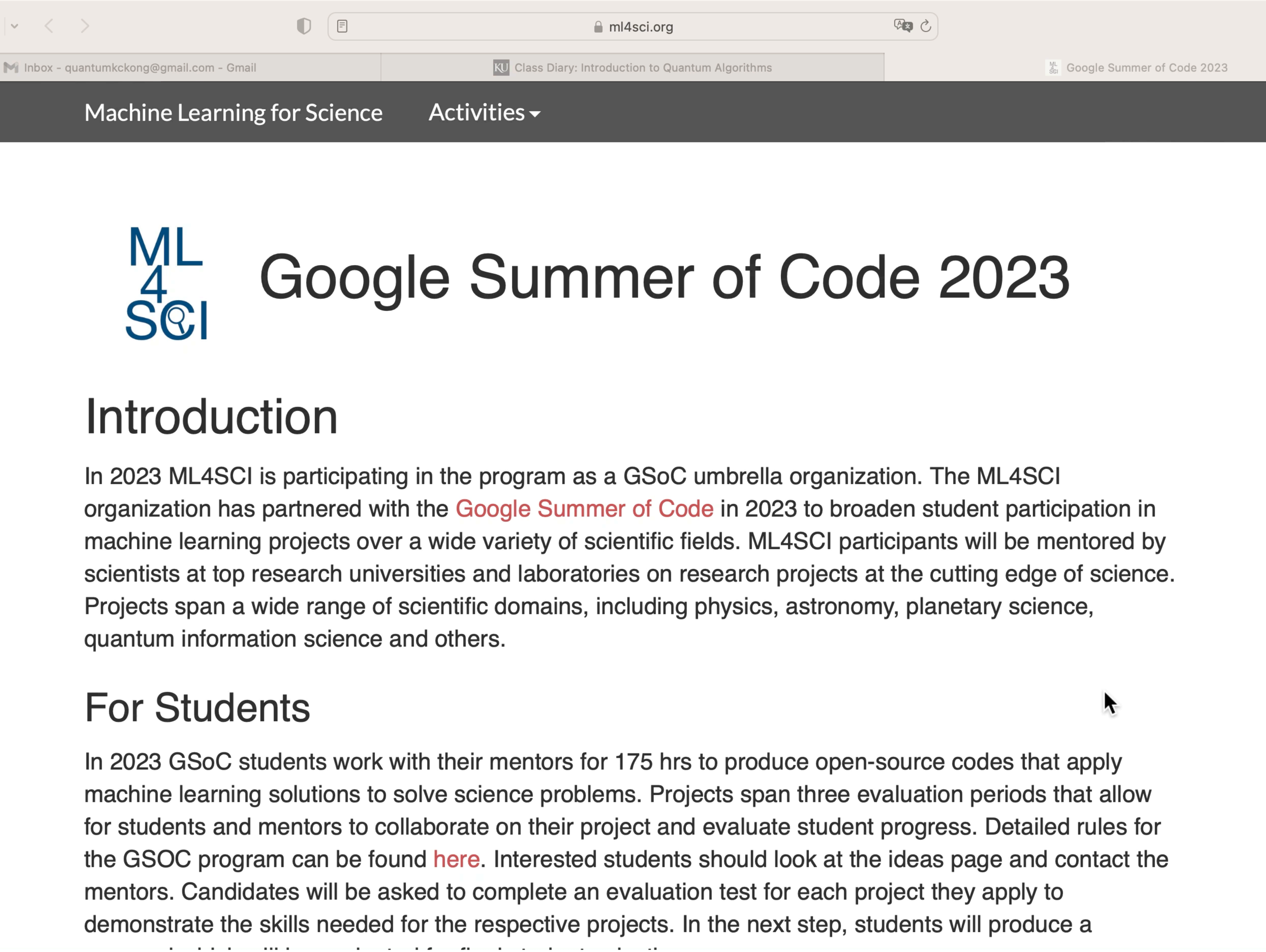

NIST
Princeton University
Fermilab
MIT
UCSB
Yale
Stanford University
HRL Laboratories
University of Maryland 1856
NASA
Institut Quantique Université de Sherbrooke
UNSW Sydney
SIMIT Shanghai Institute of Microsystem and Information Technology
Fraunhofer IPMS
Fraunhofer IPM
Jülich Forschungszentrum
PTB
Leibniz ipht
RIKEN
TII Technology Innovation Institute
cnrs
cea
myfab
VTT
ETH zürich
EPFL
TU Delft
ICFO
CQT Centre for Quantum Technologies
polifab Politecnico di Milano
research fabs
leti cea tech
imec
AIST
CATN2 Center for Advanced Technology in Nanomaterials and Nanoelectronics
Fraunhofer IPMS
GLOBALFOUNDRIES
infineon
LioniX International
skywater
tsmc
OMMIC innovating with III-V'S
pre-industry research fabs
foundry vendors
intel
IBM
Google
rigetti
IQM
KEYSIGHT
seeqc
THALES
in-house vendor fabs
mostly small fabs, superconducting electronics and III/V
with 300 mm wafers capabilities in many cases

Figure 15: some quantum processor fabs in the world, from research to large scale industry production. This covers superconducting qubits, silicon qubits and some III/V photonics fabs. Compilation: Olivier Ezratty.


ml4sci.org
Inbox - quantumkckong@gmail.com - Gmail
Class Diary: Introduction to Quantum Algorithms
Google Summer of Code 2023
Machine Learning for Science
Activities
ML
4
SCI

Google Summer of Code 2023

Introduction

In 2023 ML4SCI is participating in the program as a GSoC umbrella organization. The ML4SCI organization has partnered with the Google Summer of Code in 2023 to broaden student participation in machine learning projects over a wide variety of scientific fields. ML4SCI participants will be mentored by scientists at top research universities and laboratories on research projects at the cutting edge of science. Projects span a wide range of scientific domains, including physics, astronomy, planetary science, quantum information science and others.

For Students

In 2023 GSoC students work with their mentors for 175 hrs to produce open-source codes that apply machine learning solutions to solve science problems. Projects span three evaluation periods that allow for students and mentors to collaborate on their project and evaluate student progress. Detailed rules for the GSOC program can be found here. Interested students should look at the ideas page and contact the mentors. Candidates will be asked to complete an evaluation test for each project they apply to demonstrate the skills needed for the respective projects. In the next step, students will produce a

Why Machine Learning?

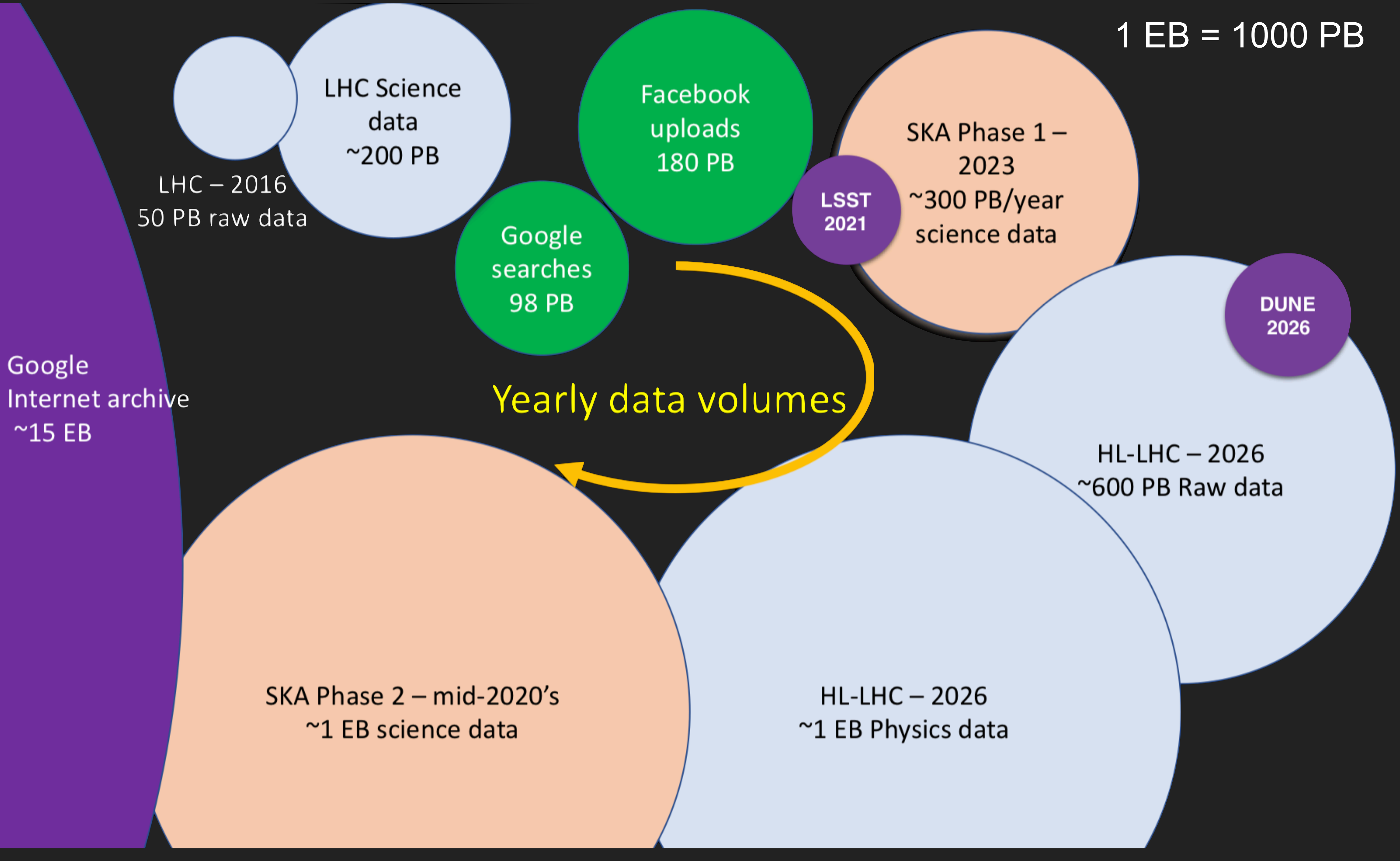
CHALLENGE: BIG DATA

Taken from J. Duarte's talk

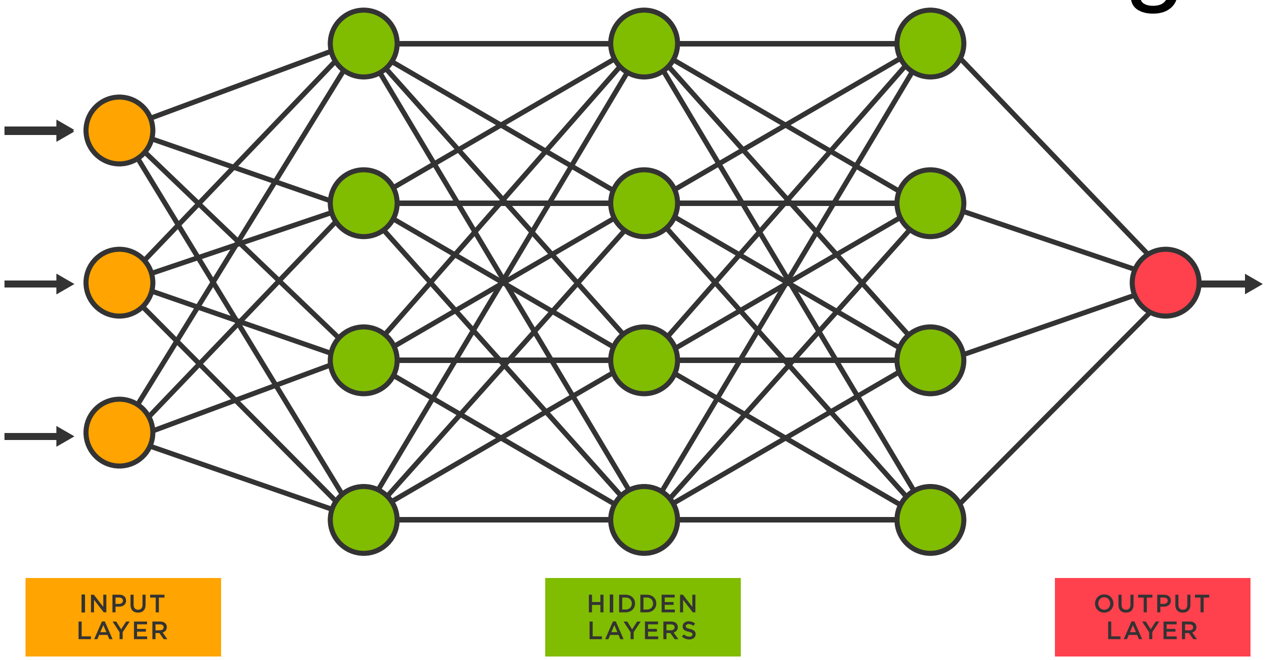
- HL-LHC will reach 1 exabyte of data per year

1 PB = 1000 TB

1 EB = 1000 PB

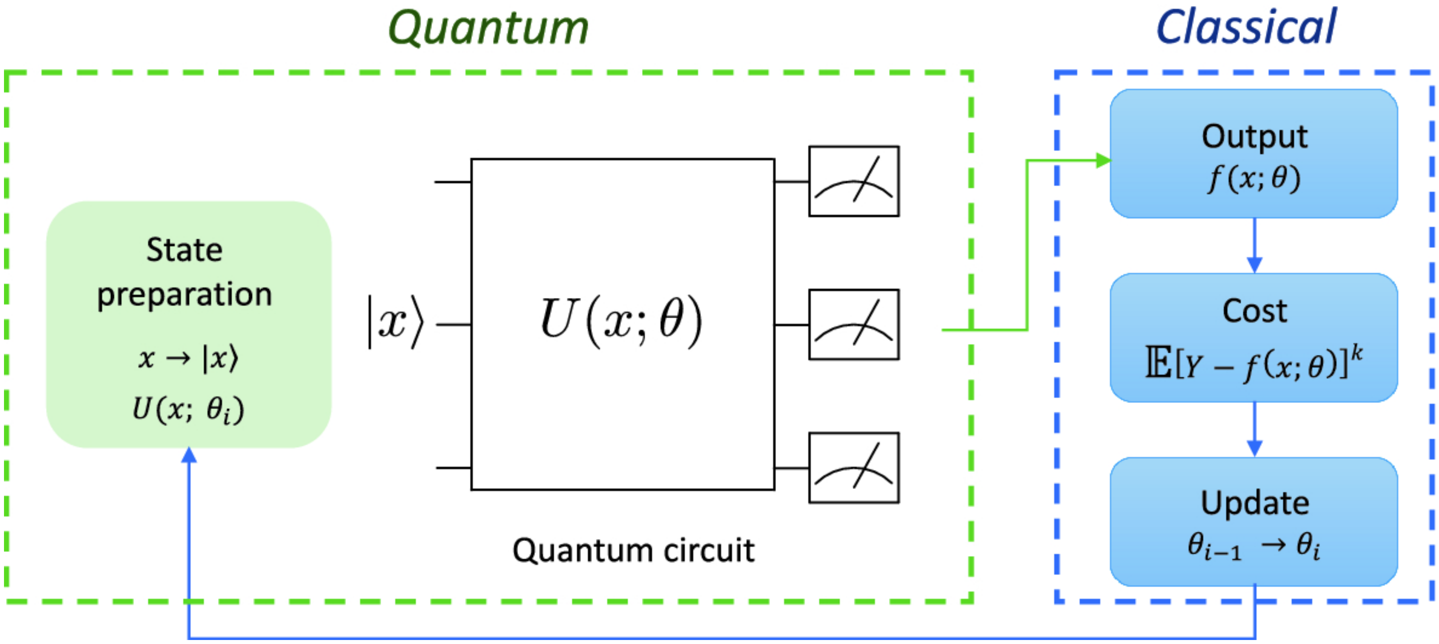


QML: Variational Quantum Algorithms


INPUT LAYER

HIDDEN LAYERS

OUTPUT LAYER


Quantum

Classical

State preparation

$x \rightarrow |x\rangle$

$U(x;\ \theta_i)$

$|x\rangle$

$U(x;\theta)$

Quantum circuit

Output

$f(x;\theta)$

Cost

$\mathbb{E}[Y - f(x;\theta)]^k$

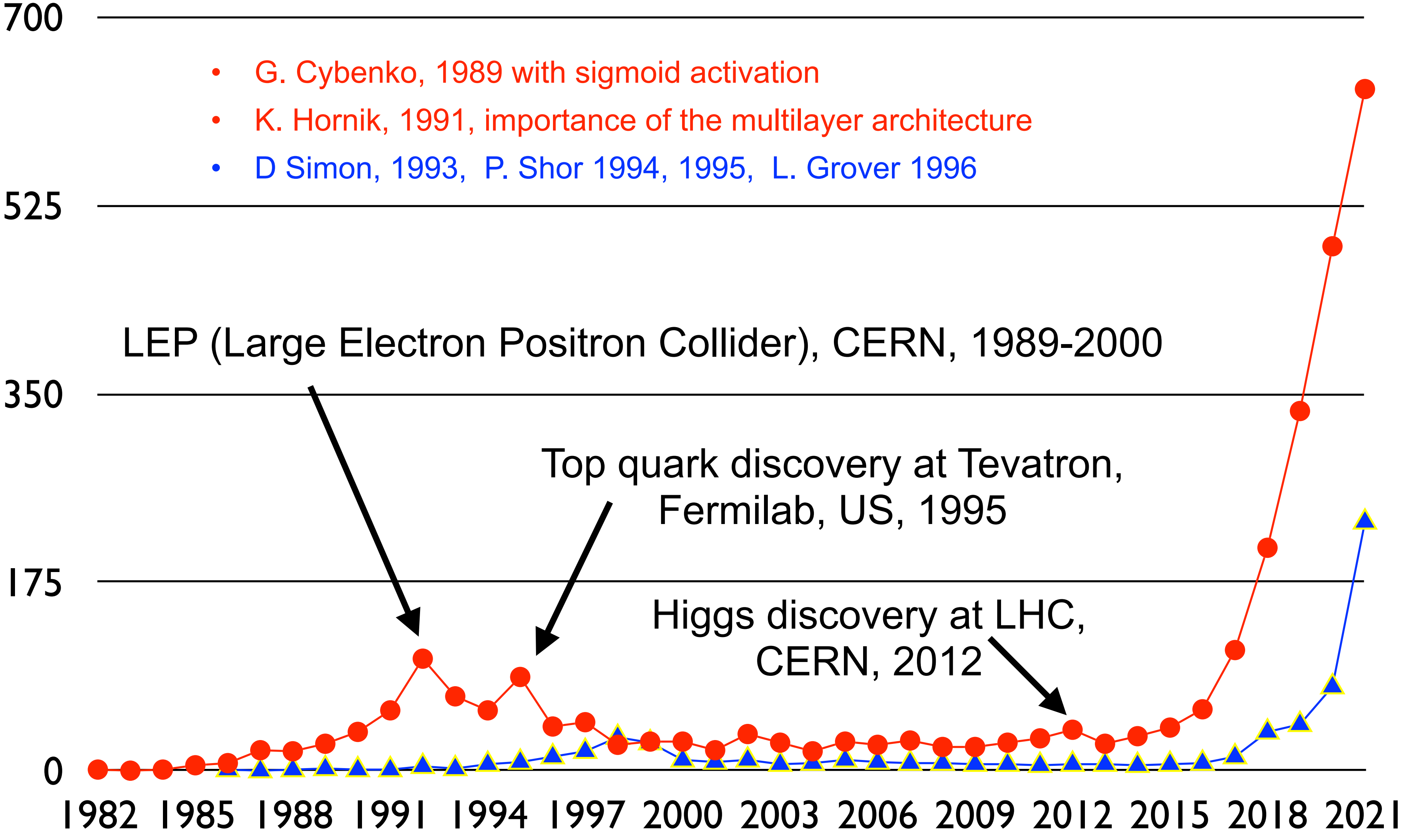
Update

$\theta_{i-1} \ \rightarrow \theta_i$

Data is obtained via **InspireHEP**

● The number of papers (in high energy physics) that has a keyword “Machine Learning”, “Deep Learning”, “Artificial Intelligence” or “Neural Networks” in their title.

▲ The number of papers that has a keyword “Quantum Computer”, ”Quantum Computing”,“Quantum Annealing” or “Quantum Machine Learning” in their title.



- G. Cybenko, 1989 with sigmoid activation
- K. Hornik, 1991, importance of the multilayer architecture
- D Simon, 1993, P. Shor 1994, 1995, L. Grover 1996

LEP (Large Electron Positron Collider), CERN, 1989-2000

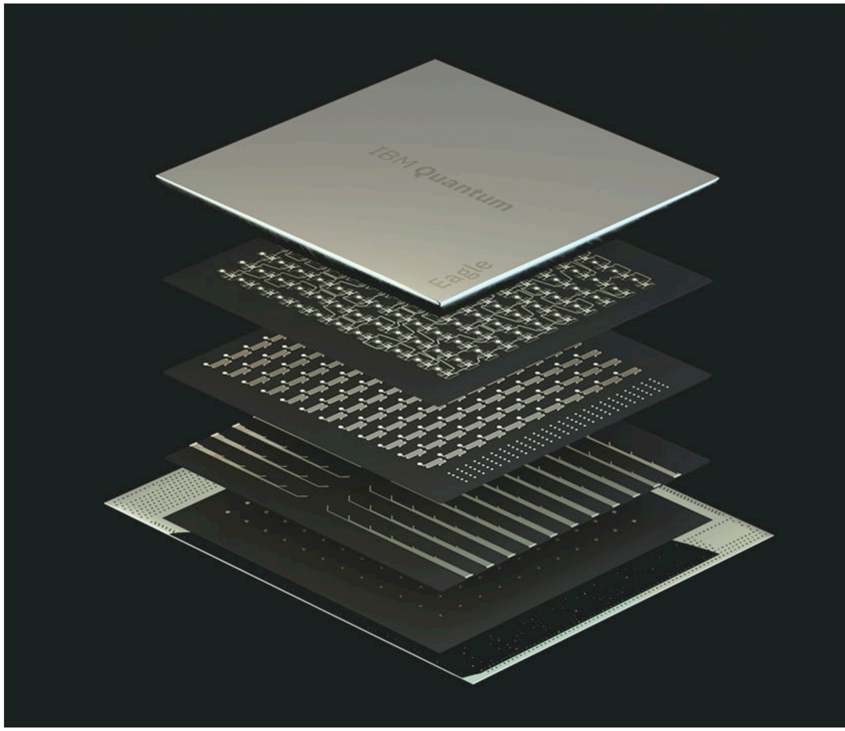
Top quark discovery at Tevatron, Fermilab, US, 1995

Higgs discovery at LHC, CERN, 2012

Single Qubit

- Notation: alternative representation
- Normalization conditions
- Quantum measurements
- Different bases
- Operators on qubits
- Simple quantum circuits

IBM 127-Qubit Quantum Processor



Qubits and Pauli's matrices

$$\sigma_1 = \sigma^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 = \sigma^y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_3 = \sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$[\sigma_i, \sigma_j] \equiv \sigma_i \sigma_j - \sigma_j \sigma_i = 2i\epsilon_{ijk}\sigma_k$$

$$\{\sigma_i, \sigma_j\} \equiv \sigma_i \sigma_j + \sigma_j \sigma_i = 2\delta_{ij}$$

$$\sigma_i \sigma_j = 2\delta_{ij} + i\,\epsilon_{ijk}\,\sigma_k$$

- Qubit $(\,|\psi\rangle, |\psi\rangle) \equiv \langle\psi|\psi\rangle = 1)$:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix}$$

$$0 \le \theta < \pi,\ 0 \le \phi < 2\pi$$

- Conjugate (dual vector or bra-vector): $\langle\psi| = (\,|\psi\rangle)^\dagger$

$$\langle\psi| = \cos\frac{\theta}{2}\langle 0| + e^{-i\phi}\sin\frac{\theta}{2}\langle 1| = \begin{pmatrix} \cos\frac{\theta}{2} & e^{-i\phi}\sin\frac{\theta}{2} \end{pmatrix}$$

- A set of all $|\psi\rangle$ (ket-vector) forms a vector space (Hilbert space)
- Pauli's matrices are generators of rotations in two dimensional complex plane.

$$R(\vec{\theta}) = \exp\left(-i\frac{\vec{\theta}\cdot\vec{\sigma}}{2}\right)$$

$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ Computational basis

$|\pm\rangle \equiv \dfrac{|0\rangle \pm |1\rangle}{\sqrt{2}} = \dfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ \pm 1 \end{pmatrix}$ Hadamard basis

- Vector, vector space, Hilbert space
- Dual vector, inner product
- Dirac notation: ket-bra
- Physical state evolves in time following the Schrödinger equation: $i\hbar\frac{\partial}{\partial t}\psi(\vec{x},t) = H\,\psi(\vec{x},t)$

$$\psi(t) = U(t)\,\psi(0)$$

$$U_I(t) = \sum_{q=0}^{\infty}(-i)^q \int_0^t \mathrm{d}t_q \cdots \int_0^{t_2} \mathrm{d}t_1 H_I(t_q)\cdots H_I(t_1)$$

- The most general unitary transformation acting on one qubit: $U(\theta) = \exp\left(i\,\vec{\theta}\cdot\frac{\vec{\sigma}}{2}\right)$

Adiabatic Theorem

- Schrödinger equation: $i\hbar \dfrac{d\psi(t)}{dt} = H(t)\,\psi(t)$
- Instantaneous eigenstate: $H(t)\,\psi_n(t) = E_n(t)\,\psi_n(t)$
- Initial condition: $\psi(t=0) = \psi_0$
- If evolution is slow enough, $\psi(t) \approx e^{i\theta(t)}\,\psi_0$

Born and Folk 1928

$$\psi(t) = U(t)\,\psi(0)$$

$$U_I(t) = \sum_{q=0}^{\infty} (-i)^q \int_0^t \mathrm{d}t_q \cdots \int_0^{t_2} \mathrm{d}t_1 H_I(t_q) \cdots H_I(t_1)$$

Dirac Bracket Notation

- Consider a quantum system with two orthonormal states, $|0\rangle$ and $|1\rangle$:

$$\langle 0|0\rangle = \langle 1|1\rangle = 1 \qquad \langle 0|1\rangle = \langle 1|0\rangle = 0 \qquad \langle i|j\rangle = \delta_{ij}$$

- In general, a qubit can be in an arbitrary superposition state $\psi = \alpha_0|0\rangle + \alpha_1|1\rangle$ with complex coefficients, α_0 and α_1, which are related to the probabilities to measure the state $|0\rangle$ and $|1\rangle$, correspondingly.

$$P(0) = |\langle 0|\psi\rangle|^2 = |\alpha_0|^2$$

$$P(1) = |\langle 1|\psi\rangle|^2 = |\alpha_1|^2$$

- The total probability is equal to 1, therefore $P(0) + P(1) = |\alpha_0|^2 + |\alpha_1|^2 = 1$
- The two complex parameters α_0 and α_1 can be represented by the two real parameters (angles) θ and ϕ (considering the normalization condition, ignoring the overall phase)

$$0 \le \theta < \pi\,,\ 0 \le \phi < 2\pi \qquad |\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix}$$

Dirac and Vector Notation

- ket: $|a\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$, 2-dimensional complex vector (amplitude vector)
- bra: $\langle b| = \left(|b\rangle\right)^\dagger = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}^\dagger = \left(b_0^* \ b_1^*\right)$
- Inner product: $\langle b|a\rangle = \left(b_0^* \ b_1^*\right)\begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = b_0^* a_0 + b_1^* a_1$
- If $a \neq b$, $\langle b|a\rangle$ is in general a complex number.
- Outer product: $|a\rangle\langle b| = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}\left(b_0^* \ b_1^*\right) = \begin{pmatrix} a_0 b_0^* & a_0 b_1^* \\ a_1 b_0^* & a_1 b_1^* \end{pmatrix}$
- Standard basis: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$$\langle 0|0\rangle = \langle 1|1\rangle = 1 \qquad \langle 0|1\rangle = \langle 1|0\rangle = 0 \qquad\qquad \langle i|j\rangle = \delta_{ij}$$

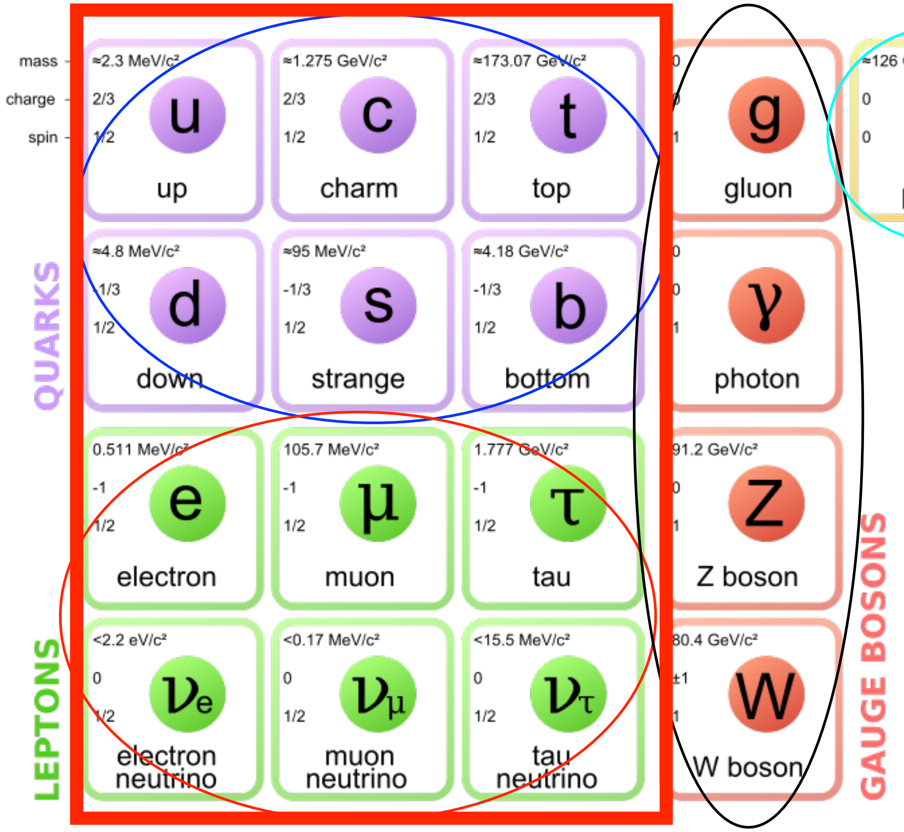
Dirac and Vector Notation

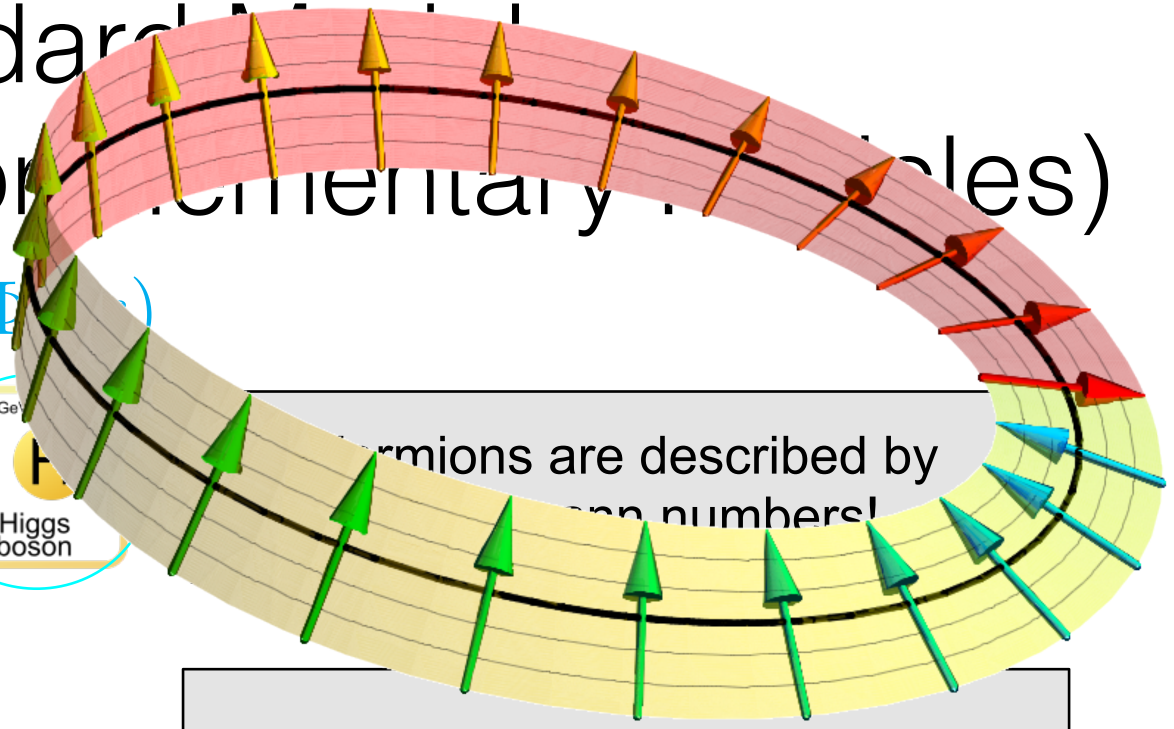
- ket: $|a\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$, 2-dimensional complex vector (amplitude vector)
- The squared ℓ_2 norm of a ket $|a\rangle$ = $\left|\left|\,|a\rangle\right|\right|^2 = \langle a|a\rangle = |a_0|^2 + |a_1|^2$

Standard
(Periodic Table fo lementary les)

$\Psi_{a\,\alpha\,f\,i}(x)$

Φ





rmions are described by
ann numbers!

Fermions are spinors and not invariant under 360 degree rotation.

$$\psi \rightarrow \psi' = \exp\left[i\, \frac{\vec{\sigma}}{2} \cdot \vec{\theta} \right] \psi$$

$\Psi_{\alpha\,f\,i}(x)$

$V_{\mu}^{A}(x)$

$F_{\mu\nu}^{A}(x)$

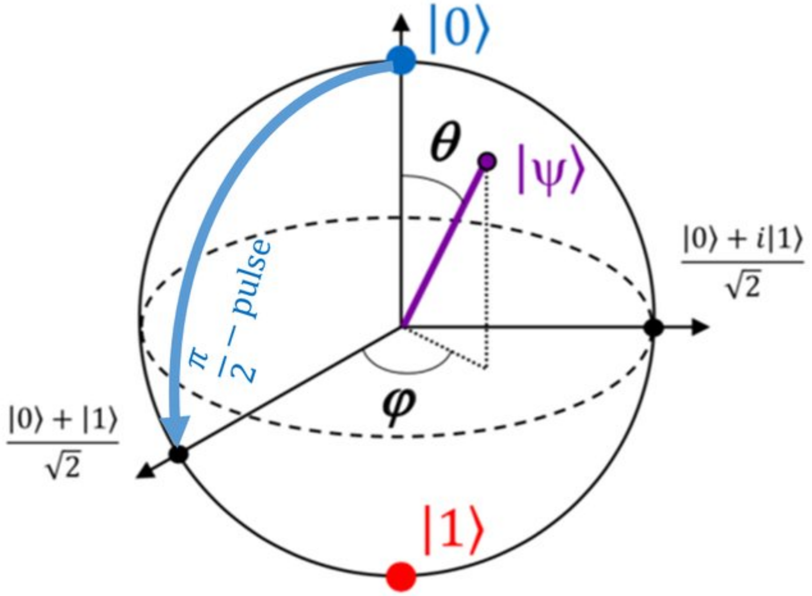
- SM is based on Lie Algebra.

(cf) Graded Lie Algebra or supersymmetry

Bloch Sphere

- Each (normalized) state of the qubit can be uniquely associated with a point on the unit sphere.

$$|\psi\rangle \;\longleftrightarrow\; (\theta,\phi) \;\longleftrightarrow \hat{r} = \begin{pmatrix} \sin\theta\cos\phi \\ \sin\theta\sin\phi \\ \cos\theta \end{pmatrix}$$



$|0\rangle$
θ
$|\psi\rangle$
$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
$\frac{\pi}{2}-pulse$
φ
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$|1\rangle$

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

$$|0\rangle : \;\; \theta = 0\,, \phi = \text{arbitrary} \longrightarrow \hat{r} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$$|1\rangle : \;\; \theta = \pi\,, \phi = \text{arbitrary} \longrightarrow \hat{r} = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}$$

$$|+\rangle : \;\; \theta = \pi/2\,, \phi = 0 \longrightarrow \hat{r} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

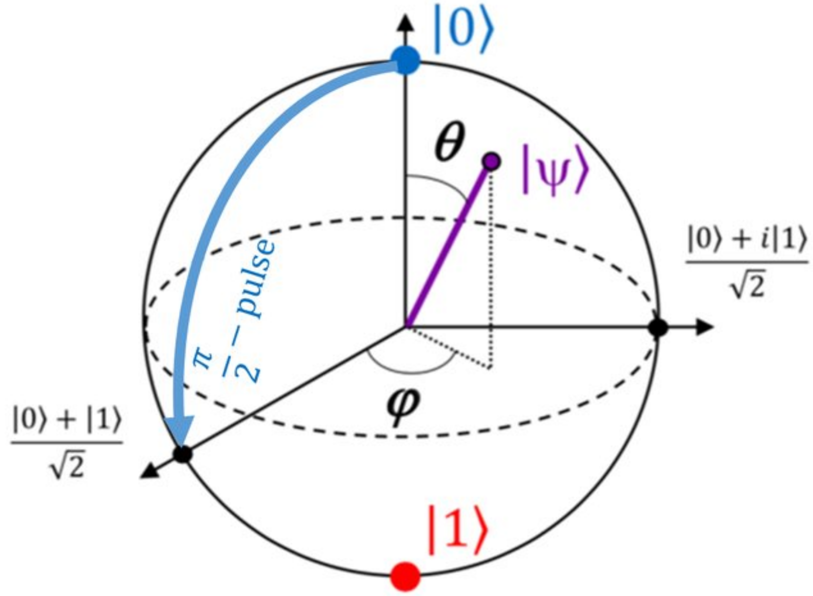
$$|+i\rangle : \;\; \theta = \pi/2\,, \phi = \pi/2 \longrightarrow \hat{r} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|-\rangle : \;\; \theta = \pi/2\,, \phi = \pi \longrightarrow \hat{r} = \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}$$

$$|+-\rangle : \;\; \theta = \pi/2\,, \phi = 3\pi/2 \longrightarrow \hat{r} = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}$$

Bloch Sphere

- $\{\,|0\rangle\,,|\,1\rangle\}$, $\{\,|+\rangle\,,|-\rangle\}$, $\{\,|+i\rangle\,,|-i\rangle\}$ are antipodal points on the Bloch sphere.
- Antipodal points are orthonormal, i.e., they represent two orthonormal qubit states (in Hilbert space)
- The antipodal point is obtained by $\theta \;\rightarrow\; \pi-\theta\,, \qquad \phi \;\rightarrow\; \pi+\phi$



$|0\rangle$
θ
$|\psi\rangle$
$\frac{|0\rangle+i|1\rangle}{\sqrt{2}}$
$\frac{\pi}{2}-pulse$
φ
$\frac{|0\rangle+|1\rangle}{\sqrt{2}}$
$|1\rangle$

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

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

$$= \sin\frac{\theta}{2}|0\rangle - e^{i\phi}\cos\frac{\theta}{2}|1\rangle$$

$$\langle\tilde{\psi}| = \sin\frac{\theta}{2}\langle 0| - e^{-i\phi}\cos\frac{\theta}{2}\langle 1|$$

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

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

$$= \sin\frac{\theta}{2}\cos\frac{\theta}{2}\langle 0|0\rangle - \cos\frac{\theta}{2}\sin\frac{\theta}{2}\langle 1|1\rangle = 0$$

Measurement in a different basis

- What if we want to measure our state $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$ in a different basis? For example,

$$\theta = \frac{\pi}{2}, \phi = 0 \quad \longrightarrow \quad |+\rangle = \cos\frac{\theta}{4}|0\rangle + \sin\frac{\theta}{4}|0\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)$$

$$\theta = \frac{\pi}{2}, \phi = \pi \quad \longrightarrow \quad |-\rangle = \cos\frac{\theta}{4}|0\rangle + e^{-i\pi}\sin\frac{\theta}{4}|0\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)$$

- Born rule: the probability that a state $|\psi\rangle$ collapses during a projective measurement onto a basis $\{|x\rangle, |x^{\perp}\rangle\}$ is given by

$$P(x) = |\langle x|\psi\rangle|^2 \qquad\qquad P(x^{\perp}) = |\langle x^{\perp}|\psi\rangle|^2$$

Measurement in a different basis

$$P(\,+\,) = \left|\frac{1}{\sqrt{2}}\Big(\langle 0| + \langle 1|\Big)\Big(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\Big)\right|^2 \;\; = \left|\frac{1}{\sqrt{2}}\cos\frac{\theta}{2} + \frac{1}{\sqrt{2}}e^{i\phi}\sin\frac{\theta}{2}\right|^2$$

$$= \frac{1}{2}\Big(1 + \sin\theta\cos\phi\Big)$$

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

$$P(\,-\,) = \frac{1}{2}\Big(1 - \sin\theta\cos\phi\Big)$$

$$|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ \pm 1 \end{pmatrix}$$

Rewrite the state $|\psi\rangle$ in the new basis $|+\rangle$ and $|-\rangle$

$$|0\rangle = \frac{1}{\sqrt{2}}\Big(|+\rangle + |-\rangle\Big) \qquad |1\rangle = \frac{1}{\sqrt{2}}\Big(|+\rangle - |-\rangle\Big)$$

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle \;\; = \frac{1}{\sqrt{2}}\cos\frac{\theta}{2}\Big(|+\rangle + |-\rangle\Big) + \frac{1}{\sqrt{2}}\sin\frac{\theta}{2}e^{i\phi}\Big(|+\rangle - |-\rangle\Big)$$

$$= \frac{1}{\sqrt{2}}\Big(\cos\frac{\theta}{2} + \sin\frac{\theta}{2}e^{i\phi}\Big)|+\rangle + \frac{1}{\sqrt{2}}\Big(\cos\frac{\theta}{2} - \sin\frac{\theta}{2}e^{i\phi}\Big)|-\rangle$$

$$P(\,+\,) = \left|\frac{1}{\sqrt{2}}\Big(\cos\frac{\theta}{2} + \sin\frac{\theta}{2}e^{i\phi}\Big)\right|^2 \qquad P(\,-\,) = \left|\frac{1}{\sqrt{2}}\Big(\cos\frac{\theta}{2} - \sin\frac{\theta}{2}e^{i\phi}\Big)\right|^2$$

- Global phases are physically irrelevant.
- Relative phase is measurable.

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

+: 100%
-: 0%

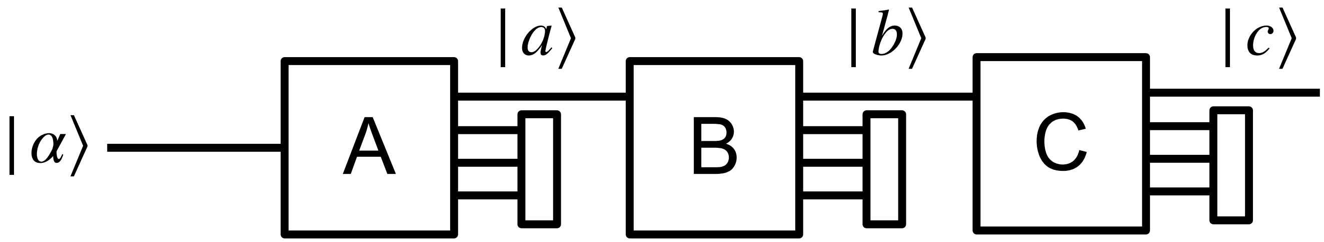
$$|i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/2}|1\rangle\right)$$

+: 50%
-: 50%

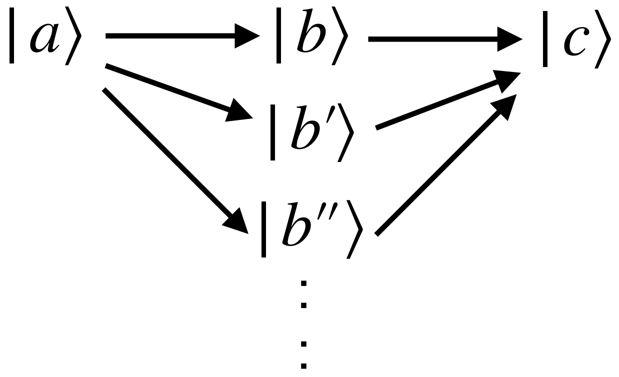
$$|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ \pm 1 \end{pmatrix}$$

Quantum Measurements

- Sequential selective measurement:



- what is the probability of obtaining $|c\rangle$?
  - Probabilities are multiplicative, we get $|\langle c|b\rangle|^2|\langle b|a\rangle|^2$
- Now let us sum over b to consider the total probability for going through all possible b routes.

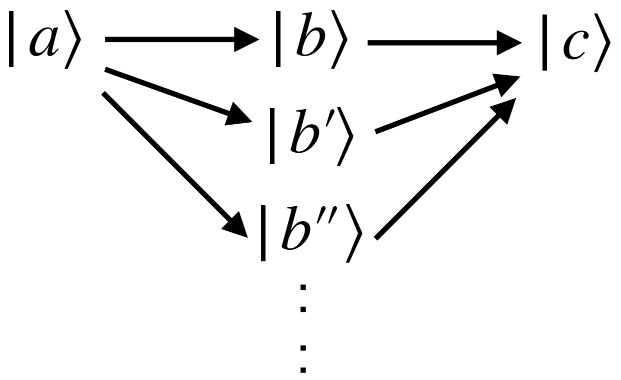


$$\text{sum of probabilities} = \sum_b |\langle c|b\rangle|^2|\langle b|a\rangle|^2$$

$$= \sum_b \langle c|b\rangle\langle b|a\rangle\langle a|b\rangle\langle b|c\rangle$$

Quantum Measurements

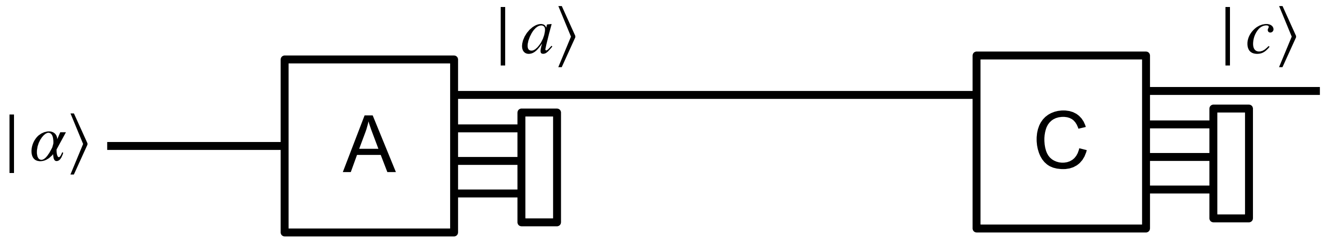
- Now let us sum over b to consider the total probability for going through all possible b routes.



$$\text{sum of probabilities} = \sum_b |\langle c|b\rangle|^2 |\langle b|a\rangle|^2$$

$$= \sum_b \langle c|b\rangle\langle b|a\rangle\langle a|b\rangle\langle b|c\rangle$$

- If B-filter is absent, probability is $|\langle c|a\rangle|^2$



different

$$|\langle c|a\rangle|^2 = |\sum_b \langle c|b\rangle\langle b|a\rangle|^2 = \sum_{b,b'} \langle c|b\rangle\langle b|a\rangle\langle a|b'\rangle\langle b'|c\rangle$$

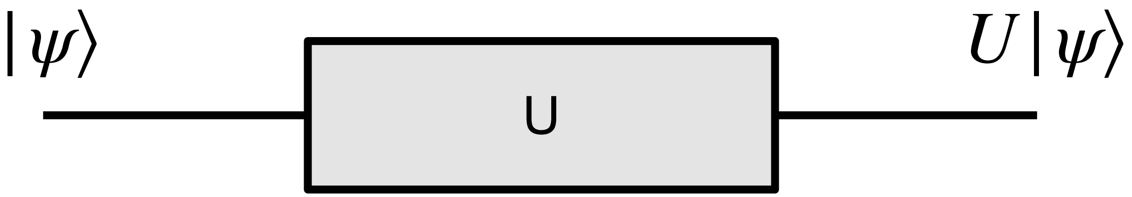
Quantum Gates

- Quantum gates act on qubits.
- Quantum gates transforms the state of a qubit into other states.
- Quantum gates must be linear that keeps the total probability equal to 1.
- Classical reversible logic gates are valid quantum gates.
- General One-Qubit Gates: one-qubit quantum gates are rotations on the Bloch sphere.

Quantum Circuits

- Quantum gates are repressed by unitary transformations (matrices), $U^\dagger U = UU^\dagger = I$ or $U^{-1} = U^\dagger$.

Input
Algorithm
Output



- A single qubit has 2 basis states, $|+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|-\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ $\qquad U_{ij} = \langle i | U | j \rangle$

$$U = U_{00}|0\rangle\langle 0| + U_{01}|0\rangle\langle 1| + U_{10}|1\rangle\langle 0| + U_{11}|1\rangle\langle 1| = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix} = \sum_{i,j=0}^{1} U_{ij}|i\rangle\langle j|$$

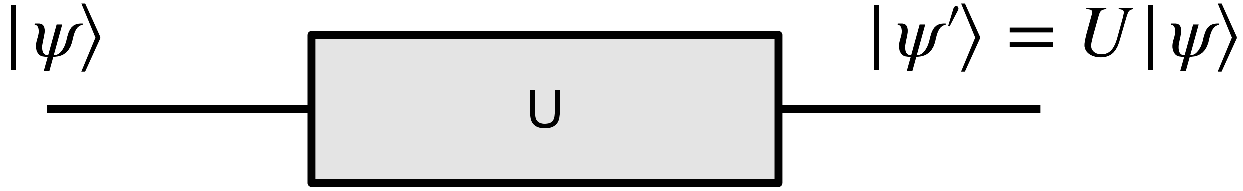
- Single qubit gates: X, Y, Z, Hadamard, phase shift etc
- Two qubit gates: Controlled , SWAP gate, Controlled Phase shift, etc
- Three quiet gates: Toffoli gates etc

$$U_{ij} = \langle i \,|\, U \,|\, j \rangle$$

$$U = IUI = \left(\sum_i |\, i \rangle \langle i \,| \right) U \left(\sum_j |\, j \rangle \langle j \,| \right) = \sum_{i,j} |\, i \rangle \Big(\langle i \,|\, U \,|\, j \rangle \Big) \langle j \,| = \sum_{i,j} |\, i \rangle \langle j \,| \Big(\langle i \,|\, U \,|\, j \rangle \Big)$$

$$U = U_{00} |\, 0 \rangle \langle 0 \,| + U_{01} |\, 0 \rangle \langle 1 \,| + U_{10} |\, 1 \rangle \langle 0 \,| + U_{11} |\, 1 \rangle \langle 1 \,| = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix} = \sum_{i,j=0}^{1} U_{ij} |\, i \rangle \langle j \,|$$

Quantum Circuits



$|\psi\rangle$

U

$|\psi'\rangle = U|\psi\rangle$

$$U = U_{00}|0\rangle\langle 0| + U_{01}|0\rangle\langle 1| + U_{10}|1\rangle\langle 0| + U_{11}|1\rangle\langle 1| = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix}$$

$$\langle\psi'|\psi'\rangle = \langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle$$

- The set of U forms a group.

$$U(N) = \{U \,|\, U^\dagger U = I\}$$
$$SU(N) = \{U \,|\, U^\dagger U = I,\ \det(U) = 1\}$$

- Group: closure, identity, inverse, associativity

More on operators/matrices

- A function of a matrix A is defined as its Taylor expansion.

$$f(A) = \sum_{n=0}^{\infty} \frac{1}{n!} A^n$$

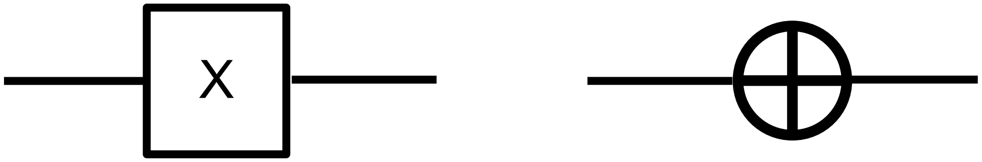
- The eigenvalue problem for A: $A\,|a\rangle = a\,|a\rangle$
- $f(A)\,|a\rangle = \sum_{n=0}^{\infty} \frac{1}{n!} A^n\,|a\rangle = \sum_{n=0}^{\infty} \frac{1}{n!} a^n\,|a\rangle = f(a)\,|a\rangle$

- Unitary matrix can be written as $U = e^{i\theta G}$, where H is a Hermitian matrix, $H^\dagger = H$

- Ex1) For 2 by 2, $U = a_0 I + a_i \sigma_i$
- Ex2) translation, time evolution

Single Qubit Gates

- X gate = Not operator = σ_X = bit flip = NOT gate



$$\sigma_X = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0| \qquad \sigma_x|j\rangle = |j \oplus 1\rangle$$

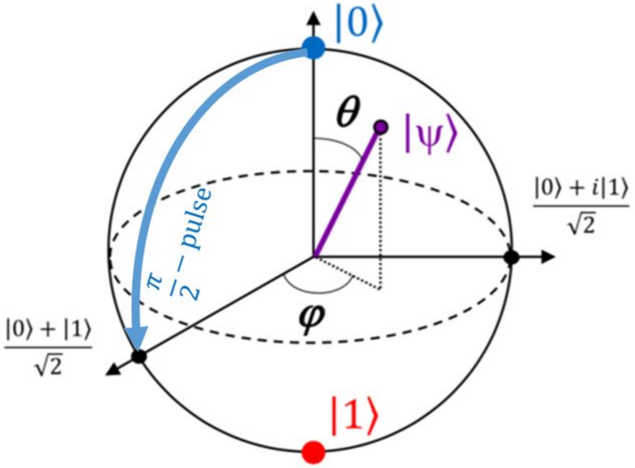
$$\sigma_x|0\rangle = |1\rangle \qquad \sigma_x|1\rangle = |0\rangle$$

$\downarrow$

addition modulo 2

- Interpretation on the Bloch sphere
  - rotation around x-axis by π
  - maps $|0\rangle \longrightarrow |1\rangle$ and $|1\rangle \longrightarrow |0\rangle$
  - maps $|+i\rangle \longrightarrow |-i\rangle$ and $|-i\rangle \longrightarrow |+i\rangle$

$$|\pm i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm i|1\rangle\right)$$

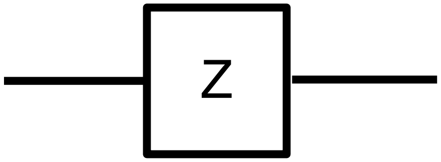

$|0\rangle$
θ
$|\psi\rangle$
$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
$\frac{\pi}{2} - pulse$
φ
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$|1\rangle$

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

Single Qubit Gates: Z-gate

- Z gate = σ_Z = phase flip

$$\sigma_Z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$



$$\sigma_Z|0\rangle = +|0\rangle \qquad \sigma_Z|1\rangle = -|1\rangle \qquad \sigma_Z|j\rangle = (-1)^j|j\rangle$$

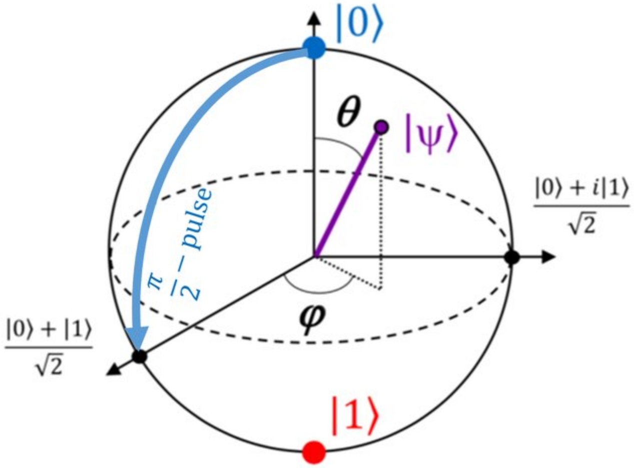
$$\sigma_Z|+\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle$$

$$\sigma_Z|-\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle$$

- Phase flip = rotation around z-axis by π

$$\sigma_Z|+i\rangle = |-i\rangle$$

$$\sigma_Z|-i\rangle = |+i\rangle$$


$|0\rangle$
θ
$|\psi\rangle$
$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
$\frac{\pi}{2} - pulse$
φ
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$|1\rangle$

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

Single Qubit Gates: Y and phase shift

- Y gate = σ_Y = bit and phase flip = rotation around y-axis by π

$$\sigma_Y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i\sigma_X\sigma_Z$$

$$\sigma_Y|+i\rangle = +|+i\rangle \qquad \sigma_Y|+\rangle = -i|-\rangle \qquad \sigma_Y|0\rangle = +i|1\rangle$$

$$\sigma_Y|-i\rangle = -|-i\rangle \qquad \sigma_Y|-\rangle = +i|+\rangle \qquad \sigma_Y|1\rangle = -i|0\rangle$$

- Phase shift operator: $R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} = P_\phi$

For $\phi = \pi$, $R_\pi = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

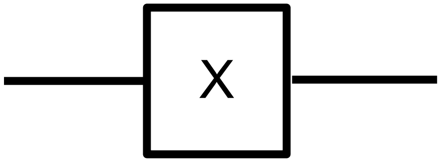
For $\phi = \pi/2$, $R_{\pi/2} = S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \sqrt{Z}$

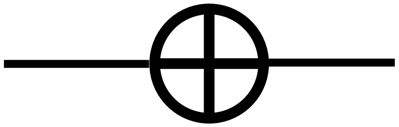
For $\phi = \pi/4$,

$$R_\pi = T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = \sqrt[4]{Z}$$

Single Qubit Gates

- X gate = Not operator = σ_X = bit flip = NOT gate





$$\sigma_X|0\rangle = |1\rangle$$

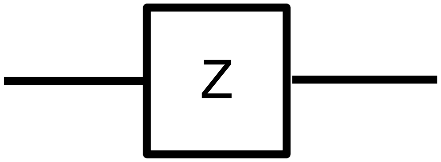
$$\sigma_X|1\rangle = |0\rangle$$

$$\sigma_X = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$\sigma_X|j\rangle = |j \oplus 1\rangle$$

- Z gate = σ_Z = phase flip

$$\sigma_Z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$



$$\sigma_Z|0\rangle = +|0\rangle \qquad \sigma_Z|1\rangle = -|1\rangle$$

$$\sigma_Z|j\rangle = (-1)^j|j\rangle$$

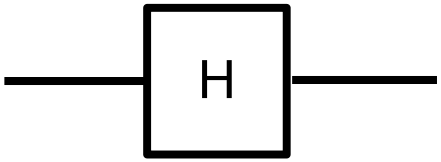
- Y gate = σ_Y = bit and phase flip

$$\sigma_Y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i\sigma_X\sigma_Z$$

$$\sigma_Y|j\rangle = i\,(-1)^j\,|j \oplus 1\rangle$$

Single Qubit Gates

- Hadamard operator: to switch between Z and X basis.



$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\Big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1| \Big)$$

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

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

$$H|x\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + (-1)^x|1\rangle \Big)$$

- The operator SH changes between the Z and Y basis.

- Most general 2 by 2 unitary matrix:

$$U^\dagger U = 1 \longrightarrow 4 \text{ conditions}$$

$$2 \times 4 = 8 \text{ parameters}$$

$$U = \begin{pmatrix} \cos\frac{\theta}{2} & e^{-i\lambda}\sin\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} & e^{i(\phi+\lambda)}\cos\frac{\theta}{2} \end{pmatrix}$$

System with two or more qubits

- H_i : Hilbert space spanned by $\{\,|0\rangle, |1\rangle\}$
- $H \equiv H_1 \otimes H_2$ is called the Hilbert space of the combined system (tensor product space of H_1 and H_2.

$$\dim(H_1) = 2 = \dim(H_2)$$

$$\dim(H_1 \otimes H_2) = 4$$

H_1	H_2	$H_1 \otimes H_2$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle = \|0\rangle \otimes \|0\rangle = \|00\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle = \|0\rangle \otimes \|1\rangle = \|01\rangle$
		$\|2\rangle = \|1\rangle \otimes \|0\rangle = \|10\rangle$
		$\|3\rangle = \|1\rangle \otimes \|1\rangle = \|11\rangle$

↓

computational basis
or standard basis

- A system of two spin-1/2 particles (qubits): $2 \otimes 2 = 3 \oplus 1$

- n-qubit system:

$$|\psi\rangle = \alpha_0 |0\cdots00\rangle + \alpha_1 |0\cdots01\rangle + \alpha_2 |0\cdots10\rangle + \cdots + \alpha_{2^n-1} |1\cdots11\rangle$$

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$$

Tensor Products of Operators

- Linearity: $\left(a_1A_1 + a_2A_2\right) \otimes B = a_1A_1 \otimes B + a_2A_2 \otimes B$
- Each term in a tensor product acts on its own component:

$$\left(A \otimes B\right) |m\, n\rangle = \left(A \otimes B\right)\left(|m\rangle \otimes |n\rangle\right) = A\,|m\rangle \otimes B\,|n\rangle$$

- Multiplication: $\left(A \otimes B\right)\left(C \otimes D\right) = \left(AC \otimes BD\right)$
- Matrix representation:

$$|a\rangle = a_0|0\rangle + a_1|1\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

$$|b\rangle = b_0|0\rangle + b_1|1\rangle = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}$$

Reducible representation

$$|a\rangle \otimes |b\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \otimes \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} = \begin{pmatrix} a_0 \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \\ \\ a_1 \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} a_0\, b_0 \\ a_0\, b_1 \\ a_1\, b_0 \\ a_1\, b_1 \end{pmatrix}$$

- Cartesian product: $A = A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) |\ a_i \in A_i\}$

$$\vec{a} = (a_1, a_2, \cdots, a_n) \in A \qquad 2\vec{a} = (2a_1, 2a_2, \cdots, 2a_n)$$

$$\dim(A_1 \times A_2) = \dim(A_1) + \dim(A_2)$$

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$$

- Tensor product: $A = A_1 \otimes A_2\,,\, |a_1\rangle \in A_1\,,\ |a_2\rangle \in A_2$

$$2\left(|a_1\rangle \otimes |a_2\rangle\right) = \left(2\,|a_1\rangle\right) \otimes |a_2\rangle = |a_1\rangle \otimes \left(2\,|a_2\rangle\right)$$

$$\dim(A_1 \otimes A_2) = \dim(A_1) \cdot \dim(A_2)$$

$$|00\rangle = |0\rangle|0\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix}1\\0\end{pmatrix} \\ 0\begin{pmatrix}1\\0\end{pmatrix} \end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \;= |0\rangle$$

$$|01\rangle = |0\rangle|1\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix}0\\1\end{pmatrix} \\ 0\begin{pmatrix}0\\1\end{pmatrix} \end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \;= |1\rangle$$

$$|10\rangle = |1\rangle|0\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix} 0\begin{pmatrix}1\\0\end{pmatrix} \\ 1\begin{pmatrix}1\\0\end{pmatrix} \end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \;= |2\rangle$$

$$|11\rangle = |1\rangle|1\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix} 0\begin{pmatrix}0\\1\end{pmatrix} \\ 1\begin{pmatrix}0\\1\end{pmatrix} \end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \;= |3\rangle$$

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = \sum_{i,j=0}^{1} a_{ij}|i\rangle \otimes |j\rangle$$

$$= \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle = \sum_{i=0}^{2^n-1} \alpha_i|i\rangle \qquad \sum_{i,j=0}^{1} |a_{ij}|^2 = \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1\,, \quad n = 2$$

Tensor Products of Operators

- Tensor product: $A = A_1 \otimes A_2\,,\, |a_1\rangle \in A_1\,,\ |a_2\rangle \in A_2$

$$2\big(\,|a_1\rangle \otimes |a_2\rangle\big) = \big(2\,|a_1\rangle\big) \otimes |a_2\rangle = |a_1\rangle \otimes \big(2\,|a_2\rangle\big)$$

$$\dim(A_1 \otimes A_2) = \dim(A_1) \cdot \dim(A_2)$$

For A with $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ basis and B with $\{\beta_1, \beta_2, \cdots, \beta_m\}$ basis, $\dim(A) = n$ and $\dim(B) = m$

$A \otimes B$ with basis $\{\alpha_i \beta_j\}$, $\dim(A \otimes B) = n \cdot m$

- Direct product:

For A with operation $\bullet$ and B with operation $\circ$, one can consider $A \times B$ with operation $\star$.

$a \in A$ $\qquad (a\,, b) \in A \times B \qquad (a\,, b) \star (a'\,, b') = (a \bullet a'\,, b \circ b') \in A \times B$

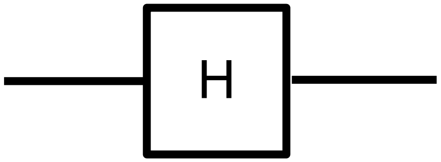
$b \in B$

element-wise operation

- For operators $\quad A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}\,,\quad B = \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix}$

$$A \otimes B = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \otimes \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} = \begin{pmatrix} a_{00}\begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} & a_{01}\begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} \\ a_{10}\begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} & a_{11}\begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} \end{pmatrix} = \begin{pmatrix} a_{00}b_{00} & a_{00}b_{01} & a_{01}b_{00} & a_{01}b_{01} \\ a_{00}b_{10} & a_{00}b_{11} & a_{01}b_{10} & a_{01}b_{11} \\ a_{10}b_{00} & a_{10}b_{01} & a_{11}b_{00} & a_{11}b_{01} \\ a_{10}b_{10} & a_{10}b_{11} & a_{11}b_{10} & a_{11}b_{11} \end{pmatrix}$$

Examples



$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\Big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1| \Big)$$

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

$$H|x\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + (-1)^x |1\rangle \Big)$$

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

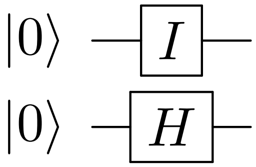
$$H = \begin{array}{c|cc} & \langle 0| & \langle 1| \\ \hline |0\rangle & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ |1\rangle & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{array} = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix}$$

$$U_{ij} = \langle i | U | j \rangle$$

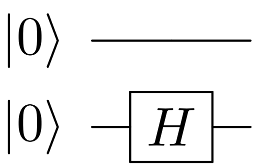
$$U = IUI = \Big(\sum_i |i\rangle\langle i|\Big) U \Big(\sum_j |j\rangle\langle j|\Big) = \sum_{i,j} |i\rangle\Big(\langle i|U|j\rangle\Big)\langle j| = \sum_{i,j} |i\rangle\langle j|\Big(\langle i|U|j\rangle\Big) = \sum_{i,j} |i\rangle\langle j| U_{ij}$$

Examples

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\Big(\,|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\,\Big)$$



or



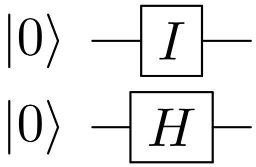
$$H \otimes I = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1\cdot\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} & 1\cdot\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \\ 1\cdot\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} & -1\cdot\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\end{pmatrix}$$

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

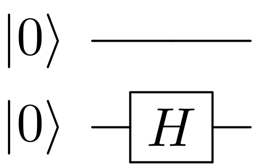
Examples

$$\begin{aligned}(H\otimes I)(|0\rangle\otimes|0\rangle) &= H|0\rangle\otimes I|0\rangle\\ &= |+\rangle\otimes|0\rangle\\ &= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle\\ &= \frac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle+|1\rangle\otimes|0\rangle).\end{aligned}$$

$$(H\otimes I)|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|10\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\1\\0\end{pmatrix}$$



or



$$(H\otimes I)|01\rangle = \frac{1}{\sqrt{2}}(|01\rangle+|11\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\0\\1\end{pmatrix},$$

$$(H\otimes I)|10\rangle = \frac{1}{\sqrt{2}}(|00\rangle-|10\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\-1\\0\end{pmatrix},$$

$$(H\otimes I)|11\rangle = \frac{1}{\sqrt{2}}(|01\rangle-|11\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\0\\-1\end{pmatrix}.$$

$$H\otimes I = \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{pmatrix}.$$

Tensor Products of Operators

- Commuting operators: $I = \sigma_0\,,\ X = \sigma_1\,,\ Y = \sigma_2\,,\ Z = \sigma_3$

$$\sigma_i\,\sigma_j = \delta_{ij} + i\,\epsilon_{ijk}\,\sigma_k \qquad M = \sum_{i=0}^{3} a_i\sigma_i\,,\ \ a_i \in \mathbb{C} \qquad H = H^\dagger = \sum_{i=0}^{3} a_i\sigma_i\,,\ \ a_i \in \mathbb{R}$$

$$|a\rangle = a_0|0\rangle + a_1|1\rangle \in H_1 \qquad |b\rangle = b_0|0\rangle + b_1|1\rangle \in H_2$$

$$I_1 \otimes I_2 = I_1 \qquad I_1 \otimes I_2 = I_2$$

$$X_1 \otimes I_2 = X_1 \qquad I_1 \otimes X_2 = X_2$$

$$Y_1 \otimes I_2 = Y_1 \qquad I_1 \otimes Y_2 = Y_2 \qquad \Longrightarrow \qquad Z_1Z_2 = Z_2Z_1$$

$$Z_1 \otimes I_2 = Z_1 \qquad I_1 \otimes Z_2 = Z_2$$

act on 1st state   act on 2nd state

- Example:

$$Z_1|0\rangle = +1|0\rangle$$

$$|\psi\rangle = |b_1b_2b_3\rangle \qquad b_i \in \{0\,,1\} \qquad Z_1|1\rangle = -1|1\rangle$$

$$\langle Z_1\rangle = \langle\psi|Z_1|\psi\rangle = \langle b_1\,b_2\,b_3|Z_1 \otimes I_2 \otimes I_3|b_1\,b_2\,b_3\rangle = \langle b_1|Z_1|b_1\rangle\langle b_2|I_2|b_2\rangle\langle b_3|I_3|b_3\rangle$$

$$= (-1)^{b_1} \qquad Z_1|j\rangle = (-1)^j|j\rangle$$

Tensor Products of Operators

- Bell basis for a two-qubit system

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big)$$

- Overall phase is not important.

$$|v\rangle \otimes \left(e^{i\phi}|w\rangle\right) = \left(e^{i\phi}|v\rangle\right) \otimes |w\rangle = e^{i\phi}\Big(|v\rangle \otimes |w\rangle\Big)$$

$$\frac{1}{\sqrt{2}}\Big(e^{i\phi}|00\rangle + e^{i\phi}|11\rangle\Big) = \frac{1}{\sqrt{2}}e^{i\phi}\Big(|00\rangle + |11\rangle\Big) \sim \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)$$

- Relative phase is important and observable. The interference term is crucial in QM.

$$\frac{1}{\sqrt{2}}\Big(e^{i\phi}|00\rangle + |11\rangle\Big) \neq \frac{1}{\sqrt{2}}\Big(|00\rangle + e^{i\phi}|11\rangle\Big) \neq \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)$$

Partial Trace

- Partial trace

$$A \otimes B = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \otimes \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} = \begin{pmatrix} a_{00}\begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} & a_{01}\begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} \\ a_{10}\begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} & a_{11}\begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} \end{pmatrix}$$

$$\begin{tikzcd}
= \begin{pmatrix} a_{00}b_{00} & a_{00}b_{01} & a_{01}b_{00} & a_{01}b_{01} \\ a_{00}b_{10} & a_{00}b_{11} & a_{01}b_{10} & a_{01}b_{11} \\ a_{10}b_{00} & a_{10}b_{01} & a_{11}b_{00} & a_{11}b_{01} \\ a_{10}b_{10} & a_{10}b_{11} & a_{11}b_{10} & a_{11}b_{11} \end{pmatrix} \arrow[r, "tr_2", "\text{tracing out 2nd system}"'] \arrow[d, "tr_1"', "\text{tracing out 1st system}"] & \begin{pmatrix} a_{00}\,tr(B) & a_{01}\,tr(B) \\ a_{10}\,tr(B) & a_{11}\,tr(B) \end{pmatrix} = tr(B)\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \\
\begin{pmatrix} b_{00}\,tr(A) & b_{01}\,tr(A) \\ b_{10}\,tr(A) & b_{11}\,tr(A) \end{pmatrix} = tr(A)\begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} &
\end{tikzcd}$$

Direct Sum of Vector Space

- If V with bases $\{\,|\alpha_1\rangle, \cdots, |\alpha_n\rangle\}$ and W with $\{\,|\beta_1\rangle, \cdots, |\beta_m\rangle\}$ are vector spaces, $V \oplus W$ is also a vector space with bases $\{\,|\alpha_1\rangle, \cdots, |\alpha_n\rangle, |\beta_1\rangle, \cdots, |\beta_m\rangle\}$ and $\dim(V \oplus W) = \dim(V) + \dim(W)$

$$|v\rangle = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \qquad |w\rangle = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \qquad |v\rangle \oplus |W\rangle = \begin{pmatrix} x_1 \\ x_2 \\ y_1 \\ y_2 \end{pmatrix}$$

$$O_1|v\rangle = O_1\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \qquad O_2|w\rangle = O_2\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

$$(O_1 + O_2)\Big(\,|v\rangle \oplus |W\rangle\Big) = \begin{pmatrix} O_1 & 0 \\ 0 & O_2 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ y_1 \\ y_2 \end{pmatrix}$$

Separable vs Entangled states

- Separable states: if a quantum state $|\psi\rangle$ is given by tensor product of two states, i.e., if $|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle$, $|\psi\rangle$ is separable.

$$|00\rangle = |0\rangle \otimes |0\rangle\, ,\ |01\rangle = |0\rangle \otimes |1\rangle$$

- Entangled states: if a quantum state is not separable, $|\psi\rangle$ is an entangled state.

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big)$$

$$|\phi\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |01\rangle \Big) = \frac{1}{\sqrt{2}}\Big(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle \Big) = \frac{1}{\sqrt{2}}|0\rangle \otimes \Big(|0\rangle + |1\rangle \Big)$$

$\longrightarrow$ if Bob measures $|0\rangle$, Alice still has 50% probability for $|0\rangle$ and $|1\rangle$.

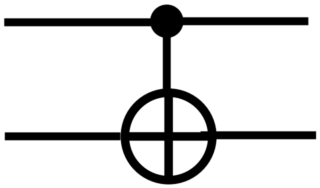
- Entangled states are crucial resources for QC, as there is no classical analog.
- Density matrix: more later

Summary of fixed 1-qubit gates:

Gate	Circuit representation	Matrix representation	Dirac representation
X	$-\boxed{X}-$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\|1\rangle\langle 0\| + \|0\rangle\langle 1\|$
Y	$-\boxed{Y}-$	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$i\,\|1\rangle\langle 0\| - i\,\|0\rangle\langle 1\|$
Z	$-\boxed{Z}-$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\|1\rangle\langle 0\| - \|0\rangle\langle 1\|$
H	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\langle 0\| + \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)\langle 1\|$
S	$-\boxed{S}-$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$	$\frac{1}{\sqrt{2}}\|0\rangle\langle 0\| + \frac{1}{\sqrt{2}}i\,\|1\rangle\langle 1\|$
T	$-\boxed{T}-$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & e^{(-i\pi/4)} \end{pmatrix}$	$\frac{1}{\sqrt{2}}\|0\rangle\langle 0\| + \frac{1}{\sqrt{2}}e^{(-i\pi/4)}\|1\rangle\langle 1\|$

Two Qubit Gates: CNOT and CU gates

- CNOT gate = Controlled Not =Controlled X
- NOT operation is performed on 2nd qubit, when the 1st qubit is in state $|1\rangle$. Otherwise 2nd qubit is unchanged.



$$\begin{array}{lcl} |00\rangle & \rightarrow & |00\rangle \\ |01\rangle & \rightarrow & |01\rangle \\ |10\rangle & \rightarrow & |11\rangle \\ |11\rangle & \rightarrow & |10\rangle \end{array}$$

$$\begin{pmatrix} |00\rangle' \\ |01\rangle' \\ |10\rangle' \\ |11\rangle' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{pmatrix}$$

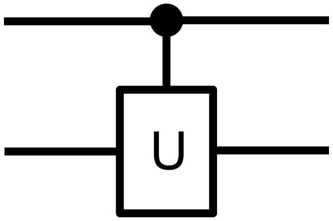
$$\begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} = \exp\left(i\frac{\pi}{4}(I - Z_1)(I - X_2) \right)$$

$$\mathrm{CNOT}|a\rangle|b\rangle = |a\rangle|a \oplus b\rangle.$$

$$|i\,j\rangle \rightarrow |i\,i \oplus j\rangle \qquad \text{(mod 2)}$$

- Generally, controlled U-gate

$$\begin{array}{lcl} |00\rangle & \rightarrow & |00\rangle \\ |01\rangle & \rightarrow & |01\rangle \\ |10\rangle & \rightarrow & |1\rangle \otimes U|0\rangle = |1\rangle \otimes \left(U_{00}|0\rangle + U_{01}|1\rangle\right) \\ |11\rangle & \rightarrow & |1\rangle \otimes U|1\rangle = |1\rangle \otimes \left(U_{10}|0\rangle + U_{11}|1\rangle\right) \end{array}$$



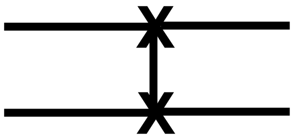
$$CU = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} = \exp\left(i\frac{1}{2}(I - Z_1)H_2 \right) \ \text{for } U = e^{iH_2} = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix}$$

$$e^{i\theta A} = \cos\theta + i\,A\,\sin\theta \ \text{ for } A^2 = I$$

U: any arbitrary unitary matrix.
U=X, Y, Z leads to CX, CY, CZ gates.

Two Qubit Gates: SWAP and CPhase gates

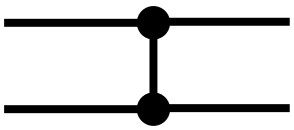
- SWAP gate: $|ab\rangle \rightarrow |ba\rangle$



$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |10\rangle \\ |10\rangle &\rightarrow |01\rangle \\ |11\rangle &\rightarrow |11\rangle \end{aligned}$$

$$\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \frac{1}{2}\left[I \otimes I + X \otimes X + Y \otimes Y + Z \otimes Z \right]$$

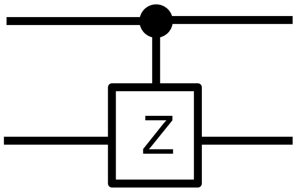
- CPhase gate = Controlled phase shift: shift phase by ϕ only if it acts on $|1\rangle$



$$|ab\rangle \rightarrow \begin{cases} |ab\rangle\, e^{i\phi} & \text{for } a = b = 1 \\ |ab\rangle & \text{otherwise} \end{cases}$$

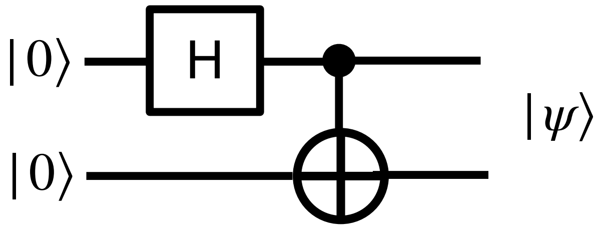
$$CPhase(\phi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes P_\phi, \qquad P_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1| e^{i\phi}$$

$$CPhase(\pi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = \mathrm{CZ} = \mathrm{Controlled\ Z}$$



Two Qubit Gates: Bell state

- Example: how to obtain Bell state.



$$
\begin{aligned}
|\psi\rangle &= \mathrm{CNOT}\,(H\otimes I)\Big[|0\rangle\otimes|0\rangle\Big] \\
&= \mathrm{CNOT}\left[\frac{1}{\sqrt{2}}\big(|0\rangle+|1\rangle\big)\otimes|0\rangle\right] \\
&= \mathrm{CNOT}\left[\frac{1}{\sqrt{2}}\big(|00\rangle+|10\rangle\big)\right] \\
&= \frac{1}{\sqrt{2}}\big(|00\rangle+|11\rangle\big) \\
&= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}
\end{aligned}
$$

$$H|x\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + (-1)^x|1\rangle\Big)$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\Big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\Big)$$

$$H|0\rangle = |+\rangle \qquad H|+\rangle = |0\rangle$$

$$H|1\rangle = |-\rangle \qquad H|-\rangle = |1\rangle$$

Quantum gate can be parametrised

Pauli rotations:

$$R_x(\theta) = e^{-i\frac{\theta}{2}\sigma_x} = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X$$

$$R_y(\theta) = e^{-i\frac{\theta}{2}\sigma_y} = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y$$

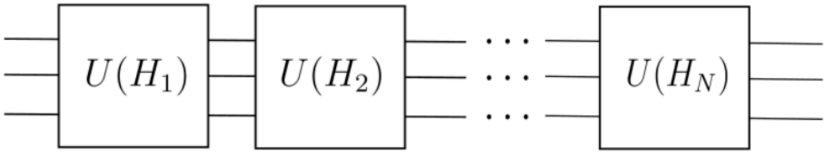
$$R_z(\theta) = e^{-i\frac{\theta}{2}\sigma_z} = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z$$

generalised form via $R(\theta_1, \theta_2, \theta_3) = R_z(\theta_1)R_y(\theta_2)R_z(\theta_3)$

$$R(\theta_1, \theta_2, \theta_3) = \begin{pmatrix} e^{i(-\frac{\theta_1}{2}-\frac{\theta_3}{2})}\cos(\frac{\theta_2}{2}) & -e^{i(-\frac{\theta_1}{2}+\frac{\theta_3}{2})}\sin(\frac{\theta_2}{2}) \\ e^{i(\frac{\theta_1}{2}-\frac{\theta_3}{2})}\sin(\frac{\theta_2}{2}) & e^{i(\frac{\theta_1}{2}+\frac{\theta_3}{2})}\cos(\frac{\theta_2}{2}) \end{pmatrix}$$

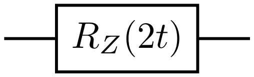
Example: Turning a Hamiltonian term into a gate

Recall $$H = H_1 + H_2 + \cdots + H_N$$



Assume, universal gate operations on device are $\{H, R_Z, CX\}$

Example 1 Assume $H_1 = Z \longrightarrow U = e^{-iZt} \longrightarrow$

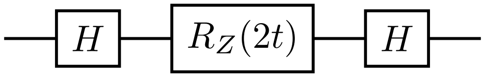


$R_Z(\theta) = e^{-i\frac{\theta}{2}Z}$

Example 2 Assume $H_2 = X \longrightarrow$ Since $HXH = Z \Rightarrow X = HZH$

$\longrightarrow U = He^{-iZt}H$ (proof via CBH Formula)

$\longrightarrow$



Example 3 $H = Z \otimes Z$ note $e^{-Z\otimes Zt} \neq e^{-iZt} \otimes e^{-iZt}$

with $(Z \otimes Z)^2 = \mathbb{I}$ one finds $e^{i(Z\otimes Z)t} = \cos(t)\mathbb{I} - i\sin(t) Z \otimes Z$

for the action on states we find

$$e^{i(Z\otimes Z)t}\left|00\right\rangle = (\cos(t)\mathbb{I} - i\sin(t)Z \otimes Z)\left|00\right\rangle = (\cos(t) - i\sin(t))\left|00\right\rangle$$

$$e^{i(Z\otimes Z)t}\left|11\right\rangle = (\cos(t)\mathbb{I} - i\sin(t)Z \otimes Z)\left|11\right\rangle = (\cos(t) - i\sin(t))\left|11\right\rangle$$

$$e^{i(Z\otimes Z)t}\left|01\right\rangle = \cos(t)\left|01\right\rangle - i\sin(t)Z\left|0\right\rangle \otimes Z\left|1\right\rangle = (\cos(t) + i\sin(t))\left|01\right\rangle$$

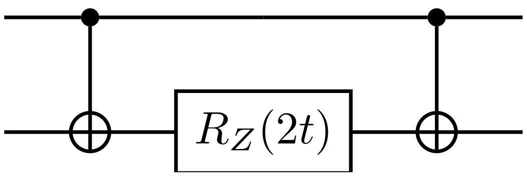
which can be written in matrix form as

$$e^{i(Z\otimes Z)t} = \left[\begin{array}{cccc} e^{-it} & 0 & 0 & 0 \\ 0 & e^{it} & 0 & 0 \\ 0 & 0 & e^{it} & 0 \\ 0 & 0 & 0 & e^{-it} \end{array}\right]\begin{array}{c} \left|00\right\rangle \\ \left|01\right\rangle \\ \left|10\right\rangle \\ \left|11\right\rangle \end{array}$$

if # of 1 is even one gets -
if #of 1 is odd one gets +

(parity of state)

circuit that implements that



with $R_Z(2t) = \begin{bmatrix} e^{-it} & 0 \\ 0 & e^{it} \end{bmatrix}$

No-cloning theorem

- Unknown quantum states can not be copied or cloned.
  - Suppose U is a unitary transformation that clones $U\big(|a\rangle|0\rangle\big) = |a\rangle|a\rangle$ for all quantum state $|a\rangle$
  - Let $|a\rangle$ and $|b\rangle$ be two orthogonal quantum states.

$$U\big(|a\rangle|0\rangle\big) = |a\rangle|a\rangle$$

$$U\big(|b\rangle|0\rangle\big) = |b\rangle|b\rangle$$

$$|c\rangle = \frac{1}{\sqrt{2}}\big(|a\rangle + |b\rangle\big)$$

$$\Rightarrow \quad U\big(|c\rangle|0\rangle\big) = \frac{1}{\sqrt{2}}\left[U|a\rangle|0\rangle + U|b\rangle|0\rangle\right] = \frac{1}{\sqrt{2}}\left[|a\rangle|a\rangle + |b\rangle|b\rangle\right]$$

$$\neq$$

$$\Rightarrow \quad U|c\rangle|0\rangle = |c\rangle|c\rangle = \frac{1}{\sqrt{2}}\big(|a\rangle + |b\rangle\big)\frac{1}{\sqrt{2}}\big(|a\rangle + |b\rangle\big) = \frac{1}{2}\big(|a\rangle|a\rangle + |a\rangle|b\rangle + |b\rangle|a\rangle + |b\rangle|b\rangle\big)$$

No-cloning theorem

- No unitary operation that can clone all quantum states.
- However it is possible to construct a quantum state from a known quantum state.

- It is possible to obtain n particles in an entangled state $a\,|\,00\cdots 0\rangle + b\,|\,11\cdots 1\rangle$ from unknown state $a\,|\,0\rangle + b\,|\,1\rangle$.

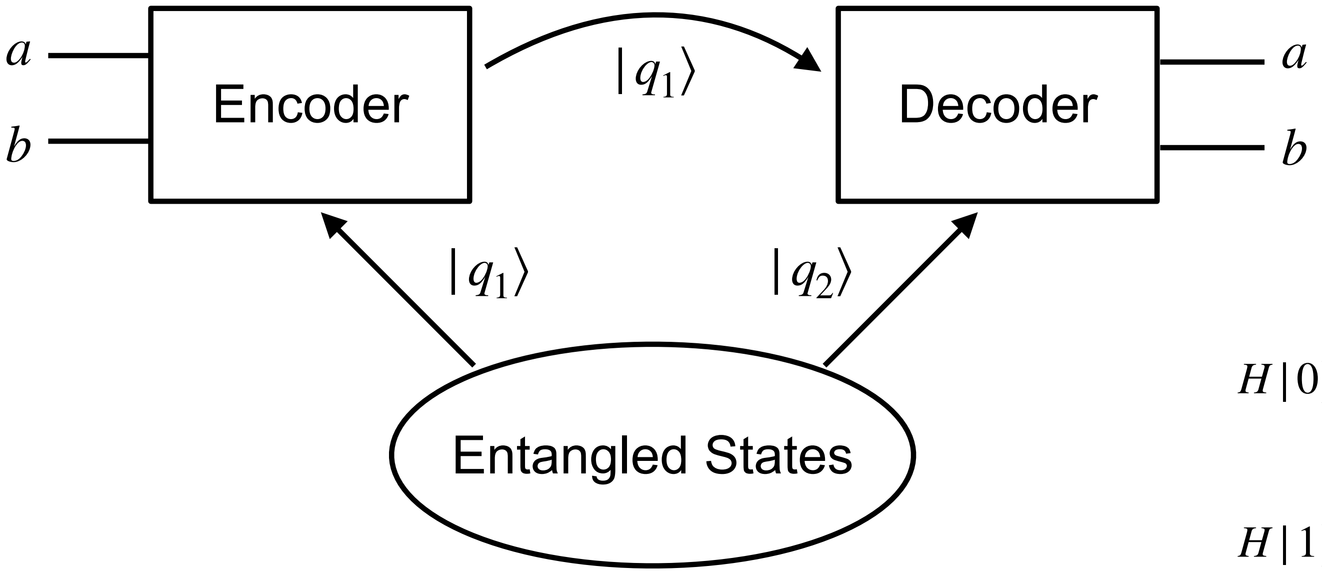
- It is not possible to create n particle state $\left(a\,|\,0\rangle + b\,|\,1\rangle\right) \otimes \cdots \otimes \left(a\,|\,0\rangle + b\,|\,1\rangle\right)$ from an unknown state $a\,|\,0\rangle + b\,|\,1\rangle$.

- Profound implication in quantum information and error correction.

Superdense Coding

Charles H. Bennett
Stephen Wiesner

1970, 1992



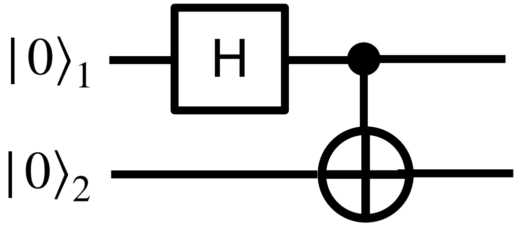
$$H|0\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)$$

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

$$H|x\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + (-1)^x|1\rangle\Big)$$

$$\text{CNOT}\,|a\,b\rangle = |a\,a \oplus b\rangle$$

- How to create two entangled states



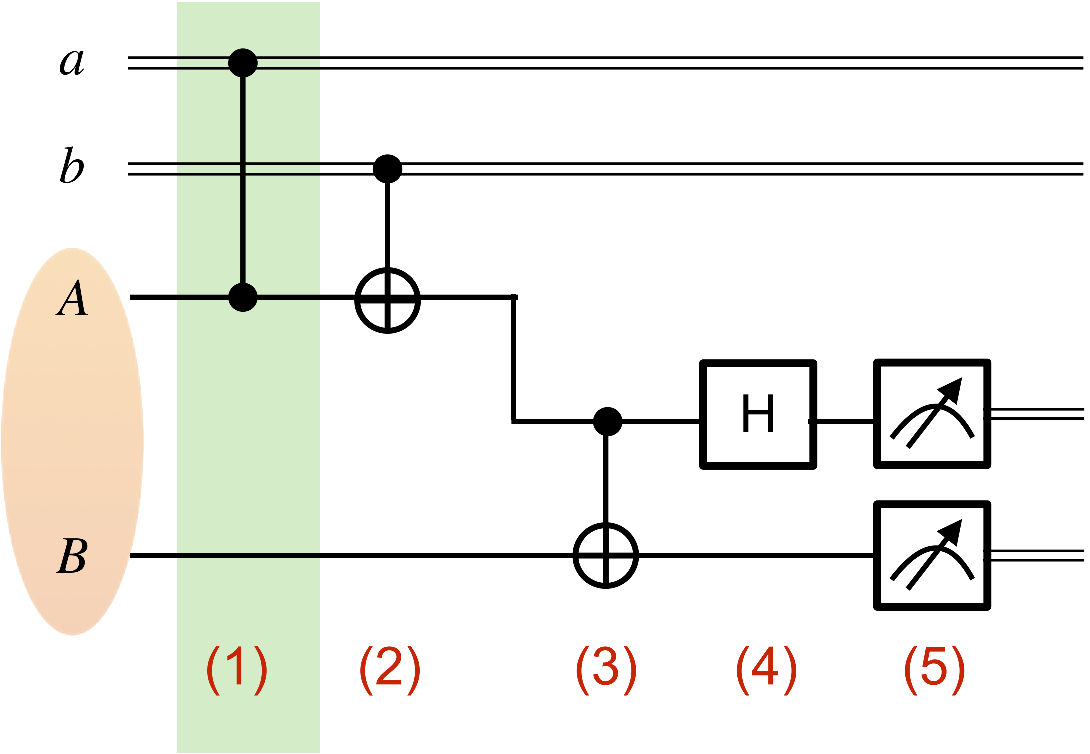
$$\text{CNOT}\Big(H \otimes I\Big)\Big(|0\rangle_1 \otimes |0\rangle_2\Big) = \text{CNOT}\,\frac{1}{\sqrt{2}}\Big(|0\rangle_1 + |1\rangle_1\Big) \otimes |0\rangle_2$$

$$= \text{CNOT}\,\frac{1}{\sqrt{2}}\Big(|00\rangle + |10\rangle\Big) = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)$$

Superdense Coding

- Initial state of qubits A and B is the entangled Bell state.

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big[\,|00\rangle \,+\, |11\rangle\,\Big]$$



(1) $a, b \in \{0,1\}$ are classical bits.

Controlled phase gate = CZ ($\phi = \pi$)

A

$$\begin{aligned} \text{if } a = 1,\ |1\rangle &\longrightarrow -|1\rangle \\ |0\rangle &\longrightarrow +|0\rangle \\ \text{if } a = 0,\ |0\rangle &\longrightarrow +|0\rangle \\ |1\rangle &\longrightarrow +|1\rangle \end{aligned}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\,|00\rangle \,+\, (-1)^a\,|11\rangle\,\Big]$$

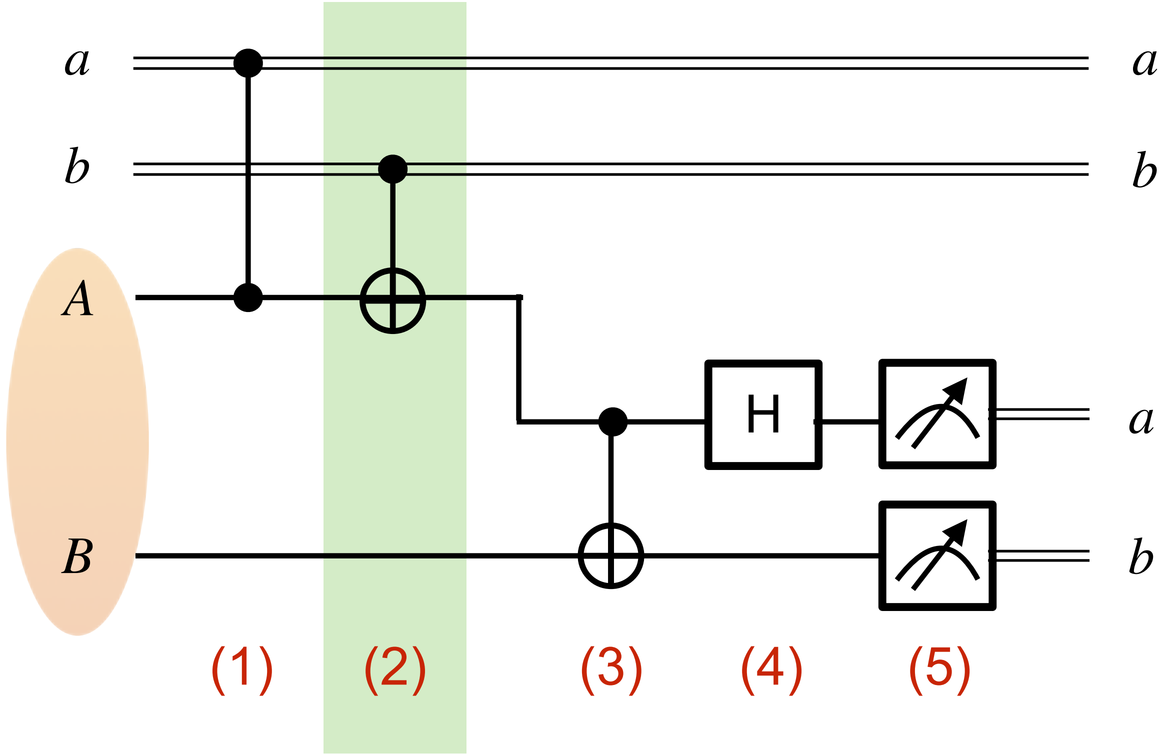
Change the phase for Alice's qubit (1st) qubit

$|\psi\rangle$= quantum state of entire system

Superdense Coding

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big[\,|00\rangle \;+\; |11\rangle\,\Big]$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\,|00\rangle \;+\; (-1)^a\,|11\rangle\,\Big]$$



(2) If b=0, the first qubit stays unchanged.

If b=1, the first qubit changes bit.

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\Big[\,|b0\rangle \;+\; (-1)^a\,|\bar{b}1\rangle\,\Big]$$

$$b = 0 \iff \bar{b} = 1$$

$$b = 1 \iff \bar{b} = 0$$

$$\begin{array}{lccc} \text{CNOT}: & (00) & \longrightarrow & (00) \\ & (01) & \longrightarrow & (01) \\ & (10) & \longrightarrow & (11) \\ & (11) & \longrightarrow & (10) \end{array}$$

b: classical bit

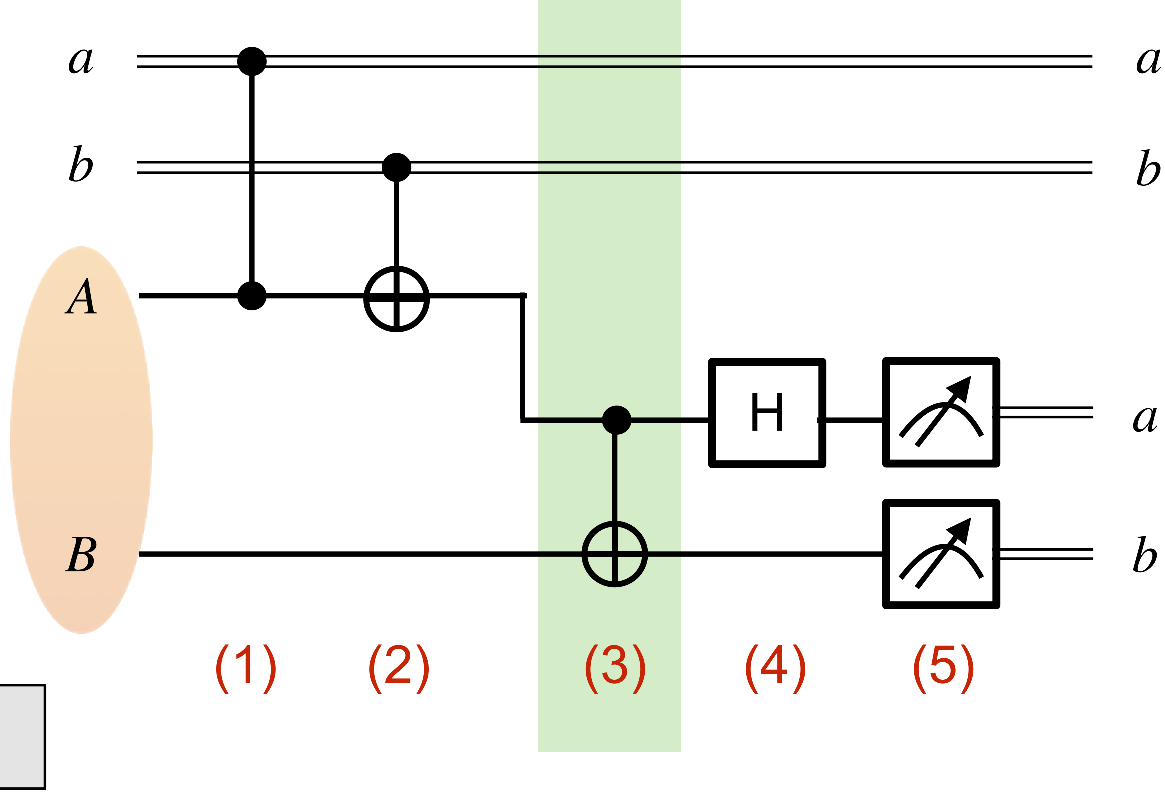
Alice’s qubit

Superdense Coding

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big[\,|00\rangle \;+\; |11\rangle\,\Big]$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\,|00\rangle \;+\; (-1)^a\,|11\rangle\,\Big]$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\Big[\,|b0\rangle \;+\; (-1)^a\,|\bar{b}1\rangle\,\Big]$$



Alice gives her qubit to Bob.

(3) Bob performs CNOT. $|\psi_3\rangle = \mathrm{CNOT}\,|\psi_2\rangle$

$$= \mathrm{CNOT}\frac{1}{\sqrt{2}}\Big[\,|b0\rangle + (-1)^a\,|\bar{b}1\rangle\Big]$$

$$= \frac{1}{\sqrt{2}}\Big[\,|bb\rangle + (-1)^a\,|\bar{b}b\rangle\Big]$$

$$\mathrm{CNOT}\,|b0\rangle = |bb\rangle$$

$$\mathrm{CNOT}\,|\bar{b}1\rangle = |\bar{b}b\rangle$$

Change the 2nd qubit conditioned upon 1st qubit.

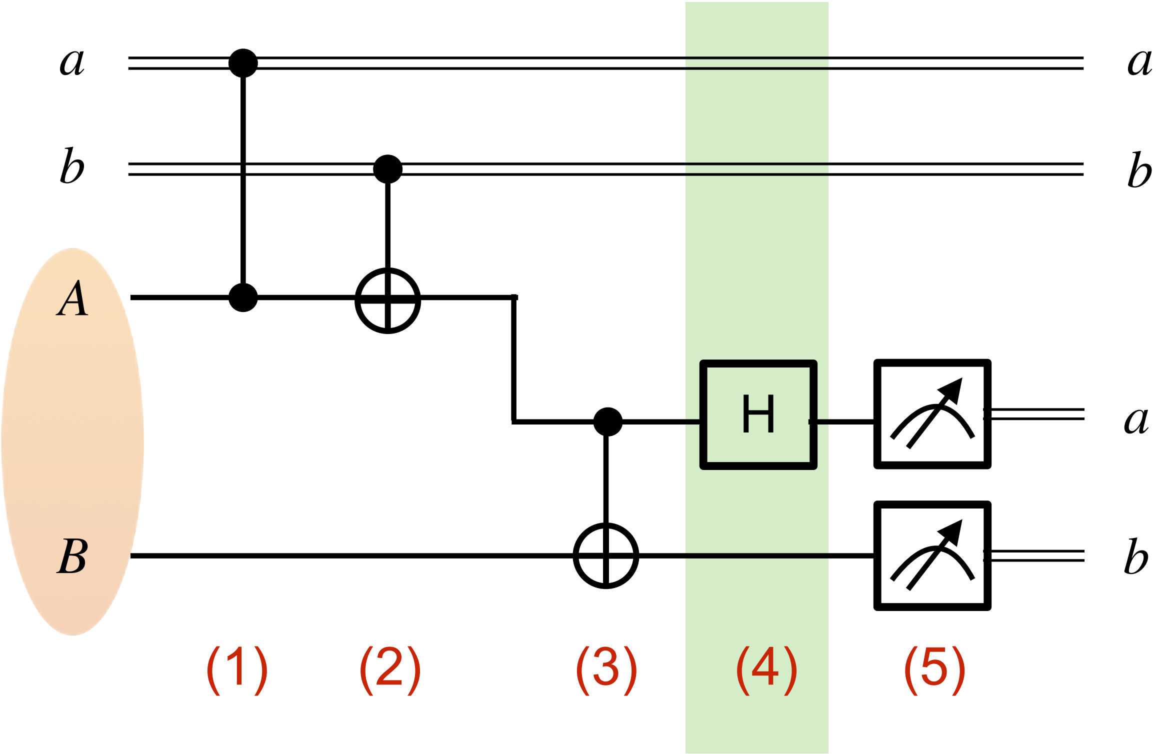
Superdense Coding

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big[\,|00\rangle\ +\ |11\rangle\,\Big]$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\,|00\rangle\ +\ (-1)^a\,|11\rangle\,\Big]$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\Big[\,|b0\rangle\ +\ (-1)^a\,|\bar{b}1\rangle\,\Big]$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\Big[\,|bb\rangle + (-1)^a\,|\bar{b}b\rangle\Big]$$



(4) Bob applies Hadamard on Alice's qubit (1st qubit).

$$|\psi_4\rangle = \Big(H\otimes I\Big)\,|\psi_3\rangle = \Big(H\otimes I\Big)\frac{1}{\sqrt{2}}\Big[\,|bb\rangle + (-1)^a\,|\bar{b}b\rangle\Big]$$

$$= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\Big[\,|0b\rangle + (-1)^b\,|1b\rangle + (-1)^a\Big(\,|0b\rangle + (-1)^{\bar{b}}\,|1b\rangle\Big)\Big]$$

$$= \frac{1}{2}\Big[\Big(1 + (-1)^a\Big)\,|0b\rangle + \Big((-1)^b + (-1)^{a+\bar{b}}\Big)\,|1b\rangle\Big]$$

$$H\,|x\rangle = \frac{1}{\sqrt{2}}\Big(\,|0\rangle + (-1)^x\,|1\rangle\Big)$$

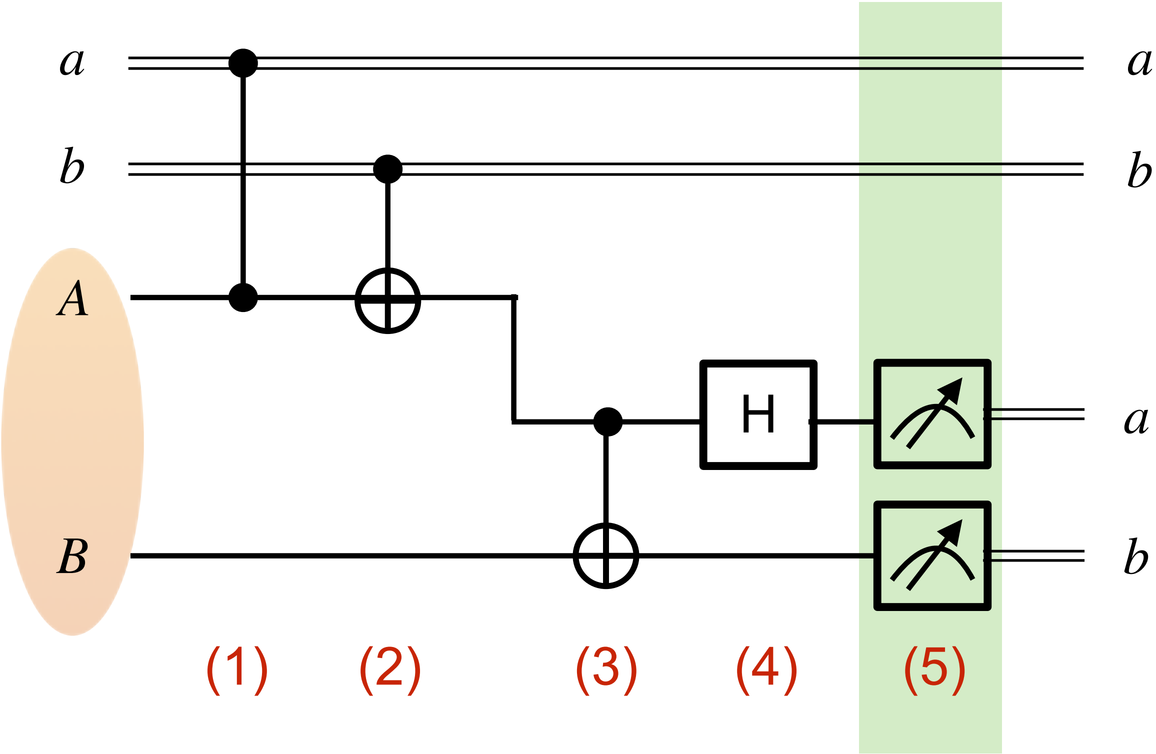
Superdense Coding

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big[\,|00\rangle \;+\; |11\rangle\,\Big]$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\,|00\rangle \;+\; (-1)^a\,|11\rangle\,\Big]$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\Big[\,|b0\rangle \;+\; (-1)^a\,|\bar{b}1\rangle\,\Big]$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\Big[\,|bb\rangle + (-1)^a\,|\bar{b}b\rangle\Big]$$



(4) Bob applies Hadamard.

$$|\psi_4\rangle = \frac{1}{2}\Big[\big(1+(-1)^a\big)\,|0\rangle + \big((-1)^b + (-1)^{a+\bar{b}}\big)\,|1\rangle\Big] \otimes |b\rangle$$

$$= \frac{1}{2}\Big[\big(1+(-1)^a\big)\,|0\rangle + (-1)^b\big(1-(-1)^a\big)\,|1\rangle\Big] \otimes |b\rangle$$

(5) Bob performs measurements on both qubits.

Superdense Coding

a	b	$\bar{b}$	$a+\bar{b}$	$\|A\rangle$	$\|B\rangle$
0	0	1	1	$\|0\rangle$	$\|0\rangle$
0	1	0	0	$\|0\rangle$	$\|1\rangle$
1	0	1	0=2	$\|1\rangle$	$\|0\rangle$
1	1	0	1	$-\|1\rangle$	$\|1\rangle$

$$|\psi_4\rangle = |A\rangle \otimes |B\rangle = \frac{1}{2}\Big[\big(1+(-1)^a\big)|0\rangle + \big((-1)^b + (-1)^{a+\bar{b}}\big)|1\rangle\Big] \otimes |B\rangle$$

$$|\psi_4\rangle = (-1)^{ab}|ab\rangle = (-1)^{ab}|a\rangle \otimes |b\rangle$$

- Measurement of two qubits yield two classical bits a and b with 100% probability.
- By initially sharing some entanglement, one can send two bits of information by sending a single qubit.
- Shared entanglement → powerful resource for quantum cryptography

Superdense Coding

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

a	b	Transformation (Alice)	New state
0	0	$I \otimes I\,|\psi_0\rangle$	$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$
0	1	$X \otimes I\,|\psi_0\rangle$	$\frac{1}{\sqrt{2}}\left(|10\rangle + |01\rangle\right)$
1	0	$Z \otimes I\,|\psi_0\rangle$	$\frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$
1	1	$Y \otimes I\,|\psi_0\rangle$	$\frac{1}{\sqrt{2}}\left(-|10\rangle + |01\rangle\right)$

- Bob measures two qubits in the standard basis to obtain two-bit binary encoding of the number that Alice wishes to send.

$\longrightarrow$

Alice gives her qubit to Bob.

CNOT (Bob)

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

$$\frac{1}{\sqrt{2}}\left(|11\rangle + |01\rangle\right) = \frac{1}{\sqrt{2}}\left(|1\rangle + |0\rangle\right) \otimes |1\rangle$$

$$\frac{1}{\sqrt{2}}\left(|00\rangle - |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \otimes |0\rangle$$

$$\frac{1}{\sqrt{2}}\left(-|11\rangle + |01\rangle\right) = \frac{1}{\sqrt{2}}\left(-|1\rangle + |0\rangle\right) \otimes |1\rangle$$

$$\xrightarrow{H \otimes I}$$

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

$$|0\rangle \otimes |1\rangle$$

$$|1\rangle \otimes |0\rangle$$

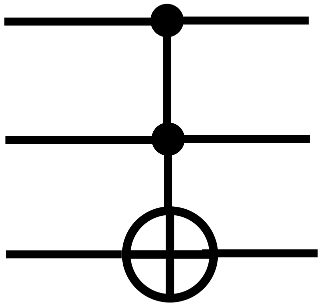
$$-|1\rangle \otimes |1\rangle$$

Comments

- This result shouldn't be surprising: it is a known result that n qubits cannot be used to store more than n bits of information.
- To devise a super-superdense coding scheme to transmit more than two bits of information with only two qubits, would mean to find a way to encode and decode more than two bits of information in the overall state of two qubits, and we know that this is not possible.
- Nonetheless, the superdense coding protocol does provide advantages with respect to the classical case. The qubit used as channel can be generated and shared a long time before the communication begins, and just be kept "in store" for whenever Alice and Bob feel the need to use it. When they finally decide to communicate, they can now "compress" two bits of information into a single qubit, thus effectively doubling their channel capacity, at the cost of "consuming" the pre-shared qubit.
- In other words, you can think of the superdense protocol as a way to "preload" the communication, in order to make it more efficient in the future. What is neat and "quantum" about this is that it can be done without any assumption on the actual information that will be transmitted later. This would not be possible in a classical context. This works for two entangled qubits only. (Security + no-cloning)
- There are many research articles on super-dense coding.

Three Qubit Gates

- Toffoli gate=Controlled CNOT=CCNOT=CCX=T
  - If 1st qubit is $|1\rangle$, perform CNOT on the second and third qubits.



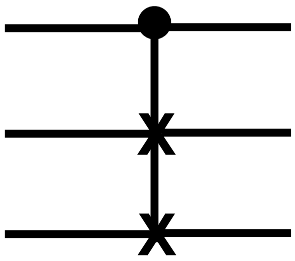
$$\begin{array}{l}
|000\rangle \\
|001\rangle \\
|010\rangle \\
|011\rangle \\
\hdashline
|100\rangle \\
|101\rangle \\
\hdashline
|110\rangle \longrightarrow |111\rangle \\
|111\rangle \quad\quad\quad\;\; |110\rangle
\end{array}$$

$$T = \left(\begin{array}{cccc:cccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
\hdashline
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{array}\right) = \left(\begin{array}{c:c}
I & 0 \\
\hdashline
0 & \text{CNOT}
\end{array}\right)$$

$$T = \exp\left[i\frac{\pi}{8}(I - Z_1)(I - Z_2)(I - X_3)\right]$$

Three Qubit Gates

- Fredkin gate=Controlled SWAP=CSWAP gate
  - If 1st qubit is $|1\rangle$, swap the second and third qubits.

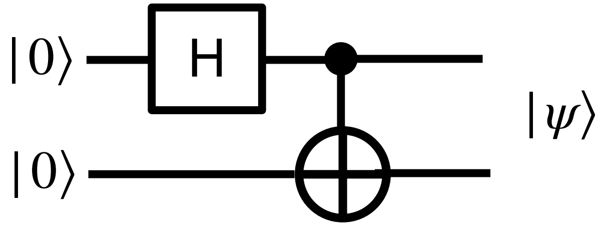


$$\begin{array}{lcl} |000\rangle & & \\ |001\rangle & & \\ |010\rangle & & \\ |011\rangle & & \\ \hdashline |100\rangle & \longrightarrow & |100\rangle \\ |101\rangle & & |110\rangle \\ |110\rangle & & |101\rangle \\ |111\rangle & & |111\rangle \end{array}$$

$$T = \left(\begin{array}{cccc:cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{c:c} I & 0 \\ \hdashline 0 & \mathrm{SWAP} \end{array}\right)$$

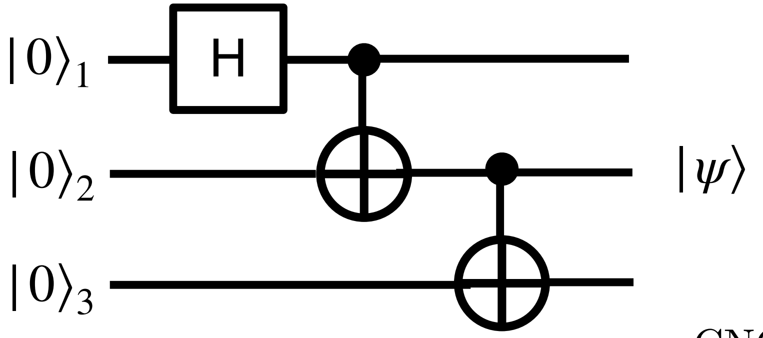
Two Qubit Gates: Bell state

- Example: how to obtain Bell state.



$$
\begin{aligned}
|\psi\rangle &= \mathrm{CNOT}\,(H \otimes I)\left[|0\rangle \otimes |0\rangle\right] \\
&= \mathrm{CNOT}\left[\frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |0\rangle\right] \\
&= \mathrm{CNOT}\left[\frac{1}{\sqrt{2}}\big(|00\rangle + |10\rangle\big)\right] = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \\
&= \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \\
&= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}
\end{aligned}
$$

An example: GHZ state



$$|\psi\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

Greenberger-Horne-Zeilinger (GHZ) state, 1989

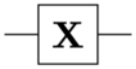
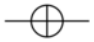
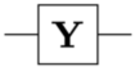
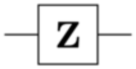
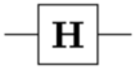
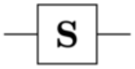
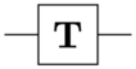
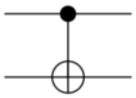
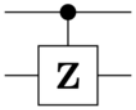
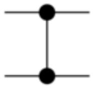
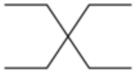
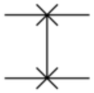
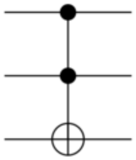
$\mathrm{CNOT}_{ij} = \mathrm{CNOT}$ with qubit i as the control and qubit j as the target.

$$\begin{aligned}
|\psi\rangle &= \left(I_1 \otimes CNOT_{23}\right)\left(CNOT_{12} \otimes I_3\right)\left(H \otimes I_2 \otimes I_3\right) |0\rangle \otimes |0\rangle \otimes |0\rangle \\
&= \left(I_1 \otimes CNOT_{23}\right) \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big) \otimes |0\rangle \\
&= \left(I_1 \otimes CNOT_{23}\right) \frac{1}{\sqrt{2}}\Big(|000\rangle + |110\rangle \Big) \\
&= \frac{1}{\sqrt{2}}\Big(|0\rangle \otimes CNOT\,|00\rangle + |1\rangle \otimes CNOT\,|10\rangle \Big) \quad = \frac{|000\rangle + |111\rangle}{\sqrt{2}}
\end{aligned}$$

For N-qubit system: $$|GHZ\rangle = \frac{|0\rangle^{\otimes N} + |1\rangle^{\otimes N}}{\sqrt{2}} = \frac{|00\cdots 0\rangle\ +\ |11\cdots 1\rangle}{\sqrt{2}}$$

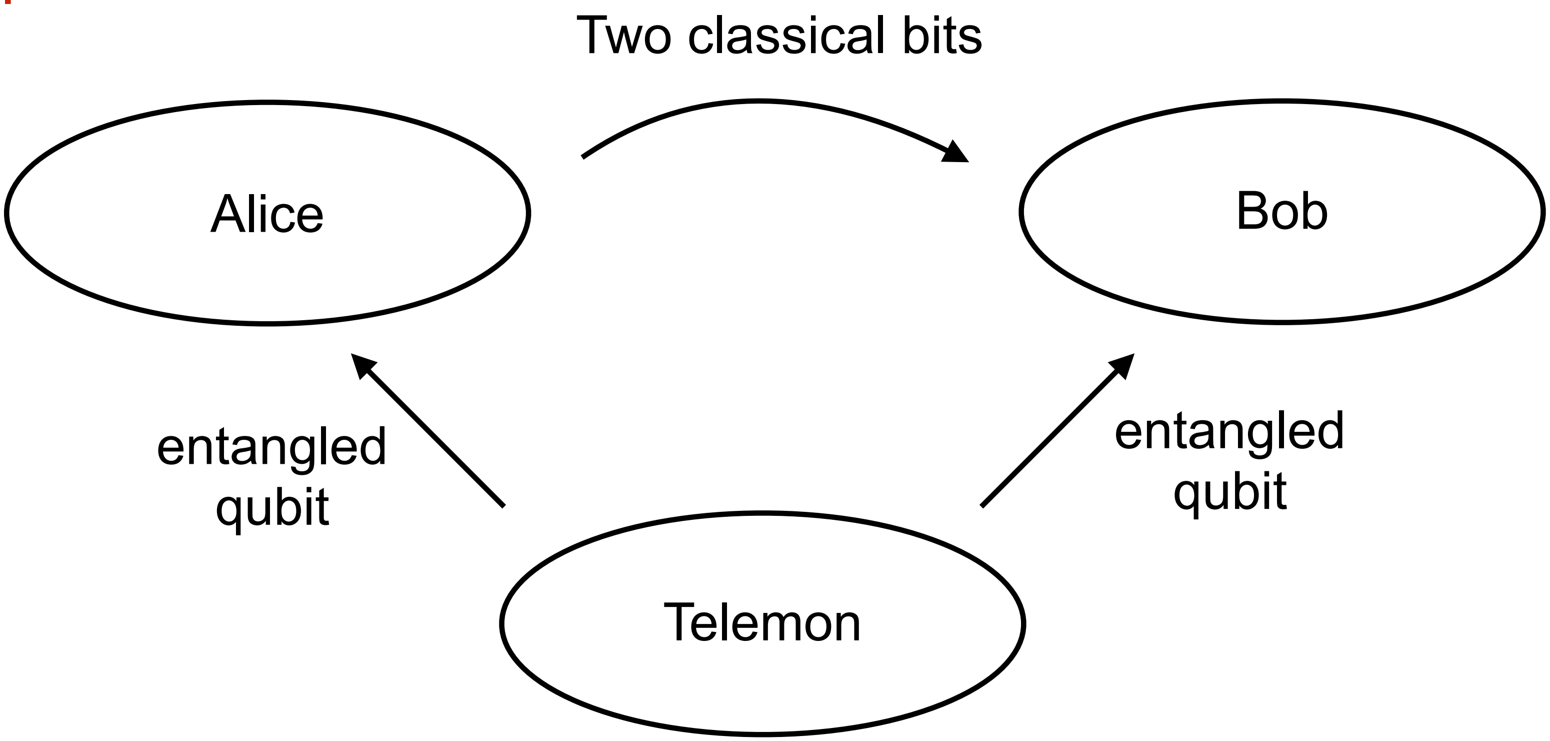
Maximally entangled quantum state

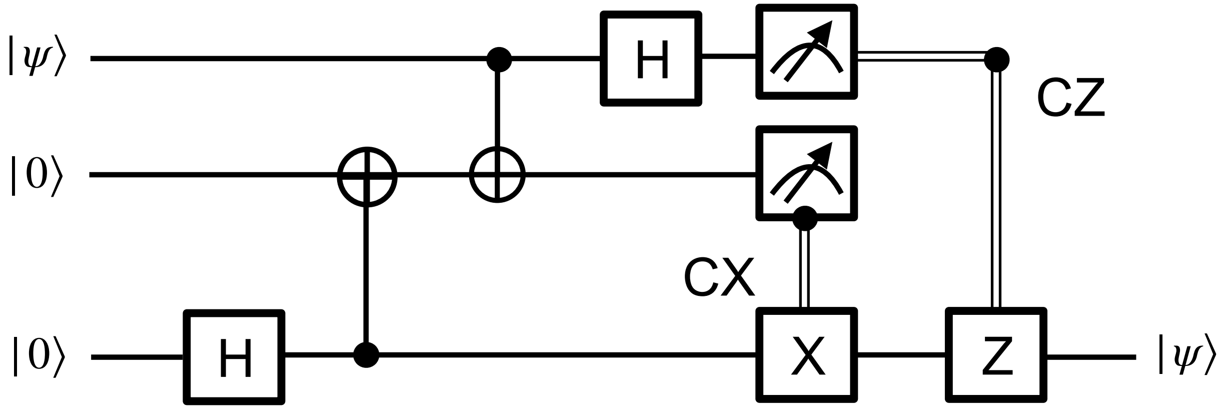
- IBMQ

Operator	Gate(s)		Matrix
Pauli-X (X)			$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)			$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)			$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)			$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)			$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
π/8 (T)			$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)			$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Teleportation

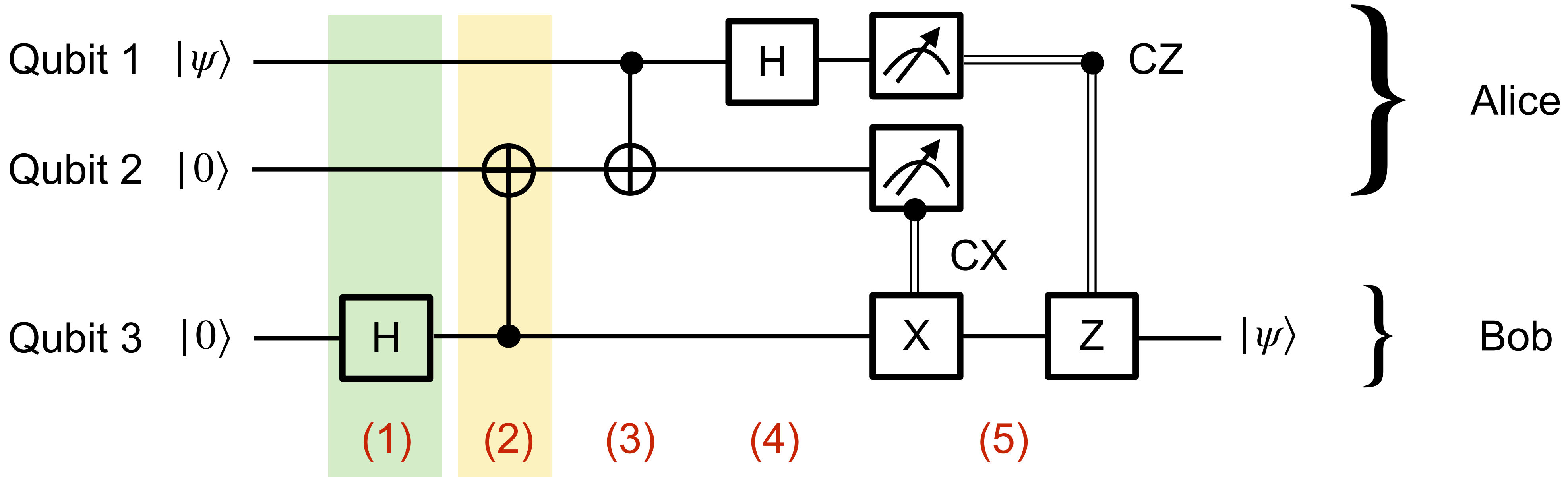
- Use two classical bits and one Bell pair to move a state from qubit 1 to qubit 3.





Teleportation

- Use two classical bits and one Bell pair to move a state from qubit 1 to qubit 3. $\mathrm{CNOT}_{ij} = \mathrm{CNOT}$ with qubit i as the control and qubit j as the target.



initial state $= |\psi_0\rangle = |\psi\rangle_1 \otimes |0\rangle_2 \otimes |0\rangle_3$

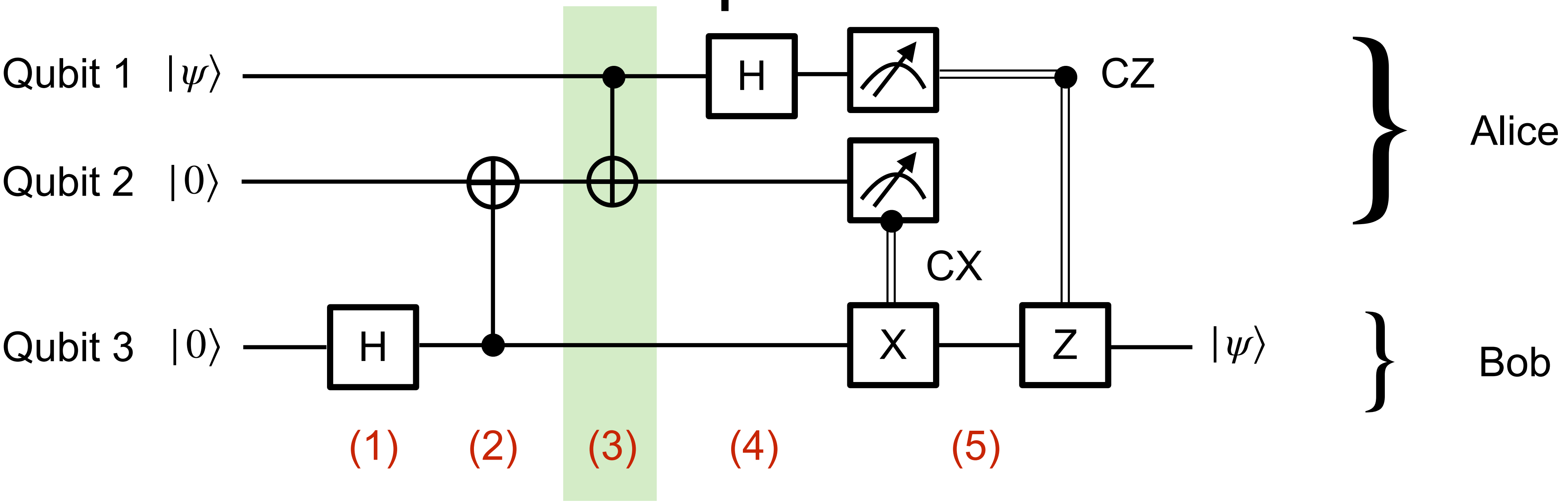
$$|\psi_1\rangle = H_3 |\psi\rangle_1 \otimes |0\rangle_2 \otimes |0\rangle_3 = |\psi\rangle_1 \otimes |0\rangle_2 \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle \Big)$$

$$|\psi_2\rangle = CNOT_{32} |\psi\rangle_1 \otimes |0\rangle_2 \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle \Big)$$

conditioned on q3

$$= |\psi\rangle_1 \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \Big)$$

Teleportation

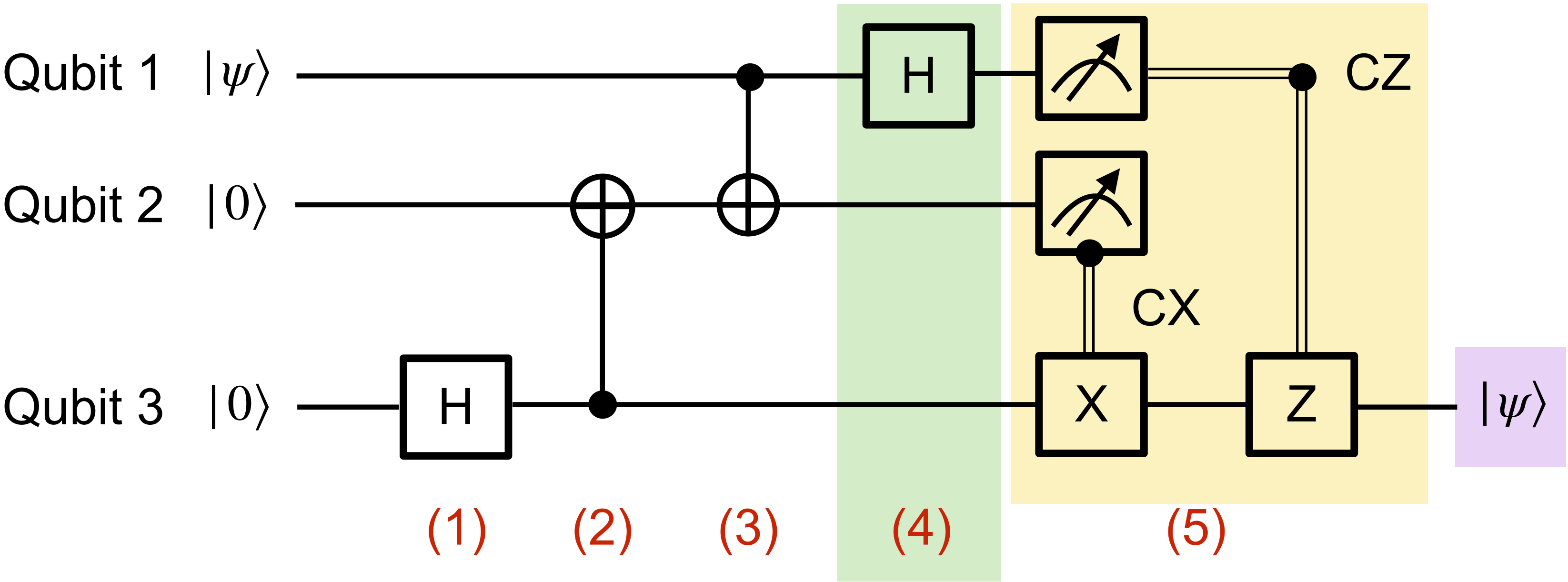


$$|\psi_2\rangle = |\psi\rangle_1 \otimes \frac{1}{\sqrt{2}}\Big(\,|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\Big)$$

$$\begin{aligned}
|\psi_3\rangle &= CNOT_{12}\ |\psi\rangle_1 \otimes \frac{1}{\sqrt{2}}\Big(\,|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\Big) \\
&= CNOT_{12}\ \big(\alpha|0\rangle + \beta|1\rangle\big) \otimes \frac{1}{\sqrt{2}}\Big(\,|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\Big) \\
&= CNOT_{12}\ \frac{1}{\sqrt{2}}\Big(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\Big) \\
&= \frac{1}{\sqrt{2}}\Big(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\Big)
\end{aligned}$$

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

Teleportation



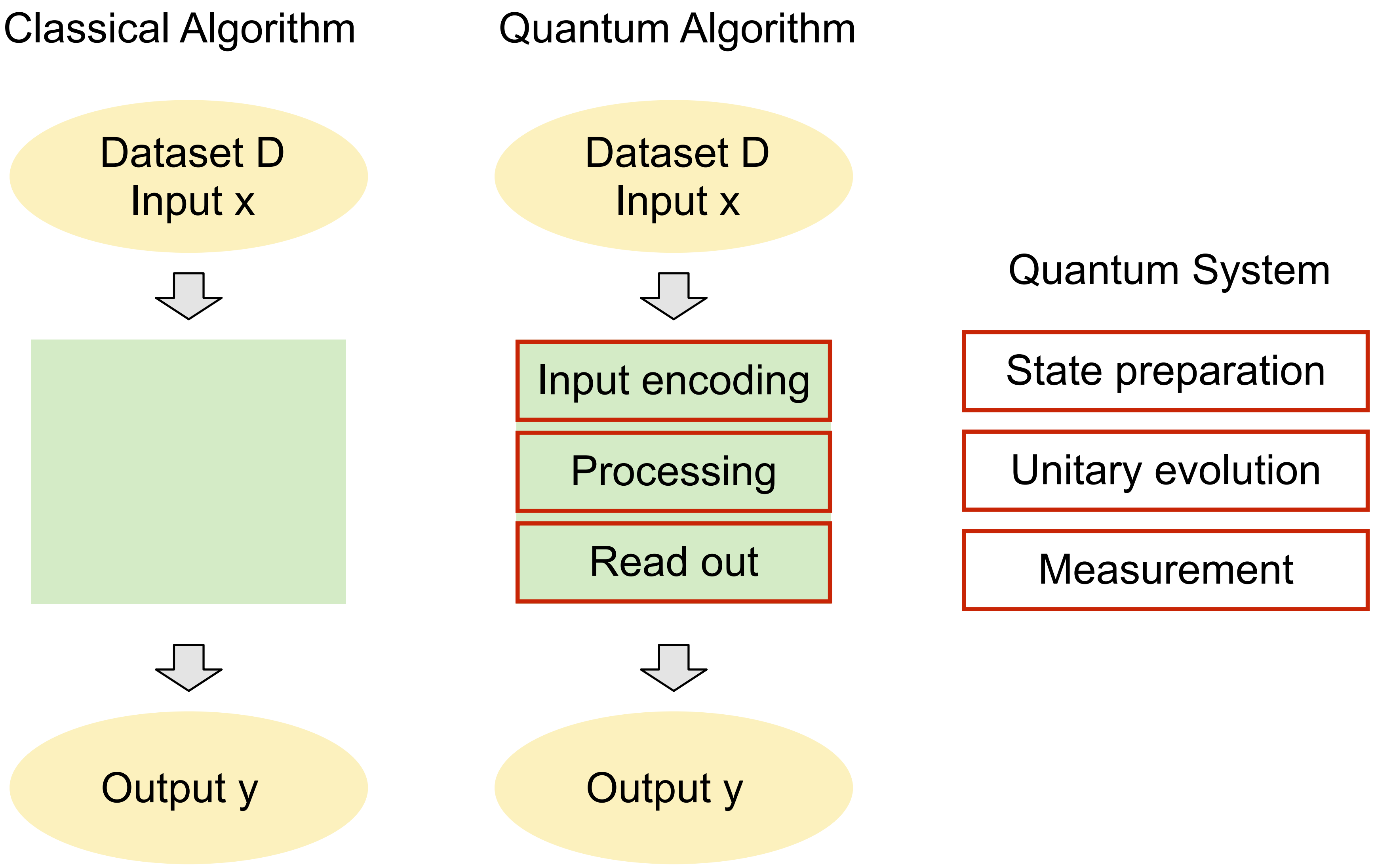
Initial state:
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\right)$$

$$|\psi_4\rangle = H_1|\psi_3\rangle = \frac{1}{2}\left[\alpha\left(|000\rangle + |100\rangle\right) + \alpha\left(|011\rangle + |111\rangle\right) + \beta\left(|010\rangle - |110\rangle\right) + \beta\left(|001\rangle - |101\rangle\right)\right]$$

qubit1	qubit2	qubit3	correction step	final state
0	0	$\alpha|0\rangle + \beta|1\rangle$	I	$\alpha|0\rangle + \beta|1\rangle$
0	1	$\beta|0\rangle + \alpha|1\rangle$	X	$\alpha|0\rangle + \beta|1\rangle$
1	0	$\alpha|0\rangle - \beta|1\rangle$	Z	$\alpha|0\rangle + \beta|1\rangle$
1	1	$-\beta|0\rangle + \alpha|1\rangle$	ZX	$\alpha|0\rangle + \beta|1\rangle$

Quantum Algorithms and Data Embedding



Classical Algorithm

Dataset D
Input x

Output y

Quantum Algorithm

Dataset D
Input x

Input encoding

Processing

Read out

Output y

Quantum System

State preparation

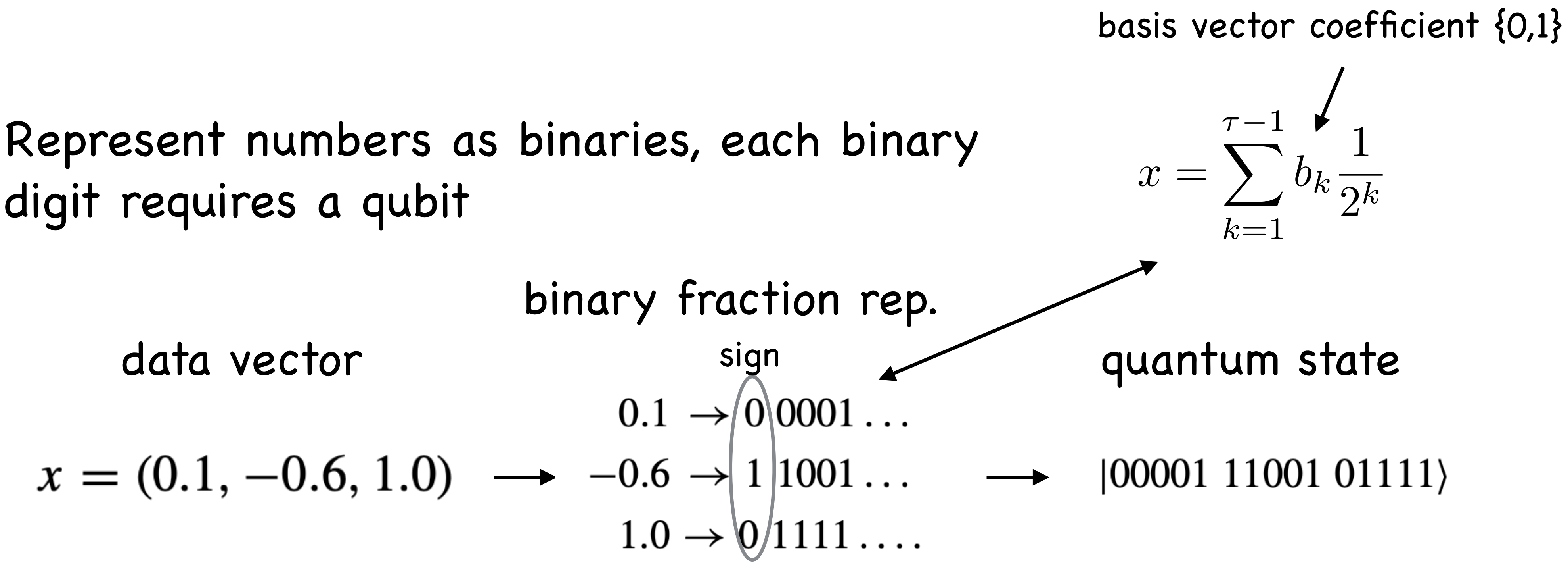
Unitary evolution

Measurement

Quantum Algorithms and Data Embedding

	Classical data	Requirement	Quantum state
Basis Encoding	$\vec{x} \in \{0,1\}^{\otimes n}$ $\vec{x} = (x_1, x_2, \cdots, x_n) \in \{0,1\}$		$\lvert\psi\rangle = \lvert x_1 x_2 \cdots x_n\rangle$ $= \lvert x_1\rangle \otimes \lvert x_2\rangle \otimes \cdots \otimes \lvert x_n\rangle$
Amplitude Encoding	$\vec{x} \in \mathbb{R}^{2^n}$ $x_i \in \mathbb{R}$	$\sum_{i=1}^{2^n} \lvert x_i\rvert^2 = 1$	$\lvert\psi_x\rangle = \sum_{i=1}^{2^n} x_i \lvert i \rangle$
	$A \in \mathbb{R}^{2^n \times 2^m}$ $\quad i = 1,\cdots,2^n$ $A_{ij} \in \mathbb{R}$ $\quad j = 1,\cdots,2^m$	$\sum_{i,j} \lvert A_{ij}\rvert^2 = 1$	$\lvert\psi_A\rangle = \sum_{i,j} A_{ij} \lvert i \rangle \otimes \lvert j \rangle$
	$A \in \mathbb{R}^{2^n \times 2^n}$	$\sum_i A_{ii} = 1$ $\quad A^\dagger = A$ $A^*_{ij} = A_{ji}$	$\rho_A = \sum_{i,j} A_{ij} \lvert i \rangle \langle j \rvert$
Time-evolution Encoding	$x \in \mathbb{R}$	$x \in [0, 2\pi)$	$U(x) = e^{-ixH}$
Hamiltonian Encoding	$A \in \mathbb{R}^{2^n \times 2^n}$	$A^\dagger = A$	$H_A = A$
	$A \in \mathbb{R}^{2^n \times 2^n}$	$A^\dagger \neq A$ (in general)	$H_A = \begin{pmatrix} 0 & A \\ A^\dagger & 0 \end{pmatrix}$

Binary encoding into basis states



Represent numbers as binaries, each binary digit requires a qubit

basis vector coefficient {0,1}

$$x = \sum_{k=1}^{\tau-1} b_k \frac{1}{2^k}$$

binary fraction rep.

data vector

sign

quantum state

$$x = (0.1, -0.6, 1.0) \longrightarrow \begin{matrix} 0.1 \rightarrow 0\ 0001\ldots \\ -0.6 \rightarrow 1\ 1001\ldots \\ 1.0 \rightarrow 0\ 1111\ldots. \end{matrix} \longrightarrow |00001\ 11001\ 01111\rangle$$

- Binary fraction = expression in power of 1/2

In decimal form: $0.j_\ell\, j_{\ell+1} \cdots j_m = \frac{j_\ell}{2} + \frac{j_{\ell+1}}{2^2} + \cdots + \frac{j_m}{2^{m-\ell+1}}$

$$j = j_1 2^7 + j_2 2^6 + j_3 2^5 + j_4 2^4 + j_5 2^3 + j_6 2^2 + j_7 2^1 + j_8 2^0$$

$$\frac{j}{2^3} = j_1 2^4 + j_2 2^3 + j_3 2^2 + j_4 2^1 + j_5 2^0 + \underbrace{j_6 2^{-1} + j_7 2^{-2} + j_8 2^{-3}}$$

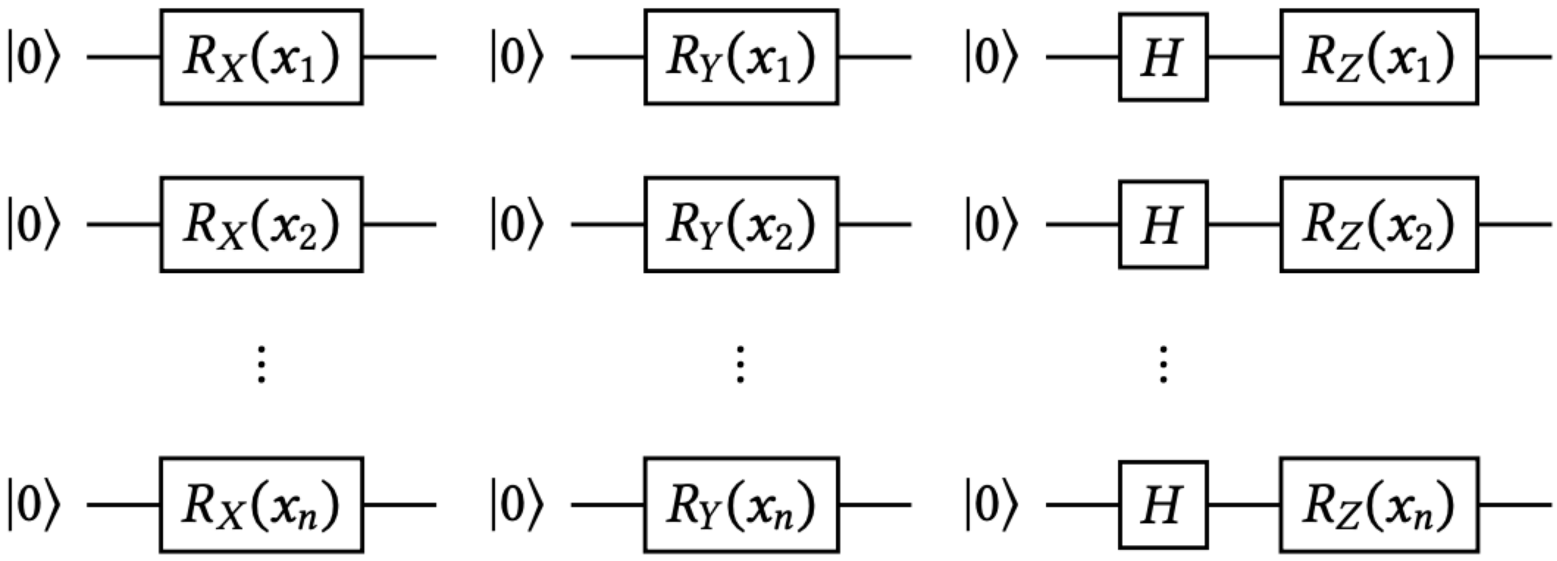
$j_1 j_2 j_3 j_4 j_5 \cdot j_6 j_7 j_8$

binary fraction: $0\,.j_6 j_7 j_8$

Angle/Rotation encoding

When used on an n-qubit circuit, this feature map of angle encoding can take up to n numerical inputs $x_1, \ldots, x_n$. The action of its circuit consists in the application of a rotation gate on each qubit j parametrised by the value x_j. In this feature map, we are using the x_j values as angles in the rotations, hence the name of the encoding.

Example



x normalised [0,2pi)

as RZ|0> doesnt do anything

Quantum versions of classical algorithms

- Any quantum computation is reversible prior to measurement. In contrast, classical computations are NOT in general reversible.
  - (ex) classical NOT operation is reversible while AND, OR NAND are not
  - Every classical computation does have a classical reversible analog (which takes slightly more computational resources)
  - The construction of efficient classical reversible versions of arbitrary Boolean circuits easily generalizes to construction of quantum circuits (that implement general classical circuits)
- Any classical reversible computation with n-input and n-ouput simply permutes $N = 2^n$ bit strings

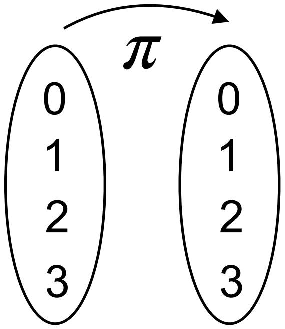
Classical computation: $\pi : \; Z_N \longrightarrow Z_N$

Quantum computation: $U_\pi : \; \sum_{x=0}^{N-1} a_x |x\rangle \longrightarrow \sum_{x=0}^{N-1} a_x |\pi(x)\rangle$

Quantum versions of classical algorithms

$n = 2,\ N = 2^2 = 4$

$$|0\rangle = |00\rangle$$
$$|1\rangle = |01\rangle$$
$$|2\rangle = |10\rangle$$
$$|3\rangle = |11\rangle$$



- Any classical computation n-inputs and m-outputs defines

$$\begin{aligned} f:\quad Z_N &\longrightarrow Z_M \\ x &\longrightarrow f(x) \end{aligned} \qquad N = 2^n \qquad M = 2^m$$

→ can be extended to a reversible function π_f acting on n+m bits

$$\begin{aligned} \pi_f:\quad Z_L &\longrightarrow Z_L \\ (x, y) &\longrightarrow (x, y \oplus f(x)) \end{aligned} \qquad L = 2^{n+m}$$

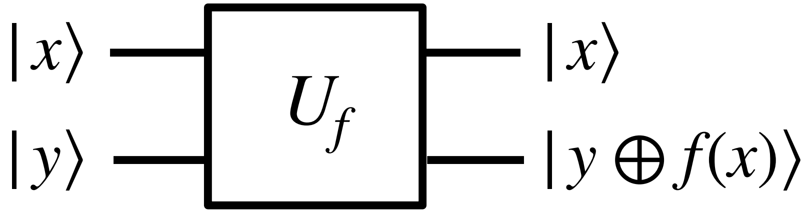
$\bigoplus$ = bitwise exclusive OR

x = n-bit string y = m-bit string L = n+m-bit string $f(x)$ = m-bit string

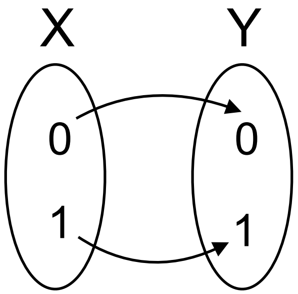
- For y=0, π acts like f: $(x,0) \longrightarrow (x, f(x))$

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

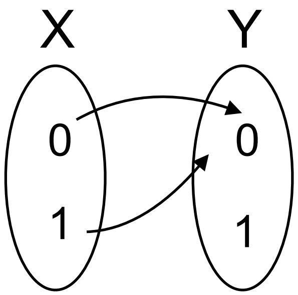
- π_f is reversible, there is a corresponding unitary transformation

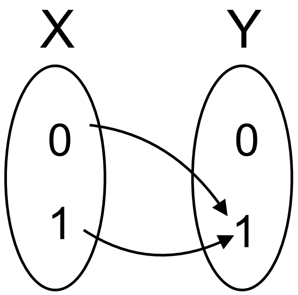


A simple QA with two qubits

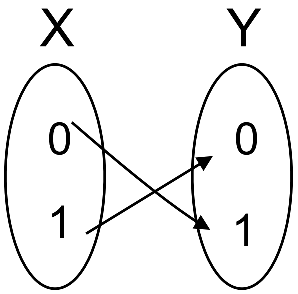


- Consider a simple function, $f(x) : \underset{\text{one-bit domain}}{\{0,1\}} \longrightarrow \underset{\text{one-bit range}}{\{0,1\}}$
- For possible functions
  - Identity: $f(0) = 0$ and $f(1) = 1$
  - Bit-flip function: $f(0) = 1$ and $f(1) = 0$
  - Constant function: $f(x) = 0$ or $f(x) = 1$



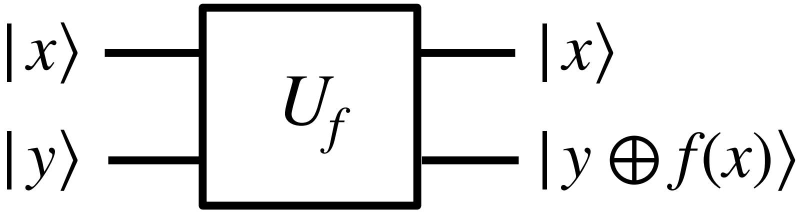


- Reconstruct a unitary transformation U_f such that $(x, y) \xrightarrow[U_f]{} (x, y \oplus f(x))$, which corresponds to $U_f\Big(|x\rangle \otimes |y\rangle \Big) = |x\rangle \otimes |y \oplus f(x)\rangle$



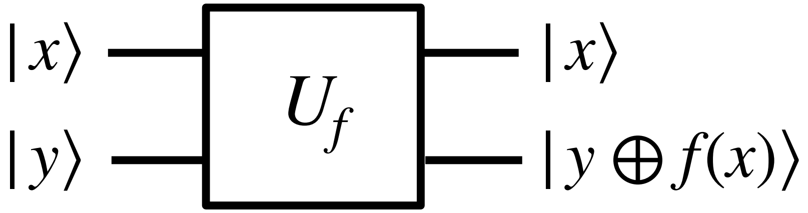
- $\oplus$ is mode 2 addition: $0 \oplus 0 = 0 = 1 \oplus 1$ and $0 \oplus 1 = 1 = 0 \oplus 1$.
- $x \longrightarrow f(x)$ is not suitable because $f(x)$ is not unitary in general.
- $(x, y) \xrightarrow{U_f} (x, y \oplus f(x)) \xrightarrow{U_f} (x, y \oplus f(x) \oplus f(x)) = (x, y)$

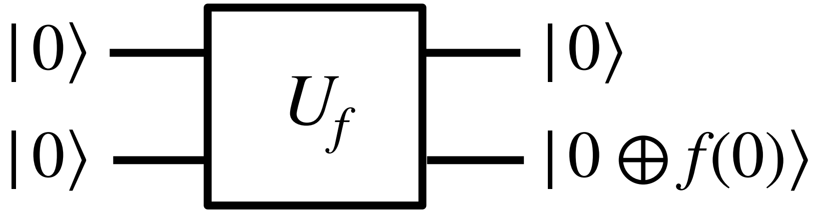
$$U_f\Big(|x\rangle \otimes |y\rangle \Big) = |x\rangle \otimes |y \oplus f(x)\rangle$$



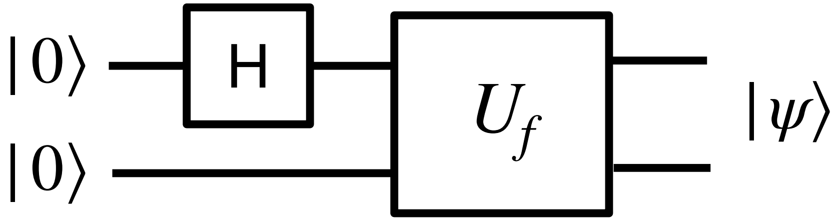
A simple QA with two qubits

- Take advantage of “quantum parallelism” (a qubit can have both $|0\rangle$ and $|1\rangle$)





- Apply Hadamard gate to the first qubit and then apply U.



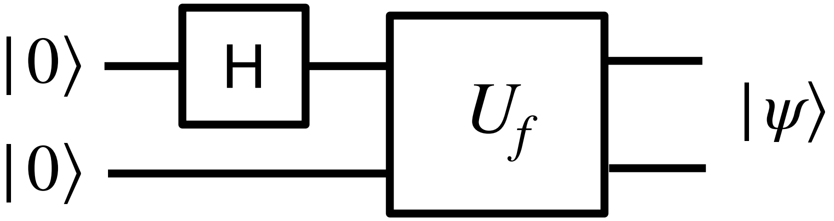
$$H|0\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)$$

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

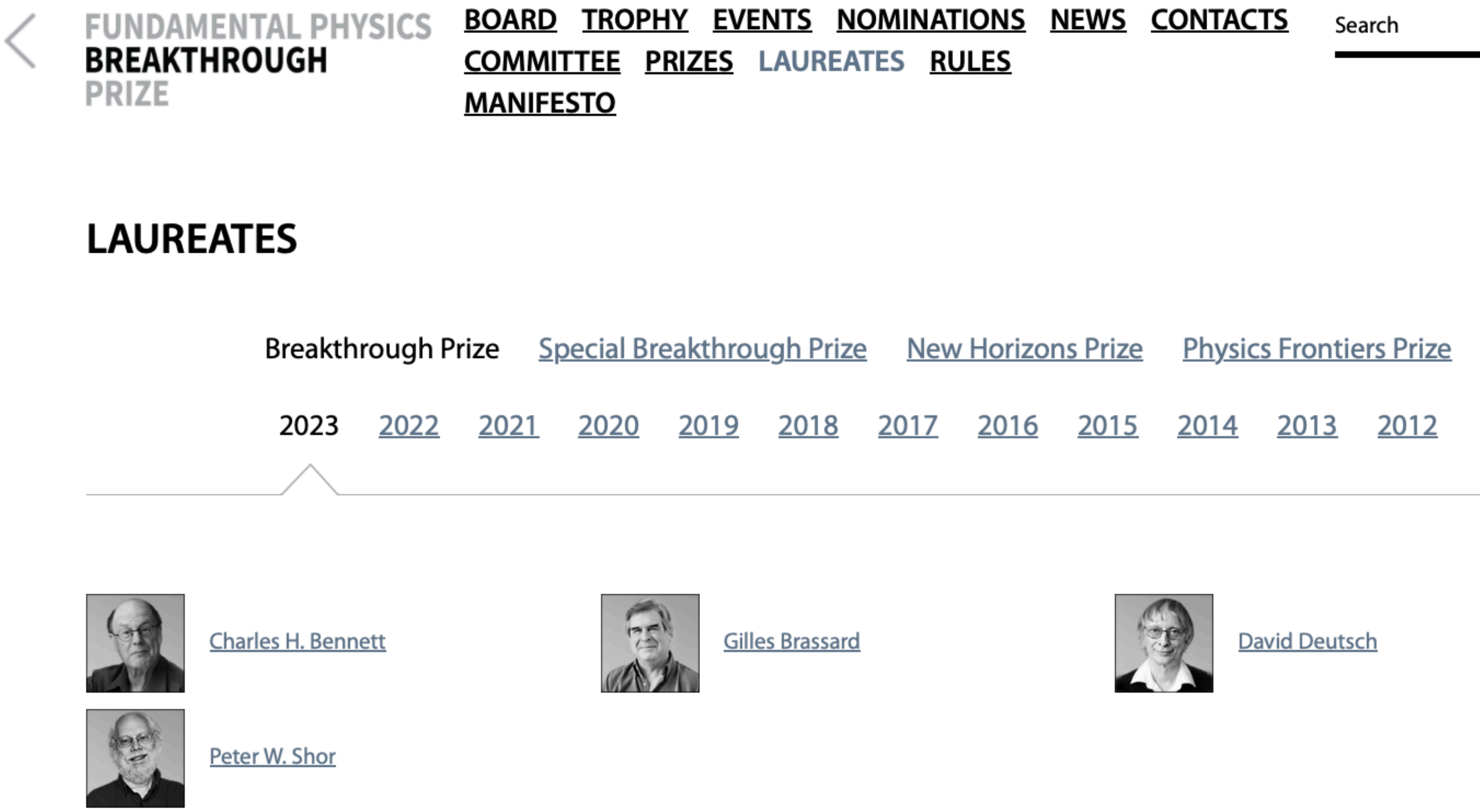
$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle\Big) = \sum_{x=0,1} \frac{1}{\sqrt{2}}|x\rangle \otimes |f(x)\rangle$$

A simple QA with two qubits

- $|\psi\rangle$ contains information on both f(0) and f(1)
  - Superposition of f(0) and f(1)
  - Need to perform measurement to access the info
  - However, measurement returns only one value of x and f(x)



$$|\psi\rangle = \frac{1}{\sqrt{2}} U_f \Big(|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle \Big) = \sum_{x=0,1} \frac{1}{\sqrt{2}} |x\rangle \otimes |f(x)\rangle$$



FUNDAMENTAL PHYSICS
BREAKTHROUGH
PRIZE

BOARD TROPHY EVENTS NOMINATIONS NEWS CONTACTS
COMMITTEE PRIZES LAUREATES RULES
MANIFESTO

Search

LAUREATES

Breakthrough Prize | Special Breakthrough Prize | New Horizons Prize | Physics Frontiers Prize

2023 | 2022 | 2021 | 2020 | 2019 | 2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012

Charles H. Bennett

Gilles Brassard

David Deutsch

Peter W. Shor

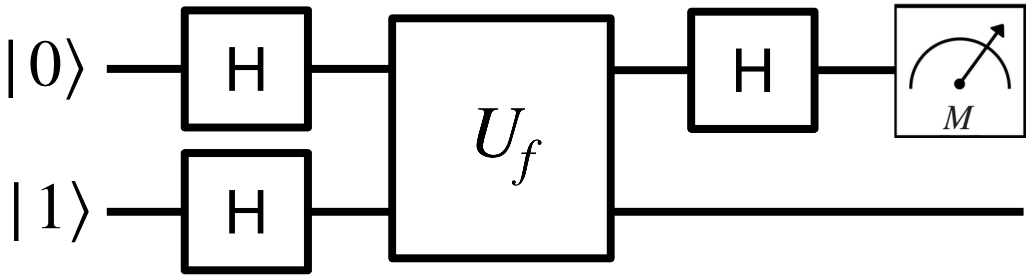
Deutsch Algorithm

1985

- We want to find out whether a particular function, with one input bit and one output bit is constant or balanced. Classically, we need to evaluate the function twice (i.e., for input = 0 and input = 1), but remarkably, we only need to evaluate the function once using quantum algorithm, by using Deutsch's algorithm.

Deutsch Algorithm

- Deutsch algorithm exploits QA to obtain information about global property of f(x).
- A function of a single qubit can be either constant $f(0) = f(1)$ or balanced $f(0) \neq f(1)$



(1) (2) (3)

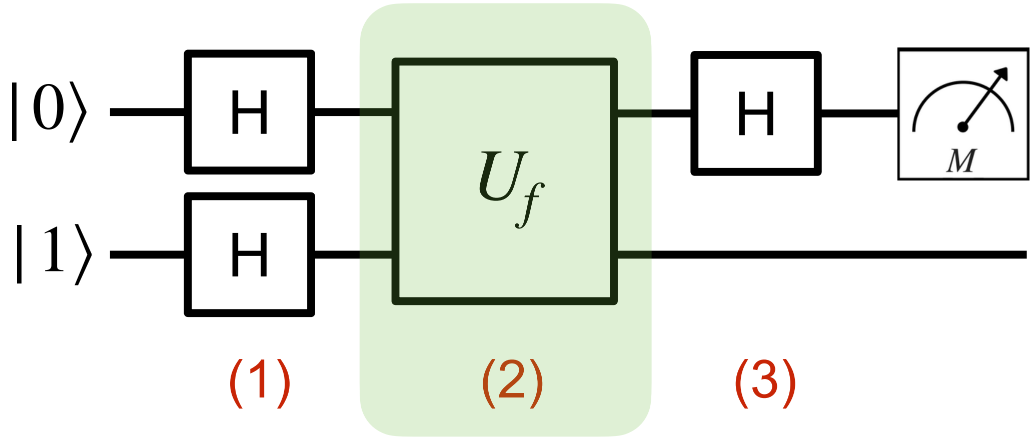
$$|\psi_0\rangle \xrightarrow{H\otimes H} |\psi_1\rangle \xrightarrow{U_f} |\psi_2\rangle \xrightarrow{H\otimes I} |\psi_3\rangle$$

$$|\psi_0\rangle \equiv |0\rangle \otimes |1\rangle = |01\rangle$$

(1) $$|\psi_1\rangle = H \otimes H|01\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)$$

$$= \frac{1}{2}\Big(|00\rangle - |01\rangle + |10\rangle - |11\rangle\Big) = \frac{1}{2}\Big(\sum_x |x\rangle\Big) \otimes \Big(|0\rangle - |1\rangle\Big)$$

Deutsch Algorithm



$$|\psi_0\rangle \equiv |0\rangle \otimes |1\rangle = |01\rangle$$

$$|\psi_1\rangle = \frac{1}{2}\Big(\sum_x |x\rangle\Big) \otimes \Big(|0\rangle - |1\rangle\Big)$$

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

(2) $|\psi_2\rangle = U_f|\psi_1\rangle$

For $f(x) = 0$: $U_f\Big[|x\rangle \otimes (|0\rangle - |1\rangle)\Big] = U_f\Big(|x\rangle \otimes |0\rangle\Big) - U_f\Big(|x\rangle \otimes |1\rangle\Big)$

$$= |x\rangle \otimes |0 + f(x)\rangle - |x\rangle \otimes |1 + f(x)\rangle$$

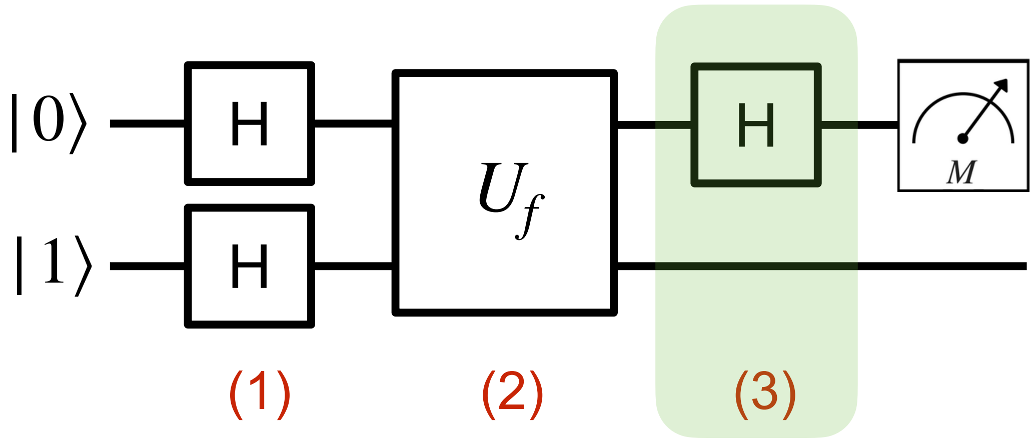
$$= |x\rangle \otimes \Big(|0\rangle - |1\rangle\Big) = (-1)^{f(x)}|x\rangle \otimes \Big(|0\rangle - |1\rangle\Big)$$

For $f(x) = 1$: $U_f\Big[|x\rangle \otimes (|0\rangle - |1\rangle)\Big] = |x\rangle \otimes \Big(|1\rangle - |0\rangle\Big) = (-1)^{f(x)}|x\rangle \otimes \Big(|0\rangle - |1\rangle\Big)$

$$|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\sum_x (-1)^{f(x)}|x\rangle\Big] \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)$$

Phase Kick-Back: Deutsch algorithm encodes the value of f(x) in the first qubit rather than in the second qubit.

Deutsch Algorithm



$$|\psi_0\rangle \equiv |0\rangle \otimes |1\rangle = |01\rangle$$

$$|\psi_1\rangle = \frac{1}{2}\Big(\sum_x |x\rangle\Big) \otimes \Big(|0\rangle - |1\rangle\Big)$$

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

(3) $$|\psi_3\rangle = \big(H \otimes I\big)|\psi_2\rangle = \big(H \otimes I\big)\frac{1}{\sqrt{2}}\Big[\sum_x (-1)^{f(x)}|x\rangle\Big] \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)$$

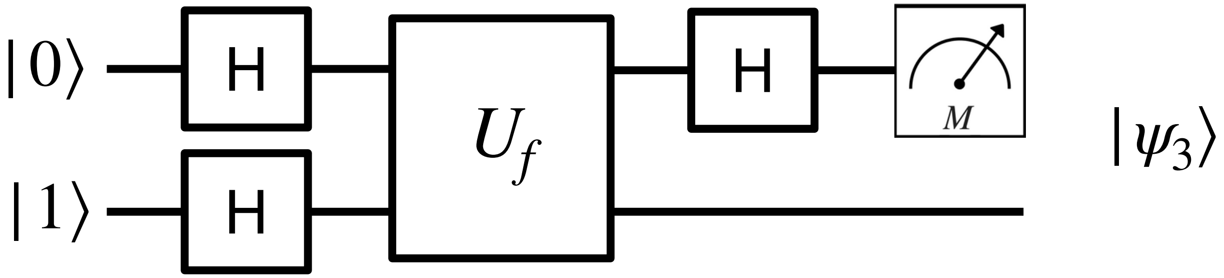
$$H\frac{1}{\sqrt{2}}\Big[\sum_x (-1)^{f(x)}|x\rangle\Big] = \frac{1}{\sqrt{2}}H\Big[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big]$$

$$= \frac{1}{\sqrt{2}}\Big[(-1)^{f(0)}\frac{|0\rangle + |1\rangle}{\sqrt{2}} + (-1)^{f(1)}\frac{|0\rangle - |1\rangle}{\sqrt{2}}\Big]$$

$$= \frac{1}{2}\Big[\Big((-1)^{f(0)} + (-1)^{f(1)}\Big)|0\rangle + \Big((-1)^{f(0)} - (-1)^{f(1)}\Big)|1\rangle\Big]$$

Deutsch Algorithm

- Deutsch algorithm exploits QA to obtain information about global property of f(x).
- A function of a single qubit can be either constant $f(0) = f(1)$ or balanced $f(0) \neq f(1)$



$$|\psi_0\rangle \xrightarrow{H\otimes H} |\psi_1\rangle \xrightarrow{U_f} |\psi_2\rangle \xrightarrow{H\otimes I} |\psi_3\rangle$$

$$|\psi_3\rangle = \frac{1}{2}\left[\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right]$$

- If measurement gives $|0\rangle$, $f(0) = f(1) \longrightarrow f(x) = \text{constant.}$
- If measurement gives $|1\rangle$, $f(0) \neq f(1) \longrightarrow f(x) = \text{balanced.}$
- Can be generalized to function with multiple input values, Deutsch-Josza algorithm

Quantum computing jargon

- Query complexity:
  - In Deutsch’s algorithm we are not using a quantum computer to evaluate a “classically difficult” function per se, but rather using quantum phenomena to reduce the number of queries we need to make to an unknown function, to ascertain some information thereabout.
- Oracles and black boxes:
  - In Deutsch’s algorithm, and other query complexity algorithms, we query U, which is known as a “black box”, or often in quantum computing an “oracle”. The oracle in Deutsch’s algorithm is sufficiently simple that we can explicitly express each possible option, but frequently in quantum computing problems are framed in terms of oracles, even when this is not the case.

Basic operations with bit strings

- x and y are two n-bit strings:

$$|x\rangle = |x_{n-1}\,x_{n-2}\,\cdots\,x_1\,x_0\rangle$$

$$x_i\,,y_i \in \{0,1\}$$

$$|y\rangle = |y_{n-1}\,y_{n-2}\,\cdots\,y_1\,y_0\rangle$$

- Hamming distance = $d_H(x,y)$ = the number of bits in which the two strings differ.

$$|x\rangle = |\,10101\,\rangle$$

$$d_H(x,y) = \,?$$

$$|y\rangle = |\,11100\,\rangle$$

- Hamming weight = $d_H(x)$ = $d_H(x{,}0)$ = the number of 1-bit in x = the Hamming distance between x and 0.
- $x \cdot y$ = the number of common 1-bit in x and y
- $x \oplus y$ = the bitwise exclusive OR = bitwise addition under mod 2
- $x \wedge y$ = the bitwise AND
- $\sim x$ = $x \oplus 111\cdots1$ = the bit string that flips 0 and 1

Useful Identities

- $x \cdot y = d_H(x \wedge y)$
- $x \cdot y = \frac{1}{2}\left(1 - (-1)^{x \cdot y}\right) \bmod 2$
- $x \cdot y + x \cdot z = x \cdot (y \oplus z) \bmod 2$
- $d_H(x \oplus y) = d_H(x) + d_H(y) \bmod 2$
- $\sum_{x=0}^{2^n-1} (-1)^{x \cdot x} = 0$ b/c successive $2i$ and $2i+1$ terms cancel
- $\sum_{x=0}^{2^n-1} (-1)^{x \cdot y} = \begin{cases} 2^n, & \text{if y} = 0 \\ 0\ , & \text{otherwise} \end{cases}$

- $$\sum_{x=0}^{2^n-1} (-1)^{x\cdot x} = 0$$
- $$\sum_{x=0}^{2^n-1} (-1)^{x\cdot y} = \begin{cases} 2^n\,, & \text{if y = 0} \\ 0\;\,, & \text{otherwise} \end{cases}$$

For $n = 2:$ $x \in \{0, 1, 2, 3\}$, or $\{00, 01, 10, 11\}$

$x \cdot x \in \{0, 1, 1, 2\}$

$$\sum_{x=0}^{2^n-1} (-1)^{x\cdot x} = (-1)^0 + (-1)^1 + (-1)^1 + (-1)^2 = 0$$

$$\sum_{x=0}^{2^n-1} (-1)^{x\cdot y} = \sum_{x=0}^{2^n-1} (-1)^{x_{n-1}y_{n-1}+x_{n-2}y_{n-2}+\cdots+x_0y_0}$$

$$= \left(\sum_{x_0=0}^{1} (-1)^{x_0y_0}\right)\left(\sum_{x_1=0}^{1} (-1)^{x_1y_1}\right) \times \cdots\cdots \times \left(\sum_{x_{n-1}=0}^{1} (-1)^{x_{n-1}y_{n-1}}\right)$$

$$= \left(1 + (-1)^{y_0}\right)\left(1 + (-1)^{y_1}\right)\cdots\cdots\left(1 + (-1)^{y_{n-1}}\right)$$

$$= 0 \qquad \text{unless } y_0 = y_1 = \cdots = y_{n-1} = 0$$

Walsh-Hadamard Transformation

$$W \equiv H \otimes H \otimes \cdots \otimes H \equiv H^{\otimes n}$$

apply H to each qubit in an n-qubit system

$$W|0\rangle = H \otimes H \otimes \cdots \otimes H\Big(|0\rangle \otimes \cdots \otimes |0\rangle \Big) \qquad N = 2^n$$

$$= \Big(H|0\rangle\Big) \otimes \cdots \otimes \Big(H|0\rangle\Big)$$

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

$$= \frac{1}{\sqrt{2^n}}\Big(|00\cdots00\rangle + |00\cdots01\rangle + |00\cdots10\rangle\cdots + |11\cdots11\rangle\Big)$$

$$W|0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

Linear combination of all possible states

Computational basis

$$|0\rangle = |00\cdots00\rangle$$

$$|1\rangle = |00\cdots01\rangle$$

$$|2\rangle = |00\cdots11\rangle$$

$$\vdots$$

$$|N-1\rangle = |11\cdots11\rangle$$

Shorthand Notation

Walsh-Hadamard Transformation

$W \equiv H \otimes H \otimes \cdots \otimes H \equiv H^{\otimes n}$ apply H to each qubit in an n-qubit system

$$W|0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \qquad N = 2^n$$

$$|r\rangle = |r_{n-1}\, r_{n-2} \cdots r_1\, r_0\rangle$$

$$|s\rangle = |s_{n-1}\, s_{n-2} \cdots s_1\, s_0\rangle \qquad r_i\,, s_i \in \{0,1\}$$

- How does W act on $|r\rangle$? $\quad W|r\rangle = \sum_s W_{rs}|s\rangle$

$$W|r\rangle = \left(H \otimes H \otimes \cdots \otimes H\right)|r_{n-1}\, r_{n-2} \cdots r_1\, r_0\rangle$$

$$= \frac{1}{\sqrt{2^n}} \Big[\underbrace{|0\rangle + (-1)^{r_{n-1}}|1\rangle}_{= \sum_{s_{n-1}=0}^{1} (-1)^{s_{n-1}\cdot r_{n-1}}|s_{n-1}\rangle}\Big] \otimes \cdots \otimes \Big[\underbrace{|0\rangle + (-1)^{r_0}|1\rangle}_{= \sum_{s_0=0}^{1} (-1)^{s_0\cdot r_0}|s_0\rangle}\Big]$$

$$= \frac{1}{2^n} \sum_{s=0}^{N-1} (-1)^{s_{n-1}\cdot r_{n-1}}|s_{n-1}\rangle \otimes \cdots \otimes (-1)^{s_1\cdot r_1}|s_1\rangle \otimes (-1)^{s_0\cdot r_0}|s_0\rangle$$

$$W(|r\rangle) = \frac{1}{2^n} \sum_{s=0}^{2^n-1} (-1)^{s\cdot r}|s\rangle \qquad W_{rs} = W_{sr} = \frac{1}{\sqrt{2}^n}(-1)^{r\cdot s}$$

Deutsch-Jozsa Algorithm

1992

- Given a function $f : Z_{2^n} \longrightarrow Z_2$ that is known to be either constant (0 on all inputs or 1 on all inputs) or balanced (1 for exactly half of the input domain and 0 for the other half), and $U_f : |x\rangle \otimes |y\rangle \longrightarrow |x\rangle \otimes |x \oplus f(x)\rangle$, determine whether the function f is constant or balanced.

- Phase change for a subset of basis vectors

$$\text{Consider a superposition} : |\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$$

$$\text{Boolean function} : f : \; Z_{2^n} \longrightarrow Z_2 \;\; \text{where} \quad f(x) = \begin{cases} 1\,, & \text{if } x \in X \subset Z_{2^n} \\ 0\,, & \text{otherwise} \end{cases}$$

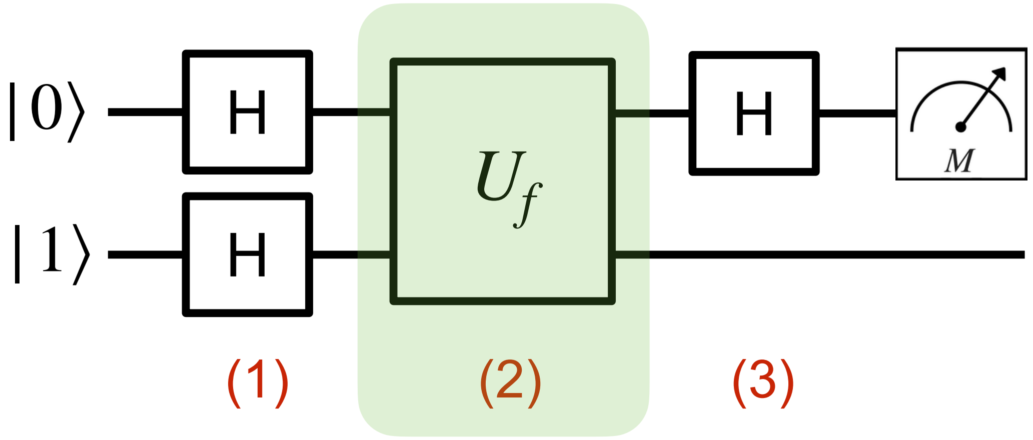
$$U_f\Big[|\psi\rangle \otimes |-\rangle\Big] = U_f\Big[\frac{1}{\sqrt{2^n}} \sum_x |x\rangle \otimes \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)\Big] \qquad \text{where } X = \{x \,|\, f(x) = 1\}$$

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

$$\text{For} : |\psi\rangle = \sum_x a_x |x\rangle$$

$$S_X^{\phi} : \sum_{x=0}^{N-1} a_x |x\rangle \longrightarrow \sum_{x \in X} a_x e^{i\phi} |x\rangle + \sum_{x \notin X} a_x |x\rangle$$

Deutsch Algorithm



$$|\psi_0\rangle \equiv |0\rangle \otimes |1\rangle = |01\rangle$$

$$|\psi_1\rangle = \frac{1}{2}\Big(\sum_x |x\rangle\Big) \otimes \Big(|0\rangle - |1\rangle\Big)$$

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

(2) $|\psi_2\rangle = U_f|\psi_1\rangle$

For $f(x) = 0$: $U_f\Big[|x\rangle \otimes (|0\rangle - |1\rangle)\Big] = U_f\Big(|x\rangle \otimes |0\rangle\Big) - U_f\Big(|x\rangle \otimes |1\rangle\Big)$

$$= |x\rangle \otimes |0 + f(x)\rangle - |x\rangle \otimes |1 + f(x)\rangle$$

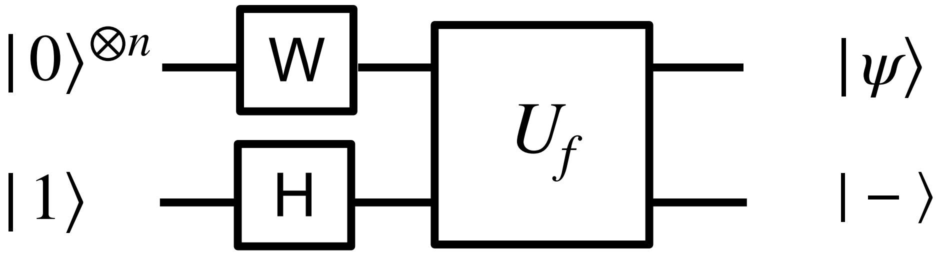
$$= |x\rangle \otimes \Big(|0\rangle - |1\rangle\Big) = (-1)^{f(x)}|x\rangle \otimes \Big(|0\rangle - |1\rangle\Big)$$

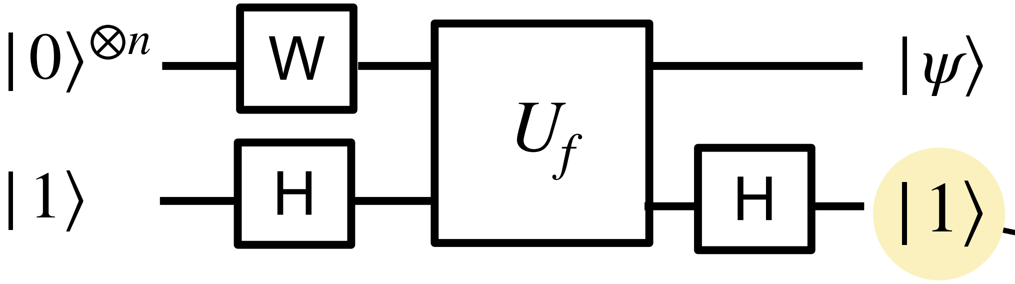
For $f(x) = 1$: $U_f\Big[|x\rangle \otimes (|0\rangle - |1\rangle)\Big] = |x\rangle \otimes \Big(|1\rangle - |0\rangle\Big) = (-1)^{f(x)}|x\rangle \otimes \Big(|0\rangle - |1\rangle\Big)$

$$|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\sum_x (-1)^{f(x)}|x\rangle\Big] \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)$$

Phase Kick-Back: Deutsch algorithm encodes the value of f(x) in the first qubit rather than in the second qubit.

Deutsch-Jozsa Algorithm





Can reuse the ancilla qubit

n = number of qubits

$N = 2^n$ = dim of Hilbert space

$$|\psi_0\rangle = W|0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

$$|\psi\rangle = \sum_x (-1)^{f(x)}|\psi_0\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^{N-1}(-1)^{f(i)}|\,i\,\rangle$$

$$W\big(|r\rangle\big) = \frac{1}{2^n}\sum_{s=0}^{2^n-1}(-1)^{s\cdot r}|s\rangle$$

$$|\phi\rangle = W|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^{N-1}(-1)^{f(i)}W|\,i\,\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^{N-1}(-1)^{f(i)}\sum_{j=0}^{N-1}\frac{1}{\sqrt{N}}(-1)^{i\cdot j}|\,j\,\rangle$$

For constant f, $(-1)^{f(i)} = (-1)^{f(0)}$ is a global phase.

- $$\sum_{x=0}^{2^n-1}(-1)^{x\cdot y} = \begin{cases} 2^n, & \text{if y} = 0 \\ 0\;, & \text{otherwise} \end{cases}$$

$$|\phi\rangle = (-1)^{f(0)}\frac{1}{N}\sum_j\underbrace{\Big(\sum_i(-1)^{i\cdot j}\Big)}_{\text{only nonzero when } j\,=\,0}|j\rangle = (-1)^{f(0)}|0\rangle$$

Deutsch-Jozsa Algorithm

$$|\phi\rangle = W|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^{N-1}(-1)^{f(i)}W|i\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^{N-1}(-1)^{f(i)}\sum_{j=0}^{N-1}\frac{1}{\sqrt{N}}(-1)^{i\cdot j}|j\rangle$$

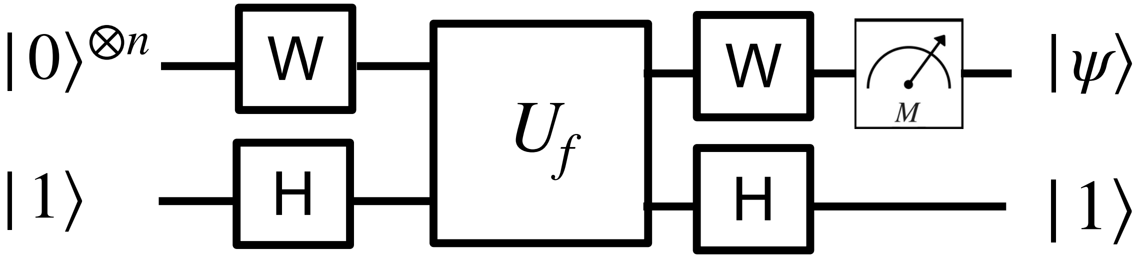
For balanced f, $|\phi\rangle = \frac{1}{2^n}\sum_{j}\left(\sum_{i\in X}(-1)^{i\cdot j} - \sum_{i\notin X}(-1)^{i\cdot j}\right)|j\rangle$ where $X = \{x\,|\,f(x) = 1\}$

For $j = 0$, amplitude is zero.

$\sum_{i\in X}(-1)^{i\cdot j} - \sum_{i\notin X}(-1)^{i\cdot j} = 0 \text{ for } j = 0$ $\Longleftrightarrow$ $|\phi\rangle$ does not contain $|0\rangle$.

- Measurement of state $|\phi\rangle$ (in the standard basis) will return $|0\rangle$ with probability 1, if f is constant, and will return a non-zero $|j\rangle$ with probability 1, if f is balanced.
- Classical algorithm must evaluate f at least $2^{n-1}+1$ times to solve the problem with certainty, while quantum algorithm solves with a single evaluation of U_f.
- There is an exponential separation between the query complexity of the QA and query complexity of any classical algorithm.
- There are classical algorithms that solve the problem in fewer evaluations but only with high probability of success (not 100% probability).

Deutsch-Jozsa Algorithm



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

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

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \sum_{x,y\in\{0,1\}} (-1)^{xy}\,|y\rangle\langle x|$$

$$H^2 = I$$

$$W \equiv H^{\otimes n} = \left(\frac{1}{\sqrt{2}} \sum_{x,y\in\{0,1\}} (-1)^{xy}\,|y\rangle\langle x| \right)^{\otimes n}$$

$$= \left(\frac{1}{\sqrt{2}} \sum_{x_0,y_0} (-1)^{x_0 y_0}\,|y_0\rangle\langle x_0| \right) \otimes \cdots \otimes \left(\frac{1}{\sqrt{2}} \sum_{x_0,y_0} (-1)^{x_{n-1},y_{n-1}}\,|y_{n-1}\rangle\langle x_{n-1}| \right)$$

$$= \frac{1}{\sqrt{2}^n} \sum_{x,y\in\{0,1\}^{\otimes n}} (-1)^{x\cdot y}\,|y\rangle\langle x|$$

$$x \cdot y = x_o y_0 + x_1 y_1 + \cdots + x_{n-1} y_{n-1}$$

$$H^{\otimes n} \frac{1}{\sqrt{2}^n} \sum_x |x\rangle = 0$$

$$H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2}^n} \sum_x |x\rangle$$

Bernstein-Vazirani Algorithm

1997

- A n-bit function $f: \ \{0,1\}^{\otimes n} \ \longrightarrow \ \{0,1\}$, which outputs a singlet bit, is guaranteed to be of the form $f_s(x) = x \cdot s$, where s is an unknown n-bit string and $x \cdot s = x_0 s_0 + \cdots + x_{n-1}s_{n-1} = \sum_{i=0}^{n-1} x_i s_i \pmod 2$. Find the unknown string $s = (s_0 s_1 \cdots s_{n-1})$.
- Best classical algorithm uses $\mathcal{O}(n)$ calls to $f_s(x) = x \cdot s \mod 2$. Each query gives one bit of information of s (because f outputs one bit).

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

$$U_f = \sum_x \sum_y |x\rangle\langle x| \otimes |y \oplus f(x)\rangle\langle y|$$

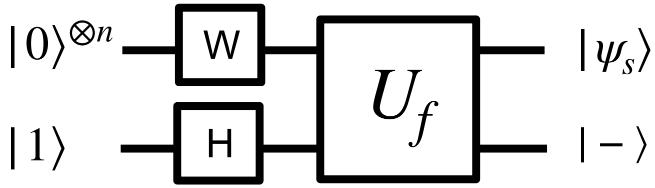
$$f_s(x) = x \cdot s \mod 2$$

$$U_f = \sum_{x\in\{0,1\}^{\otimes n}} \sum_{y\in\{0,1\}^{\otimes n}} |x\rangle\langle x| \otimes |y \oplus s \cdot x\rangle\langle y|$$

- How do we find s with less than n queries? → Use superposition (over all possible input bit strings)

$$U_f\Big(\,|\psi\rangle \otimes |-\rangle\Big) = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \otimes |-\rangle$$

$$|\psi_s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^{\otimes n}} (-1)^{f(x)} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^{\otimes n}} (-1)^{x\cdot s} |x\rangle$$



Bernstein-Vazirani Algorithm

- $|\psi_s\rangle$ states are orthogonal! $\langle\psi_s|\psi_t\rangle = \delta_{st}$

$$\langle\psi_s|\psi_t\rangle = \frac{1}{2^n}\sum_{x\in\{0,1\}^{\otimes n}}(-1)^{x\cdot s}\langle x|\sum_{y\in\{0,1\}^{\otimes n}}(-1)^{y\cdot t}|y\rangle = \frac{1}{2^n}\sum_{x,y}(-1)^{x\cdot s+y\cdot t}\langle x|y\rangle$$

$$= \frac{1}{2^n}\sum_{x\in\{0,1\}^{\otimes n}}(-1)^{x\cdot s+x\cdot t} = \frac{1}{2^n}\sum_{x\in\{0,1\}^{\otimes n}}(-1)^{x\cdot(s\oplus t)}$$

$$x\cdot s = x_0s_0+\cdots+x_{n-1}s_{n-1}$$

$$x\cdot s + x\cdot t = x\cdot(s\oplus t)\ (\mathrm{mod}\ 2)$$

$$\sum_{x\in\{0,1\}^{\otimes n}}(-1)^{x\cdot k} = \sum_{x\in\{0,1\}^{\otimes n}}(-1)^{x_0k_0+\cdots+x_{n-1}k_{n-1}} = \sum_{x_0\in\{0,1\}}(-1)^{x_0k_0}\sum_{x_1\in\{0,1\}}(-1)^{x_1k_1}\cdots\sum_{x_{n-1}\in\{0,1\}}(-1)^{x_{n-1}k_{n-1}}$$

$$= 2\delta_{k_00}\times 2\delta_{k_10}\cdots\times 2\delta_{k_{n-1}0} = 2^n\delta_{k0}$$

$$\sum_{x=0}^{2^n-1}(-1)^{x\cdot y} = \begin{cases} 2^n\,, & \text{if } y=0 \\ 0\,, & \text{otherwise}\end{cases}$$

$$\langle\psi_s|\psi_t\rangle = \delta_{s\oplus t,0} = \delta_{s\,t}$$

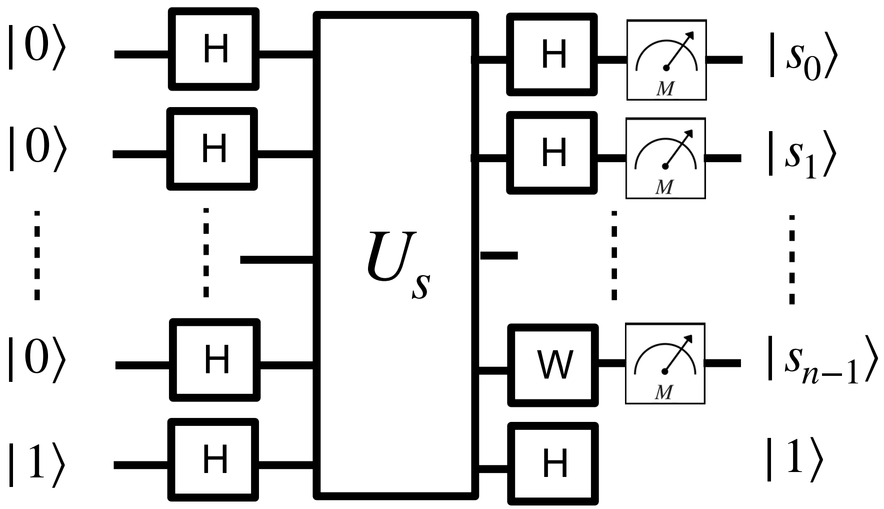
- Orthogonal set of vectors from a basis and we can “measure in this basis”.
- Equivalent to performing unitary transformation and measuring in the computational basis, from which we should be able to extract the string s.

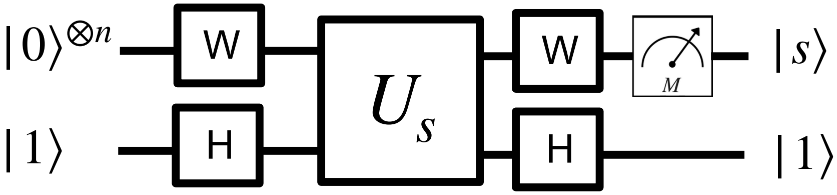
$$W \equiv H^{\otimes n} = \frac{1}{\sqrt{2}^n}\sum_{x,y\in\{0,1\}^{\otimes n}}(-1)^{x\cdot y}|y\rangle\langle x| = \sum_{y\in\{0,1\}^{\otimes n}}|y\rangle\langle\psi_y|$$

$$\langle\psi_s| = \frac{1}{2^n}\sum_{x\in\{0,1\}^{\otimes n}}(-1)^{x\cdot s}\langle x|$$

Bernstein-Vazirani Algorithm

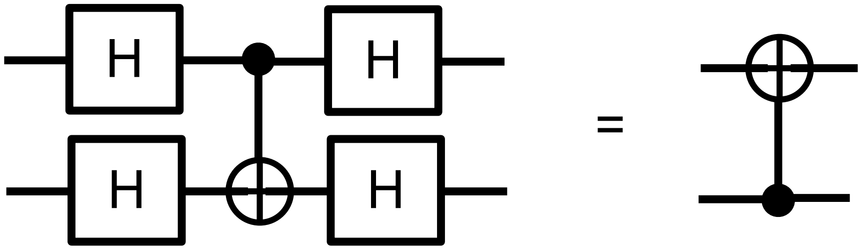
- Apply $H^{\otimes n}$ to $|\psi_s\rangle$: $\quad H^{\otimes n}|\psi_s\rangle = \sum_y |y\rangle\langle\psi_y|\psi_s\rangle = |s\rangle$ in 100% probability





Circuit for Berstein-Vazirani algorithm

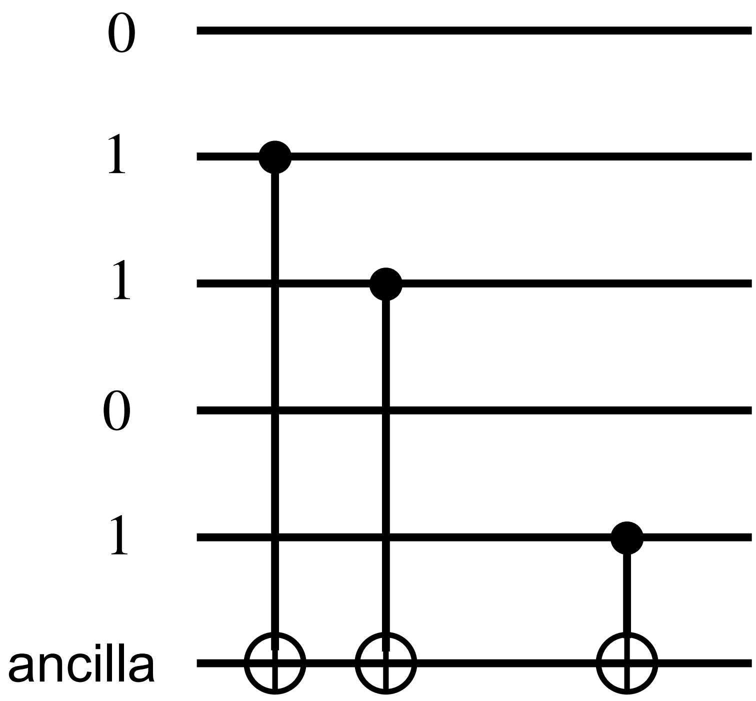
- Simpler explanation: Berstein-Vazirani algorithm behaves as if it were a circuit consisting only of CNOT operations from ancilla to the qubits corresponding to 1-bit of s.

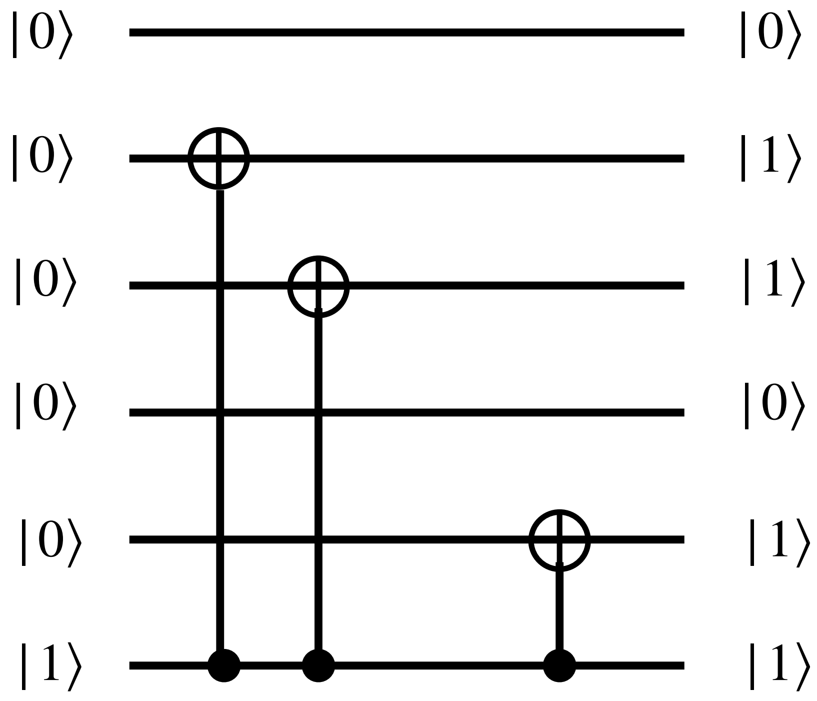


Bernstein-Vazirani Algorithm

- Berstein-Vazirani algorithm behaves as if it were a circuit consisting only of CNOT operations from ancilla to the qubits corresponding to 1-bit of s.

$s = 01101$





- For s=01101, the black box for U_s behaves as if it contained this circuit, consisting of CNOT gates for each 1-bit of s.

- BV algorithm behaves as if it were implemented by this simple circuit, consisting of a CNOT for each 1-bit of s.

1	3	5	7	9	11	13	15
17	19	21	23	25	27	29	31
33	35	37	39	41	43	45	47
49	51	53	55	57	59	61	63

2	3	6	7	10	11	14	15
18	19	22	23	26	27	30	31
34	35	38	39	42	43	46	47
50	51	54	55	58	59	62	63

4	5	6	7	12	13	14	15
20	21	22	23	28	29	30	31
36	37	38	39	44	45	46	47
52	53	54	55	60	61	62	63

8	9	10	11	12	13	14	15
24	25	26	27	28	29	30	31
40	41	42	43	44	45	46	47
56	57	58	59	60	61	62	63

16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

Simon’s Algorithm

- Given a 2-to-1 function f such that $f(x) = f(x \oplus a)$ for all $x \in \mathbb{Z}_2^n$, find the hidden string $a \in \mathbb{Z}_2^n$. (Simon’s algorithm shows structural similarities to Shor’s algorithm)

$$|x\rangle = |x_0 x_1 \cdots x_{n-1}\rangle$$

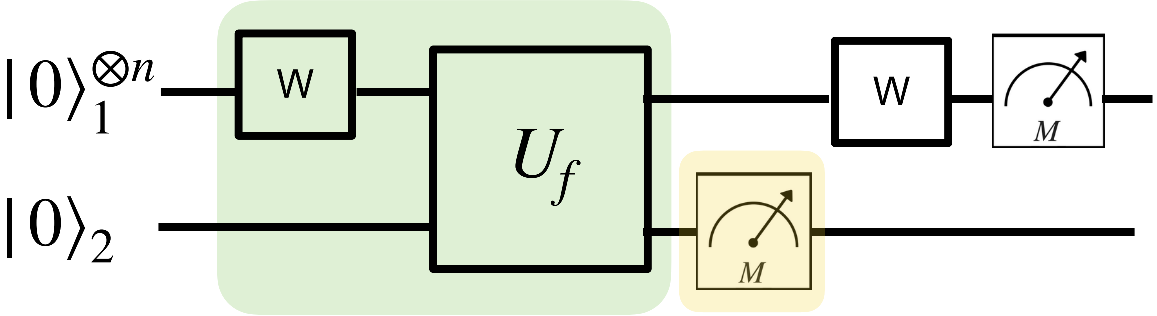
$$U_f : |x\rangle \otimes |y\rangle \longrightarrow |x\rangle \otimes |y \oplus f(x)\rangle$$

$$x_i \in \{0,1\}$$

$$U_f \left[W|0\rangle^{\otimes n} \otimes |0\rangle \right] = U_f \frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes |0\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes |f(x)\rangle$$

$$N = 2^n$$

- Suppose we perform a measurement on 2nd qubit and $f(x_0)$ is the measured value. Then the 1st qubit becomes $\frac{1}{\sqrt{2}}\Big(|x_0\rangle + |f(x_0)\rangle \Big) = \frac{1}{\sqrt{2}}\Big(|x_0\rangle + |x \oplus a\rangle \Big)$.



Simon’s Algorithm

- Apply Walsh-Hadamard:

$$W\left[\frac{1}{\sqrt{2}}\left(|x_0\rangle + |x_0 \oplus a\rangle\right)\right] = \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}^n}\sum_y \left\{(-1)^{x_0\cdot y} + (-1)^{(x_0\oplus a)\cdot y}\right\}|y\rangle\right]$$

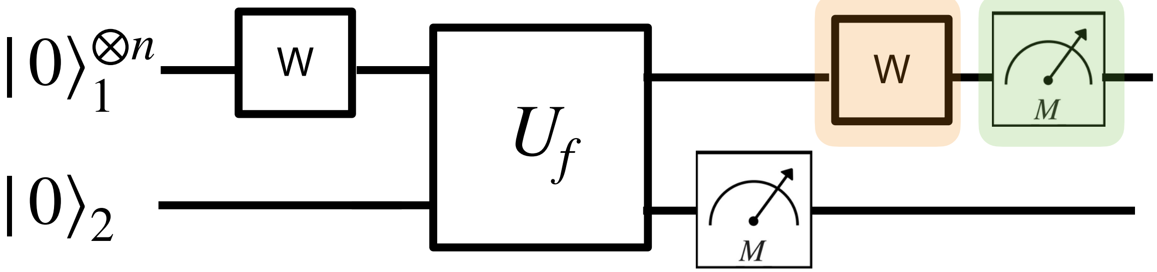
$$= \frac{1}{\sqrt{2}^{n+1}}\sum_y (-1)^{x_0\cdot y}\left(1 + (-1)^{a\cdot y}\right)|y\rangle$$

$$= \frac{1}{\sqrt{2}^{n+1}}\sum_{y\cdot a=even}(-1)^{x_0\cdot y}|y\rangle$$

$$W(|r\rangle) = \frac{1}{2^n}\sum_{s=0}^{2^n-1}(-1)^{s\cdot r}|r\rangle$$

$$W_{rs} = W_{sr} = \frac{1}{\sqrt{2}^n}(-1)^{r\cdot s}$$

- Measurement on the 1st qubit results in a random y such that $y \cdot a = 0 \mod 2$.
- Unknown a_i must satisfy $y_0a_0 + y_1a_1 + \cdots y_{n-1}a_{n-1} = 0 \mod 2$.



Simon’s Algorithm

- Repeat the same procedure until n linearly independent equations have been found. Each time computation is repeated, at least 50% of the time, the resulting equation can be independent.
- Repeating 2n times, there is a 50% chance that n-linearly independent equations can be found.
- The equation can be solved to find the string a in $\mathcal{O}(n^2)$ steps.
- With high likelihood, the hidden string a will be found with $\mathcal{O}(n)$ calls to U_f , followed by $\mathcal{O}(n^2)$ steps to solve the resulting set of equations.
- Classical algorithm needs $\mathcal{O}(2^{n/2})$ calls to f .

Simon's Algorithm: probability of finding n-linearly independent equations

- Consider we have a string, $x = (x_1 x_2 x_3 \cdots x_n)$.
- 1st measurement: $P_1 = 1$
- After 1st measurement, what is the probability that next measurement will be linearly independent? $P_2 = 1 - 1/2^n$
- Probability that next measurement will be linearly independent: $P_3 = 1 - 2/2^n$
- Probability that next string x_{m+1} is linearly independent: $P_m = 1 - 2^m/2^n$
- Probability of $n - 1$ being linearly independent:

$$P = \left(1 - \frac{1}{2^n}\right)\left(1 - \frac{2}{2^n}\right)\cdots\left(1 - \frac{2^{n-2}}{2^n}\right) \geq 1 - \sum_{k=2}^{n} \frac{1}{2^k} = 1 - \frac{\frac{1}{4}\left(1 - \frac{1}{2^{n-1}}\right)}{1 - \frac{1}{2}} \geq \frac{1}{2} + \frac{1}{2^n}$$

$$(1-a)(1-b) = 1 - a - b + ab \geq 1 - a - b \quad \text{for } 0 < a, b < 1$$

Discrete Fourier Transformation

- Simon's algorithm ⟶ Shor's algorithm (factoring numbers) makes use of QFT.
- Discrete Fourier Transformation (DFT): signal processing, quantum theory (position ↔ momentum).
- Assume a vector f of N complex numbers: $f_k\,,\ k = 0,1,\cdots,N-1$
- DFT is a mapping from N complex # to N complex #.

$$\text{DFT}:\ f_k \longrightarrow \tilde{f}_j = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} w^{-jk} f_k \qquad\qquad w = \exp\left(\frac{2\pi i}{N}\right)$$

$$\text{Inverse DFT}:\ \tilde{f}_k \longrightarrow f_j = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} w^{jk} \tilde{f}_k$$

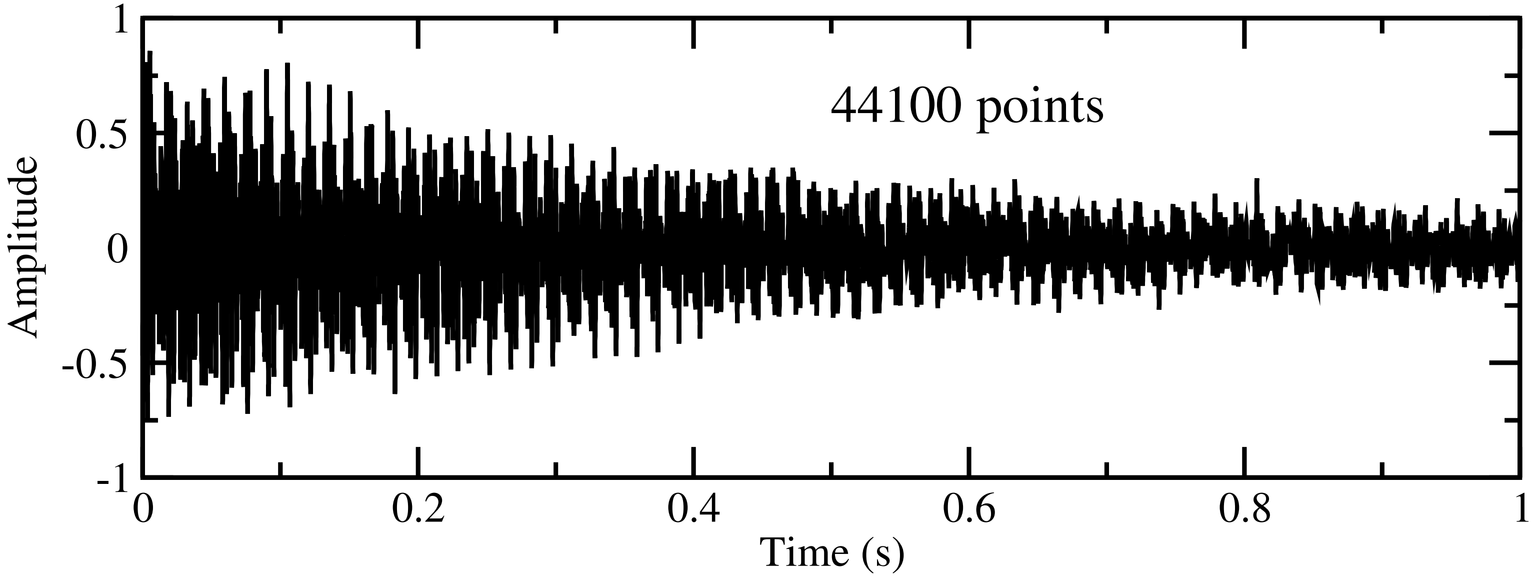
$$f_j = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} w^{jk}\tilde{f}_k = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} w^{jk}\left(\frac{1}{\sqrt{N}}\sum_{\ell=0}^{N-1} w^{-\ell k} f_\ell\right) = \frac{1}{N}\sum_{\ell}\overbrace{\sum_{k=0}^{N-1} w^{(j-\ell)k}}^{\text{nonzero only when } j=\ell} f_\ell = \sum_{\ell} f_\ell\,\delta_{j\ell} = f_j$$

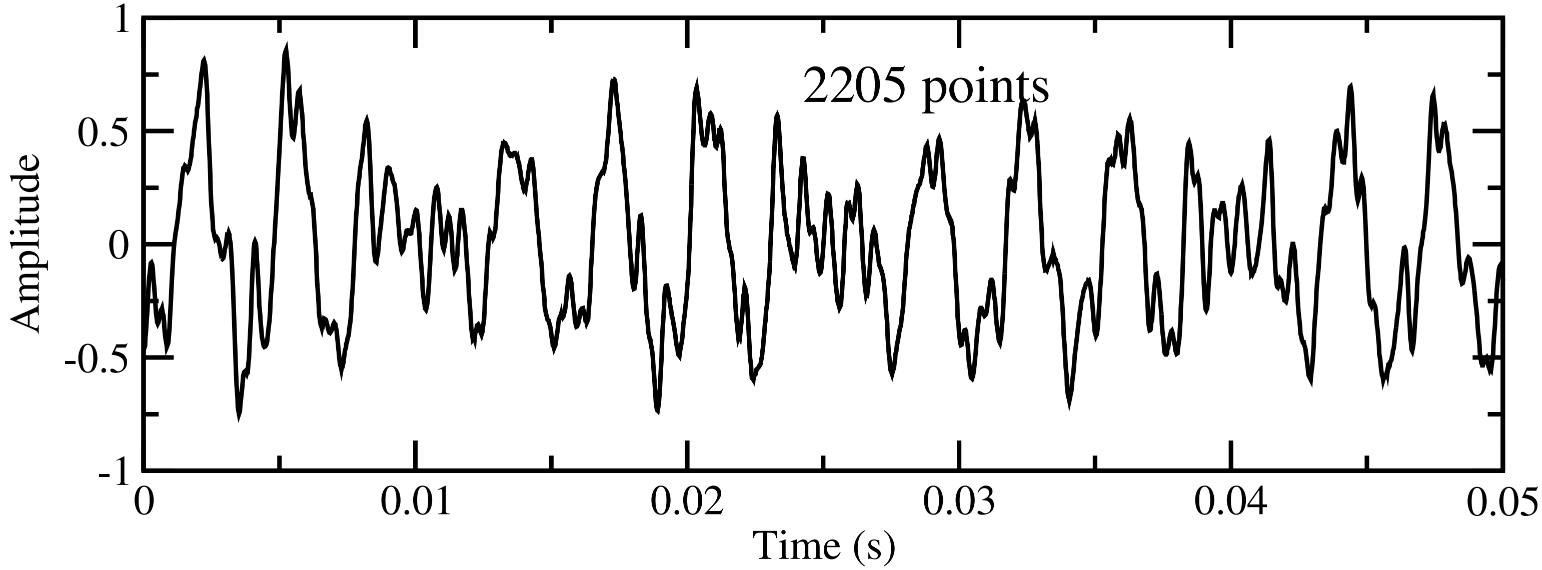
$$\boxed{\frac{1}{N}\sum_{k=0}^{N-1} w^{(j-\ell)k} = \delta_{j\ell}}$$

$$\frac{1}{N}\sum_{k=0}^{N-1} w^{(j-\ell)k} = \begin{cases} \dfrac{1}{N}\,\dfrac{1-\exp\left(\frac{2\pi i}{N}(j-\ell)N\right)}{1-\exp\left(\frac{2\pi i}{N}\right)} = 0\,, & \text{if } j \neq \ell \\ 1\,, & \text{if } j = \ell \end{cases}$$

Discrete Fourier Transformation

Example from introduction to classical and quantum computing by Wong





Vibrations of a piano playing a C major chord (made of middle C and the E and G notes above it) for one second

Discrete Fourier Transformation

Sound was *sampled* at a rate of 44100 Hertz (Hz), or 44100 points per second.

0.00000,-0.46933 a_0

0.00002,-0.46011 a_1

0.00005,-0.44931

0.00007,-0.41455 a_4

0.00009,-0.38632

0.00011,-0.34164

0.00014,-0.28851

...

0.99993,0.12177

0.99995,0.12454

0.99998,0.13571 a_{N-1}

N=44,100

$$\phi_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j e^{2\pi i jk/N}.$$

$$\phi_0 = \frac{1}{\sqrt{44100}}\Big(-0.46933e^{2\pi i(0)(0)/44100} - 0.46011e^{2\pi i(1)(0)/44100} + \dots$$
$$+0.13571e^{2\pi i(44099)(0)/44100}\Big) = -0.0973861,$$

$$\phi_1 = \frac{1}{\sqrt{44100}}\Big(-0.46933e^{2\pi i(0)(1)/44100} - 0.46011e^{2\pi i(1)(1)/44100} + \dots$$
$$+0.13571e^{2\pi i(44099)(1)/44100}\Big) = -0.118737 + 0.136405i,$$

$$\phi_2 = \frac{1}{\sqrt{44100}}\Big(-0.46933e^{2\pi i(0)(2)/44100} - 0.46011e^{2\pi i(1)(2)/44100} + \dots$$
$$+0.13571e^{2\pi i(44099)(2)/44100}\Big) = -0.106039 + 0.0597867i,$$

$$\vdots$$

$$\phi_{44098} = \frac{1}{\sqrt{44100}}\Big(-0.46933e^{2\pi i(0)(44098)/44100} - 0.46011e^{2\pi i(1)(44098)/44100} + \dots$$
$$+0.13571e^{2\pi i(44099)(44098)/44100}\Big) = -0.106039 - 0.0597867i$$

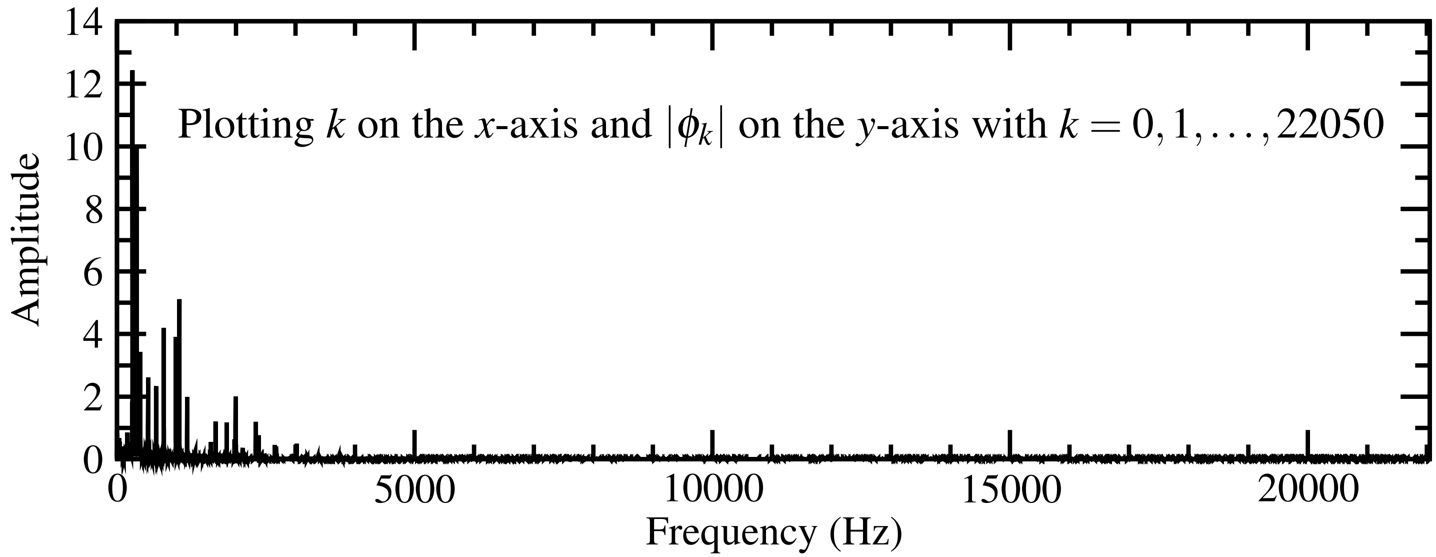
$$\phi_{44099} = \frac{1}{\sqrt{44100}}\Big(-0.46933e^{2\pi i(0)(44099)/44100} - 0.46011e^{2\pi i(1)(44099)/44100} + \dots$$
$$+0.13571e^{2\pi i(44099)(44099)/44100}\Big) = -0.118737 - 0.136405i.$$

Discrete Fourier Transformation

$\phi_k = \phi^*_{N-k}$ for $k = 1, 2, \ldots, N/2-1$, so ϕ_0 and $\phi_{N/2}$ are unique.

N=44,100

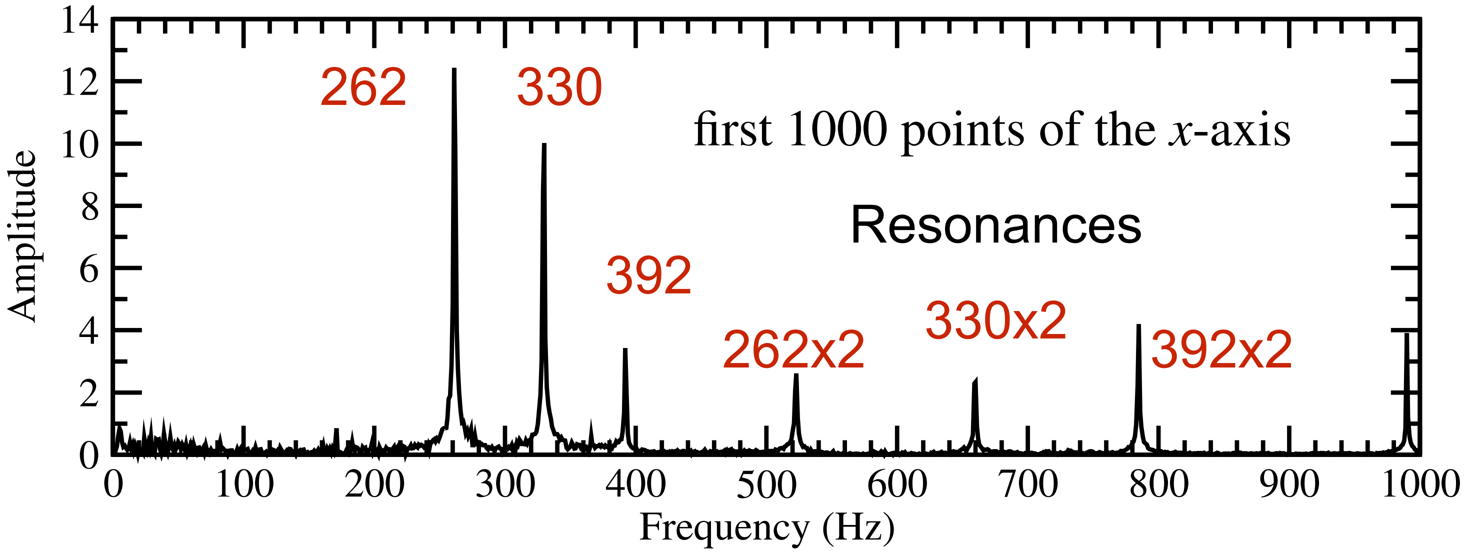
$$|\phi_0| = 0.097386$$
$$|\phi_1| = 0.180844$$
$$|\phi_2| = 0.121732$$
$$\vdots$$
$$|\phi_{44098}| = 0.121732$$
$$|\phi_{44099}| = 0.180844.$$



Middle C = 261.6256 Hz

E = 329.6276 Hz

G = 391.9954 Hz



Resonances=integer multiple of fundamental frequencies

Another example of FT

Discrete Fourier Transformation

- Convolution (circular convolution, periodic convolution, cyclic convolution)

$$(f*g)_j = \sum_{i=0}^{N-1} f_i\, g_{j-i}\ , \quad \text{where } g_{-m} = g_{N-m} \text{ (periodic condition)}$$

$$(f*g)(t) = \int_{-\infty}^{\infty} f(\tau)g(t-\tau)d\tau$$

- DFT turns convolution into point wise vector multiplication.

$$\text{DFT of } f*g = \tilde{c}_k = \tilde{f}_k\, \tilde{g}_k$$

$$\tilde{c}_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} w^{-jk}\,(f*g)_j = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} w^{-jk}\Big(\sum_{i=0}^{N-1} f_i\, g_{j-i}\Big)$$

$$= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} w^{-jk} \sum_{i=0}^{N-1}\Big(\frac{1}{\sqrt{N}}\sum_{\ell} w^{i\ell}\tilde{f}_\ell\Big)\Big(\frac{1}{\sqrt{N}}\sum_{m} w^{(j-i)m}\tilde{g}_m\Big) = \frac{1}{\sqrt{N}^3}\sum_{j,i,\ell,m} \tilde{f}_\ell\, \tilde{g}_m\, \overset{\delta_{mk}}{\overbrace{w^{-jk}\, w^{i\ell}\, w^{jm}}}\, \overset{\delta_{ik}}{w^{-im}} = \tilde{f}_k\, \tilde{g}_k$$

$$\underbrace{w^{i\ell}\, w^{jm}\, w^{-im}}_{\delta_{\ell k}}$$

$$\text{DFT}: \ f_k \longrightarrow \tilde{f}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{-jk} f_k$$

$$\boxed{\frac{1}{N}\sum_{k=0}^{N-1} w^{(j-\ell)k} = \delta_{j\ell}} \qquad w = \exp\Big(\frac{2\pi i}{N}\Big)$$

$$\text{Inverse DFT}: \ \tilde{f}_k \longrightarrow \tilde{f}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{jk} \tilde{f}_k$$

Fast Fourier Transformation

$$\tilde{f}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{-jk} f_k$$

$$w = \exp\left(\frac{2\pi i}{N}\right) \qquad w^N = 1$$

$$w^{N-1} = w^N w^{-1} = w^{-1}$$

$$\begin{pmatrix} \tilde{f}_0 \\ \tilde{f}_1 \\ \vdots \\ \tilde{f}_{N-1} \end{pmatrix} = \frac{1}{\sqrt{N}} \underbrace{\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w^{-1} & w^{-2} & \cdots & w^{N-1} \\ 1 & w^{-2} & w^{-4} & \cdots & w^{-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{N-1} & w^{2N-2} & \cdots & w \end{pmatrix}}_{D^{-1} = D^{\dagger}} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{N-1} \end{pmatrix}$$

Unitary

$$\begin{bmatrix} \omega_N^{0\cdot 0} & \omega_N^{0\cdot 1} & \cdots & \omega_N^{0\cdot(N-1)} \\ \omega_N^{1\cdot 0} & \omega_N^{1\cdot 1} & \cdots & \omega_N^{1\cdot(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_N^{(N-1)\cdot 0} & \omega_N^{(N-1)\cdot 1} & \cdots & \omega_N^{(N-1)\cdot(N-1)} \end{bmatrix}$$

- How many math operations are needed for DFT?
  - N multiplications for each $\tilde{f}_j \rightarrow N^2$ complex multiplications
  - Addition $\rightarrow N(N-1)$ complex addition

Fast Fourier Transformation

$$\tilde{f}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{-jk} f_k$$

$$\begin{pmatrix} \tilde{f}_0 \\ \tilde{f}_1 \\ \vdots \\ \tilde{f}_{N-1} \end{pmatrix} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w^{-1} & w^{-2} & \cdots & w^{N-1} \\ 1 & w^{-2} & w^{-4} & \cdots & w^{-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{N-1} & w^{2N-2} & \cdots & w \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{N-1} \end{pmatrix}$$

$$w = \exp\left(\frac{2\pi i}{N}\right) \qquad w^N = 1$$

$$w^{N-1} = w^N w^{-1} = w^{-1}$$

- FFT offers less math operations.

Assume $N = 2^n$: $w^{k+N/2} = -w^k,\ w^{k+N} = w^k$ $w_N = \exp\left(\frac{2\pi i}{N}\right)$

$$\tilde{f}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{-ik} f_i = \frac{1}{\sqrt{N}} \left[\sum_{i=0}^{N/2-1} w^{-2ij} e_i + \sum_{i=0}^{N/2-1} w^{-(2i+1)j} o_i \right]$$

$$f = (f_0, f_1, f_2, f_3, \cdots, f_{N-2}, f_{N-1})$$

$$= (e_0, o_0, e_1, o_1, \cdots, e_{N/2}, o_{N/2})$$

$$w^{-j} w^{-2ij} = w^{-j} w_{N/2}^{-ij}$$

$$\exp\left[\frac{2\pi i}{N}(-2ij)\right] = \exp\left[\frac{2\pi i}{N/2}(-ij)\right] = w_{N/2}^{-ij}$$

Fast Fourier Transformation

$$\tilde{f}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{-ik} f_i = \frac{1}{\sqrt{N}} \left[\sum_{i=0}^{N/2-1} w^{-2ij} e_i + \sum_{i=0}^{N/2-1} w^{-(2i+1)j} o_i \right]$$

$$f = (f_0, f_1, f_2, f_3, \cdots, f_{N-2}, f_{N-1})$$
$$= (e_0, o_0, e_1, o_1, \cdots, e_{N/2}, o_{N/2})$$

$$w^{-j} w^{-2ij} = w^{-j} w_{N/2}^{-ij}$$

$$\exp\left[\frac{2\pi i}{N}(-2ij)\right] = \exp\left[\frac{2\pi i}{N/2}(-ij)\right] = w_{N/2}^{-ij}$$

$$w_N = \exp\left(\frac{2\pi i}{N}\right)$$

$$\tilde{f}_j = \frac{1}{\sqrt{N}} \left[\sum_{i=0}^{N/2-1} \left(e_i + w_N^{-j} o_i\right) w_{N/2}^{-ij} \right]$$

$$w_{N/2} = \exp\left(\frac{\pi i}{N}\right)$$

DFT of f in terms of DFT of e and o.

$$\tilde{f}_j = \tilde{e}_j + w_N^{-j} \tilde{o}_j \qquad j = 0, 1, \cdots, N-1$$

$$\sqrt{2}\,\tilde{f}_j = \tilde{e}_j + w_N^{-j} \tilde{o}_j, \qquad 0 \le j \le \frac{N}{2} - 1$$

$$\sqrt{2}\,\tilde{f}_j = \tilde{e}_j - w_N^{-j} \tilde{o}_j, \qquad \frac{N}{2} \le j \le N - 1$$

DFT of e and f are periodic with period N/2.

Fast Fourier Transformation

- To compute e and o : $2\left(\frac{N}{2}\right)^2 = \frac{N^2}{2}$
- Need $\frac{N}{2}$ to compute $w_N^{-j}\,\tilde{o}_j \;\rightarrow$ need $\frac{N^2}{2}+\frac{N}{2}$ complex multiplication as opposed to N^2 in DFT.
- A reduction of about a factor of 2 for large N.
- For $N = 2^n$, the number of multiplication is bounded by $2^n n = N \log N$

A simple application of FFT

- Consider two polynomials with complex coefficients

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1}$$

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{N-1} x^{N-1}$$

$$\Rightarrow \quad f(x)\, g(x) = \sum_{i,j=0}^{N-1} a_i\, b_j\, x^{i+j} = \sum_{k=0}^{2N-2} c_k\, x^k$$

$$c_k = \sum_{\ell}^{N-1} a_\ell\, b_{k-\ell}$$

Sum is over valid polynomial terms. If $k - \ell < 0$, no terms in the sum.

- Computation requires N^2 multiplication
- c_k looks like convolution.
- Consider 2N dim vectors:

$$a = (a_0, \cdots, a_{N-1}, 0, \cdots, 0)$$

$$b = (b_0, \cdots, b_{N-1}, 0, \cdots, 0)$$

$$c_k = \sum_{\ell}^{2N-1} a_\ell\, b_{k-\ell} \pmod{2N}$$

- Compute DFT of vectors a and b → point wise multiplication of the two vectors → Inverse DFT →requires $\mathcal{O}(N \log N)$ operations

$$\tilde{f}_k\, \tilde{g}_k = \tilde{c}_k = \text{DFT of } f * g \qquad f * g = \sum_{j=0}^{N-1} f_j\, g_{i-j}$$

Quantum Fourier Transformation

- For classical discrete Fourier transformation

$$y_k = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} w^{jk} x_j \qquad w = \exp\left(\frac{2\pi i}{2^n}\right) \qquad N = 2^n$$

- QFT is defined similarly $\quad F: \ |j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} w^{jk} |k\rangle = F|j\rangle$

- For arbitrary quantum states, $\quad F: \ |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} x_j |j\rangle \longrightarrow |y\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} y_k |k\rangle$

$$F|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} x_j F|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} x_j w^{jk} |k\rangle$$

- For a single quantum state, $\quad F|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} w^{jk} |k\rangle \qquad F|j'\rangle = \frac{1}{\sqrt{2^n}} \sum_{j'=0}^{2^n-1} w^{j'k'} |k'\rangle$

$$\langle j'|F^\dagger F|j\rangle = \frac{1}{2^n} \sum_{k=0}^{2^n-1} \sum_{k'=0}^{2^n-1} w^{-j'k'} w^{jk} \langle k'|k\rangle = \frac{1}{2^n} \sum_{k=0}^{2^n-1} w^{(j-j')k} = \delta_{jj'}$$

$$\frac{1}{2^n} \sum_{k=0}^{2^n-1} w^{(j-\ell)k} = \delta_{j\ell}$$

$F^\dagger F = 1$ and QFT is a unitary transformation.

Quantum Fourier Transformation

For $$j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0 = \sum_{i=1}^{n} j_i\, 2^{n-i}$$

$$k = k_1 2^{n-1} + k_2 2^{n-2} + \cdots + k_n 2^0 = \sum_{i=1}^{n} k_i\, 2^{n-i}$$

$$\frac{1}{2^n} \sum_{k=0}^{2^n-1} w^{(j-\ell)k} = \delta_{j\ell}$$

$$N = 2^n$$

$$w = \exp\left(\frac{2\pi i}{2^n}\right)$$

$$F\,|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} w^{jk}\,|k\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left(\frac{2\pi ij}{2^n} \sum_{\ell=1}^{n} k_\ell 2^{n-\ell}\right) |k\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left(2\pi ij \sum_{\ell=1}^{n} k_\ell 2^{-\ell}\right) |k\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left(2\pi ijk_1 2^{-1}\right) \exp\left(2\pi ijk_2 2^{-2}\right) \cdots \exp\left(2\pi ijk_n 2^{-n}\right) |k\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \underbrace{\exp\left(2\pi ijk_1 2^{-1}\right)}_{= |0\rangle + \exp\left(2\pi ij 2^{-1}\right) |1\rangle} \exp\left(2\pi ijk_2 2^{-2}\right) \cdots \underbrace{\exp\left(2\pi ijk_n 2^{-n}\right)}_{= |0\rangle + \exp\left(2\pi ij 2^{-n}\right) |1\rangle} |k_1\, k_2\, \cdots\, k_n\rangle$$

Quantum Fourier Transformation

$$F\,|j\rangle = \frac{1}{\sqrt{2}^{n}}\left(|0\rangle + \exp\!\left(\frac{2\pi i j}{2}\right)|1\rangle\right)\left(|0\rangle + \exp\!\left(\frac{2\pi i j}{2^2}\right)|1\rangle\right)\cdots\left(|0\rangle + \exp\!\left(\frac{2\pi i j}{2^n}\right)|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}^{n}} \bigotimes_{k=1}^{n}\left(|0\rangle + \exp\!\left(\frac{2\pi i j}{2^k}\right)|1\rangle\right)$$

$$j_i = 0\,,1$$

$$1 \le k \le n$$

$$0 \le j \le 2^n - 1$$

- Binary fraction = expression in power of 1/2

In decimal form: $0.j_\ell\, j_{\ell+1} \cdots j_m = \dfrac{j_\ell}{2} + \dfrac{j_{\ell+1}}{2^2} + \cdots + \dfrac{j_m}{2^{m-\ell+1}}$

j is not necessarily an integer: $\dfrac{j}{2^k} = j_1\, j_2 \cdots j_{n-k} \cdot j_{n-k+1} \cdots j_n = \displaystyle\sum_{\nu=1}^{n} j_\nu\, 2^{n-\nu-k}$

If $n = 8$ and $k = 3$, $j = j_1 2^7 + j_2 2^6 + j_3 2^5 + j_4 2^4 + j_5 2^3 + j_6 2^2 + j_7 2^1 + j_8 2^0$

$$\frac{j}{2^3} = j_1 2^4 + j_2 2^3 + j_3 2^2 + j_4 2^1 + j_5 2^0 + \underbrace{j_6 2^{-1} + j_7 2^{-2} + j_8 2^{-3}}$$

$$j_1 j_2 j_3 j_4 j_5 \cdot j_6 j_7 j_8$$

binary fraction: $0\,.j_6 j_7 j_8$

Quantum Fourier Transformation

$$j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_{n-3} 2^3 + j_{n-2} 2^2 + j_{n-1} 2^1 + j_n 2^0 = \sum_{\nu=1}^{n} j_\nu 2^{n-\nu}$$

$$\frac{j}{2^k} = \frac{j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_{n-3} 2^3 + j_{n-2} 2^2 + j_{n-1} 2^1 + j_n 2^0}{2^k} = \sum_{\nu=1}^{n} \frac{j_\nu\, 2^{n-\nu}}{2^k} = \sum_{\nu=1}^{n} j_\nu\, 2^{n-\nu-k}$$

$$= j_1 j_2 \cdots j_{n-k} \,.\, j_{n-k+1} \cdots j_n$$

$$\exp\left(2\pi i \frac{j}{2^k}\right) = \exp\left(2\pi i\, j_1 j_2 \cdots j_{n-k} \,.\, j_{n-k+1} \cdots j_n \ \cdots\ j_n\right) = \exp\left(2\pi i\, 0\,.\, j_{n-k-1} \ \cdots\ j_n\right)$$

$$F\,|\,j\rangle = \frac{1}{\sqrt{2}^{\,n}} \left(\,|\,0\rangle + \exp\left(\frac{2\pi i j}{2}\right)|\,1\rangle\right)\left(\,|\,0\rangle + \exp\left(\frac{2\pi i j}{2^2}\right)|\,1\rangle\right)\cdots\left(\,|\,0\rangle + \exp\left(\frac{2\pi i j}{2^n}\right)|\,1\rangle\right)$$

$$= \frac{1}{\sqrt{2}^{\,n}} \bigotimes_{k=1}^{n} \left(\,|\,0\rangle + \exp\left(\frac{2\pi i j}{2^k}\right)|\,1\rangle\right) = \frac{1}{\sqrt{2}^{\,n}} \bigotimes_{k=1}^{n} \left(\,|\,0\rangle + \exp\left(2\pi i\, 0\,.\, j_{n-k-1} \ \cdots\ j_n\right)|\,1\rangle\right)$$

$$= \frac{1}{\sqrt{2}^{\,n}} \left(\,|\,0\rangle + \exp\left(2\pi i\, 0\,.\, j_n\right)|\,1\rangle\right)\left(\,|\,0\rangle + \exp\left(2\pi i\, 0\,.\, j_{n-1} j_n\right)|\,1\rangle\right)$$

$$\cdots\left(\,|\,0\rangle + \exp\left(2\pi i\, 0\,.\, j_1 j_2 \cdots j_n\right)|\,1\rangle\right)$$

Quantum Circuit for QFT

- $|j_\ell\rangle$ transforms into $\frac{1}{\sqrt{2}}\left[\,|0\rangle + \exp\left(2\pi i\,0\,.j_\ell\cdots j_n\right)|1\rangle\right]$

$$= \frac{1}{\sqrt{2}}\left[\,|0\rangle + \underbrace{e^{2\pi i\,0.j_\ell}}\,\underbrace{e^{2\pi i 0.0 j_{\ell+1\cdots j_n}/2}}\,|1\rangle\right]$$

Controlled by the value of j_kth qubit.

$$\exp\left(2\pi i\frac{j_\ell}{2}\right) = \exp\left(\pi i j_\ell\right) = (-1)^{j_\ell}$$

use $R_k = \begin{pmatrix}1 & 0\\ 0 & e^{2\pi i/2^k}\end{pmatrix}$

if $\begin{cases} j_k = 0\,, & R = 1\\ j_k = 1\,, & R = R_k\end{cases}$

1st qubit: $|0\rangle + \exp\left(2\pi i\,0\,.j_\ell\cdots j_n\right)|1\rangle$

Start with $|j\rangle = |j_1\rangle|j_2 j_3\cdots j_n\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{j_1}|1\rangle\right)|j_2 j_3\cdots j_n\rangle$

$$\exp\left(2\pi i\frac{j_1}{2}\right) = \exp\left(2\pi i\,0.j_1\right)$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\,0.j_1}|1\rangle\right)|j_2 j_3\cdots j_n\rangle$$

$\xrightarrow{\mathrm{R_2\ on\ q_1\ with\ q_2\ control}}$ $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\,0.j_1}\,e^{2\pi i\,j_2/2^2}|1\rangle\right)|j_2 j_3\cdots j_n\rangle$

$$R_2 = \begin{pmatrix}1 & 0\\ 0 & e^{2\pi i/2^2}\end{pmatrix}$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\,0.j_1 j_2}|1\rangle\right)|j_2 j_3\cdots j_n\rangle$$

Quantum Circuit for QFT

$$\xrightarrow{\text{R}_3 \text{ on q}_1 \text{ with q}_3 \text{ control}} \quad \frac{1}{\sqrt{2}}\Big(\,|0\rangle + e^{2\pi i\,0.j_1 j_2 j_3}\,|1\rangle\Big)\,|j_2 j_3 \cdots j_n\rangle$$

$$\xrightarrow[\text{to q}_n]{\text{continue down}} \quad \frac{1}{\sqrt{2}}\Big(\,|0\rangle + e^{2\pi i\,0.j_1 j_2 j_3 \cdots j_n}\,|1\rangle\Big)\,|j_2 j_3 \cdots j_n\rangle$$

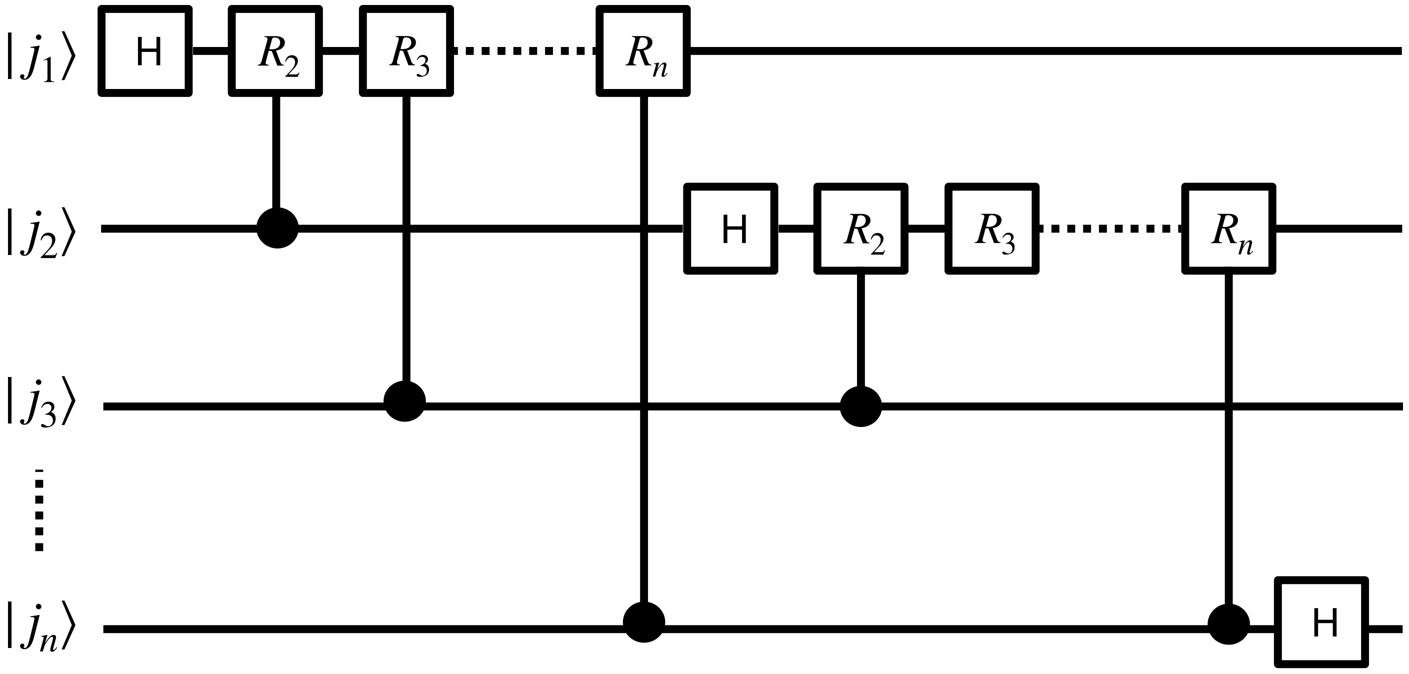
The entire procedure is repeated for all other qubits, $j_2\,, j_3\,, \cdots\; j_n$

$$\frac{1}{\sqrt{2}^n}\Big[\,|0\rangle + e^{2\pi i\,0.j_1 \cdots j_n}\,|1\rangle\Big]\Big[\,|0\rangle + e^{2\pi i\,0.j_2 \cdots j_n}\,|1\rangle\Big]\;\cdots\;\Big[\,|0\rangle + e^{2\pi i\,0.j_n}\,|1\rangle\Big]$$

Use SWAP gate or relabel to obtain: $F\,|\,j\rangle = \dfrac{1}{\sqrt{2}^n} \displaystyle\bigotimes_{k=1}^{n} \Big(\,|0\rangle + \exp\Big(\frac{2\pi i j}{2^k}\Big)\,|1\rangle\Big)$

$$\frac{1}{\sqrt{2}^n}\Big[\,|0\rangle + e^{2\pi i\,0.j_n}\,|1\rangle\Big]\Big[\,|0\rangle + e^{2\pi i\,0.j_2 \cdots j_n}\,|1\rangle\Big]\;\cdots\;\Big[\,|0\rangle + e^{2\pi i\,0.j_1 \cdots j_n}\,|1\rangle\Big]$$

Quantum Circuit for QFT



$$\frac{1}{\sqrt{2}}\left[\,|0\rangle + e^{2\pi i\,0.j_1\cdots j_n}\,|1\rangle\,\right]$$

$$\frac{1}{\sqrt{2}}\left[\,|0\rangle + e^{2\pi i\,0.j_2\cdots j_n}\,|1\rangle\,\right]$$

$$\vdots$$

$$\frac{1}{\sqrt{2}}\left[\,|0\rangle + (-1)^{j_n}\,|1\rangle\,\right]$$

$$= \frac{1}{\sqrt{2}}\left[\,|0\rangle + e^{2\pi i\,0.j_1}\,|1\rangle\,\right]$$

How many gates are required?

$$\left.\begin{array}{lll} q_1\text{:} & \text{H + (n-1) controlled R gates} & \longrightarrow \text{n} \\ q_2\text{:} & \text{H + (n-2) controlled R gates} & \longrightarrow \text{n-1} \\ \vdots & \qquad\qquad\vdots & \qquad\vdots \\ q_n\text{:} & \text{H + 0 controlled R gates} & \longrightarrow \text{1} \end{array}\right\} \frac{n(n+1)}{2}$$

Also need $\mathcal{O}(n/2)$ SWAP gates

Overall scaling of QFT is $\mathcal{O}(n^2)$

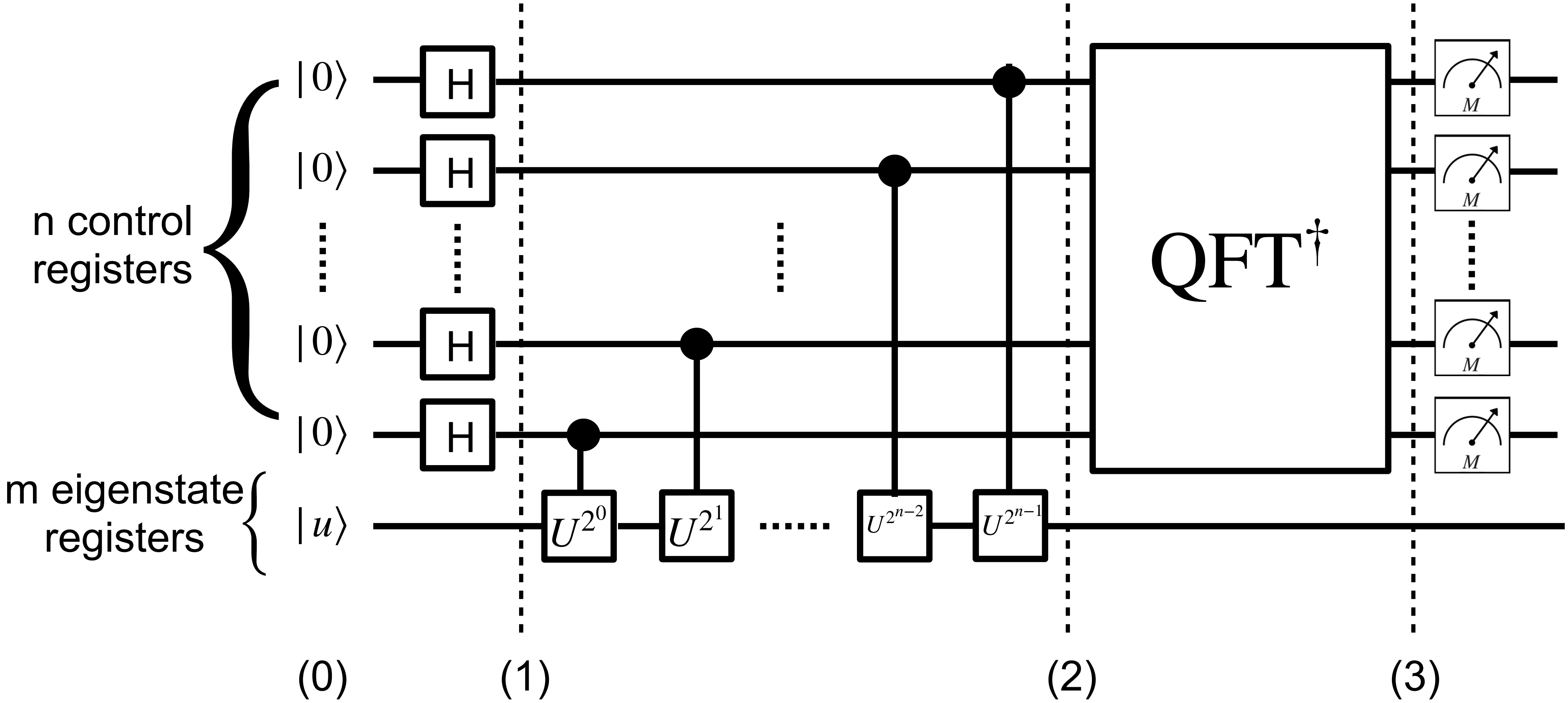
- Classical Fourier Transform scales as $\mathcal{O}(N^2) = \mathcal{O}((2^n)^2)$
- FFT: $\mathcal{O}(Nln(N))$ for $N = 2^n$

Quantum Phase Estimation and Finding Eigenvalues

- Good example of phase kickback and use of QFT
- Unitary operator $U: \; U|u\rangle = e^{i\phi}|u\rangle, \qquad 0 \le \phi < 2\pi$
- How to find eigenvalue? = How to measure the phase?
- How to find ϕ to a given level of precision?
- Find the best n-bit estimate of the phase ϕ
- Given a unitary matrix U and one of its eigenvectors $|u\rangle$, find or estimate its eigenvalue.

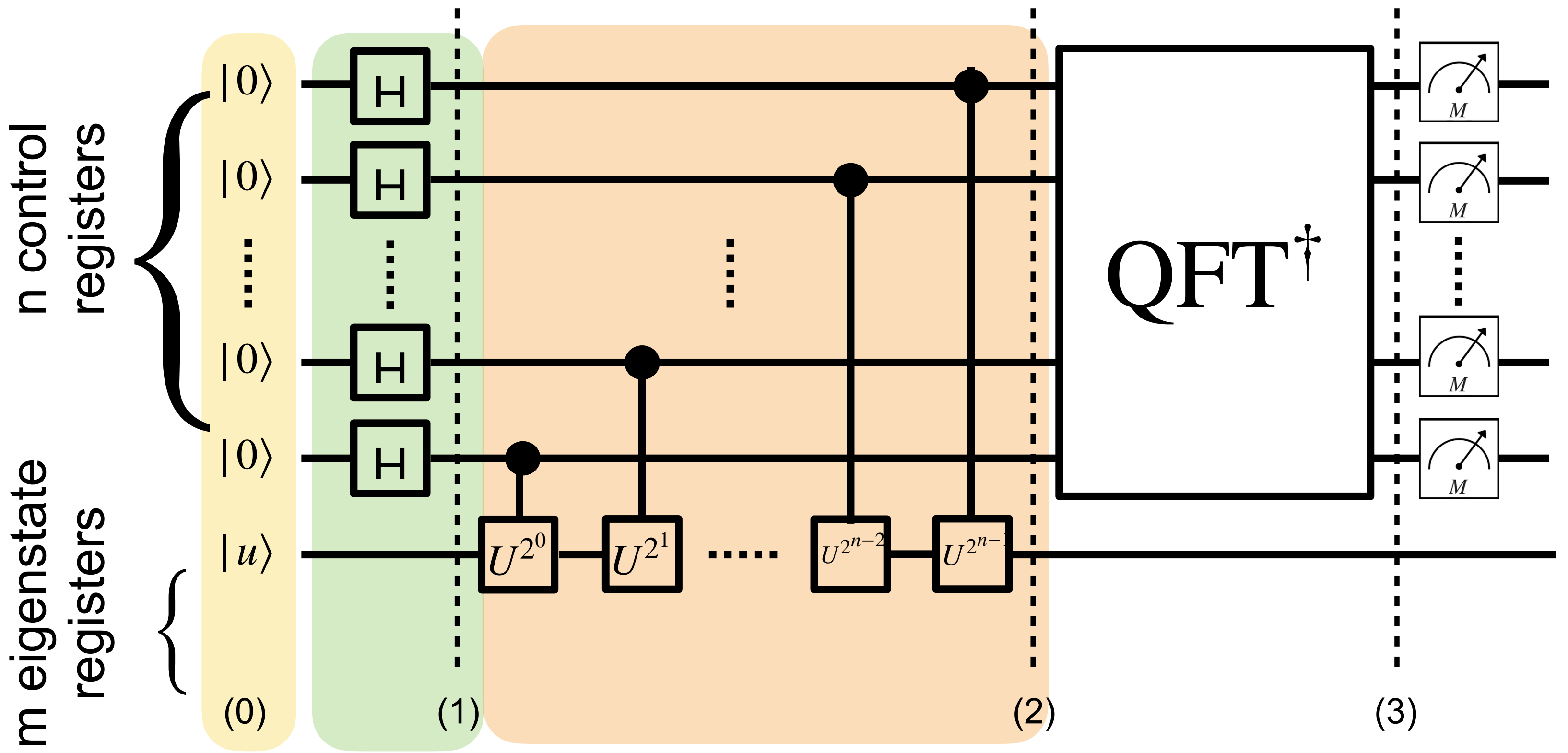
$$U^{2j}|u\rangle = \left(e^{i\phi}\right)^{2^j}|u\rangle = e^{i\phi\,2^j}|u\rangle$$

Quantum Circuit for QPE



$$\mathrm{QPE} = H + \text{controlled} - U^{2^j} + \mathrm{QFT}^\dagger$$

Quantum Circuit for QPE



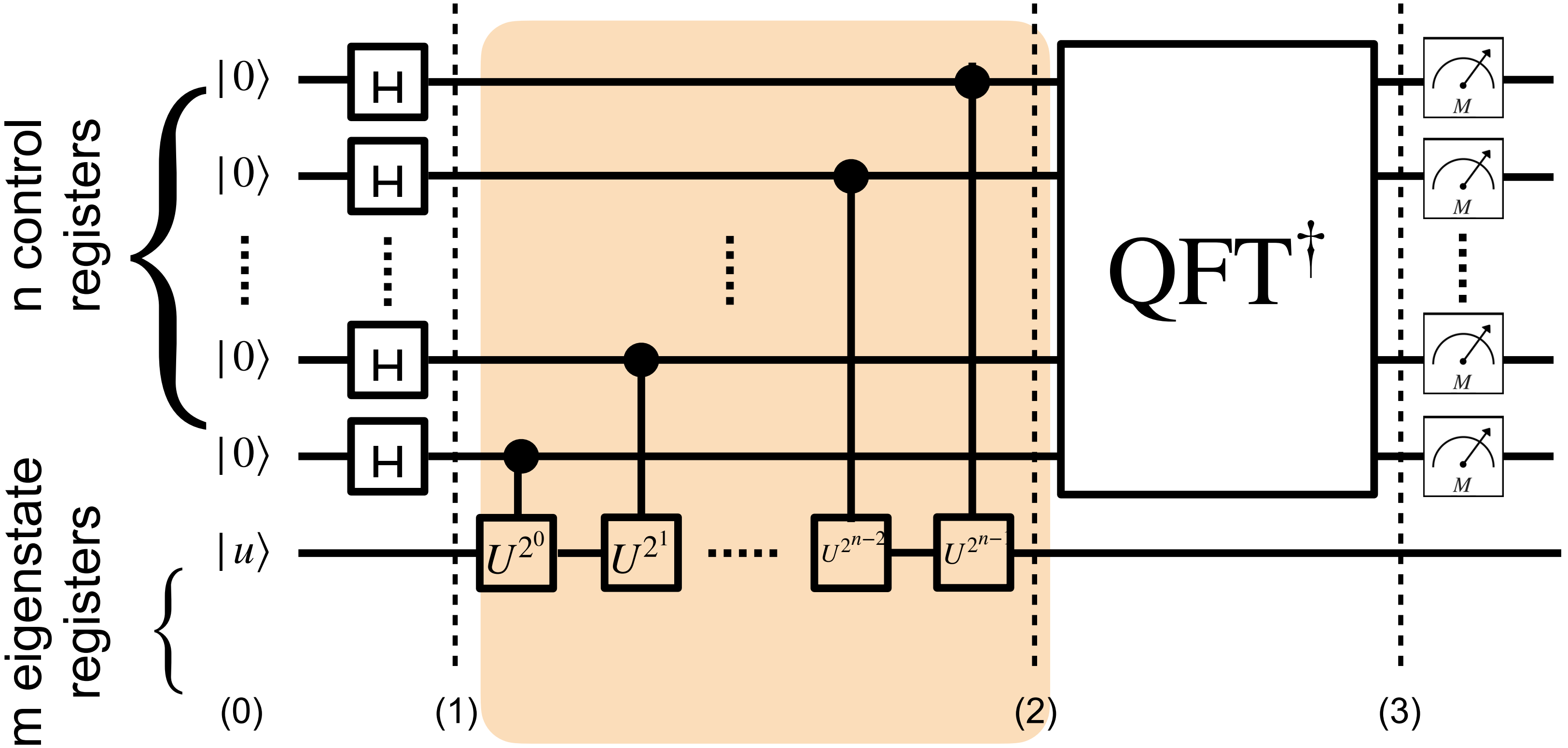
$$\text{QPE} \; = H + \text{controlled} - U^{2^j} + \text{QFT}^\dagger$$

$$|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |u\rangle$$

$$|\psi_1\rangle = \Big(H|0\rangle\Big)^{\otimes n} \otimes |u\rangle = \frac{1}{\sqrt{2}^n}\Big(|0\rangle + |1\rangle\Big)^{\otimes n} \otimes |u\rangle$$

$$|\psi_2\rangle = \prod_{j=0}^{n-1} \mathrm{CU}^{2^j} \frac{1}{\sqrt{2}^n}\Big(|0\rangle + |1\rangle\Big)^{\otimes n} \otimes |u\rangle$$

Quantum Circuit for QPE



$$|\psi_2\rangle = \prod_{j=0}^{n-1} \mathrm{CU}^{2^j} \frac{1}{\sqrt{2^n}}\Big(|0\rangle + |1\rangle\Big)^{\otimes n} \otimes |u\rangle$$

$$\frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \otimes |u\rangle \xrightarrow{\mathrm{CU}^{2^j}} \frac{1}{\sqrt{2}}\Big(|0\rangle \otimes |u\rangle + U^{2^j}|1\rangle \otimes |u\rangle\Big)$$

$$= \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{i\phi\, 2^j}|1\rangle\Big) \otimes |u\rangle$$

Quantum Circuit for QPE

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}}\Big(|0\rangle + e^{i\phi\,2^{n-1}}|1\rangle\Big)\Big(|0\rangle + e^{i\phi\,2^{n-2}}|1\rangle\Big)\cdots\Big(|0\rangle + e^{i2\phi}|1\rangle\Big)\Big(|0\rangle + e^{i\phi}|1\rangle\Big) \otimes |u\rangle$$

$$= \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1} \underbrace{e^{i\phi y}}_{}|y\rangle \otimes |u\rangle$$

Phase kick-back: phase factor $e^{i\phi y}$ has been propagated back from the second eigenstate register to the first control register

$$\text{QFT}\,|a\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{2\pi i a k/2^n}|k\rangle \xrightarrow{\qquad} \frac{2\pi i a}{2^n} = i\phi \xrightarrow{\qquad} \boxed{\phi = 2\pi\Big(\frac{a}{2^n} + \delta\Big)}$$

$$a = a_{n-1}a_{n-2}\cdots a_0$$

- $\dfrac{2\pi a}{2^n}$ is the best n-bit binary approximation of ϕ .
- $0 \le |\delta| \le \dfrac{1}{2^{n+1}}$ is the associated error.

$$F\,|j\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1} w^{jk}|k\rangle$$

$$w = \exp\Big(\frac{2\pi i}{2^n}\Big)$$

$$\text{QFT}^{-1}|y\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1} e^{-2\pi i x y)/2^n}|x\rangle$$

$$|\psi_3\rangle = \text{QFT}^{-1}|\psi_2\rangle = \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1} e^{2\pi i(a-x)y/2^n}\, e^{2\pi i\delta y}\,|x\rangle \otimes |u\rangle$$

Operate only n control register.

Quantum Circuit for QPE

$$|\psi_3\rangle = \mathrm{QFT}^{-1}|\psi_2\rangle = \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1} e^{2\pi i(a-x)y/2^n} e^{2\pi i\delta y}|x\rangle \otimes |u\rangle$$

Operate only n control register.

(1) If $\delta = 0$, $\frac{1}{2^n}\sum_{y=0}^{2^n-1}\exp\left(\frac{2\pi i(a-x)y}{2^n}\right) = \delta_{ax} \longrightarrow |\psi_3\rangle = |a\rangle \otimes |u\rangle \longrightarrow \phi = \frac{2\pi a}{2^n}$

(2) If $\delta \neq 0$, Measuring 1st register and getting the state $|x\rangle = |a\rangle$ is the best n-bit estimate of ϕ. The corresponding probability is $P_a = |C_a|^2 \geq \frac{4}{\pi^2} \approx 0.405$

Quantum Circuit for QPE

$$\phi = \frac{2\pi a}{2^n}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} e^{2\pi i x \phi} |x\rangle \otimes |u\rangle$$

$$\mathrm{QFT}^{-1}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{-2\pi i x y/2^n} |y\rangle$$

$$|\psi_3\rangle = \mathrm{QFT}^{-1}|\psi_2\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} e^{2\pi i x(\phi - y/2^n)} |y\rangle \otimes |u\rangle$$

Probability of observing $|y\rangle$ = $P(y) = \left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} e^{2\pi i x(\phi - y/2^n)} \right|^2 = \frac{1}{2^{2n}} \left| \frac{1 - r^{2^n}}{1 - r} \right|^2, \quad r \equiv \exp\left[2\pi i \left(\phi - \frac{y}{2^n}\right)\right]$

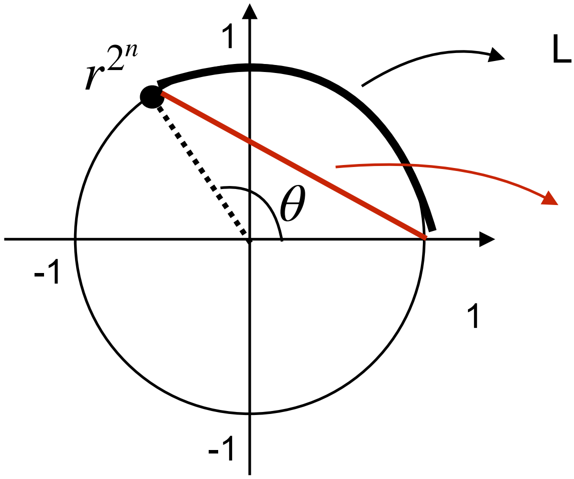
(1) If $\phi = \frac{y}{2^n}, \quad |\psi_3\rangle = |y\rangle \otimes |u\rangle \qquad P(\phi = \frac{y}{2^n}) = 100\,\%$

(2) If $\phi \neq \frac{y}{2^n}, \quad \text{closest n} - \text{bit approximation to } \phi = 0.\nu_1\nu_2\cdots\nu_n \equiv \nu \qquad \phi - \nu \equiv \delta, \quad 0 \le |\delta| \le \frac{1}{2^{n+1}}$

$$r \equiv \exp\left[2\pi i \left(\phi - \frac{y}{2^n}\right)\right] = \exp(2\pi i \delta)$$

$$P(y) = \frac{1}{2^{2n}} \left| \frac{1 - r^{2^n}}{1 - r} \right|^2,$$

$$r^{2^n} = \left[\exp(2\pi i \delta)\right]^{2^n} = \exp(2\pi i \delta 2^n) = e^{i\theta}$$

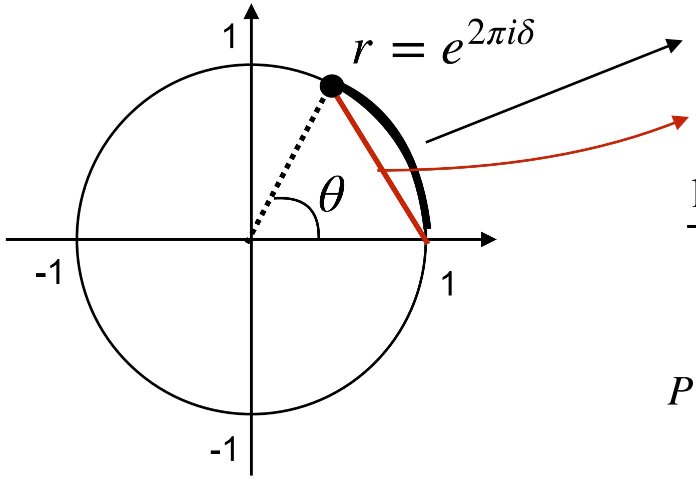


Length of minor arc
$= \theta = 2\pi\delta 2^n$

Length of a cord from 1 to r^{2^n}
$= |1 - r^{2^n}|$

$$\frac{\text{length of minor arc}}{\text{length of cord}} = \frac{2\pi\delta 2^n}{|1 - r^{2^n}|} \le \frac{\text{half circumference}}{\text{diameter}} \le \frac{\pi R}{2R} = \frac{\pi}{2} \longrightarrow |1 - r^{2^n}| \ge 4\delta 2^n$$

Quantum Circuit for QPE



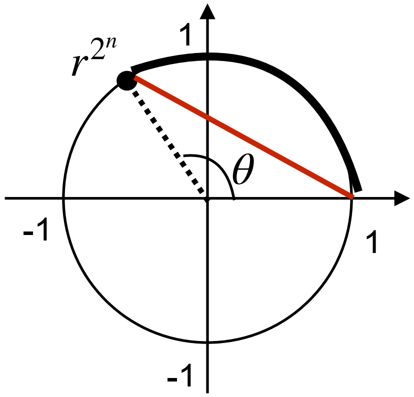
Length of minor arc = $\theta = 2\pi\delta$

Length of a cord from 1 to r = $|1-r|$

$$\frac{\text{length of minor arc}}{\text{length of cord}} = \frac{2\pi\delta}{|1-r|} > 1, \qquad |1-r| < 2\pi\delta$$

$$P(y) = \frac{1}{2^{2n}}\left|\frac{1-r^{2^n}}{1-r}\right|^2 \geq \frac{1}{2^{2n}}\left(\frac{4\delta 2^n}{2\pi\delta}\right)^2 = \frac{4}{\pi^2} > 0.405$$

- We will get the correct answer with probability greater than a constant.
- Probability of getting incorrect outcome can be calculated using $|\delta| > \frac{1}{2^{n+1}}$



$|1-r^{2^n}| < 2$

$$\frac{\text{length of minor arc}}{\text{length of cord}} = \frac{2\pi\delta}{|1-r|} < \frac{\pi}{2}, \qquad |1-r| > 4\delta$$

$$P(y) = \frac{1}{2^{2n}}\left|\frac{1-r^{2^n}}{1-r}\right|^2 \leq \frac{1}{2^{2n}}\left(\frac{2}{4\delta}\right)^2 = \frac{1}{2^{2n}(2\delta)^2}$$

If $\delta = \frac{c}{2^n}$, $P(c) \leq \frac{1}{4c^2}$

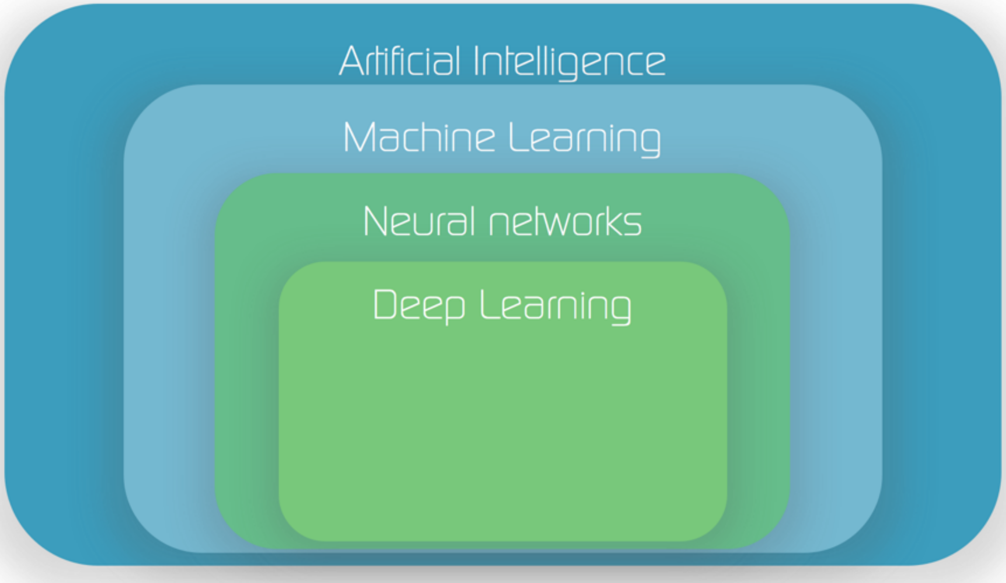
- N-bit estimate of phase ϕ is obtained with a high probability.
- Need to repeat the calculation multiple times.
- Increasing n will increase the probability of success (not obvious but true).
- Increasing n (# of qubits) will improve the precision of the phase estimate.

$$\frac{\text{length of minor arc}}{\text{length of cord}} \leq \frac{\text{half circumference}}{\text{diameter}} \leq \frac{\pi R}{2R} = \frac{\pi}{2}$$

Machine Learning?

What is Machine Learning?

- Typically problems in physics can be formulated in terms of a search for some function $f : \mathbb{X} \rightarrow \mathbb{Y}$, from the space of the observed $\mathbb{X}$ to a low dimensional space of a desired target space/label $\mathbb{Y}$, which optimizes some metric (of our choice). The metric is often called a loss function and written as $L(\vec{y}, f(\vec{x}))$.
- A learning algorithm would find the function that optimizes L over all possible values of $(\vec{x}, \vec{y})$.
- But this is intractable owning to the curse of dimensionality and an infinite number of functions to choose from. Instead one has labeled training data $\{\vec{x}_i, \vec{y}_i\}_{i=1}^{N}$ sampled from $p(\vec{x}, \vec{y})$. Furthermore the function space is restricted to a model - a highly flexible family of functions $f_\phi(\vec{x})$ parameterized by ϕ .
- Sounds familiar?



Universal Approximation Theorem

- A feed-forward network with a single hidden layer containing a finite number of neurons can approximate continuous functions on compact subsets of R^n, under mild assumptions on the activation function.

Let $\varphi : \mathbb{R} \to \mathbb{R}$ be a nonconstant, bounded, and continuous function (called the *activation function*). Let I_m denote the m-dimensional unit hypercube $[0,1]^m$. The space of real-valued continuous functions on I_m is denoted by $C(I_m)$. Then, given any $\varepsilon > 0$ and any function $f \in C(I_m)$, there exist an integer N, real constants $v_i, b_i \in \mathbb{R}$ and real vectors $w_i \in \mathbb{R}^m$ for $i = 1, \ldots, N$, such that we may define:

$$F(x) = \sum_{i=1}^{N} v_i \varphi\left(w_i^T x + b_i\right)$$

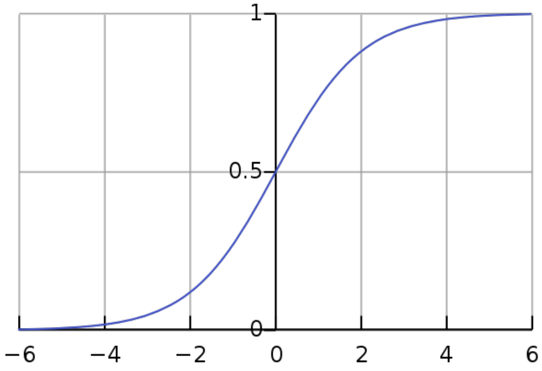
as an approximate realization of the function f; that is,

$$|F(x) - f(x)| < \varepsilon$$

for all $x \in I_m$. In other words, functions of the form $F(x)$ are dense in $C(I_m)$.

- A. N. Kolmogorov, 1957
- G. Cybenko, 1989 with sigmoid activation
- K. Hornik, 1991, importance of the multilayer architecture
- Z. Lu et al, 2017, with deep neural network and ReLu activation

$$S(x) = \frac{1}{1 + e^{-x}} = \frac{e^x}{e^x + 1}$$



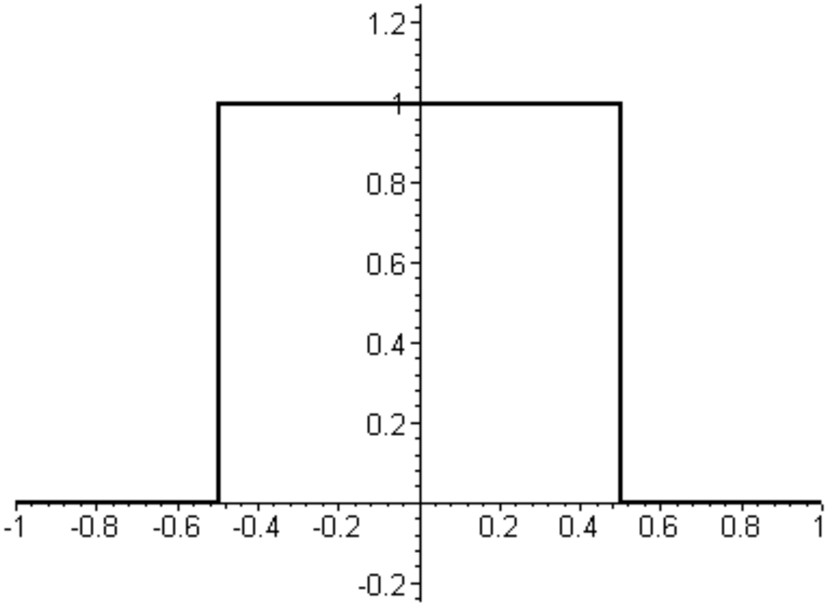
Let $p > 0$ be a fixed number and $f(x)$ be a periodic function with period $2p$, defined on $(-p, p)$. The Fourier series of $f(x)$ is a way of expanding the function $f(x)$ into an infinite series involving sines and cosines:

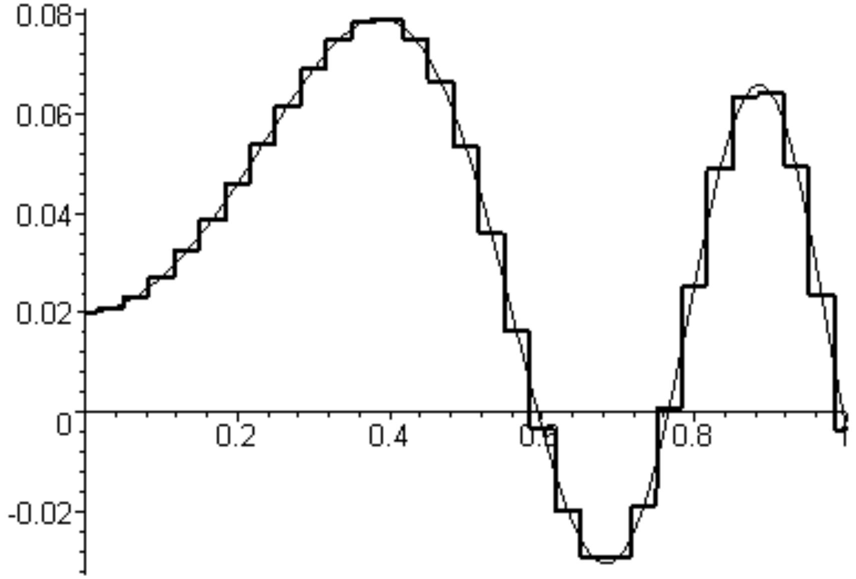
$$f(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos(\frac{n\pi x}{p}) + \sum_{n=1}^{\infty} b_n \sin(\frac{n\pi x}{p}) \tag{2.1}$$

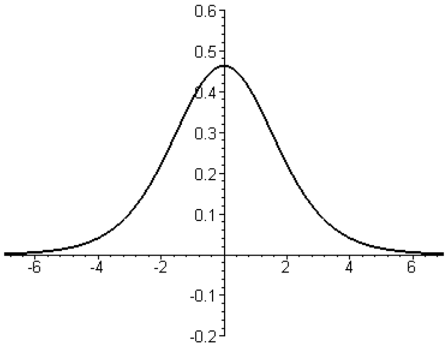
where a_0, a_n, and b_n are called the Fourier coefficients of $f(x)$, and are given by the formulas

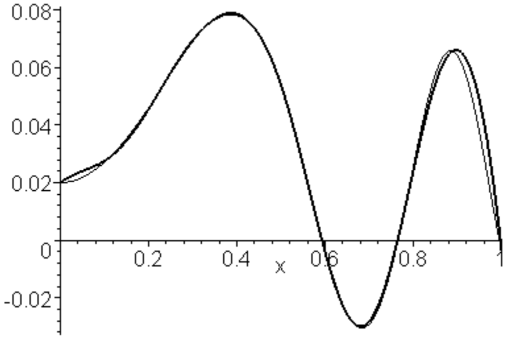
$$a_0 = \frac{1}{p}\int_{-p}^{p} f(x)\ dx, \qquad a_n = \frac{1}{p}\int_{-p}^{p} f(x)\cos(\frac{n\pi x}{p})\ dx, \tag{2.2}$$

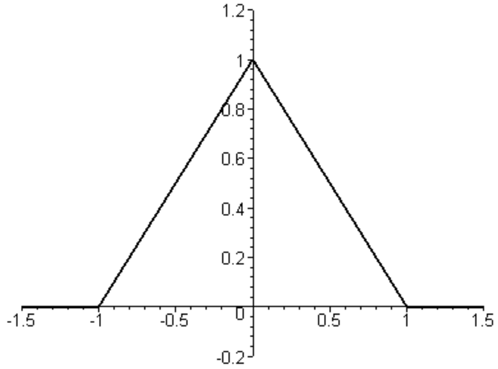
$$b_n = \frac{1}{p}\int_{-p}^{p} f(x)\sin(\frac{n\pi x}{p})\ dx,$$

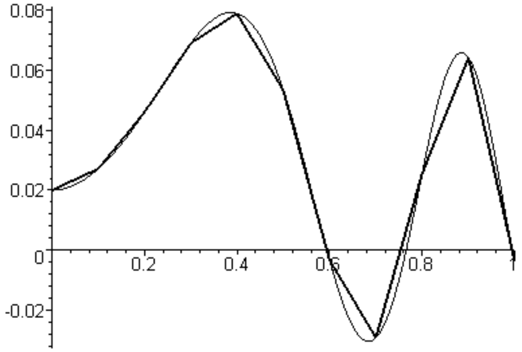

1.2
1
0.8
0.6
0.4
0.2
-0.2
-1
-0.8
-0.6
-0.4
-0.2
0.2
0.4
0.6
0.8
1


0.08
0.06
0.04
0.02
0
-0.02
0.2
0.4
0.6
0.8
1


0.6
0.5
0.4
0.3
0.2
0.1
-0.1
-0.2
-6
-4
-2
2
4
6


0.08
0.06
0.04
0.02
0
-0.02
0.2
0.4
x
0.6
0.8
1

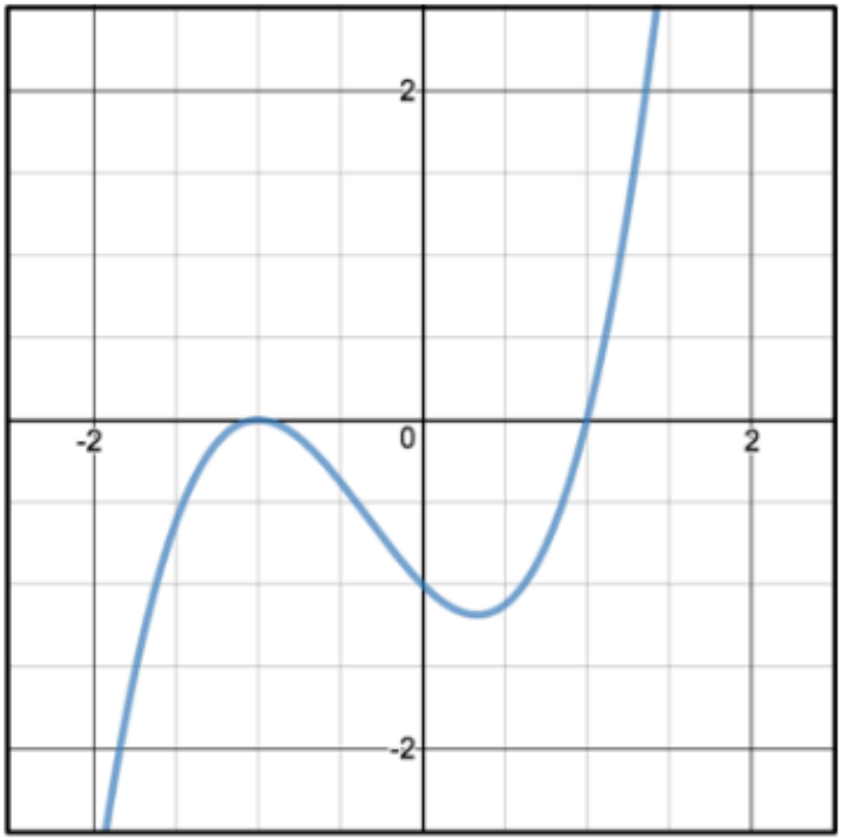

1.2
1
0.8
0.6
0.4
0.2
0
-0.2
-1.5
-1
-0.5
0.5
1
1.5


0.08
0.06
0.04
0.02
0
-0.02
0.2
0.4
0.6
0.8
1

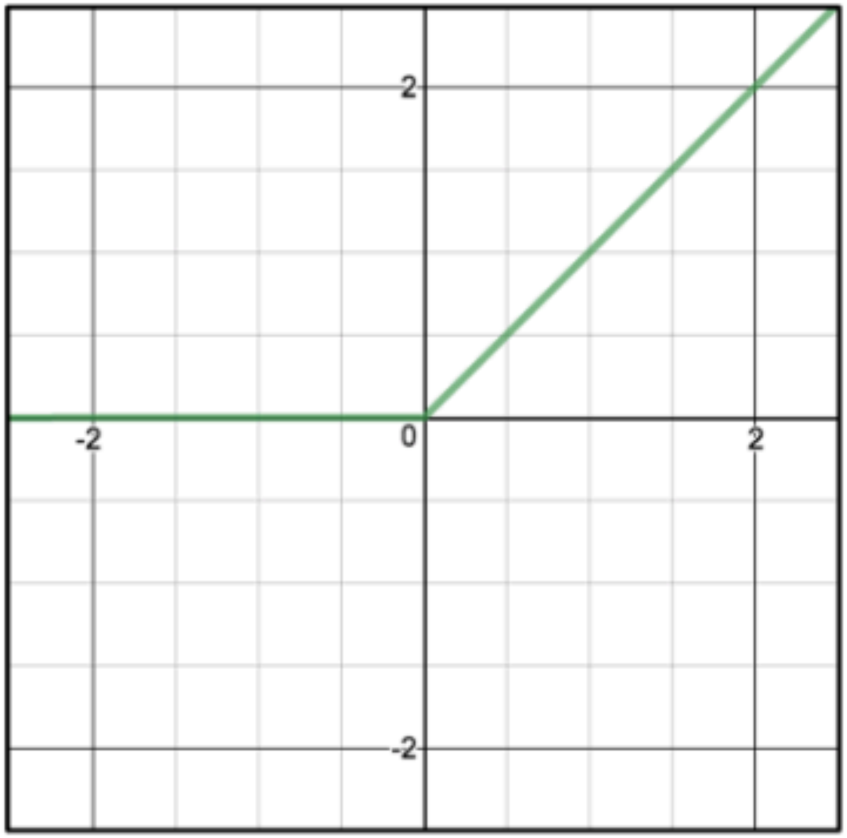
Neural network is a function-approximator.

Rectified Linear Unit

$f(x) = x^3 + x^2 - x - 1$



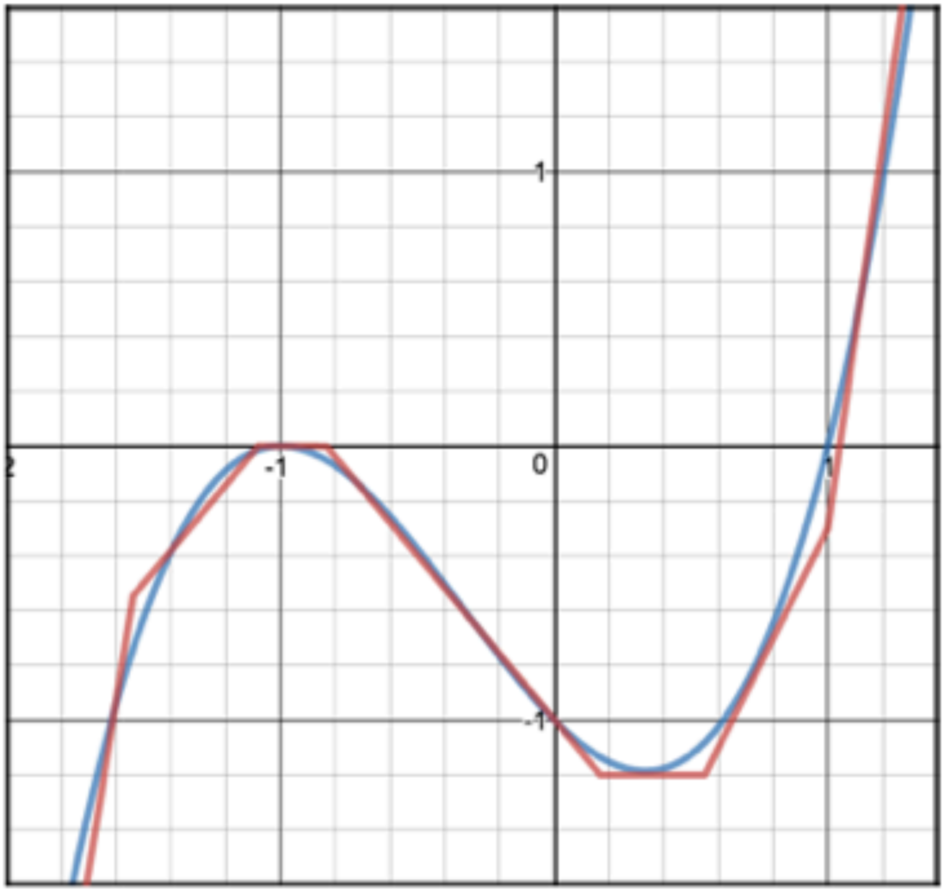
ReLU



ReLu = max(0, x)

Example by Joe Klein

$f(x) = x^3 + x^2 - x - 1$



$$n_1(x) = Relu(-5x - 7.7)$$

$$n_2(x) = Relu(-1.2x - 1.3)$$

$$n_3(x) = Relu(1.2x + 1)$$

$$n_4(x) = Relu(1.2x - .2)$$

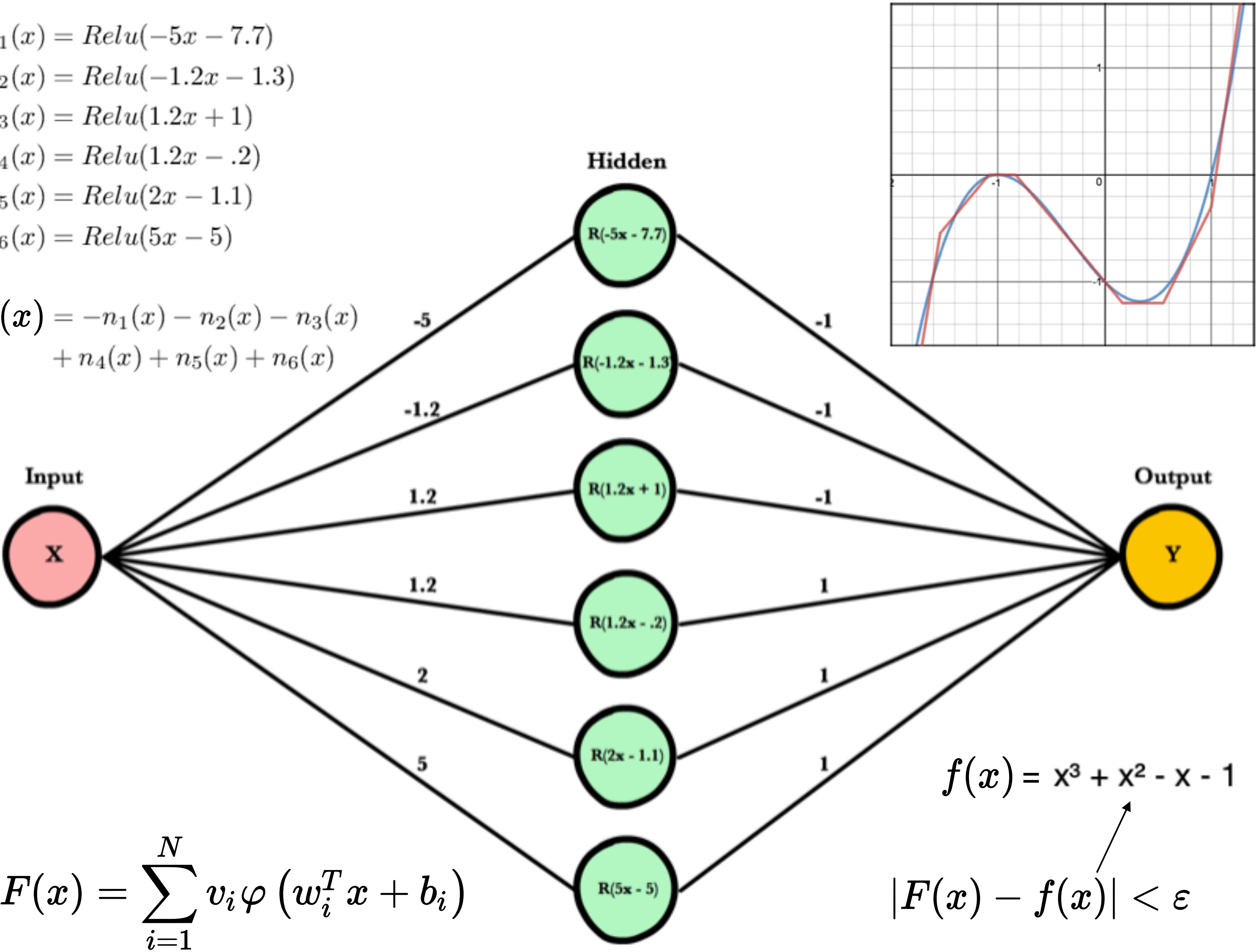
$$n_5(x) = Relu(2x - 1.1)$$

$$n_6(x) = Relu(5x - 5)$$

$$F(x) = -n_1(x) - n_2(x) - n_3(x) + n_4(x) + n_5(x) + n_6(x)$$

$$n_1(x) = Relu(-5x - 7.7)$$
$$n_2(x) = Relu(-1.2x - 1.3)$$
$$n_3(x) = Relu(1.2x + 1)$$
$$n_4(x) = Relu(1.2x - .2)$$
$$n_5(x) = Relu(2x - 1.1)$$
$$n_6(x) = Relu(5x - 5)$$

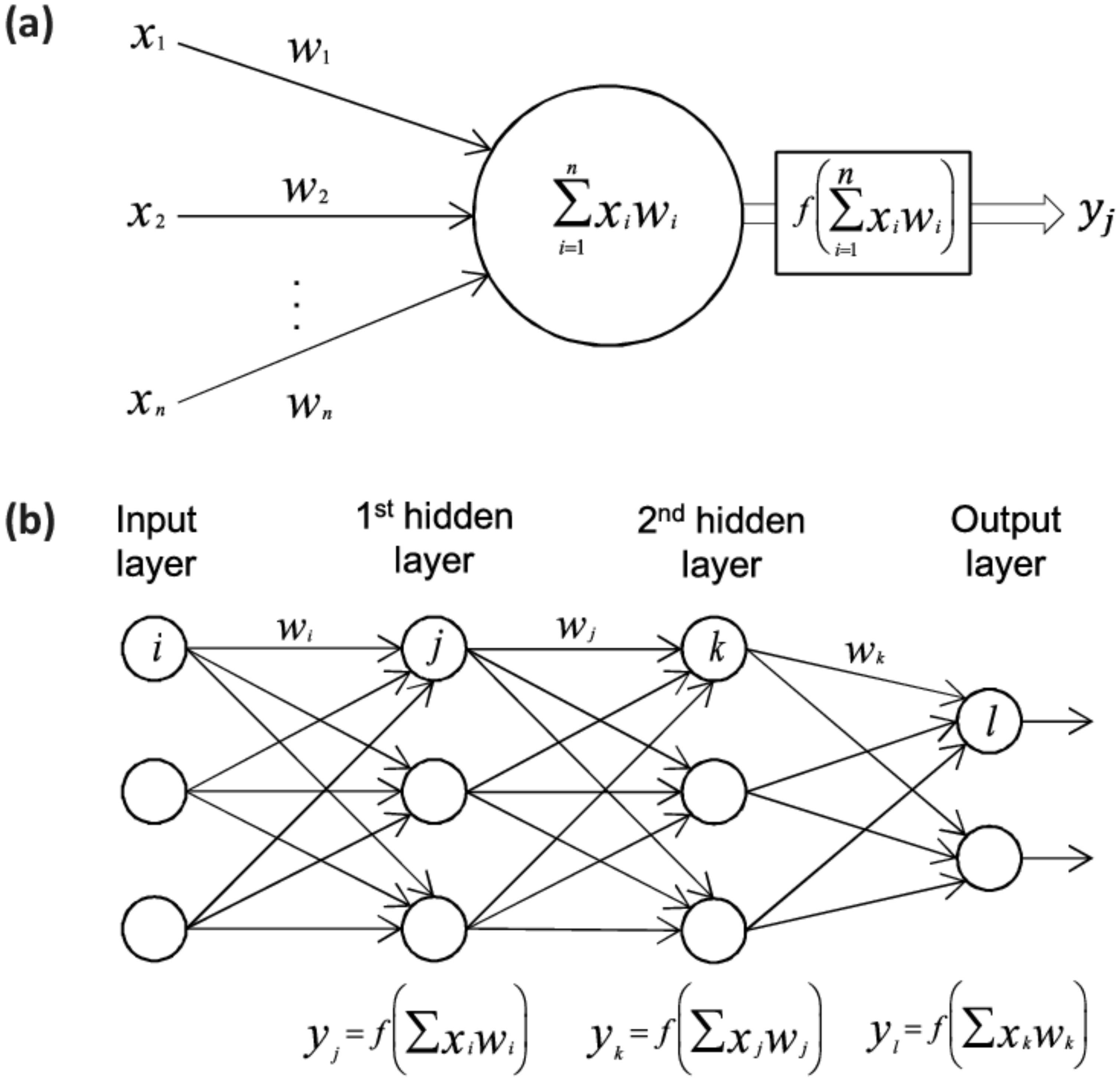
$$F(x) = -n_1(x) - n_2(x) - n_3(x) + n_4(x) + n_5(x) + n_6(x)$$



$f(x)$ = x³ + x² - x - 1

$$F(x) = \sum_{i=1}^{N} v_i \varphi\left(w_i^T x + b_i\right)$$

$$|F(x) - f(x)| < \varepsilon$$


(a)
x_1
w_1
x_2
w_2
x_n
w_n
$\sum_{i=1}^{n} x_i w_i$
$f\left(\sum_{i=1}^{n} x_i w_i\right)$
y_j
(b)
Input layer
1st hidden layer
2nd hidden layer
Output layer
i
w_i
j
w_j
k
w_k
l
$y_j = f\left(\sum x_i w_i\right)$
$y_k = f\left(\sum x_j w_j\right)$
$y_l = f\left(\sum x_k w_k\right)$

Physical Qubits

- Photon polarization
- Trapped ions
- Cold atoms
- Nuclear magnetic resonances: spin of nuclei
- Quantum dots
- Defect qubits
- Superconductors

Quantum versions of simple classical gates

Let $b_0, b_1 \in \{0,1\}$ (binary variables)

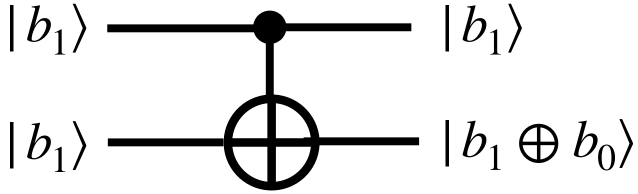
NOT

already reversible

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

XOR

b_1	b_0	b_1 XOR b_0
0	0	0
0	1	1
1	0	1
1	1	0



$$\begin{aligned}
|00\rangle &\longrightarrow |0\ 0 \oplus 0\rangle = |00\rangle \\
|01\rangle &\longrightarrow |0\ 1 \oplus 0\rangle = |01\rangle \\
|10\rangle &\longrightarrow |1\ 1 \oplus 0\rangle = |11\rangle \\
|11\rangle &\longrightarrow |1\ 1 \oplus 1\rangle = |10\rangle
\end{aligned}$$

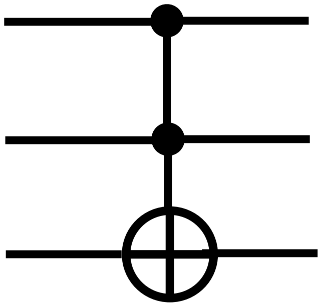
AND

b_1	b_0	b_1 AND b_0
0	0	0
0	1	0
1	0	0
1	1	1

Impossible to perform a reversible AND operation with two bits.

Quantum versions of simple classical gates

- Toffoli gate = T = CCX = CCNOT = Controlled-controlled NOT gate



$$\begin{array}{lcl}
|000\rangle & \longrightarrow & |000\rangle \\
|001\rangle & & \\
|010\rangle & & \\
|011\rangle & & \\
\hdashline
|100\rangle & & \\
|101\rangle & & \\
\hdashline
|110\rangle & \longrightarrow & |111\rangle \\
|111\rangle & & |110\rangle
\end{array}$$

$$T = \left(\begin{array}{cccc:cccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
\hdashline
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{array}\right) = \left(\begin{array}{c:c} I & 0 \\ \hdashline 0 & \mathrm{CNOT} \end{array}\right)$$

$$T\,|b_1\,b_0\,0\rangle = |b_1\,b_0\,b_1 \wedge b_0\rangle$$

$$T\,|b_1\,b_0\,1\rangle = |b_1\,b_0\,1 \oplus b_1 \wedge b_0\rangle$$

$\wedge =$ classical AND $\qquad \sim\, =$ NOT

- Toffoli gate T can be used to construct a complete set of Boolean connectives (NOT, AND, XOR, NAND)

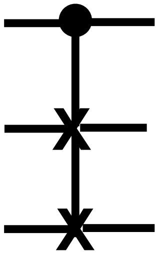
$$T\,|1\,1\,x\rangle = |1\,1\;\sim x\rangle$$

$$T\,|x\,y\,0\rangle = |x\,y\,x \wedge y\rangle$$

$$T\,|1\,x\,y\rangle = |1\,x\,x \oplus y\rangle$$

$$T\,|x\,y\,1\rangle = |x\,y\;\sim (x \wedge y)\rangle$$

- Alternative: Fredkin gate F=controlled SWAP



$$F\,|x\,0\,1\rangle = |x\,x\;\sim x\rangle$$

$$F\,|x\,y\,1\rangle = |x\,(y \vee x)\,y \vee (\sim x)\rangle$$

$$F\,|x\,0\,y\rangle = |x\,(y \wedge x)\,y \wedge (\sim x)\rangle$$