Basics of Quantum Computing

Edoardo Charbon
EPFL
edoardo.charbon@epfl.ch

December 1st, 2017

Outline

- Introduction
- The quantum bit
- 1-qubit quantum gates
- Measuring qubits
- 2-qubit quantum gates
- Quantum Fourier transform & quantum arithmetic
- Examples of a quantum algorithm
- Future challenges

Introduction

Quantum Computing

A computation is a physical process. It may be performed by a piece of electronics or on an abacus, or in your brain, but it is a process that takes place in nature and as such it is subject to the laws of physics.

Quantum computers are machines that rely on characteristically quantum phenomena, such as quantum interference and quantum entanglement in order to perform computation.

– Artur Ekert

Overarching goal

Solve intractable problems with massive speedup in computation…

…using the superposition and entanglement, two of the cornerstones quantum mechanics

The 2012 Nobel Prize

Serge Haroche David Wineland

2012 Physics Nobel Prize

Both Laureates work in the field of quantum optics studying the fundamental interaction between light and matter, a field which has seen considerable progress since the mid-1980s. Their ground-breaking methods have enabled this field of research to take the very first steps towards building a new type of super fast computer based on quantum physics. Perhaps the quantum computer will change our everyday lives in this century in the same radical way as the classical computer did in the last century.

–Announcement 2012 Nobel Prize

Status of Quantum Algorithms

math.nist.gov/quantum/zoo/

Quantum Algorithm Zoo

This is a comprehensive catalog of quantum algorithms. If you notice any errors or omissions, please email me at stephen.jordan@nist.gov. Your help is appreciated and will be acknowledged.

Algebraic and Number Theoretic Algorithms

Algorithm: Factoring
Speedup: Superpolynomial
Description: Given an *n*-bit integer, find the prime factorization. The quantum algorithm of Peter Shor solves this in poly(*n*) time [82,125]. The fastest known classical algorithm requires time superpolynomial in *n*. Shor's algorithm breaks the RSA cryptosystem. At the core of this algorithm is order finding, which can be reduced to the Abelian hidden subgroup problem.

Algorithm: Discrete-log
Speedup: Superpolynomial
Description: We are given three *n*-bit numbers *a*, *b*, and *N*, with the promise that $b = a^s \mod N$ for some *s*. The task is to find *s*. As shown by Shor [82], this can be achieved on a quantum computer in poly(*n*) time. The fastest known classical algorithm requires time superpolynomial in *n*. By similar

~50 algorithms with quantum speedup, but most people know 2.

The Quantum Hype

Google

News Startups Mobile Gadgets Enterprise Social Trending Apple Google Fac

Google AI quantum computing

Google Partners With UCSB To Build Quantum Processors For Artificial Intelligence

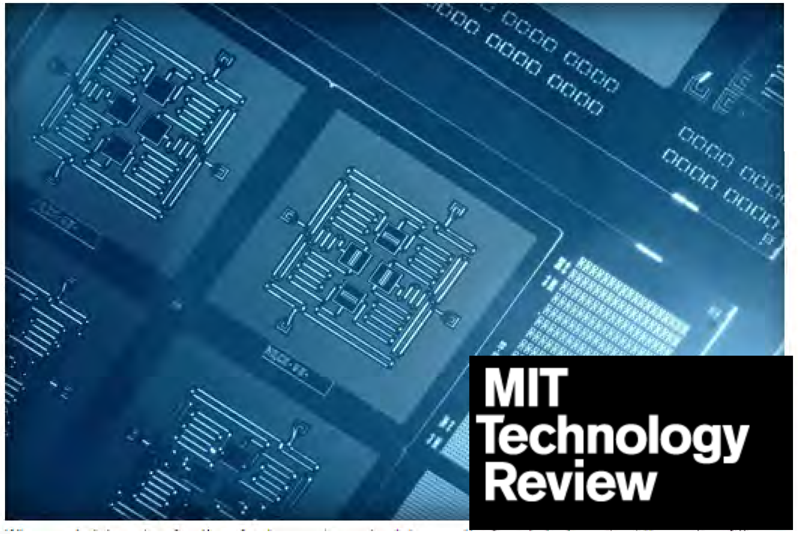
Posted Sep 2, 2014 by Frederic Lardinois (@fredericl)

2,888 SHARES

IBM Shows Off a Quantum Computing Chip

A new superconducting chip made by IBM demonstrates a technique crucial to the development of quantum computers.

By Tom Simonite on April 29, 2015

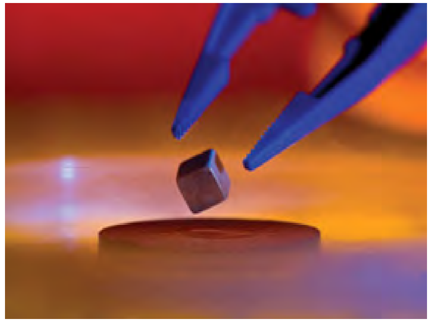


Microsoft

QuArC at Microsoft Research Station Q @ UCSB

The Quantum Hype

Some of the Proposed Applications



Energy

Room-temperature superconductivity

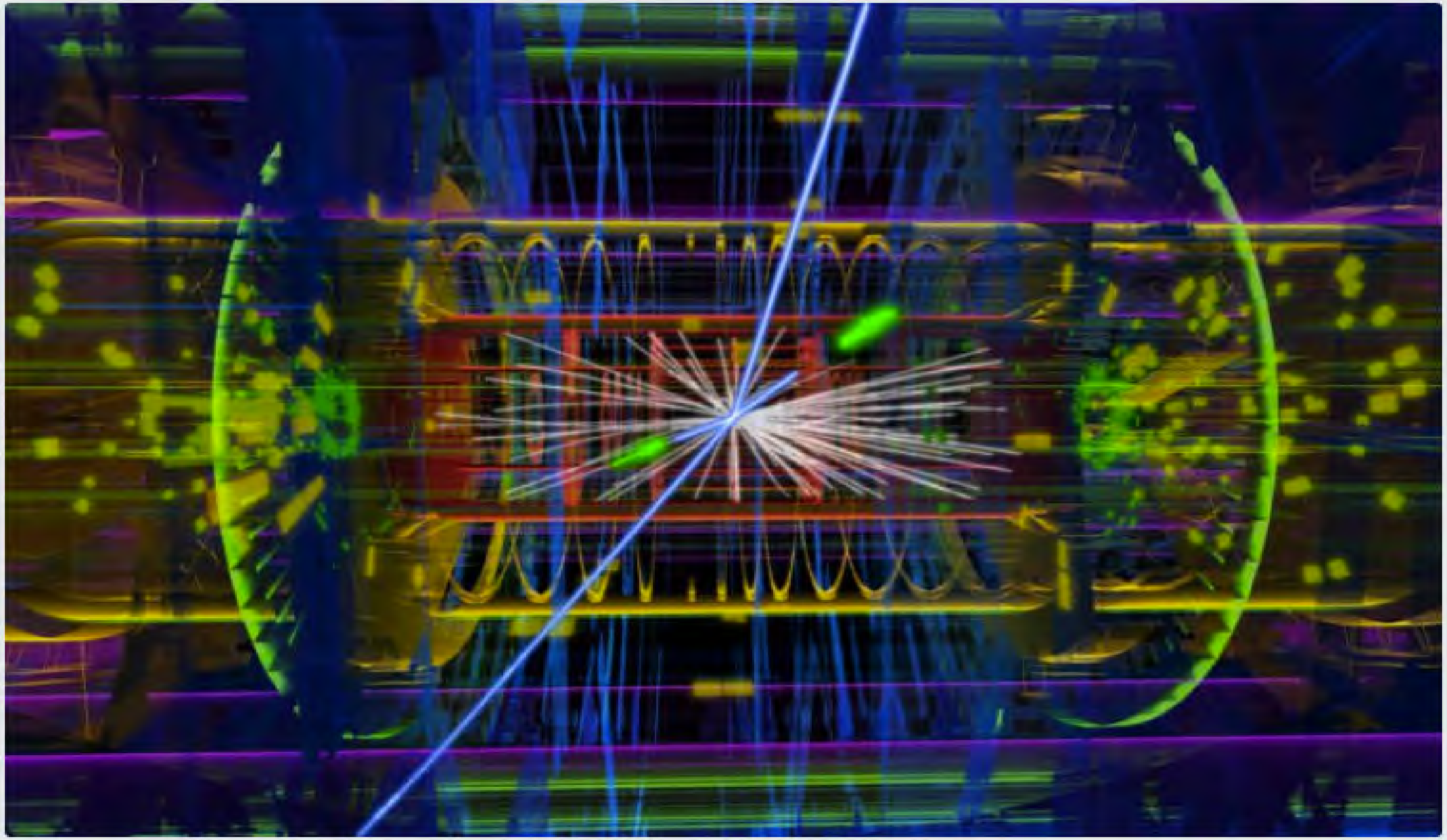
Health

Quantum chemistry

Internet Security

Source: L. Vandersypen, ISSCC 2017

Recent News



OCT 26, 2017

Ars Technica: Higgs Boson Uncovered By Quantum Algorithm On D-Wave Machine

What is D-Wave

The Quantum Bit

Also known as qubit

Definition

- A quantum bit or qubit is a quantum system in which the Boolean states 0 and 1 are represented by a pair of mutually orthogonal quantum states labeled as |0> and |1>.
- Superposition of states is represented as follows

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

- $\alpha_0, \alpha_1 \in C$ — α_i is a probability amplitude
- $|\alpha_0|^2 + |\alpha_1|^2 = 1$ — $|\alpha_i|^2$ Is the probability of finding the qubit in state $|i\rangle$ when you measure it.

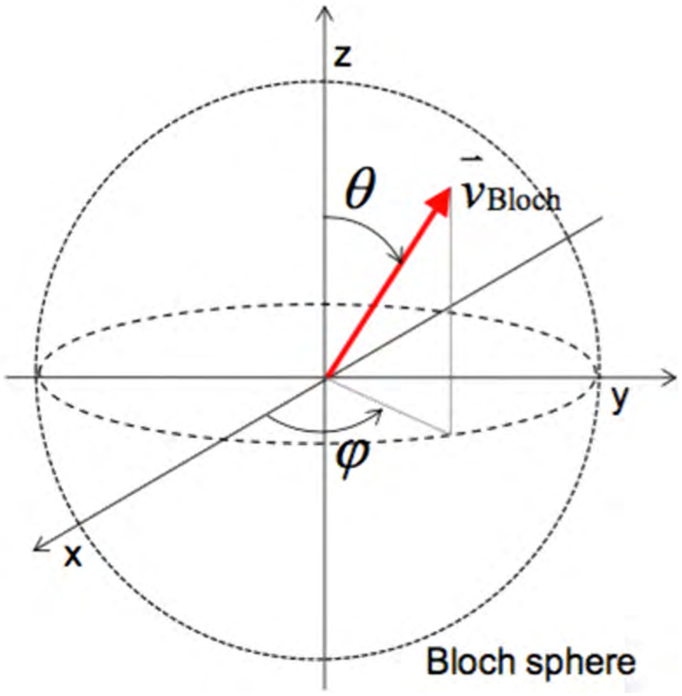
Bloch Sphere

- $\alpha_0, \alpha_1 \in C$
- $|\alpha_0|^2 + |\alpha_1|^2 = 1$

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

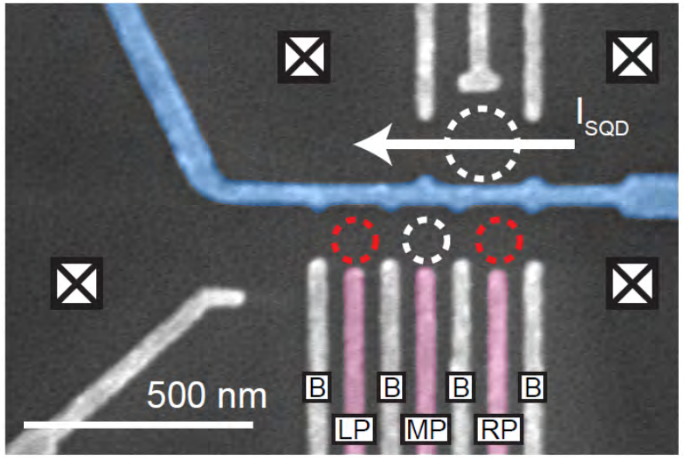
θ is polar angle

φ is azimuthal angle

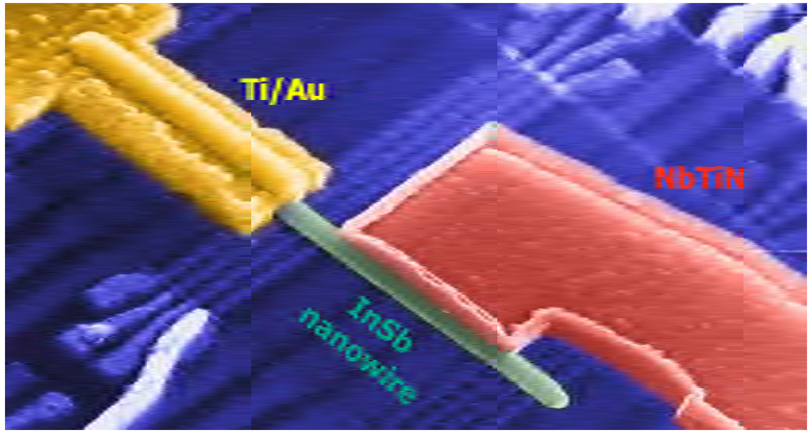


- A single qubit is represented in three dimensions
- X,Y,Z axes represent possible projections for qubit readout
- The x-y plane is important – see its importance later

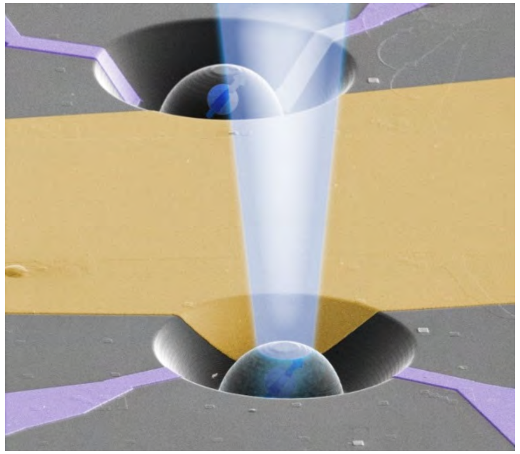
Qubit Implementations



Semiconductor quantum dots



Semiconductor-superconductor hybrids


Impurities in diamond

- ☐ Different substrates make them more or less amenable to integration in standard processes
- ☐ Different dimensions make them more or less scalable to large arrays
- ☐ *Readout techniques make them compatible with classical electronics resp. electro-optics techniques*

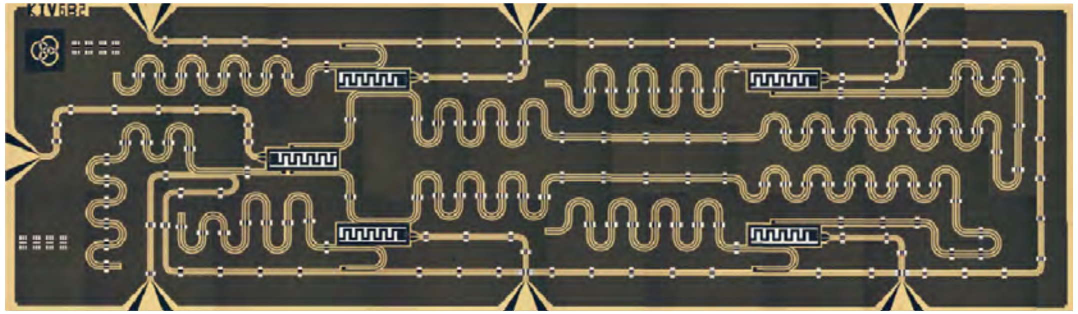

Superconducting circuits

Image source: L. Vandersypen, 2017

Salient Properties of Qubits

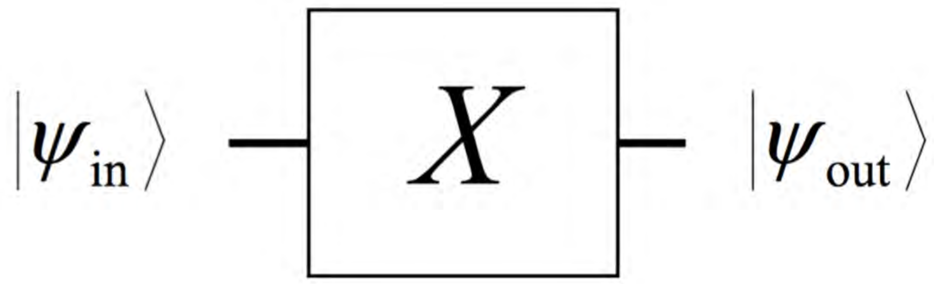
- Coherence time................................μs – ms
- Fidelity of operations......................... 99-99.999%
- Miniaturization capability .... nm – mm
- Scalability...................................... 10^6 – 10^9

- Differentiating factor between technologies: **scalability** to large arrays, implying requirements on
  - Size/pitch of qubits
  - Yield
  - Reliability
  - Coherence
  - Control

DiVincenzo Criteria for Quantum Computing

1. A scalable physical system with well characterized qubits.
2. The ability to initialize the state of the qubits to a simple fiducial state.
3. Long relevant decoherence times.
4. A “universal” set of quantum gates.
5. A qubit-specific measurement capability.
6. The ability to interconvert stationary and flying qubits.
7. The ability to faithfully transmit flying qubits between specified locations.

1-Qubit Quantum Gates



Notations

$$|0\rangle \doteq \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle \doteq \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi\rangle \doteq \alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

Recall:

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

- $\alpha_0, \alpha_1 \in C$ — α_i is a probability amplitude
- $|\alpha_0|^2 + |\alpha_1|^2 = 1$ — $|\alpha_i|^2$ Is the probability of finding the qubit in state $|i\rangle$ when you measure it.

Normalization

A quantum state $|\psi\rangle \doteq \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ is nomalized iff $\langle\psi|\psi\rangle = 1$,

$$\langle\psi|\psi\rangle = \begin{pmatrix} \alpha_0^* & \alpha_1^* \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \alpha_0\alpha_0^* + \alpha_1\alpha_1^* = |\alpha_0|^2 + |\alpha_1|^2$$

- Note:

  $\langle\psi|\psi\rangle$: self inner product or self overlap

Orthogonality

Two quantum states $|\psi\rangle \doteq \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ and $|\psi'\rangle \doteq \begin{pmatrix} \alpha_0^{'} \\ \alpha_1^{'} \end{pmatrix}$

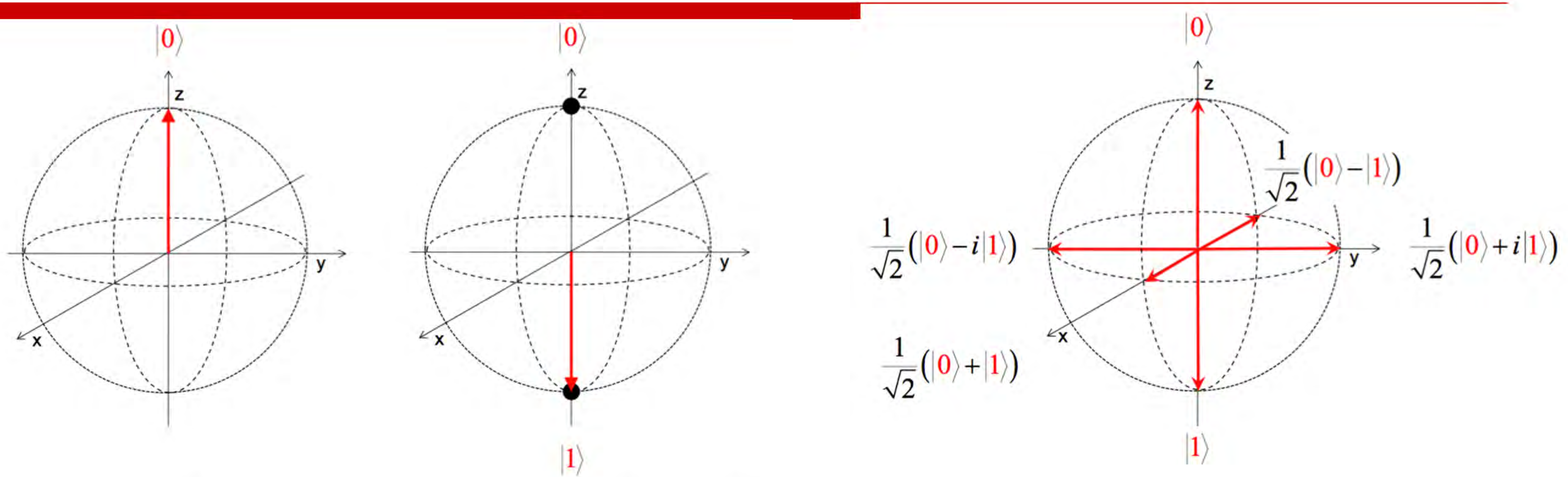
are mutually othogonal iff $\langle\psi|\psi'\rangle = \begin{pmatrix} \alpha_0^* & \alpha_1^* \end{pmatrix} \begin{pmatrix} \alpha_0^{'} \\ \alpha_1^{'} \end{pmatrix}$

$= \alpha_0^* \alpha_0^{'} + \alpha_1^* \alpha_1^{'} = 0$

- Note:

  $\langle\psi|\psi'\rangle$: inner product or overlap

Qubit States on Bloch Sphere



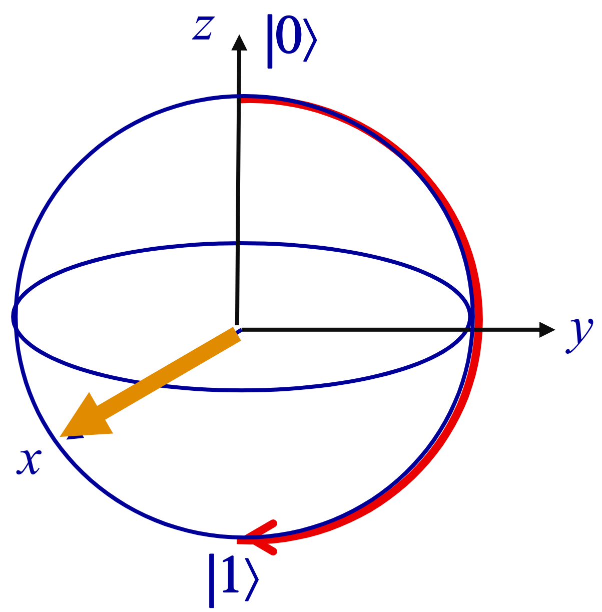
- Vectorial representation: up = |0>, down = |1>
- X-Y plane: ***maximum superposition*** state
  - Clifford or stabilizer states
  - Used for maximum parallelism

1-Qubit Gate

- When a gate is used the qubit is transformed and the result is *deterministic*
- This remains the case until it is read out
- A 1-qubit gate will rotate the qubit in the Bloch sphere

- Example:

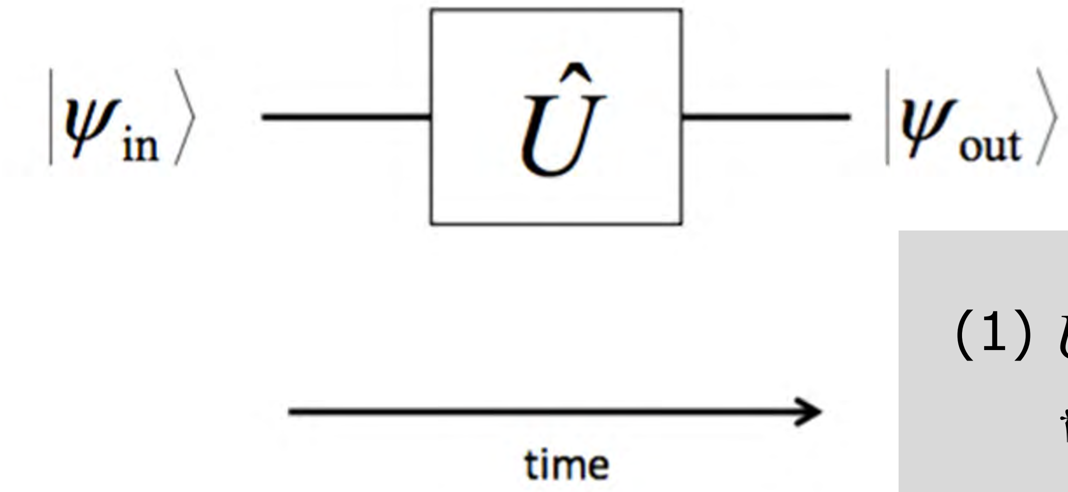
$$|\psi_{in}\rangle \; -\boxed{X}- \; |\psi_{out}\rangle$$



- This is a π-rotation wrt X axis

Unitary Transform

- A unitary transformation is a specific ***rotation*** on the Bloch sphere where condition (1) is satisfied
- Note that a transform requires ***time*** to be executed

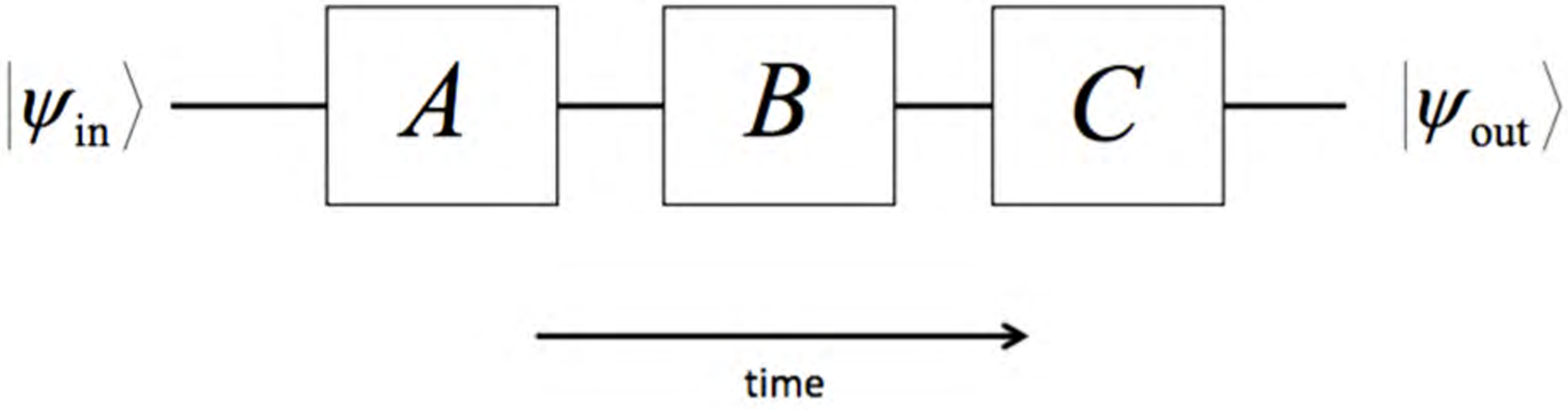


(1) $\hat{U}$ is a unitary operator when: $\hat{U}\hat{U}^{\dagger} = \hat{U}^{\dagger}\hat{U} = \hat{I}$

† = conjugate and transpose

Chain Transformations

- A chain transformations is written from left to right but mathematically from right to left
- The input is on the right and the output on the left!



$$|\psi_{out}\rangle = CBA|\psi_{in}\rangle$$

Standard Transformations

Identity	$-\boxed{I}-$	$\hat{I} \doteq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	
Pauli X	$-\boxed{X}-$	$\hat{X} \doteq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	also denoted σ_x
Pauli Y	$-\boxed{Y}-$	$\hat{Y} \doteq \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	also denoted σ_y
Pauli Z	$-\boxed{Z}-$	$\hat{Z} \doteq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	also denoted σ_z

Some properties: $\hat{X} = \hat{X}^\dagger$ hermitian

$\hat{X}\hat{X}^\dagger = \hat{Y}\hat{Y}^\dagger = \hat{Z}\hat{Z}^\dagger = \hat{I}$ unitary

You'll check some of these in Hwk #1!

$\hat{X}\hat{Y} = i\hat{Z} \quad \hat{Y}\hat{X} = -i\hat{Z}$

definition

$[A,B] \equiv AB - BA$

$[\hat{X},\hat{Y}] = 2i\hat{Z},\ [\hat{Z},\hat{X}] = 2i\hat{Y},\ [\hat{Y},\hat{Z}] = 2i\hat{X}$

$\{A,B\} \equiv AB + BA$

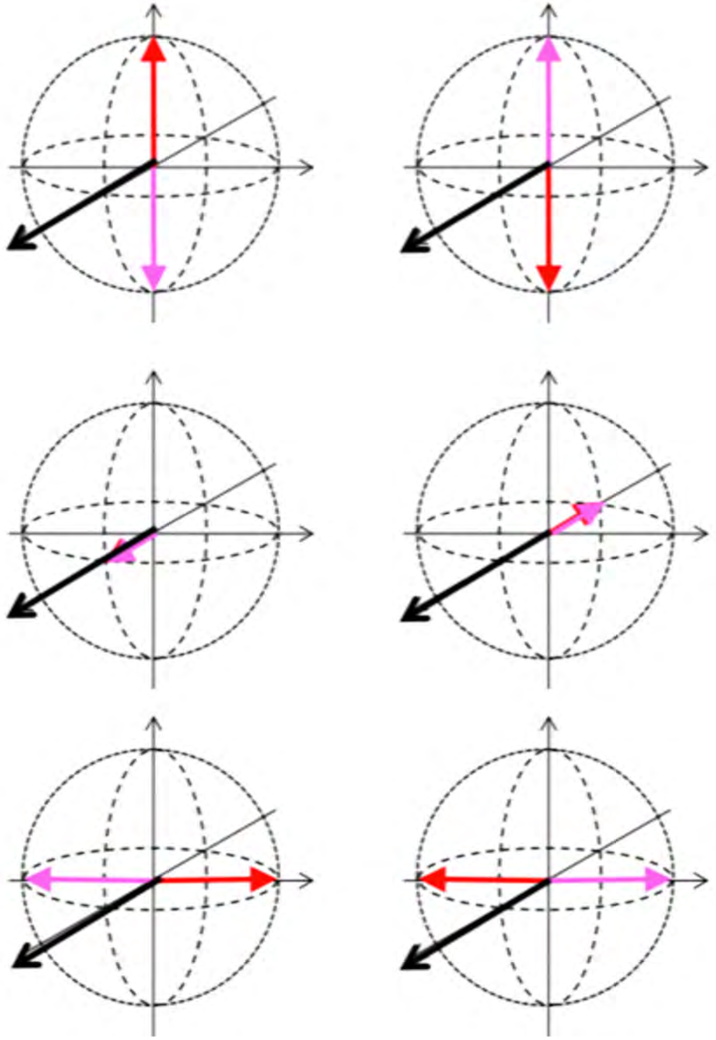
$\{\hat{X},\hat{Y}\} = \{\hat{Z},\hat{X}\} = \{\hat{Y},\hat{Z}\} = 0$

Source:
Leo DiCarlo

X-Rotation Examples

$|\psi\rangle$ —[X]— $|\psi\rangle$

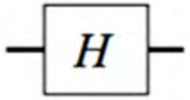
	X	
$\lvert 0\rangle$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\lvert 1\rangle$
$\lvert 1\rangle$		$\lvert 0\rangle$
$\lvert 0\rangle + \lvert 1\rangle$		$+1(\lvert 0\rangle + \lvert 1\rangle)$
$\lvert 0\rangle - \lvert 1\rangle$		$-1(\lvert 0\rangle - \lvert 1\rangle)$
$\lvert 0\rangle + i\lvert 1\rangle$		$i(\lvert 0\rangle - i\lvert 1\rangle)$
$\lvert 0\rangle - i\lvert 1\rangle$		$-i(\lvert 0\rangle + i\lvert 1\rangle)$



Source:
Leo DiCarlo

Hadamard Gate

Hadamard*



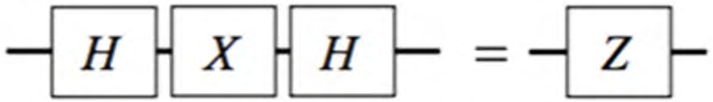
$$\hat{H} \doteq \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

properties: $H = H^{\dagger}$

$$H^2 = I$$

exercise: show $\hat{H}\,\hat{X}\,\hat{H} = \hat{Z}$

$$\hat{H}\,\hat{Z}\,\hat{H} = \hat{X}$$



Source:
Leo DiCarlo

Hadamard Gate

$|\psi\rangle$ — $\boxed{H}$ — $|\psi\rangle$

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

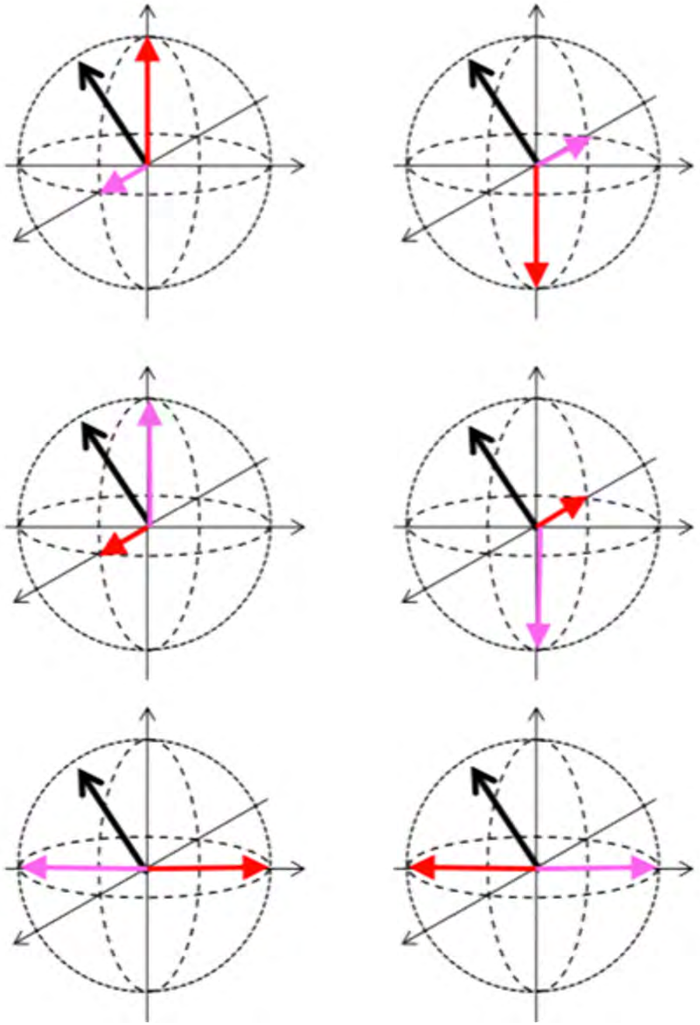
$|1\rangle \quad |0\rangle - |1\rangle$

$|0\rangle + |1\rangle \quad |0\rangle$

$|0\rangle - |1\rangle \quad |1\rangle$

$|0\rangle + i|1\rangle \quad e^{i\pi/4}\left(|0\rangle - i|1\rangle\right)$

$|0\rangle - i|1\rangle \quad e^{-i\pi/4}\left(|0\rangle - i|1\rangle\right)$

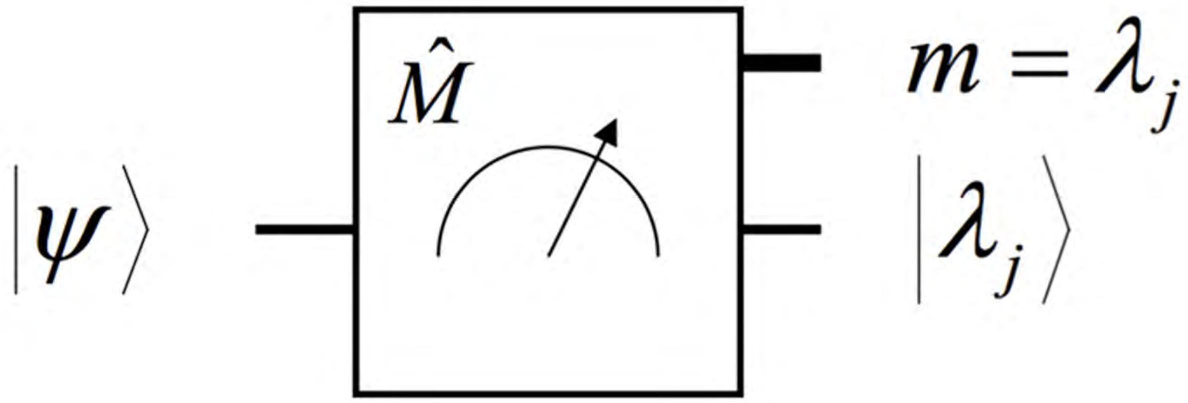


Source:
Leo DiCarlo

Measuring Qubits

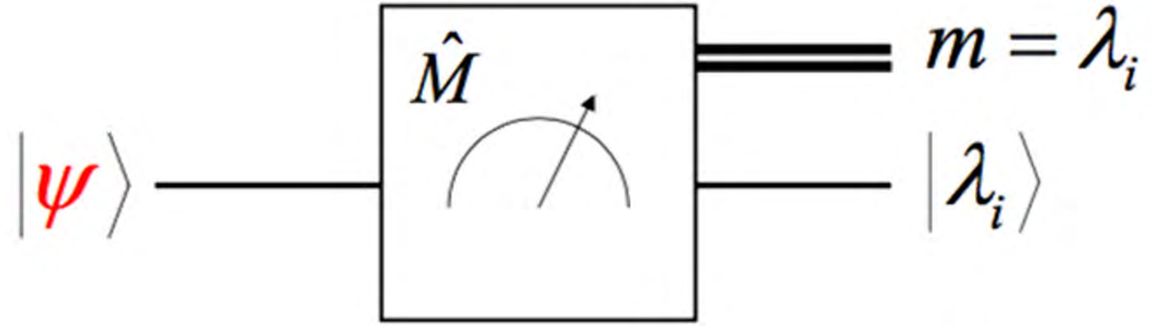
The Concept

- We need to understand how to measure a qubit
- When a qubit in the Bloch sphere is read its wavefunction is collapsed and a *probabilistic* measurement results from the measurement
- Note that up to measurement, the state is deterministic!



The Concept (2)

- Every measurement is associated with an operator $\hat{M}$ called hermitian operator.
- The eigenvalues λ_i of the hermitian.
- Post-measurement state of the qubit is $|\lambda_i>$ the eigenstate of the hermitian.
- The probability of the result being λ_i is computed as $|<\lambda_j|\psi>|^2$ the squared overlap between input state and eigenstate.

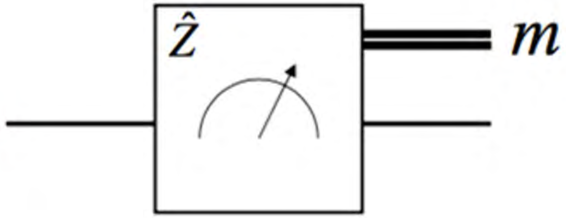


with probability $\left|\langle \lambda_j | \psi \rangle\right|^2$

where $\hat{M}|\lambda_j\rangle = \lambda_j |\lambda_j\rangle$

Example

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$



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

$$\langle +1|\psi\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \alpha_0$$

$$\langle -1|\psi\rangle = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \alpha_1$$

eigenvalues $+1, \quad -1$

eigenvectors $|+1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |-1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

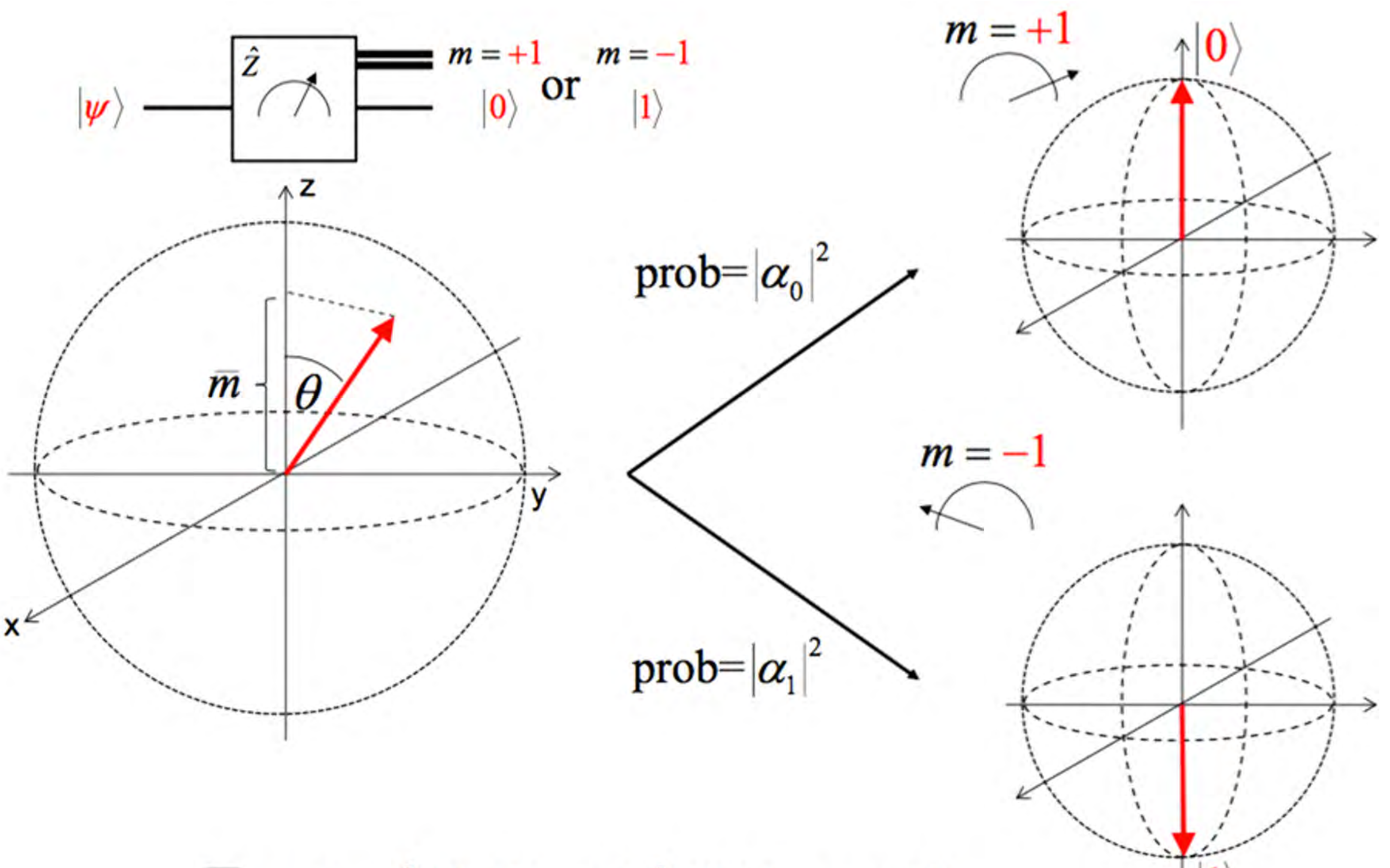
probabilities: $|\alpha_0|^2 \quad |\alpha_1|^2$

average:

$$\begin{aligned} \bar{m} &= +1|\alpha_0|^2 - 1|\alpha_1|^2 \\ &= \cos^2(\theta/2) - \sin^2(\theta/2) \\ &= \cos(\theta) \end{aligned}$$

Source:
Leo DiCarlo

Example (2)



$$\bar{m} = +1\cos^2(\theta/2) - 1\sin^2(\theta/2) = \cos(\theta)$$

2-Qubit Quantum Gates

2-Qubit States

- When we go from a single qubit to two qubits, we write the new ensemble, for instance, as

$$|0\rangle \rightarrow |0\rangle \otimes |1\rangle = |01\rangle$$

- With 2 qubits the possible states are $2^2=4$
- When superposition is achieved, then 4 states can occur simultaneously
- Example:
  - Suppose we had 100 qubits, then we would need $2^{100} = 1.26\times10^{30}$ states to fully describe the system
  - In superposition, these states would exist simultaneously

2-Qubit States

$$|\Psi\rangle = \alpha_{11}|11\rangle + \alpha_{10}|10\rangle + \alpha_{01}|01\rangle + \alpha_{00}|00\rangle \doteq \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

$$\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11} \in C$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

Global phase is not relevant.

- How to describe two-qubit system in a Bloch sphere?
  - Not possible
  - One needs an alternative representation
  - Try two Bloch spheres!

Entanglement: Definition

Two qubits in the state

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

are entangled if and only if (iff) they have nonzero *concurrence*

$$C(|\Psi\rangle) \equiv 2|\alpha_{00}\alpha_{11} - \alpha_{01}\alpha_{10}|$$

$$\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \qquad C = 1$$

$$\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \qquad C = 0$$

$$\frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle) \qquad C = 1$$

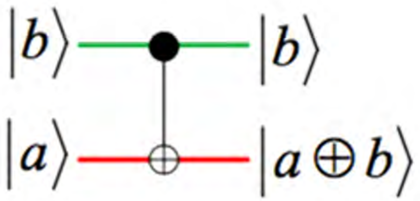
$$\frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |11\rangle) \qquad C = 2/3$$

Entanglement: Meaning & Effects

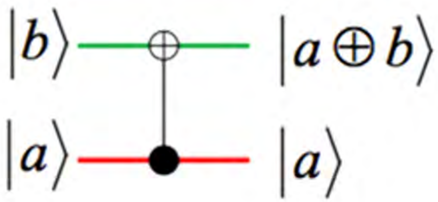
- If the state of one qubit is measured, then the state of the other qubit is also projected in the same way.
- Entanglement is used, besides quantum computing, in
  - Quantum key distribution (QKD) for secure communications
  - Quantum imaging for image quality improvement
  - Astronomy and astrophysics
  - Etc.
- Example:
  - Entanglement can inform sender (Bob) and receiver (Alice) of an attempt to tamper with information encoded in photons sent over an unsecure channel (by Eve)

2-Qubit Gates: C-NOT

Controlled-Not gates



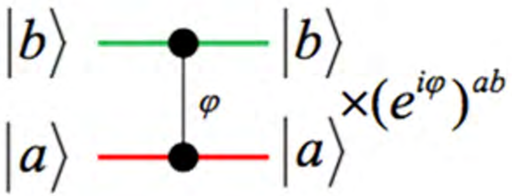
$$\begin{array}{cc} \begin{array}{cccc} |00\rangle & & & |11\rangle \end{array} & \\ \text{C-NOT}_{gr} \doteq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} & \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \end{array}$$



$$\text{C-NOT}_{rg} \doteq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

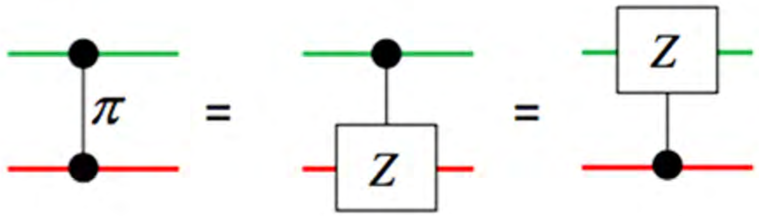
2-Qubit Gates: Controlled-Phase

Controlled-Phase



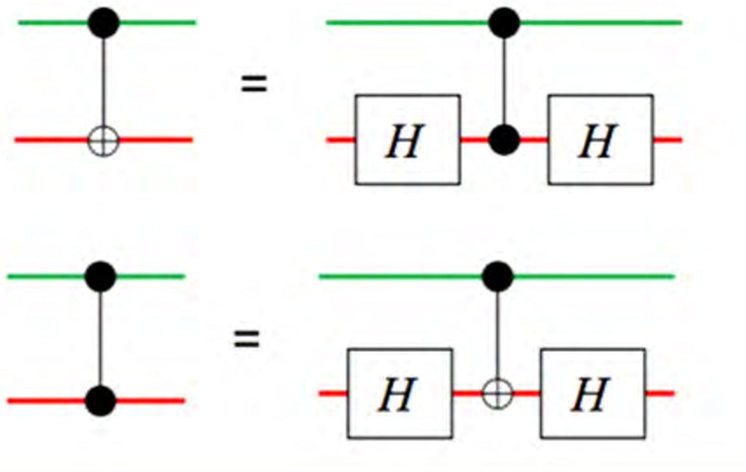
$$\mathrm{C-PHASE}_{\varphi} \doteq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{pmatrix}$$

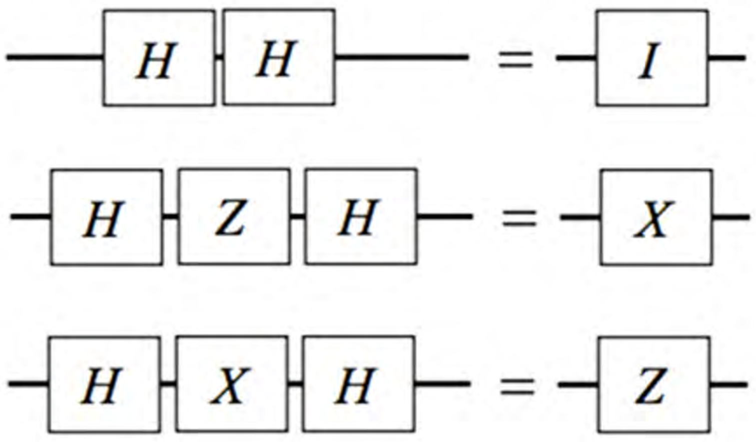
NOTE:
This gate has no equivalent in classical gates.



2-Qubit Gates: Important Properties

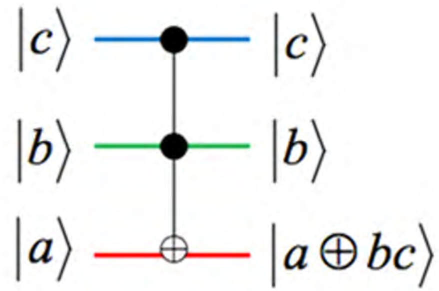
- C-NOT & one-qubit rotations are *universal*: ***any unitary operation on any number of qubits can be compiled into a quantum circuit using C-NOTs and one-qubit rotations***
- C-PHASE, C-PHASE+one-qubit-rotations are also universal
- C-NOT and controlled-phase can be interchanged by way of Hadamard transformations
- Note that a chain of Hadamard is the identity; other gates can also be collapsed





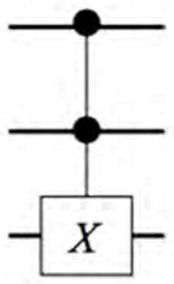
3-Qubit Gates: Toffoli Gate

- The Toffoli gate is a combination of C-NOT and control-phase gates
- Other names:
  - Controlled-Controlled-X (C-C-X)
  - Controlled-Controlled-Not (C-C-NOT)



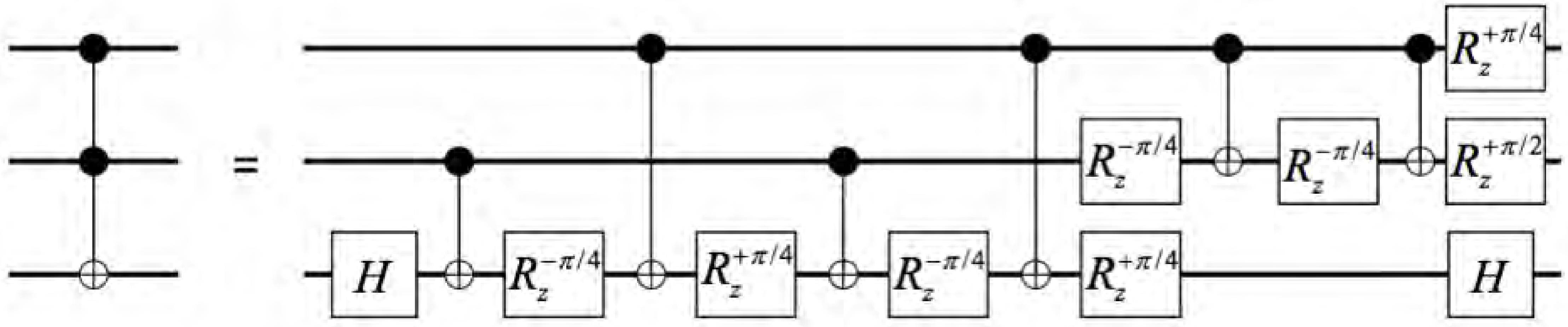
$$
\text{TOFFOLI} \doteq
\begin{array}{c}
\begin{array}{cccccccc} |000\rangle & & & \cdots & & & & |111\rangle \end{array} \\
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}
\end{array}
\begin{array}{c} |000\rangle \\ \\ \\ \vdots \\ \\ \\ |111\rangle \end{array}
$$

Alternative symbol:



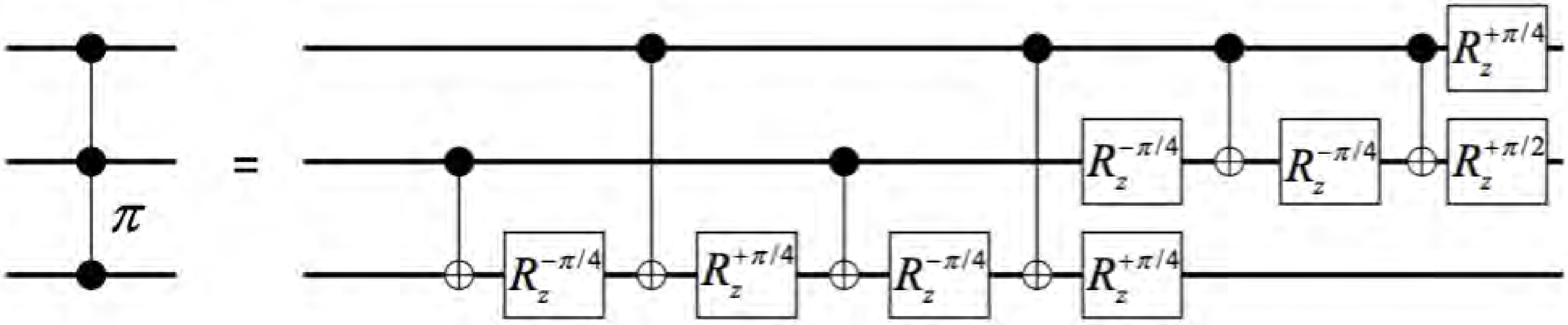
Toffoli Gate as 1- and 2-Qubit Gates

- The Toffoli gate can be decomposed in 1-qubit gates (Hadamard, +π/2, ±π/4) and 2-qubit gates (C-NOT)
- Below the decomposition is shown:



Another 3-qubit Gate: C-C-Phase

- C-C-phase gate can be decomposed in 1-qubit gates (Hadamard, +π/2, ±π/4) and 2-qubit gates (C-NOT)
- Below the decomposition is shown:



Quantum Fourier Transform

Quantum FT

$$|\Psi_{out}\rangle = \left(\frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \sum_{k=0}^{N-1} e^{\frac{i2\pi lk}{N}} |l\rangle\langle k| \right) |\Psi_{in}\rangle$$

$$\alpha_l' = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{i2\pi lk}{N}} \alpha_k$$

N=2

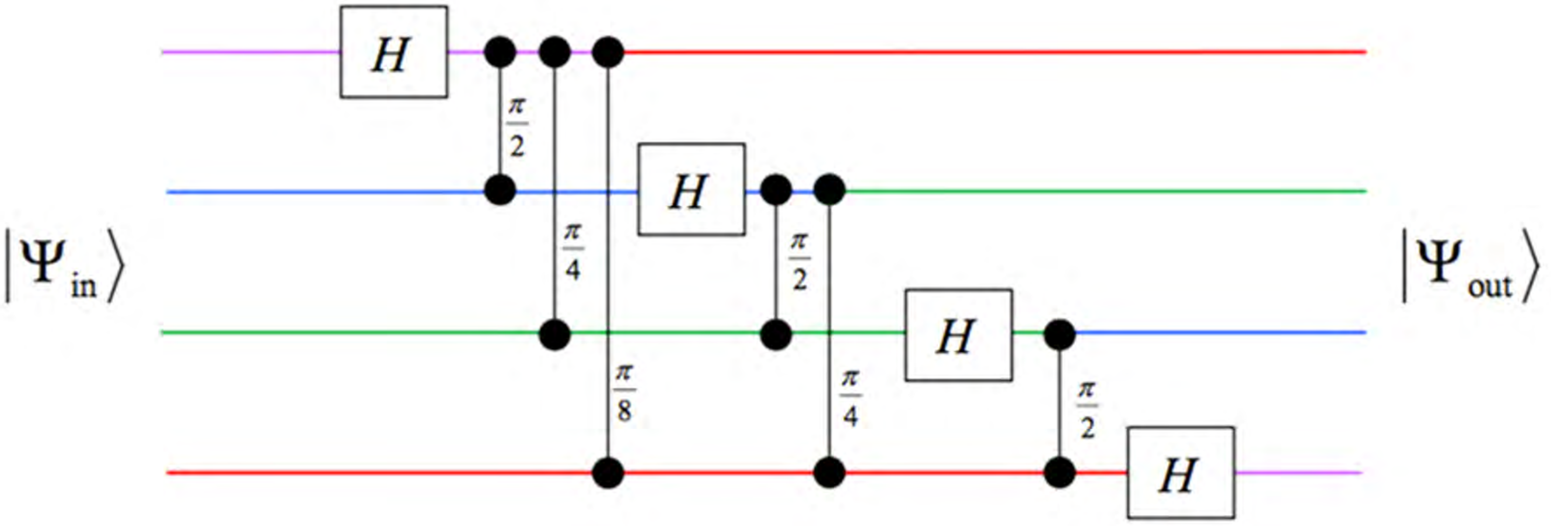
$$U_{QFT} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H$$

N=4

$$U_{QFT} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & +i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & +i \end{pmatrix}$$

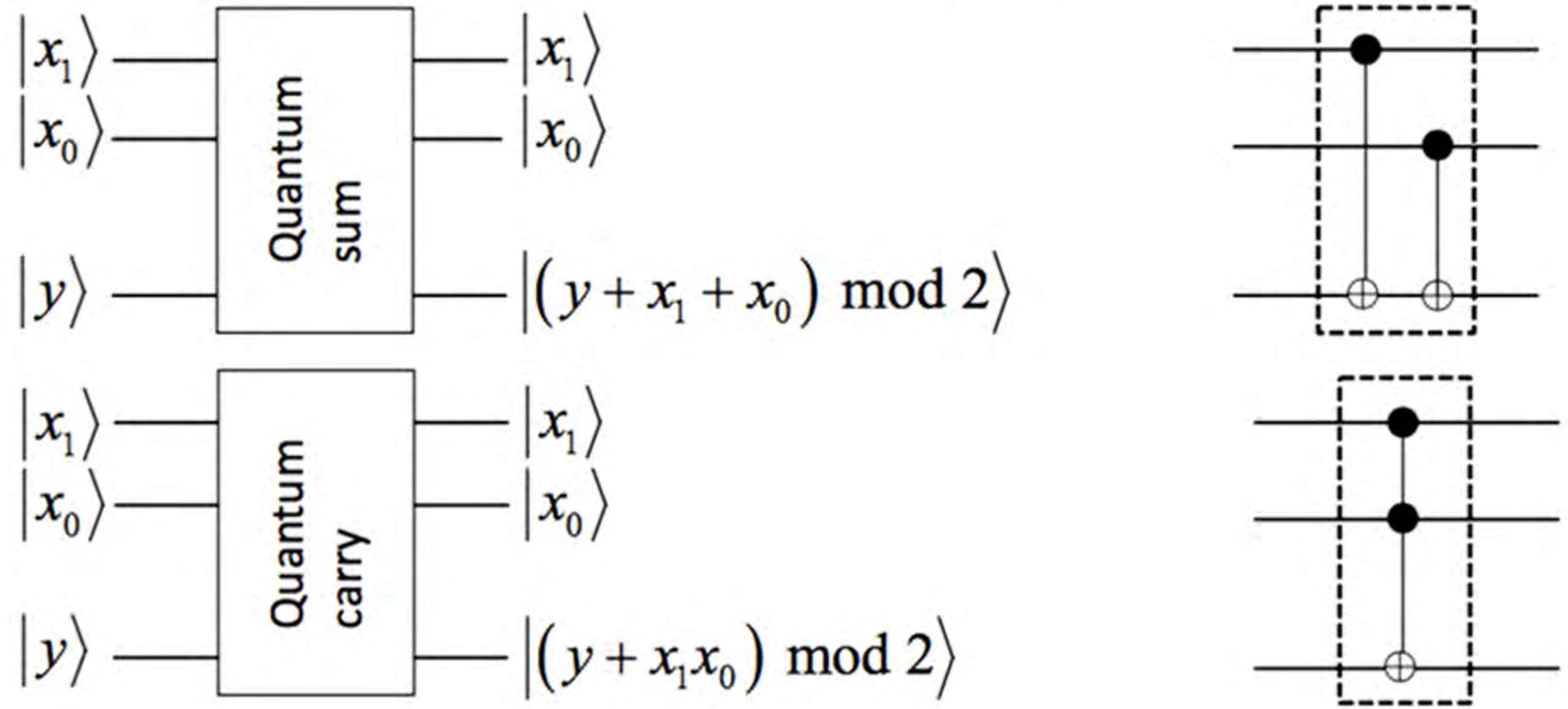
Quantum FT (2)

- Complexity: $O(n^2)$ since it requires $n(n+1)/2$ gates.
- Below is a re-write of the QFT based on Hadamard and rotation gates
- One can prepare all the qubits in superposition state so as to achieve FT of all variables in one shot (quantum parallelism)



Example: Quantum Arithmetic

- Quantum equivalents of conventional arithmetic modulo 2 can be implemented from basic 2-qubit gates
- Examples of quantum sum & carry are shown here:



Examples of a Quantum Algorithm

Steps to Run a Quantum Algorithm

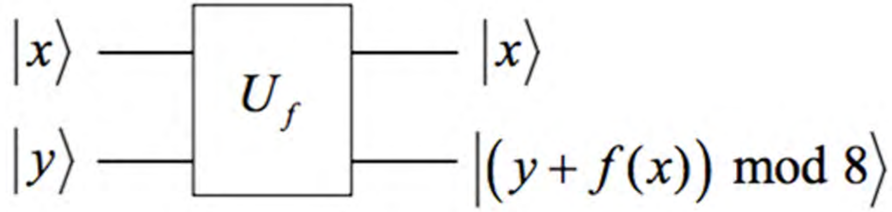
1. Prepare qubits in maximal superposition
2. Encode a function in a unitary using 1- and 2-qubit gates
3. Process
4. Measure

Note that ***entanglement*** and ***disentanglement*** between qubits is reuired in steps (2) and (3)

Note that during the whole process (except measurement), we need to ensure ***quantum coherence***!

Encoding a Boolean Function

$f(x) = x^2 \bmod 8,$
with
$x = x_1 x_0$ a 2-bit number

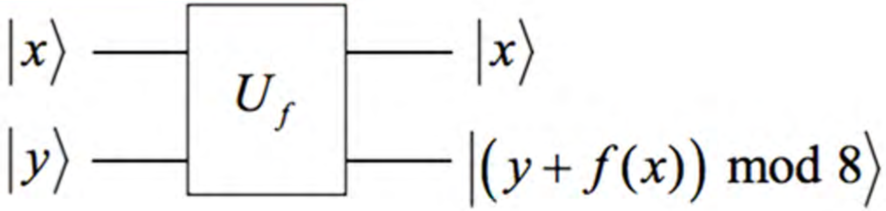


$$
\begin{array}{cccc}
 & & x_1 & x_0 \\
\times & & x_1 & x_0 \\
\hline
 & & x_1 x_0 & x_0 \\
+ & x_1 & x_1 x_0 & 0 \\
\hline
 & x_1 x_0 \oplus x_1 & 0 & x_0 \\
\hline
 & x_1 \overline{x}_0 & 0 & x_0
\end{array}
$$

Source:
Leo DiCarlo

Encoding a Boolean Function (2)

$$f(x) = x^2 \text{ mod } 8,$$
$$\text{with } x \in \{0,1\}^{\otimes 2}$$



$$\begin{array}{cccc} & x_1\bar{x}_0 & 0 & x_0 \\ + & y_2 & y_1 & y_0 \\ \hline & x_0 y_0 y_1 \oplus x_1 \bar{x}_0 \oplus y_2 & x_0 y_0 \oplus y_1 & x_0 \oplus y_0 \end{array}$$

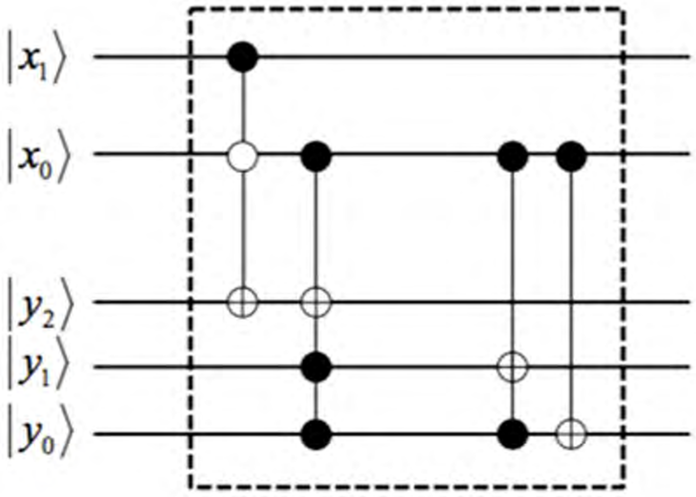
So we need a circuit that implements the unitary transformation:

$$x_1 \longrightarrow x_1$$
$$x_0 \longrightarrow x_0$$
$$y_2 \longrightarrow x_0 y_0 y_1 \oplus x_1 \bar{x}_0 \oplus y_2$$
$$y_1 \longrightarrow x_0 y_0 \oplus y_1$$
$$y_0 \longrightarrow x_0 \oplus y_0$$

Source:
Leo DiCarlo

Encoding a Boolean Function (3)

$$x_1 \longrightarrow x_1$$
$$x_0 \longrightarrow x_0$$
$$y_2 \longrightarrow x_0 y_0 y_1 \oplus x_1 \bar{x}_0 \oplus y_2$$
$$y_1 \longrightarrow x_0 y_0 \oplus y_1$$
$$y_0 \longrightarrow x_0 \oplus y_0$$



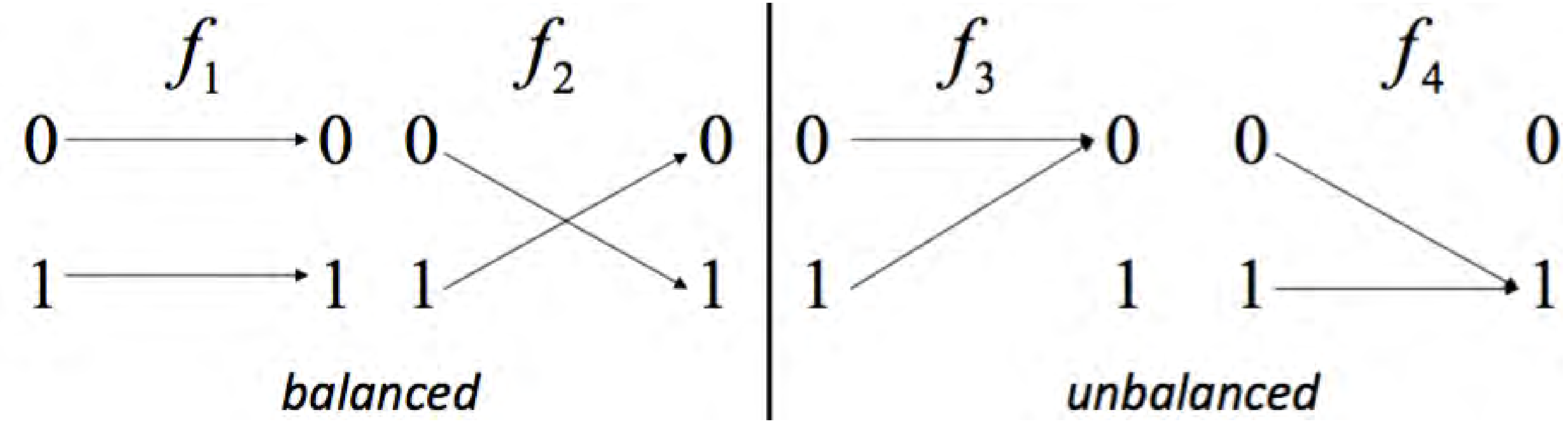
Source:
Leo DiCarlo

Other Famous Algorithms

- Deutsch problem and quantum/classical solution
  - for solving inverse problems
- Grover's quantum algorithm
  - for sorting and other problems
- Shor's algorithm
  - for prime decomposition
  - This algorithm could put RSA encryption out of commission (or at least require major changes to the RSA mechanism)

Deutsch Problem

- **Classical version:** you are given a black box with two Boolean inputs and 4 possible functions. You need to find which one it is.
- **Quantum version:** you are given a black box with one of the 4 functions encoded in a Unitary. You need to find which function has been encoded.
- All possible functions are shown here:



BUF INV NAND NOR

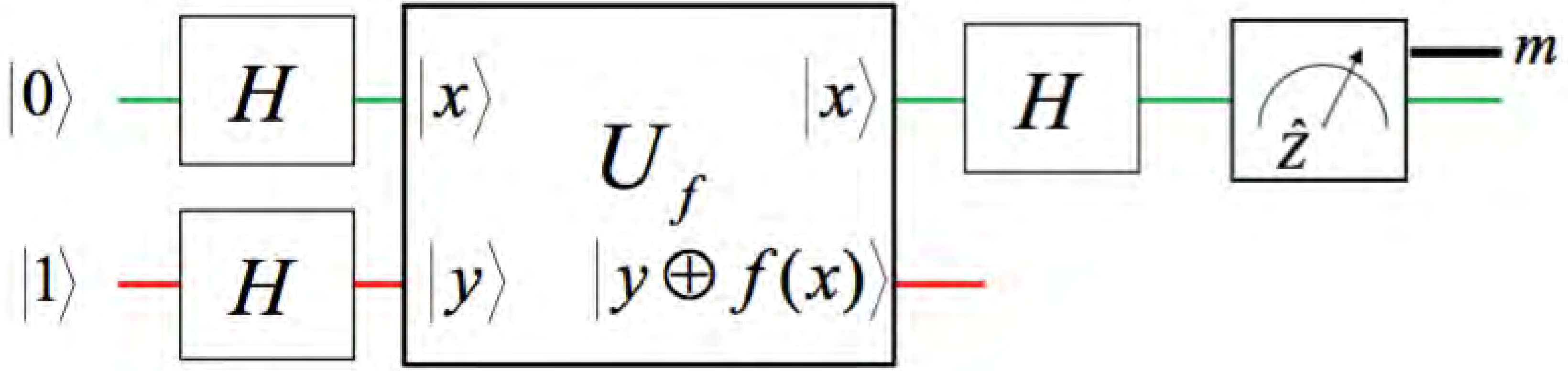
Deutsch Problem (2)

- **Classical solution:** Call the function twice to see if it's balanced or not.
- **Quantum version:** Encode the mystery function in the Unitary, as follows:

$$U_{f_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad U_{f_2} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad U_{f_3} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad U_{f_4} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Deutsch Problem (3)

- Execute with ***only one call*** of the Unitary function:



$m = +1 \longrightarrow$ function is unbalanced

$m = -1 \longrightarrow$ function is balanced

Search Problem – Grover's Algorithm

- The problem
  - Find if x^* among 4 possible options: 00, 01, 10, 11
  - Mathematically, function $f(x)$ will return 1 if $x=x^*$, 0 otherwise

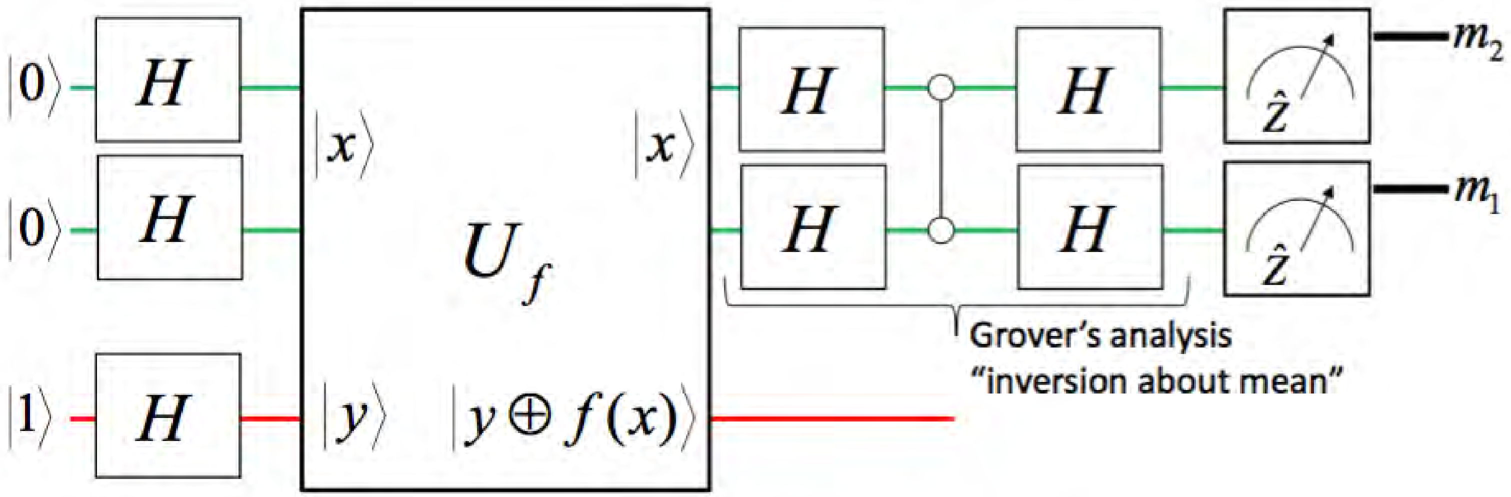
- The solution
  - Classically, it takes 2.25 attempts, on average, to find the correct result
  - With Grover's algorithm only one call of the function will give the result!

- The Unitary to use is (let $x^*=11$, in this case):

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

Search Problem – Grover's Algorithm (2)

- Execute with ***only one call*** of the Unitary function:

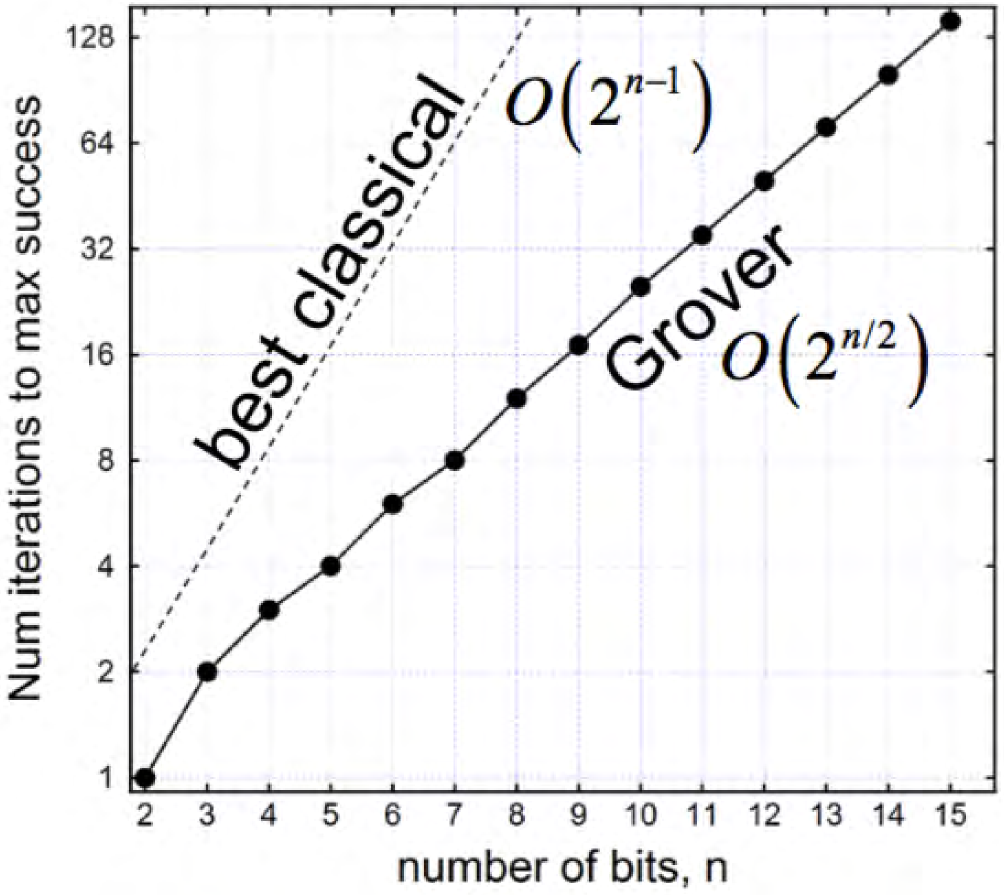


- Answer:

$$(m_2, m_1) = \begin{cases} (+1,+1) \\ (+1,-1) \\ (-1,+1) \\ (-1,-1) \end{cases} \Rightarrow \begin{matrix} x^* = 00 \\ x^* = 01 \\ x^* = 10 \\ x^* = 11 \end{matrix}$$

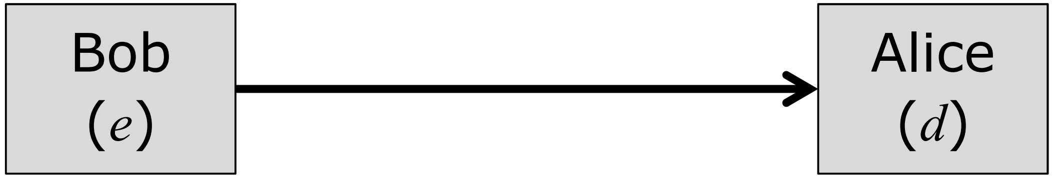
Search Problem – Grover's Algorithm (2)

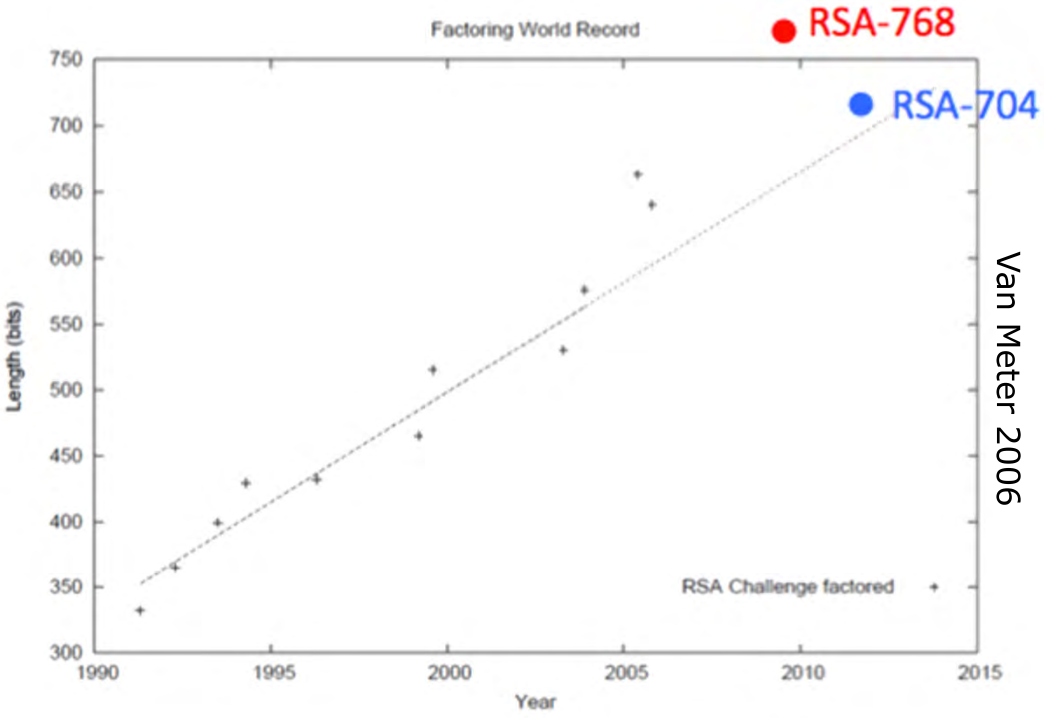
- Grover's algorithm grows (number of calls) with the square root of the number of bits
- The best classical algorithm still has a higher complexity



Shor's Algorithm Justification

- Let us look at RSA (Rivest, Shamir and Adleman) protocol
- Bob takes 2 prime numbers p, q and computes $N=pq$. He chooses e coprime with $(p-1)(q-1)$. He announces N, e.
- Encryption of M: based on e
- Decryption of P: based on d such that
  (de) mod$((p-1)(q-1))=1$





Van Meter 2006

- To crack RSA you need to find p and q from N, which is hard!
- This is the goal of Shor's algorithm

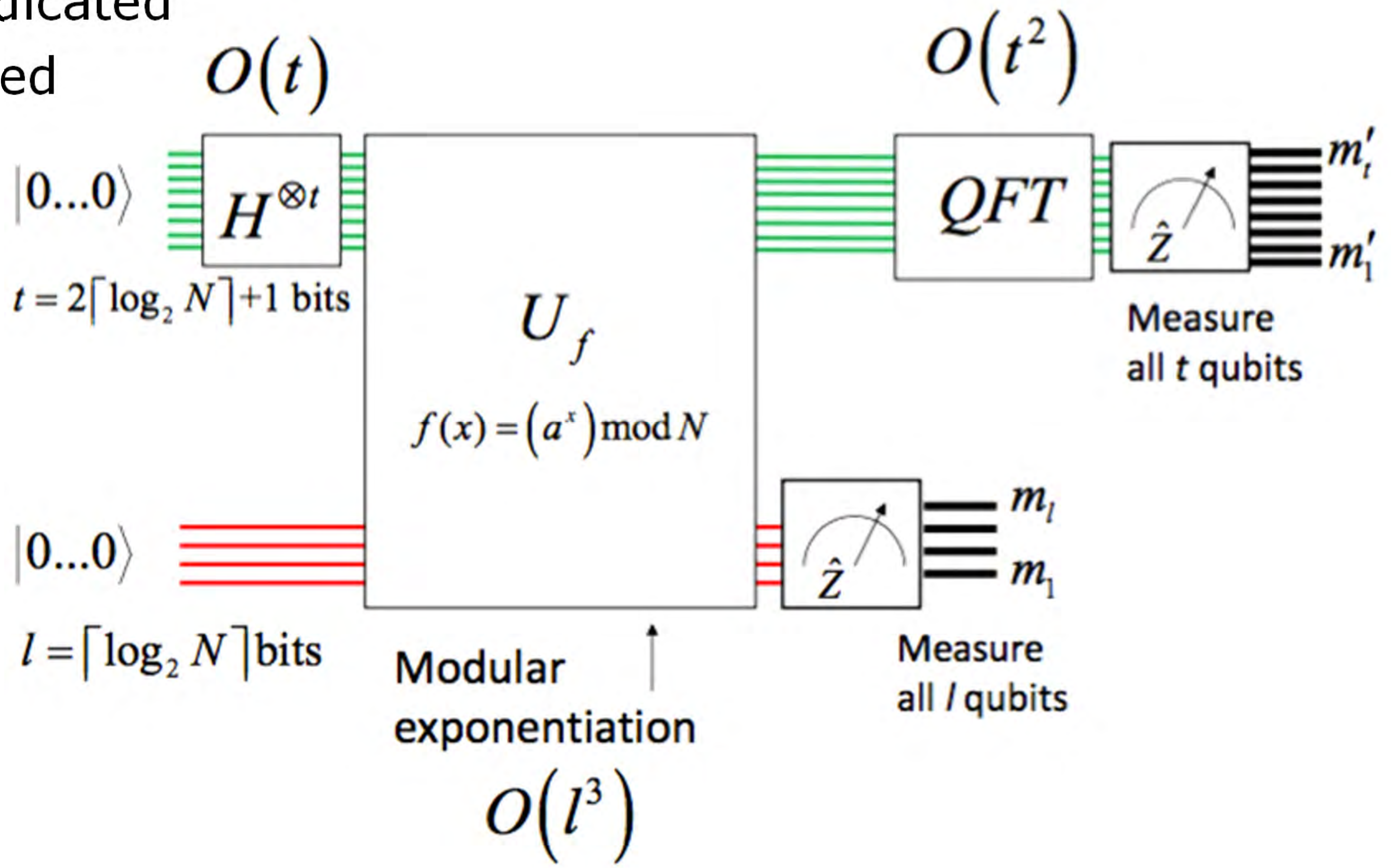
Example

- N=15, p=3, q=5
- $(p\text{-}1)(q\text{-}1)$=8
- e = {3,5,7}; let e=3 (e.g.), then d=3
- 1-to-1 alphabet for encryption and decryption is hereafter:

M	$\xrightarrow[e=3]{(M^e) \bmod N}$	P	$\xrightarrow[d=3]{(P^d) \bmod N}$	M
0		0		0
1		1		1
2		8		2
3		12		3
4		4		4
5		5		5
6		6		6
7		13		7
8		2		8
9		9		9
10		10		10
11		11		11
12		3		12
13		7		13
14		14		14

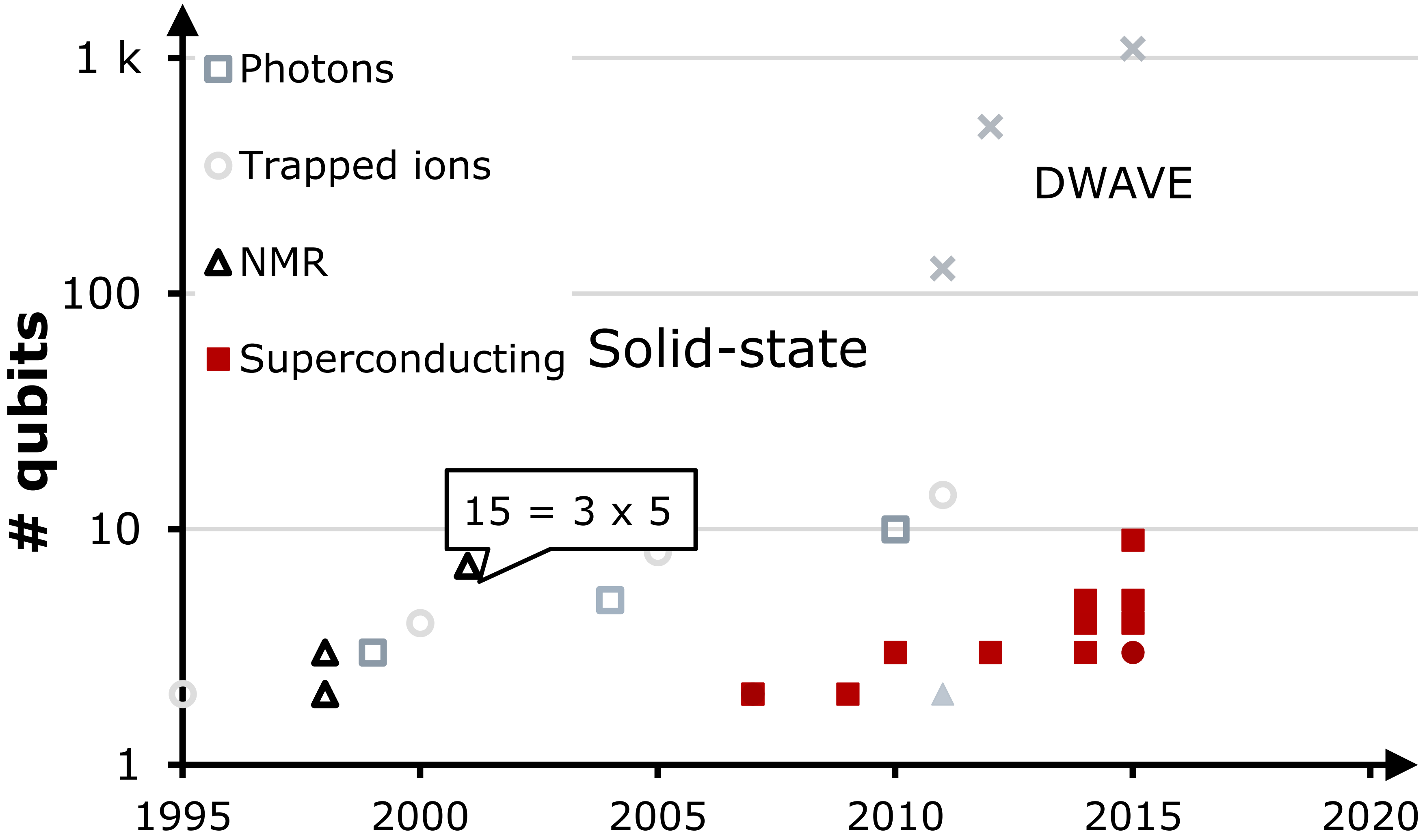
Shor's (Period Finding) Algorithm Concept

- U_f is chosen as indicated
- QFT and H are used

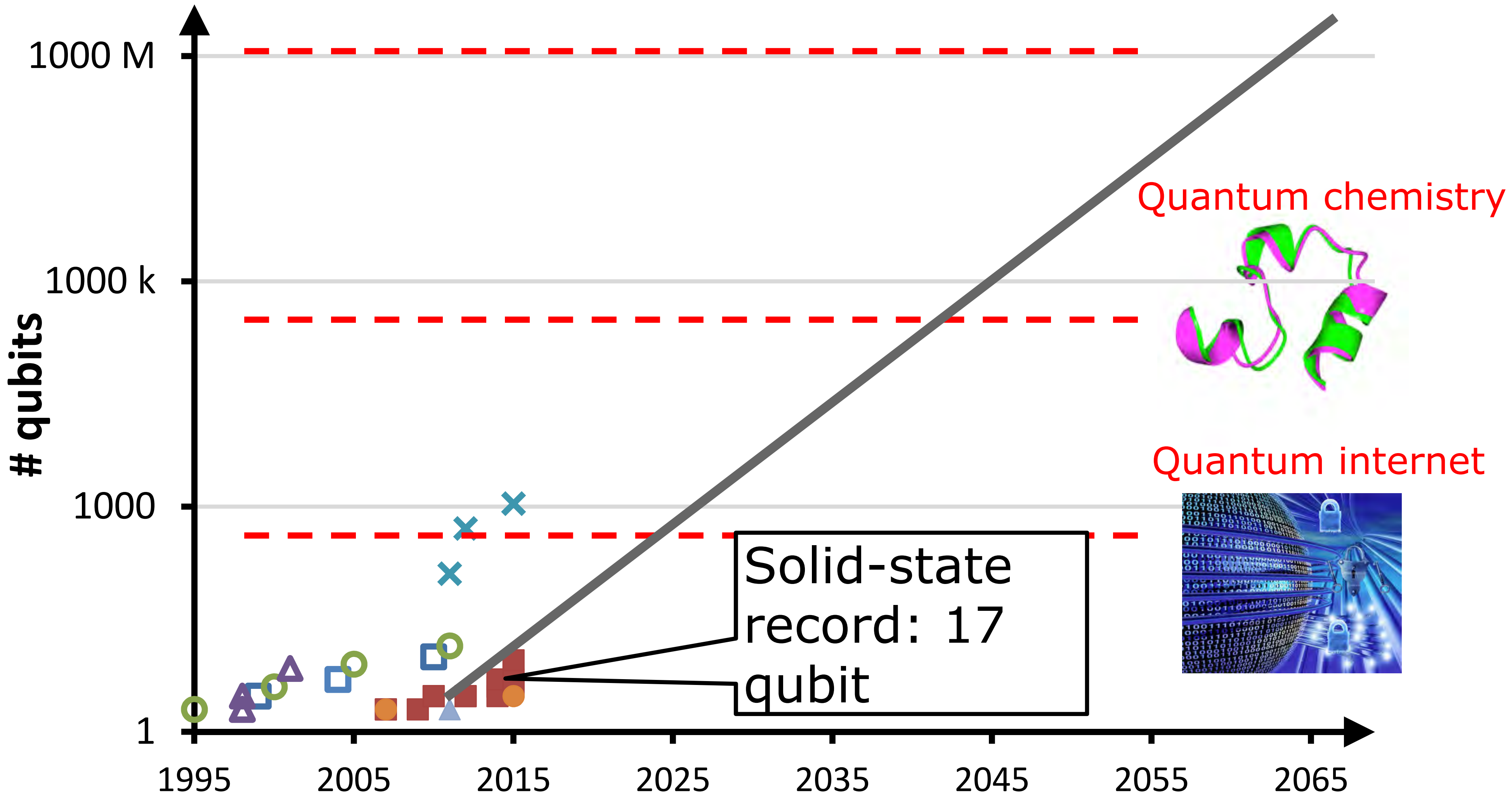


Future Challenges

Development of a Practical QC

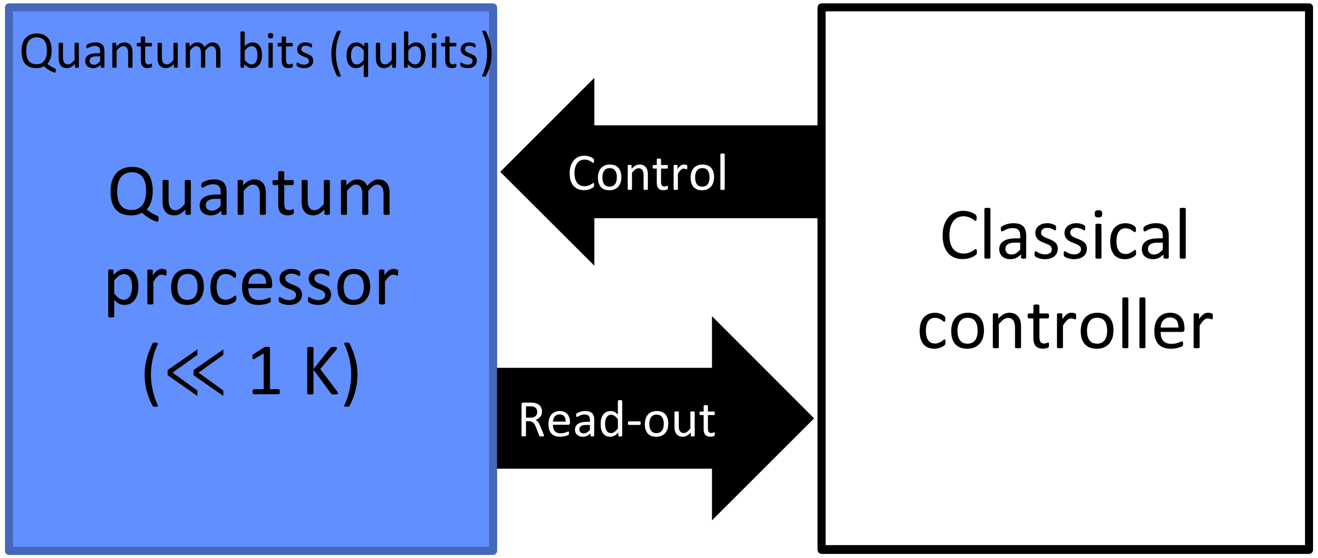


Development of a Practical QC (2)



Development of a Practical QC (3)

- Qubits are fragile and tend to loose coherence quickly
- Using a classical controller it is possible to perform a real-time error correction to ensure that the qubits remain coherent
- The classical controller is also used to execute quantum algorithms in a sequence that is determined by the compiler

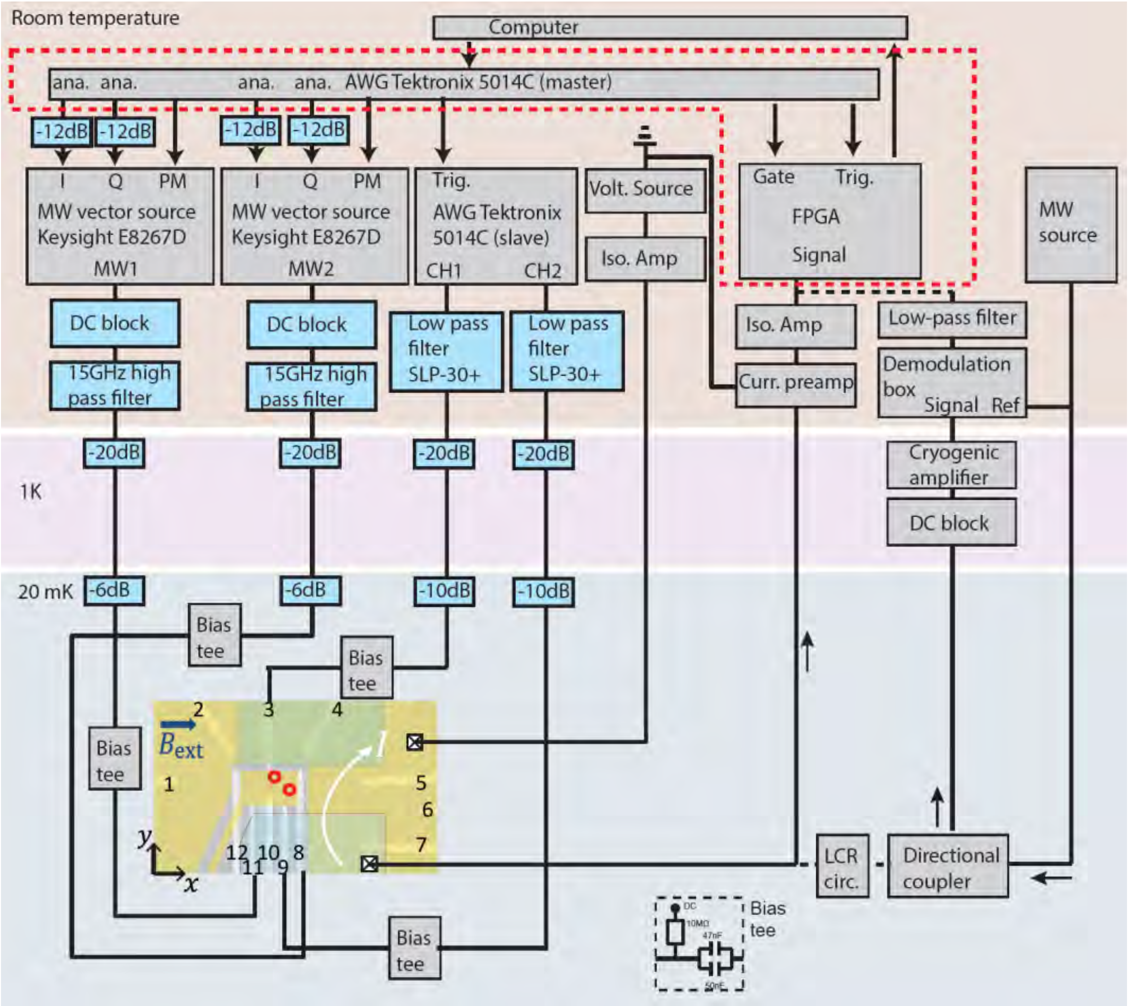


The Quantum Stack

- Similarly to classical processors that, over the years, developed several layers separating the user from the hardware, so the QC is developing a unique stack
- The stack performs several tasks: compilation, error correction, execution, etc.
- The stack is structured as follows:
  - Top: quantum algorithms
  - Middle: quantum assembly (QASM) and quantum instruction set architecture (QISA)
  - Bottom: classical analog/digital electronics that interfaces with qubits

Conventional Classical Controller

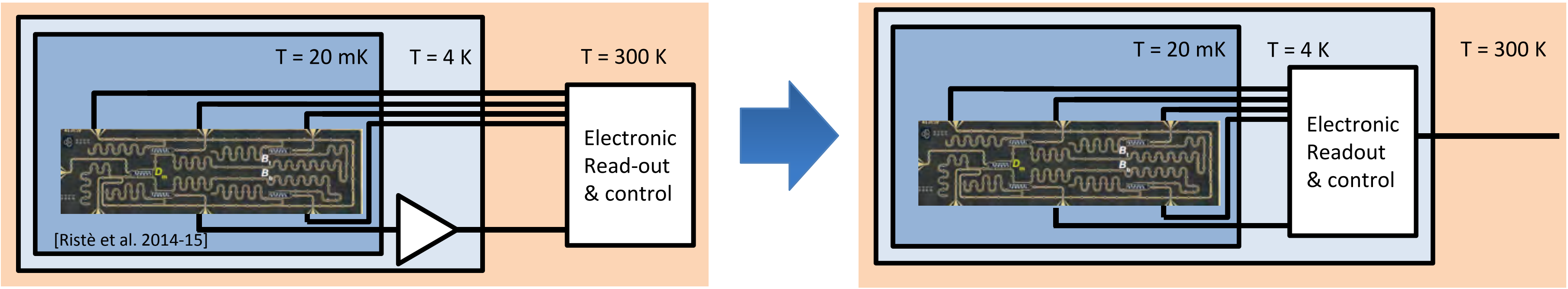
- Classical controllers are implemented as arbitrary waveform generators (AWGs) operating at room temperature
- Ad hoc signals are transferred to the qubits electrically (DC,…, RF signals) in gradual steps from 300K to 20mK
- At each temperature step the signal is attenuated and the noise equivalent temperature is reduced (thermalization)
- The readout is performed in the opposite direction, whereas low noise amplifiers are placed at low temperature (typically 1K) and readout electronics at room temperature



Courtesy of T. Watson (Vandersypen Lab)

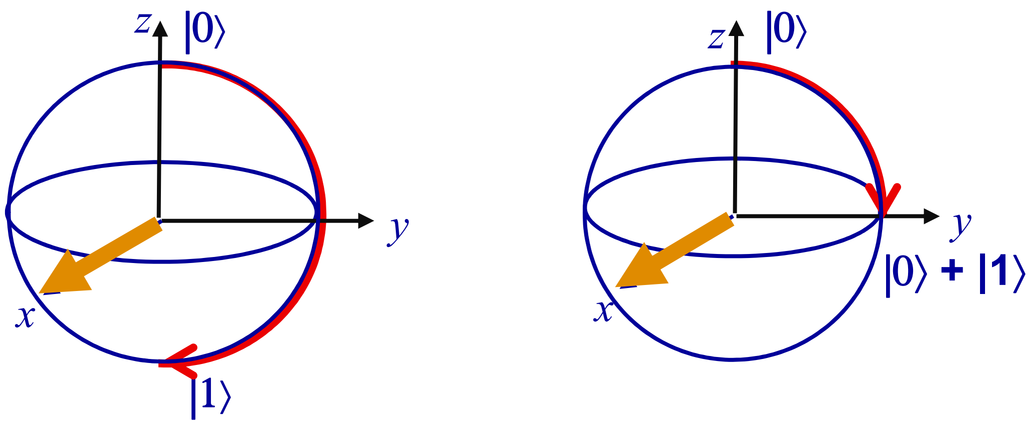
Cryogenic Classical Controller

- Goal: perform qubit control as close as possible to the quantum processor
- Pros:
  - Compactness
  - Scalability
  - Reliability
- Risks:
  - CMOS operation may be altered beyond repair
  - Noise performance may be insufficient
  - Packaging may be difficult



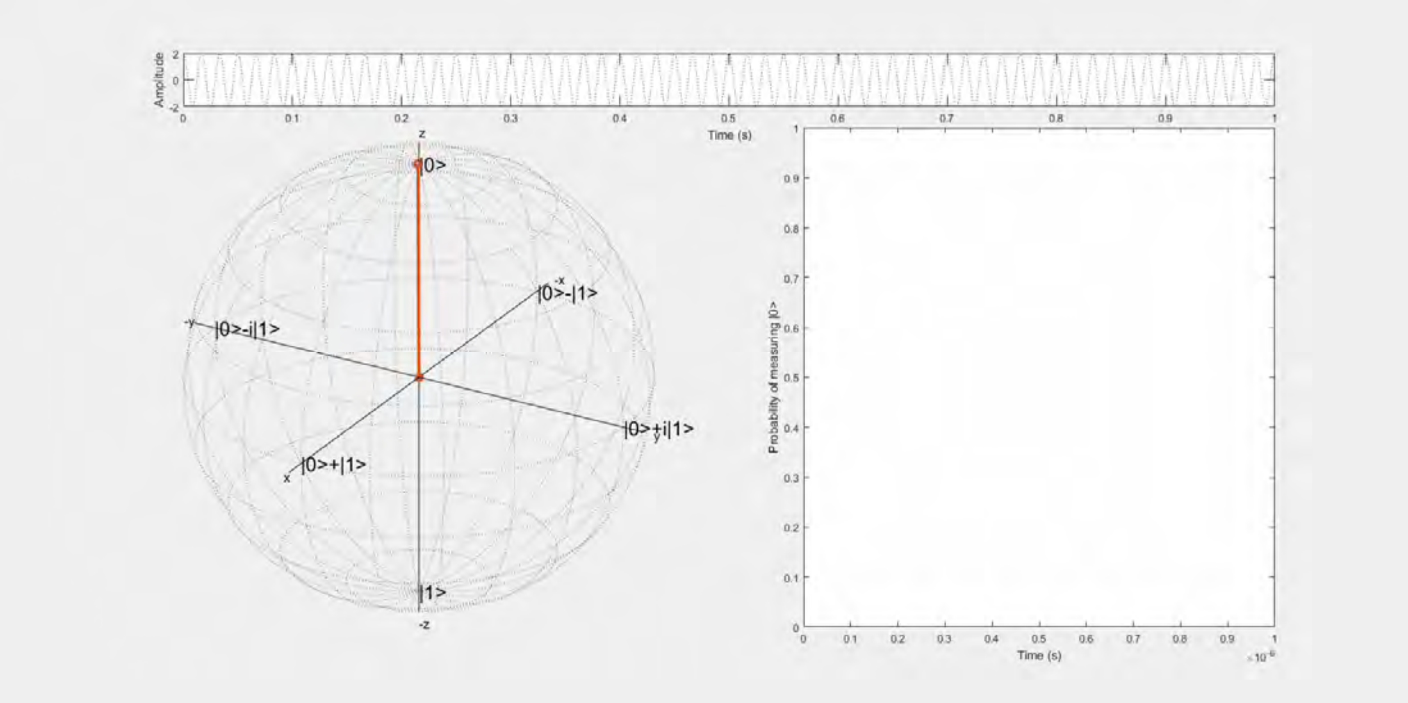
Cryogenic Classical Controller

- Control
  - Initialization
    - Errors due to non-ideality of qubits
  - 1-qubit, 2-qubit operations
    - Errors due to imperfect control and noise



- Readout
  - Measure the quantum state
    - Errors of measurement

Fidelity



- Qubit rotations in reality are not perfect due to errors, noise and other non-idealities
- Intuition: fidelity relates to the distance of the final state wrt the intended state. See simulation of a qubit rotation

Fidelity vs. Power

1-qubit gate:
Oscillator phase noise
Timing accuracy
…

Fidelity
(99.9%)

⟺

2-qubit gate:
Voltage drift
Timing jitter
…

⟺

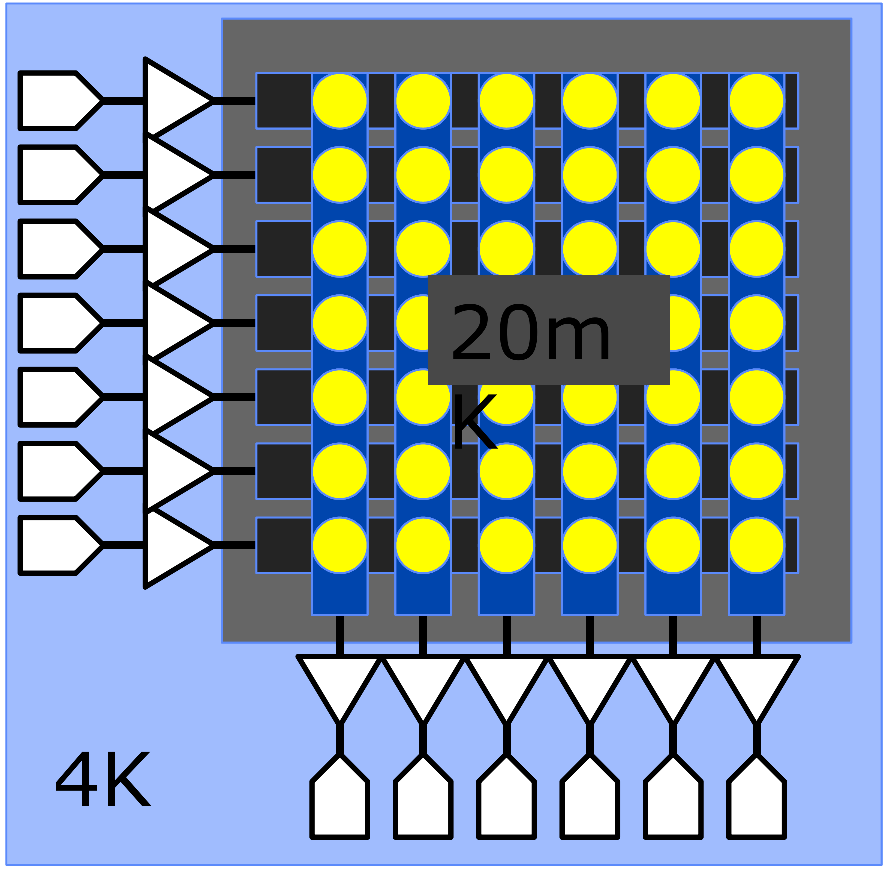
Power
(~ 1 mW/qubit)

Qubit read-out:
Amplitude noise
…

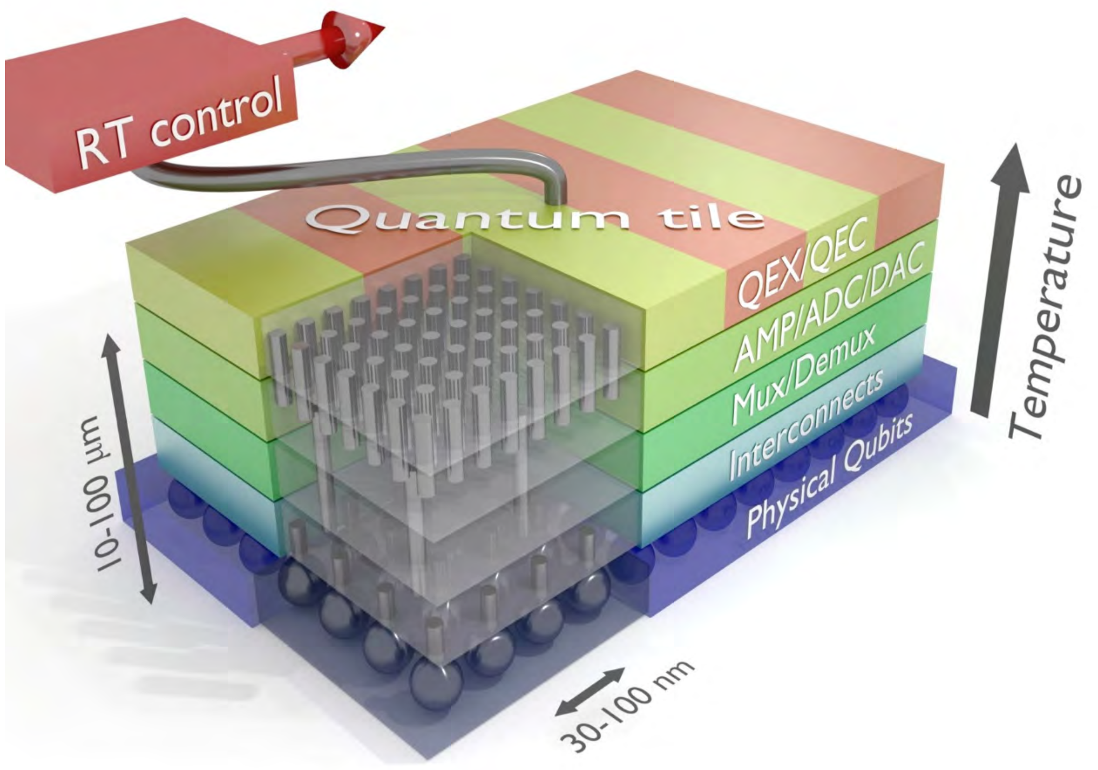
- Fidelity is usually expressed as a percentage, ofter referred to as x9's (e.g. 5 9's = 99.999%)
- Higher fidelity usually requires high power, which is budgeted, espcially at low temperatures (e.g. μW of thermal absorption at mK, while W at 4K)

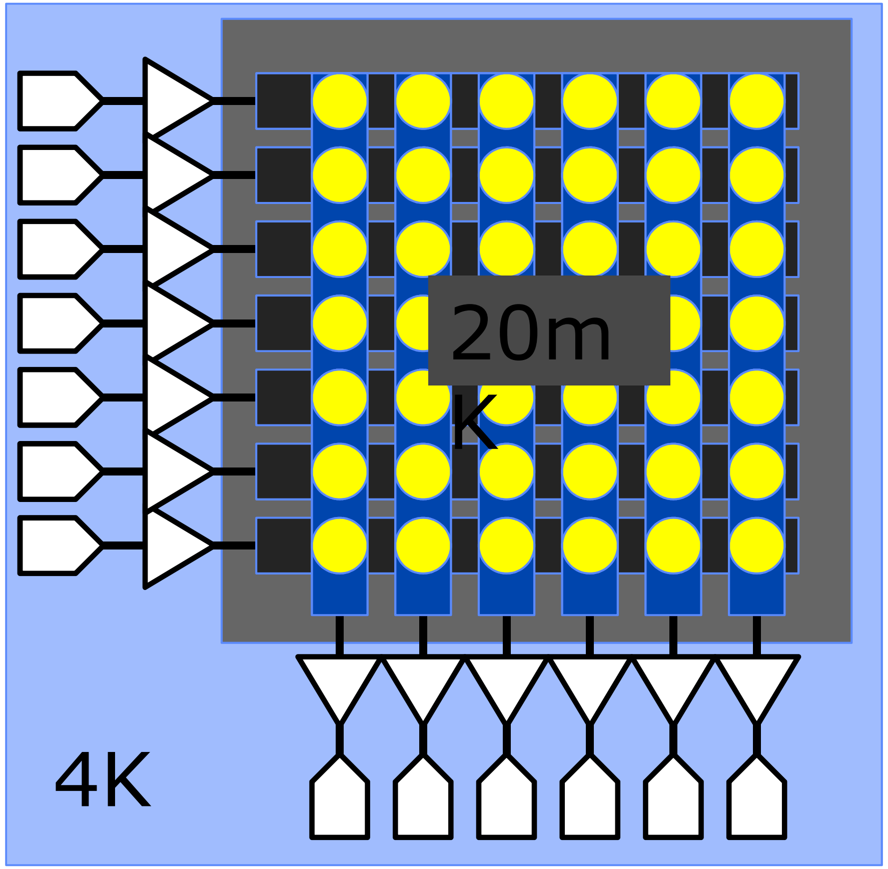
Scaling Up

- Large numbers of qubits are sought
- The issue is how to control and readout a qubit if a dozen wires per qubit are required
- Possible solutions:
  - Use imaging sensor readout as inspiration
  - Deep-sub-volt logic enabled by cryo-operation
  - Sub-threshold operation to minimize power
- Challenges:
  - Power budget
  - Complexity of interconnect
  - Yield and uniformity issues



Scaling Up


RT control
Quantum tile
QEX/QEC
AMP/ADC/DAC
Mux/Demux
Interconnects
Physical Qubits
Temperature
10-100 µm
30-100 nm


20m
K
4K

Conclusions

- We have introduced the basic concepts of quantum computing and quantum bits
- We have outlined the metrics for qubits
- The anatomy of a quantum computer and of a quantum algorithm has been presented in detail, along with examples
- We have discussed the challenges for future large scale quantum computers, including
  - Scalability
  - Reliability
  - Yield
- We have outlined a possible path to a real machine

Acknowledgements: Intel Corp. & QuTech

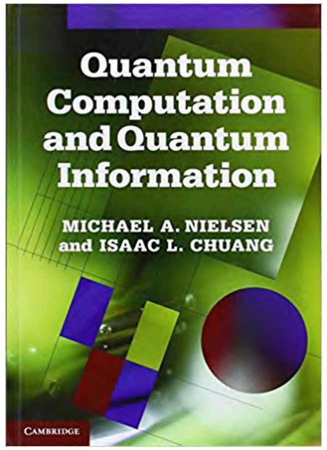
Thank You

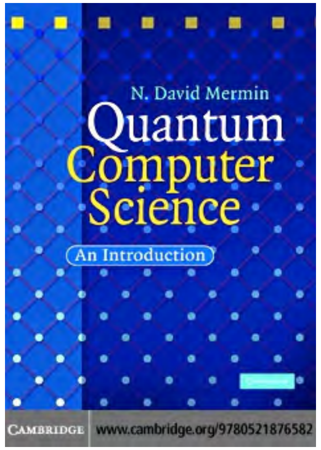
http://aqua.epfl.ch

http://qutech.tudelft.nl

Key References

- **N.D. Mermin, "Quantum Computer Science: An Introduction," Cambridge University Press, 5th printing, 2016. ISBN 978-0-521-87658-2**
- **M.A. Nielsen, I.I. Chuang, "Quantum Computation and Quantum Information", Cambridge Press, 3rd printing, 2017. ISBN 978-1-107-00217-3**
- A. Montanaro, "Quantum Algorithms: an Overview", npj Quantum Information 2, 15023 EP (2016), review article.
- A. Aspect, J. Dalibard, and G. Roger, ''Experimental test of Bell's inequalities using time-varying analyzers,'' Phys. Rev. Lett. 49, 1804–1807 (1982).
- D. Wecker, B. Bauer, B. K. Clark, M. B. Hastings, and M. Troyer, Phys. Rev. A 90, 022305 (2014).
- E. Charbon, F. Sebastiano, A. Vladimirescu, H. Homulle, S. Visser, L. Song, and R. M. Incandela, IEEE International Electron Devices Meeting (IEDM) pp. 13.5.1–13.5.4 (2016).
- F. Sebastiano, H. Homulle, B. Patra, R. Incandela, J. van Dijk, L. Song, M. Babaie, A. Vladimirescu, and E. Charbon, ACM Design Automation Conference (DAC) pp. 13:1–13:6 (2017).
- H. Ball, W. D. Oliver, and M. J. Biercuk, npj Quantum Information 2, 16033 EP (2016), review article.
- L. Vandersypen, H. Bluhm, J. Clarke, A. Dzurak, R. Ishi- hara, A. Morello, D. Reilly, L. Schreiber, and M. Veld- horst, arXiv preprint arXiv:1612.05936 (2016).





Key References (2)

- M. Veldhorst, H. Eenink, C. Yang, and A. Dzurak, arXiv preprint arXiv:1609.09700 (2016).
- J. R. Petta, A. C. Johnson, J. M. Taylor, E. A. Laird, A. Yacoby, M. D. Lukin, C. M. Marcus, M. P. Hanson, and A. C. Gossard, Science 309, 2180 (2005).
- M. Veldhorst, J. Hwang, C. Yang, A. Leenstra, B. De Ronde, J. Dehollain, J. Muhonen, F. Hudson, K. Itoh, A. Morello, et al., Nature nanotechnology 9, 981 (2014).
- N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography", Rev. of Mod. Phys, 74 (2002).
- D. Rotta, F. Sebastiano, E. Charbon, E. Prati, "Quantum information density scaling and qubit operation time constraints of CMOS silicon-based quantum computer architectures", npj Quantum Information (2017) 3:26 ; doi:10.1038/s41534-017-0023-5, review article.
- N.C. Jones, et al., "Layered architecture for quantum computing". Phys. Rev. X 2, 31007 (2012).
- P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Sci. Stat. Comput. 26, 1484 (1997).
- P.W. Shor, "Scheme for reducing decoherence in quantum computer memory", Phys. Rev. A 52, 2493–2496 (1995).
- A. Steane, "Error correcting codes in quantum theory", Phys. Rev. Lett. 77, 793–797 (1996).
- S.J. Devitt, W.J. Munro, K. Nemoto, "Quantum error correction for beginners", Rep. Prog. Phys. 76, 76001 (2013).