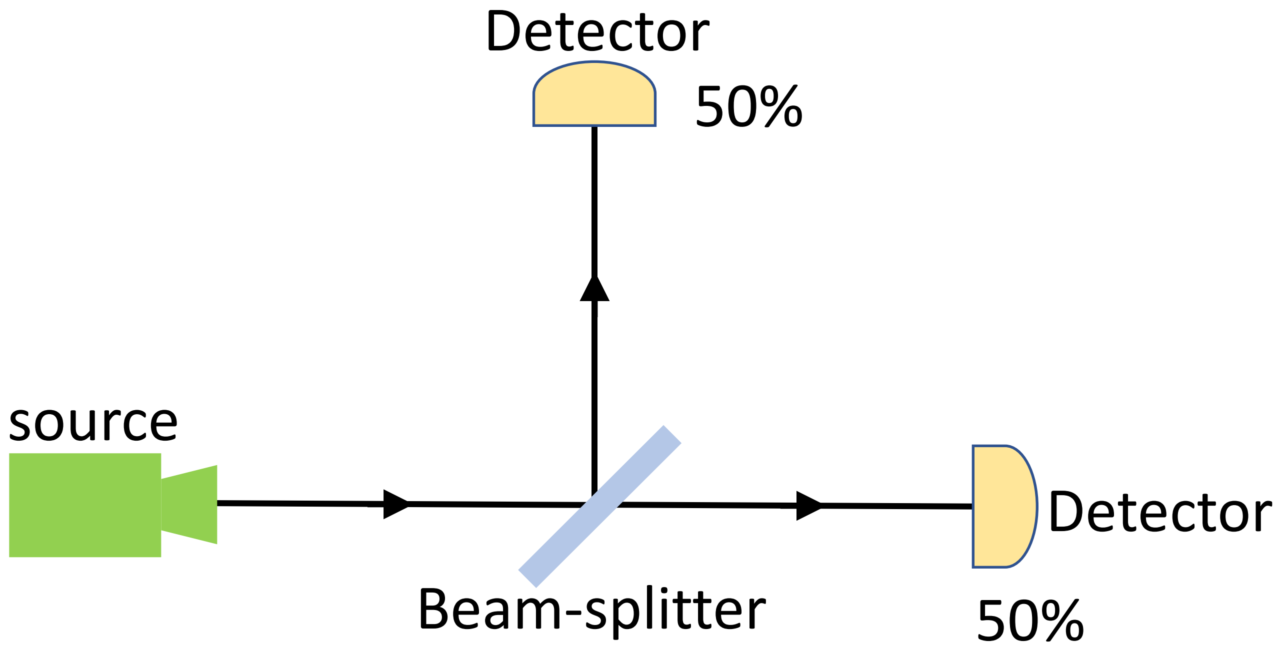
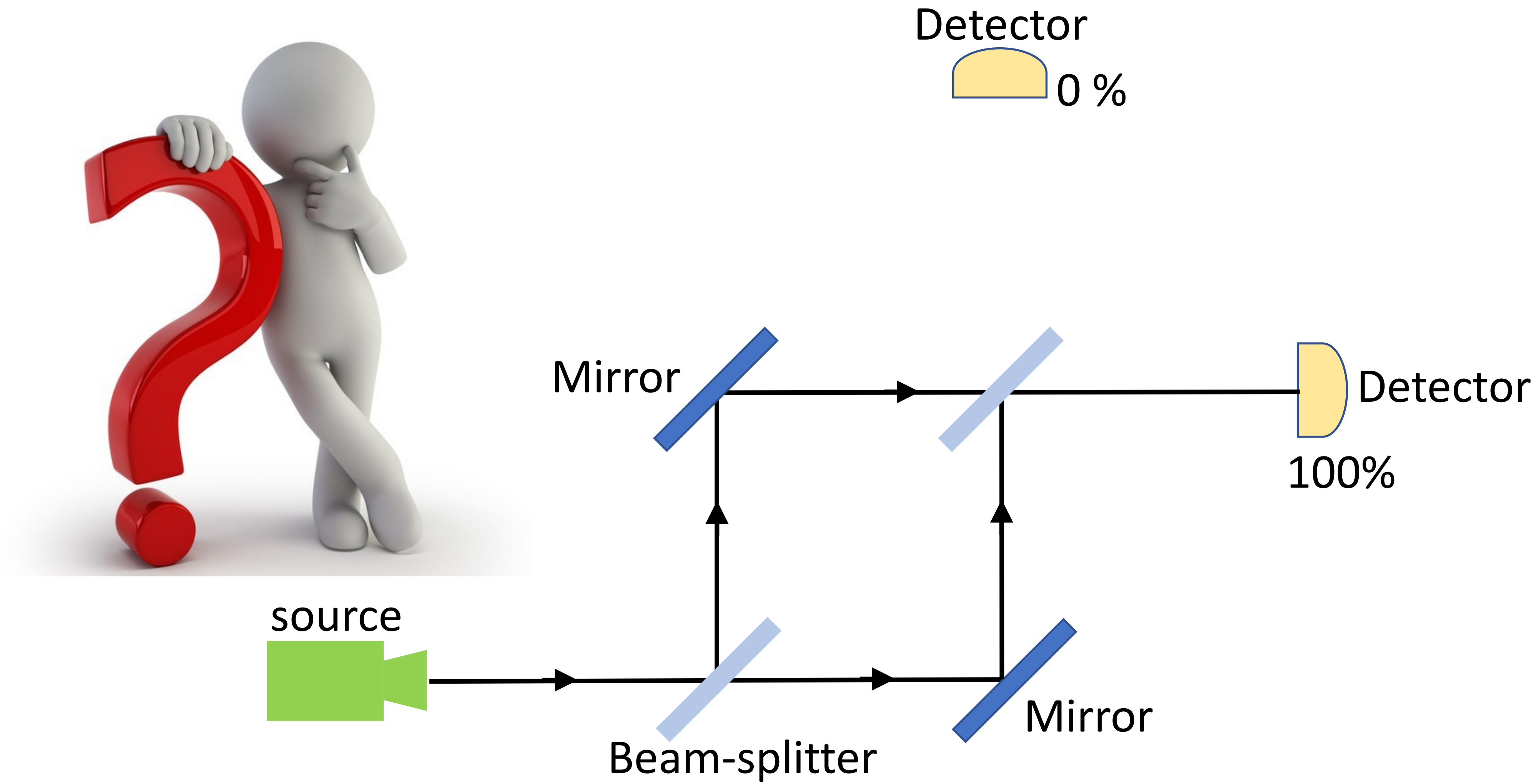
0. Intro & Useful info

Quantum Computing

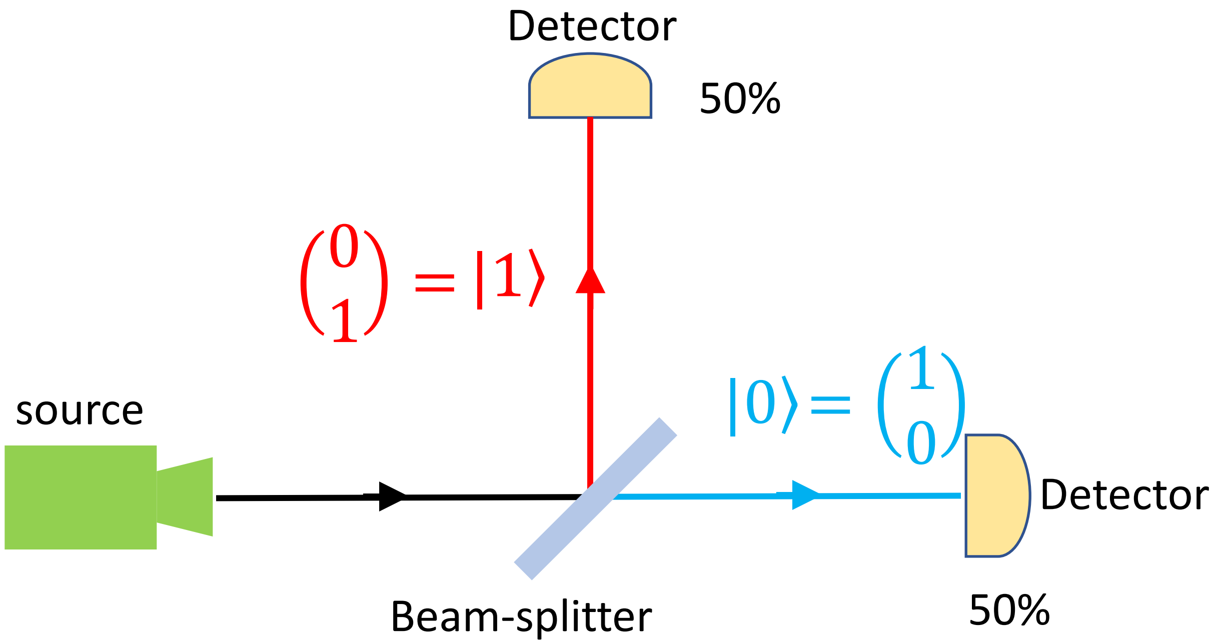
Into the Quantum



Into the Quantum



Into the Quantum



$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}$$

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

→ We correctly get 0.5 probability of detection for each path

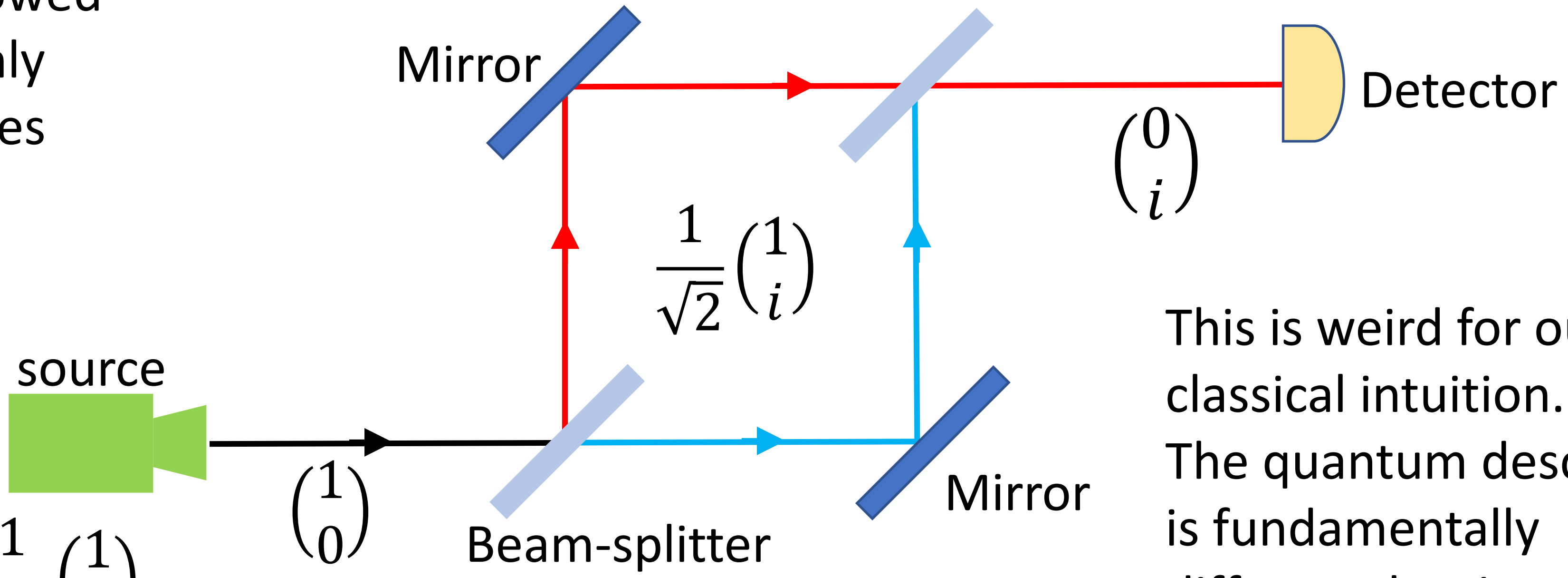
Into the Quantum

https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/Mach-Zehnder-Interferometer/Mach_Zehnder_Interferometer.html

Detector

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

Superposition followed by **interference**: only the red path survives



This is weird for our classical intuition.
The quantum description is fundamentally different, but it works!

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

Into the Quantum

Quantum Computing

https://www.youtube.com/watch?v=rg4Fnag4V-E	Quantum magnet (spin quantization)
https://www.youtube.com/watch?v=rQJ4yX1l6to	Double slit experiment (superposition, interference)

Quantum Computing

NIELS
BOHR

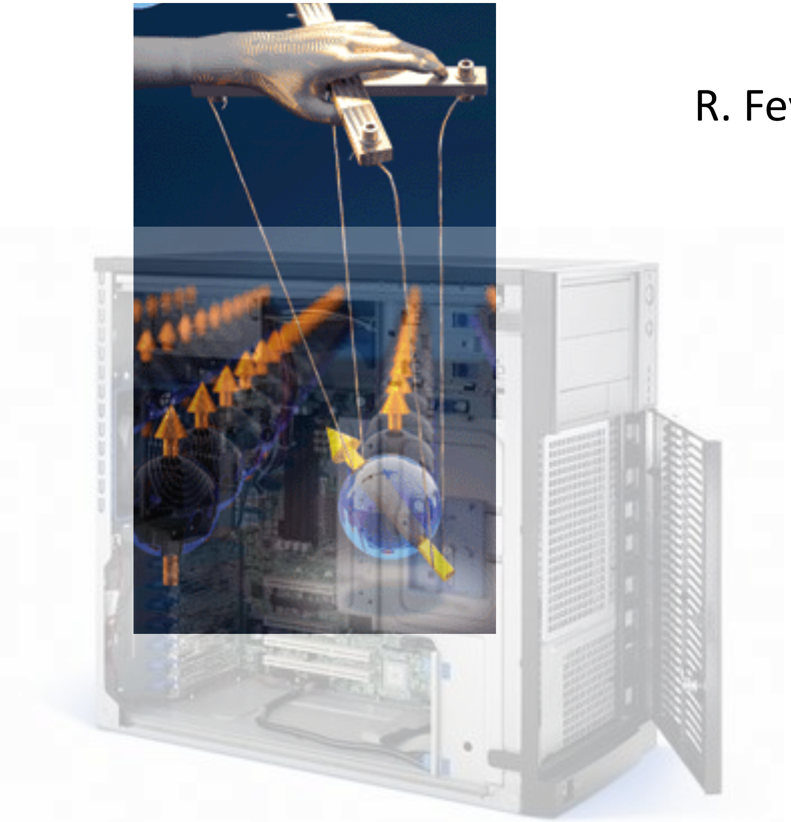
"If quantum mechanics hasn't profoundly shocked you, you haven't understood it yet."

I think it is safe to say that no one understands Quantum Mechanics.

RICHARD
FEYNMAN

Why quantum computing?

*"Nature isn't classical, dammit, and if you want to make a **simulation of nature**, you'd better make it **quantum mechanical**, and by golly it's a wonderful problem, because it doesn't look so easy"*



R. Feynman, 1982

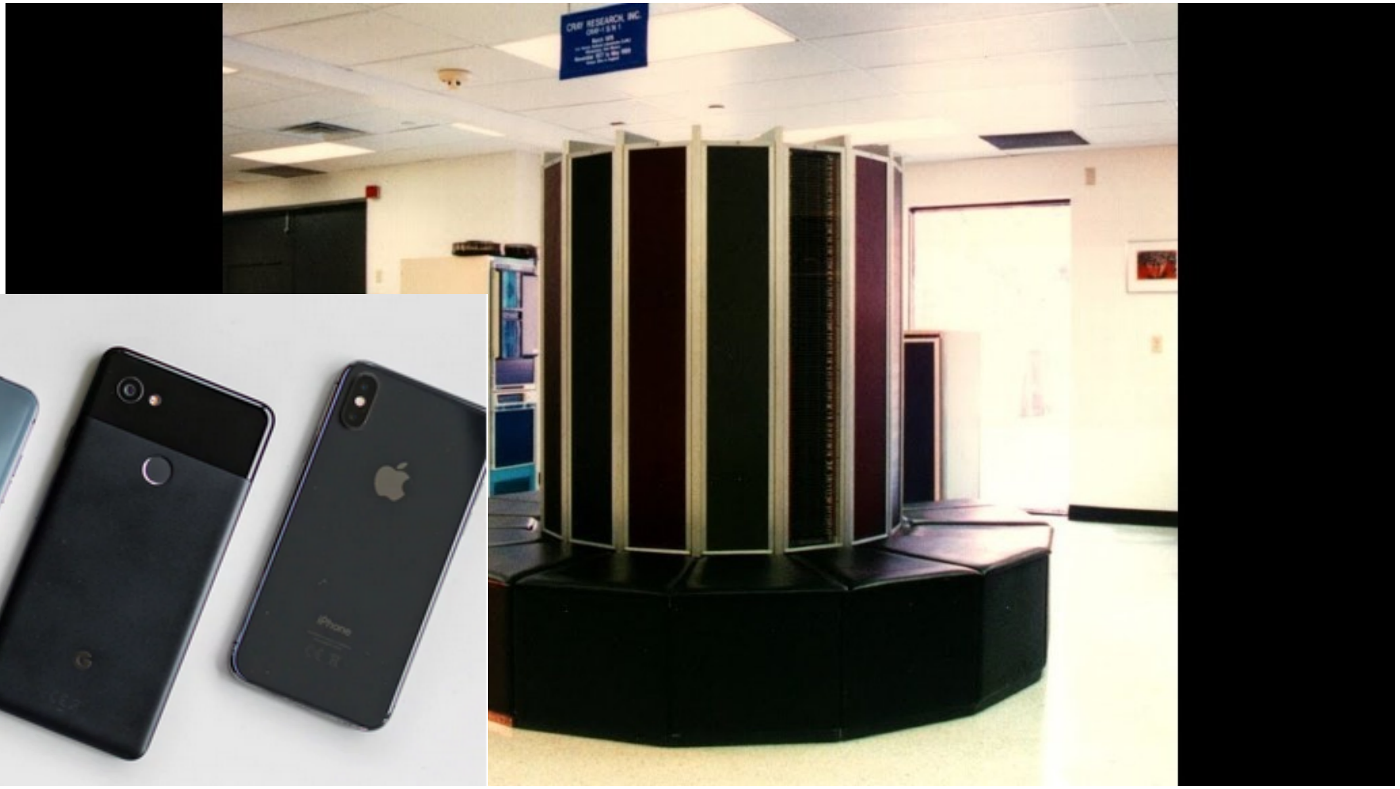
Why quantum computing?

- Quantum Mechanics is the most precise description we have of Nature.
- By mimicking nature, a quantum computer will be able to solve problems intractable for any classical device.
- We know several problems characterized by quantum speedup
- … many others still have to be identified!
- In general we need to design new algorithms different from classical ones, based on some key ingredients in a quantum computer: **superposition, interference, entanglement**. This could pave the way to the solution of hard classical.
- We need to develop hardware and **software**
- We need **quantum-programmers!**

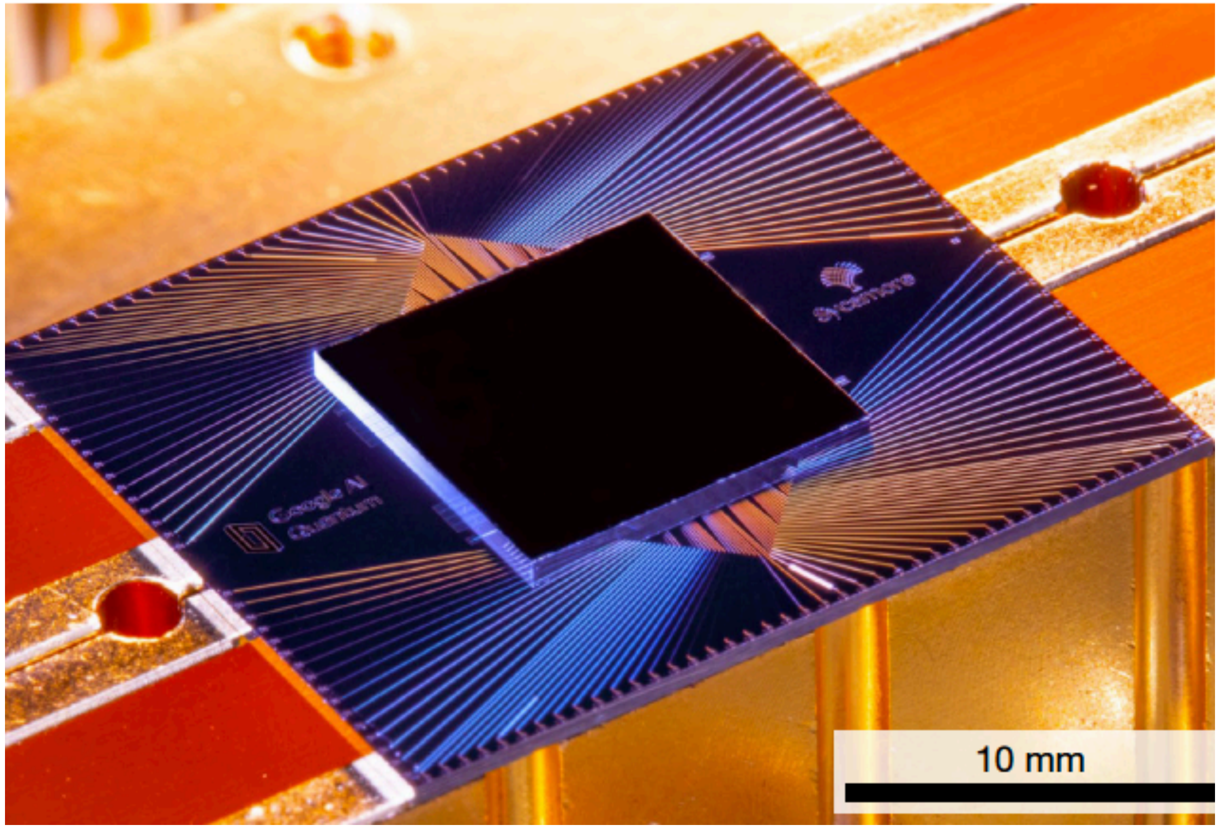
Why quantum computing?

1976 Apple

CERN & CINECA Cray 1



The 2nd quantum revolution



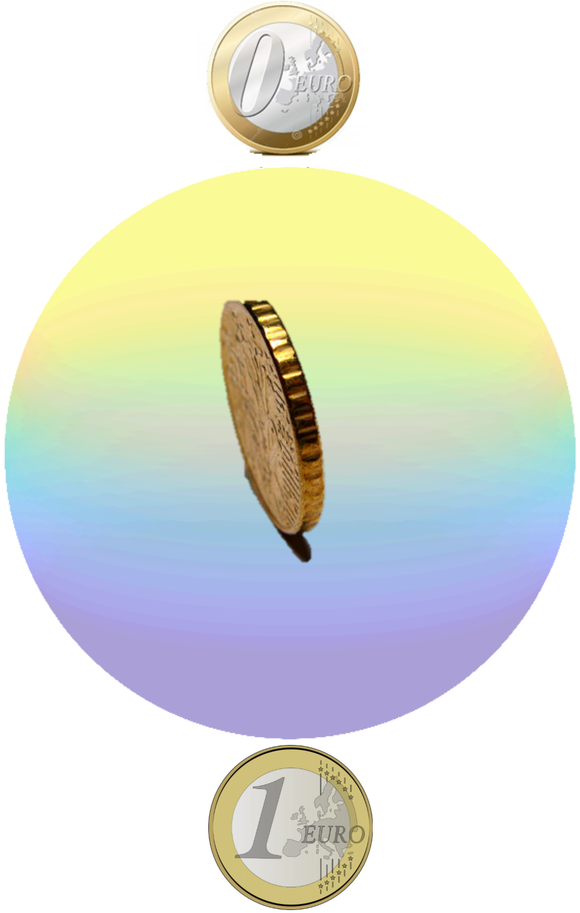
Google says that Sycamore takes 200 s instead of 10,000 years

Nature **574**, 505 (2019)

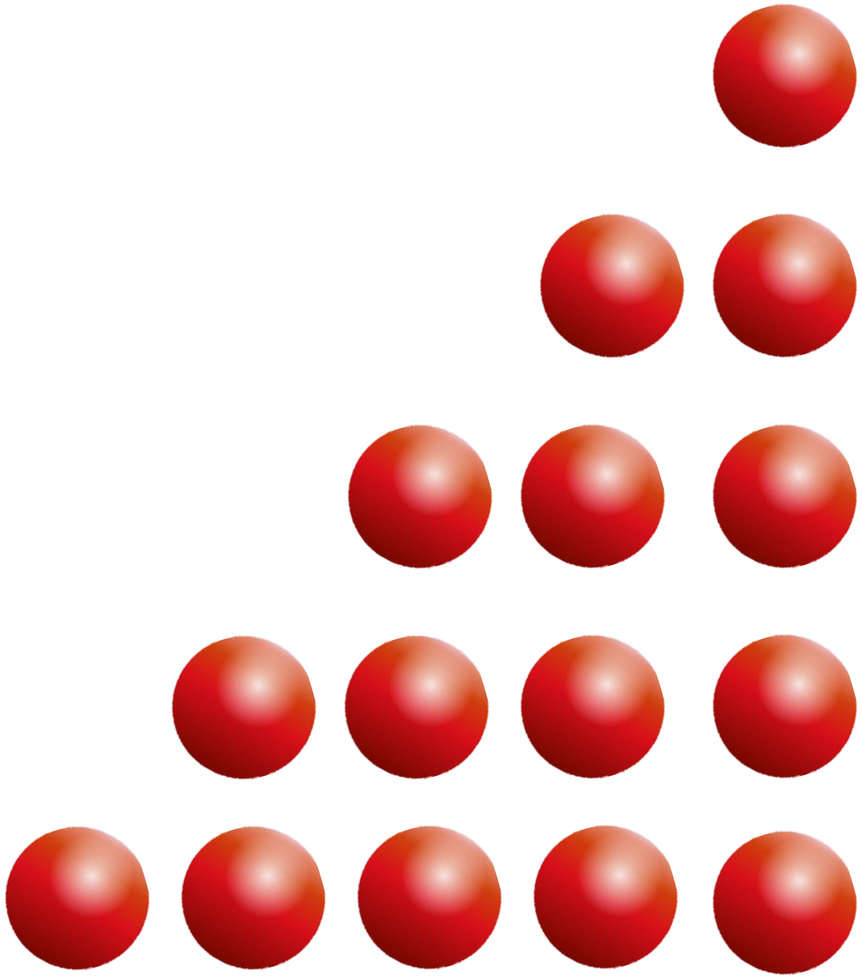
Quantum Computing

BIT

QU-BIT



QU-BITS



BITS

0, 1

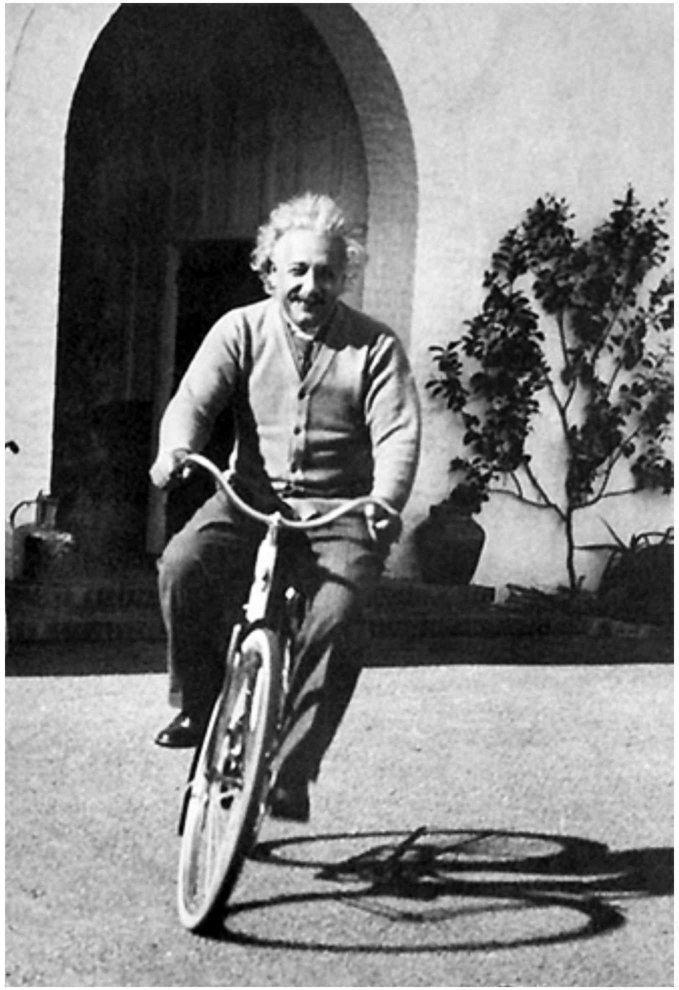
00, 01, 10, 11

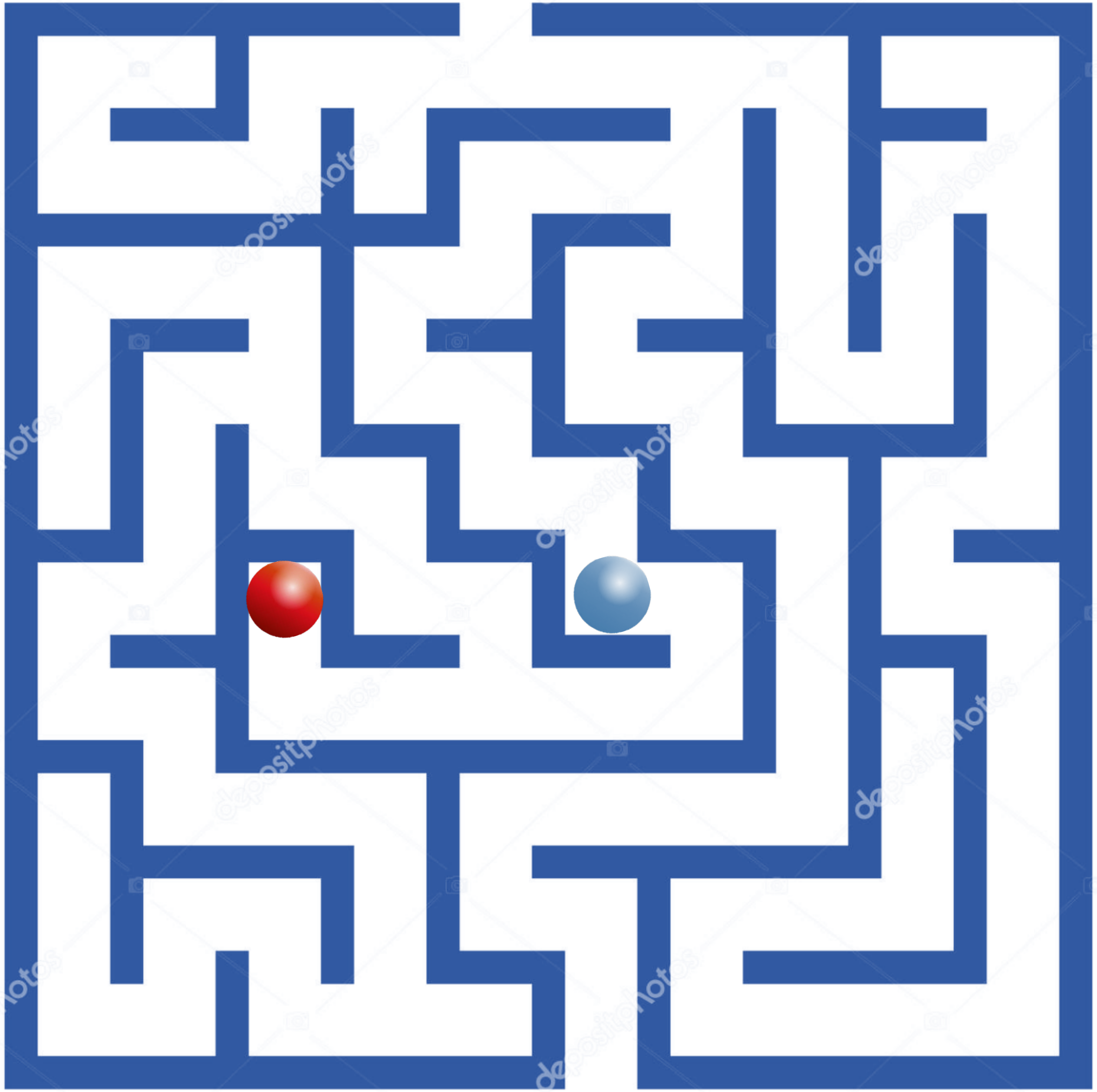
000, 001, 010, 011, 100, 101, 110, 111

0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111,
1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111

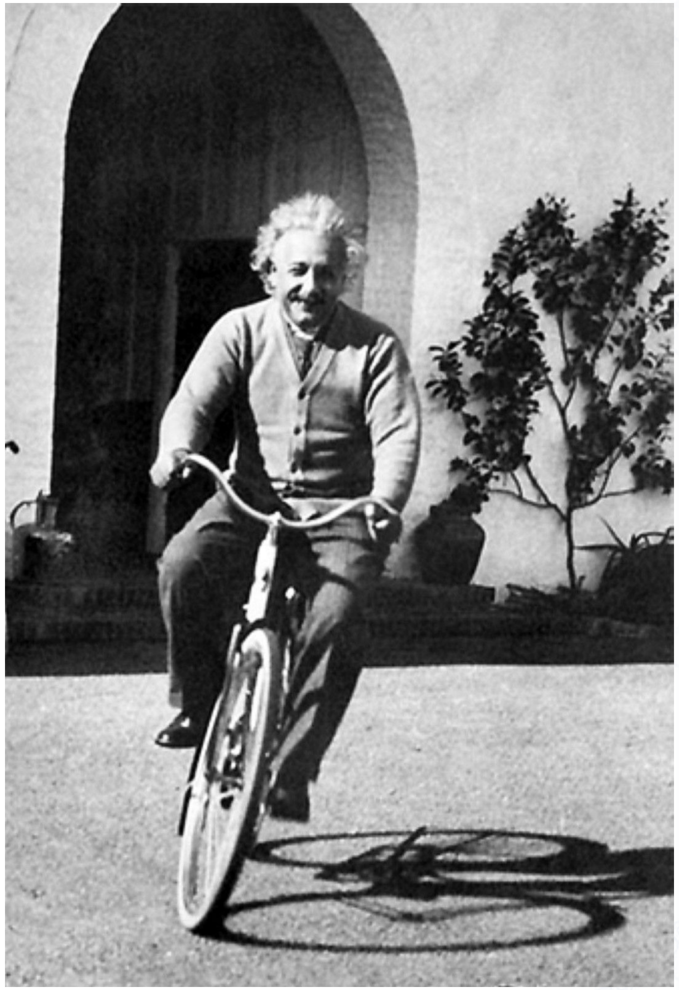
00000, 00001, 00010, 00011, 00100, 00101, 00110, 00111,
01000, 01001, 01010, 01011, 01100, 01101, 01110, 01111,
10000, 10001, 10010, 10011, 10100, 10101, 10110, 10111,
11000, 11001, 11010, 11011, 11100, 11101, 11110, 11111

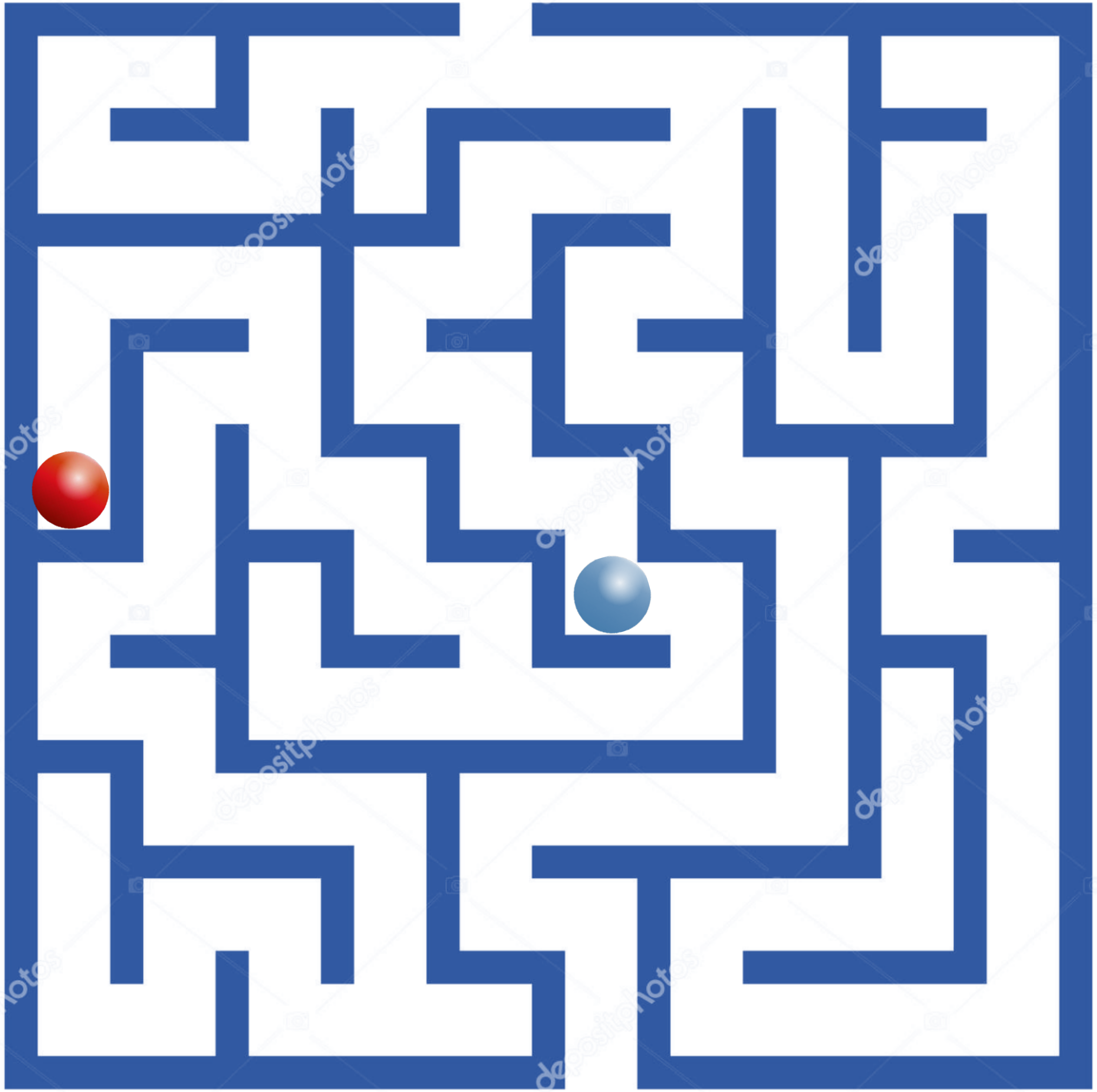
CLASSICAL COMPUTER



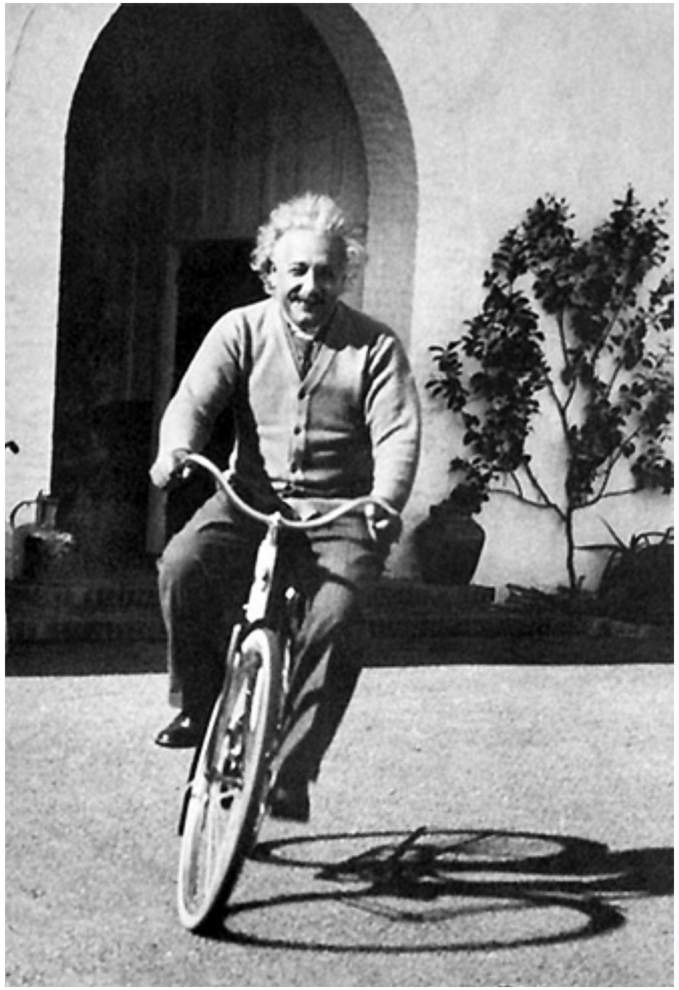


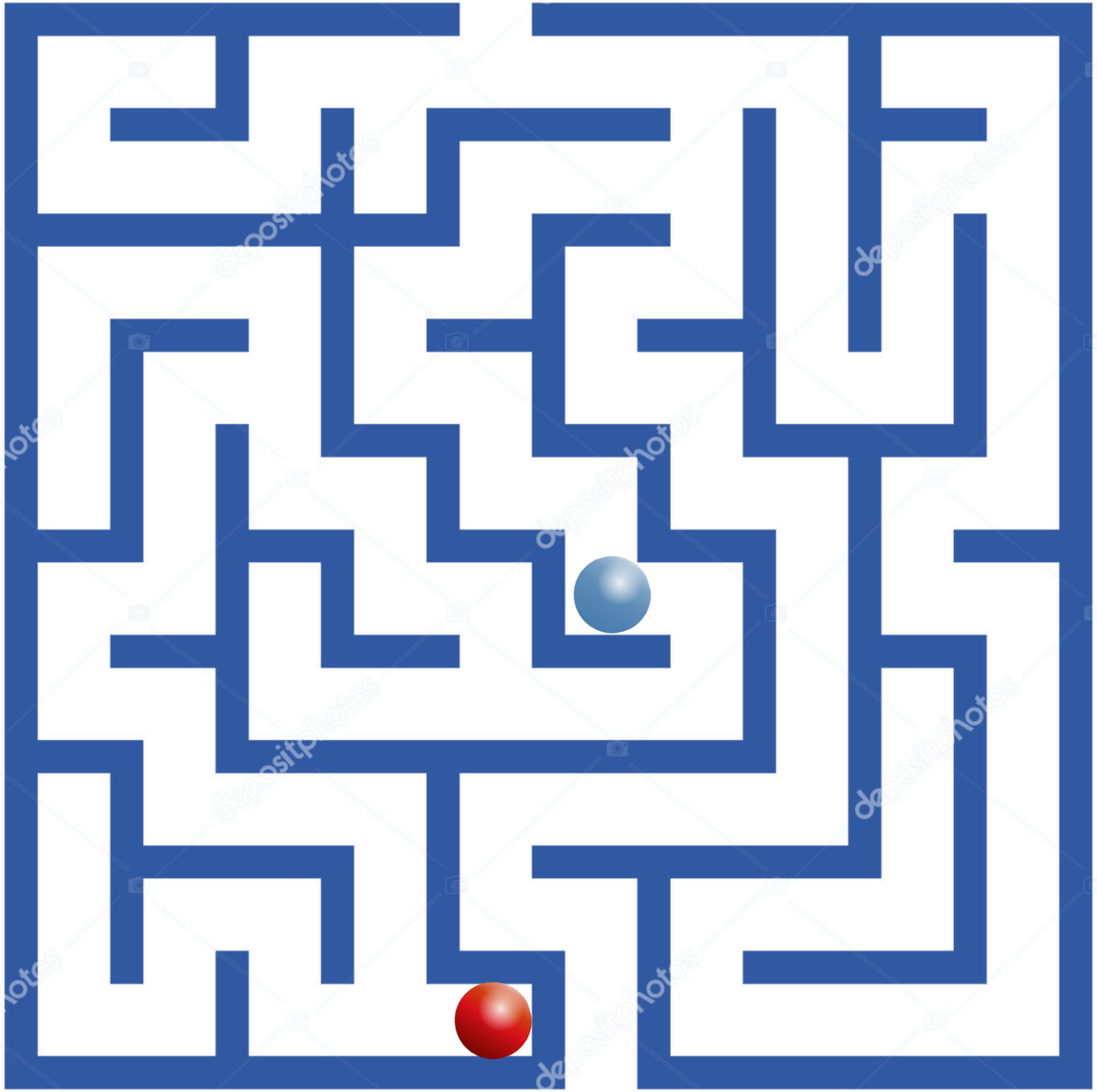
CLASSICAL COMPUTER





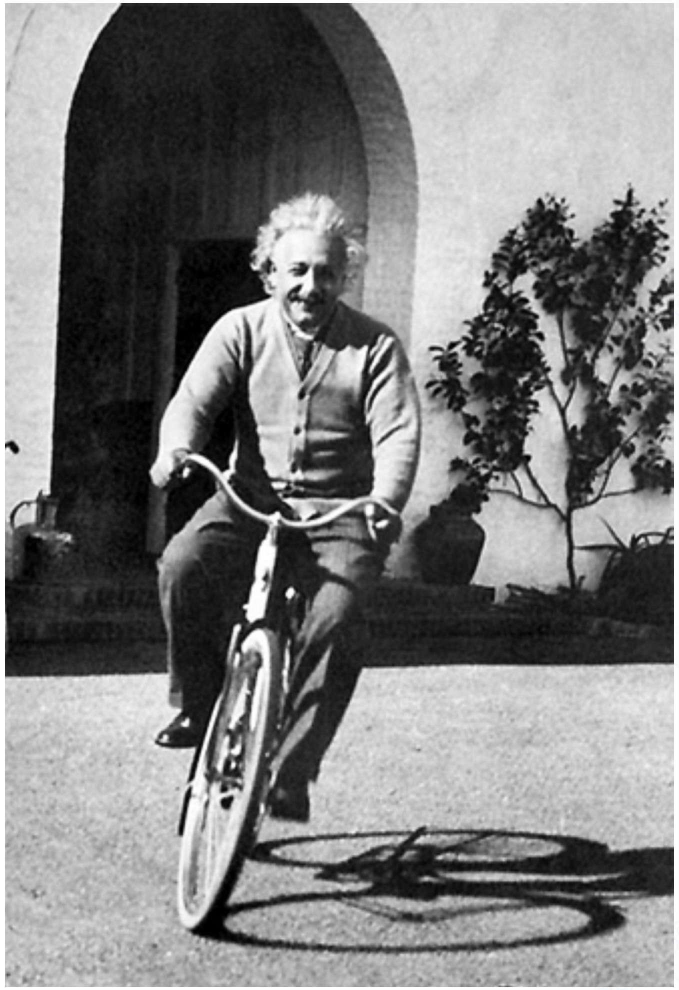
CLASSICAL COMPUTER

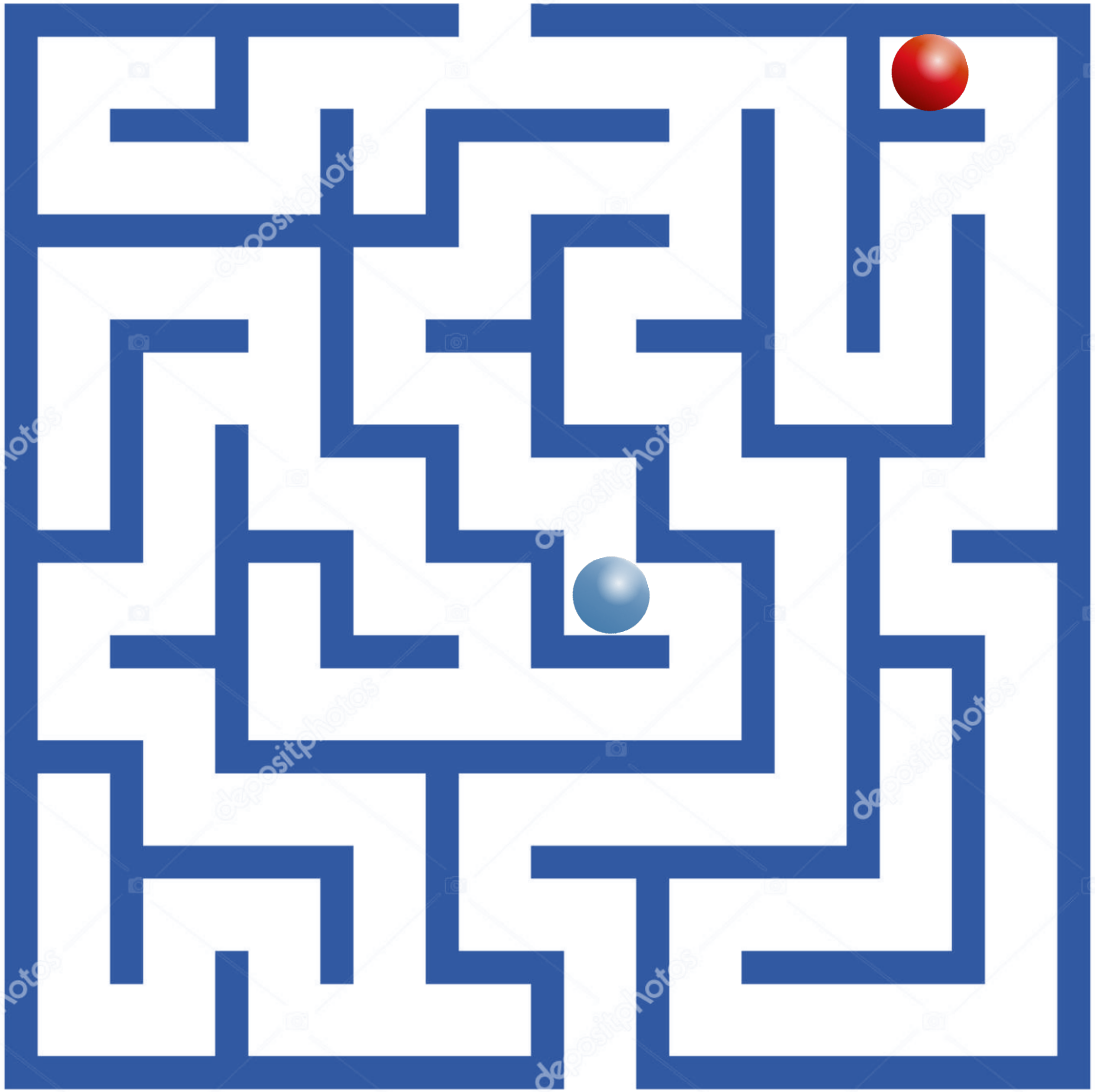




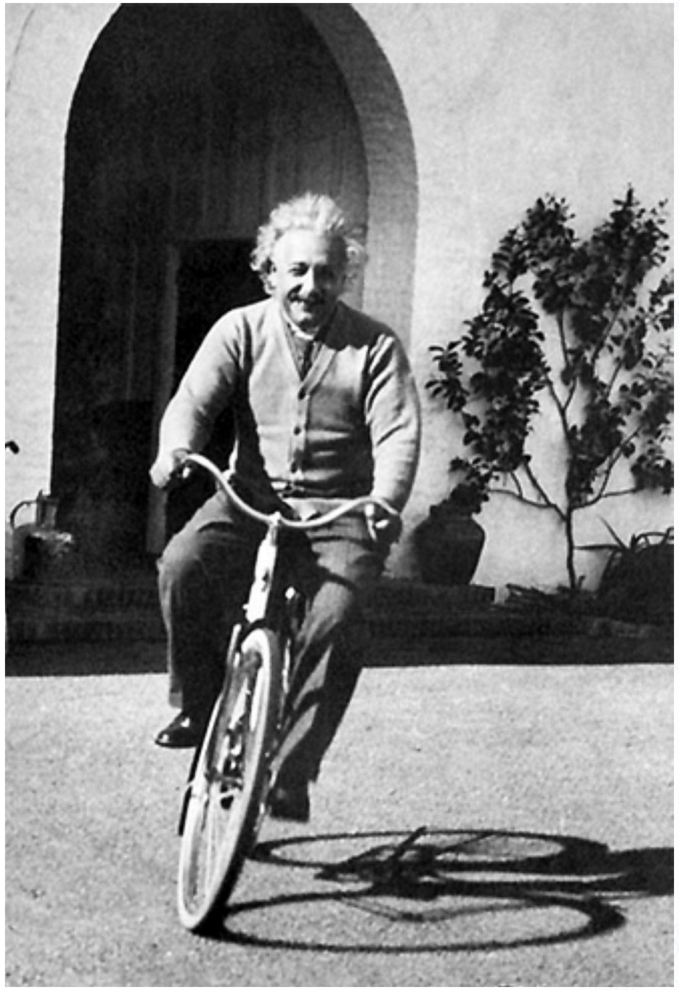
Quantum Computing

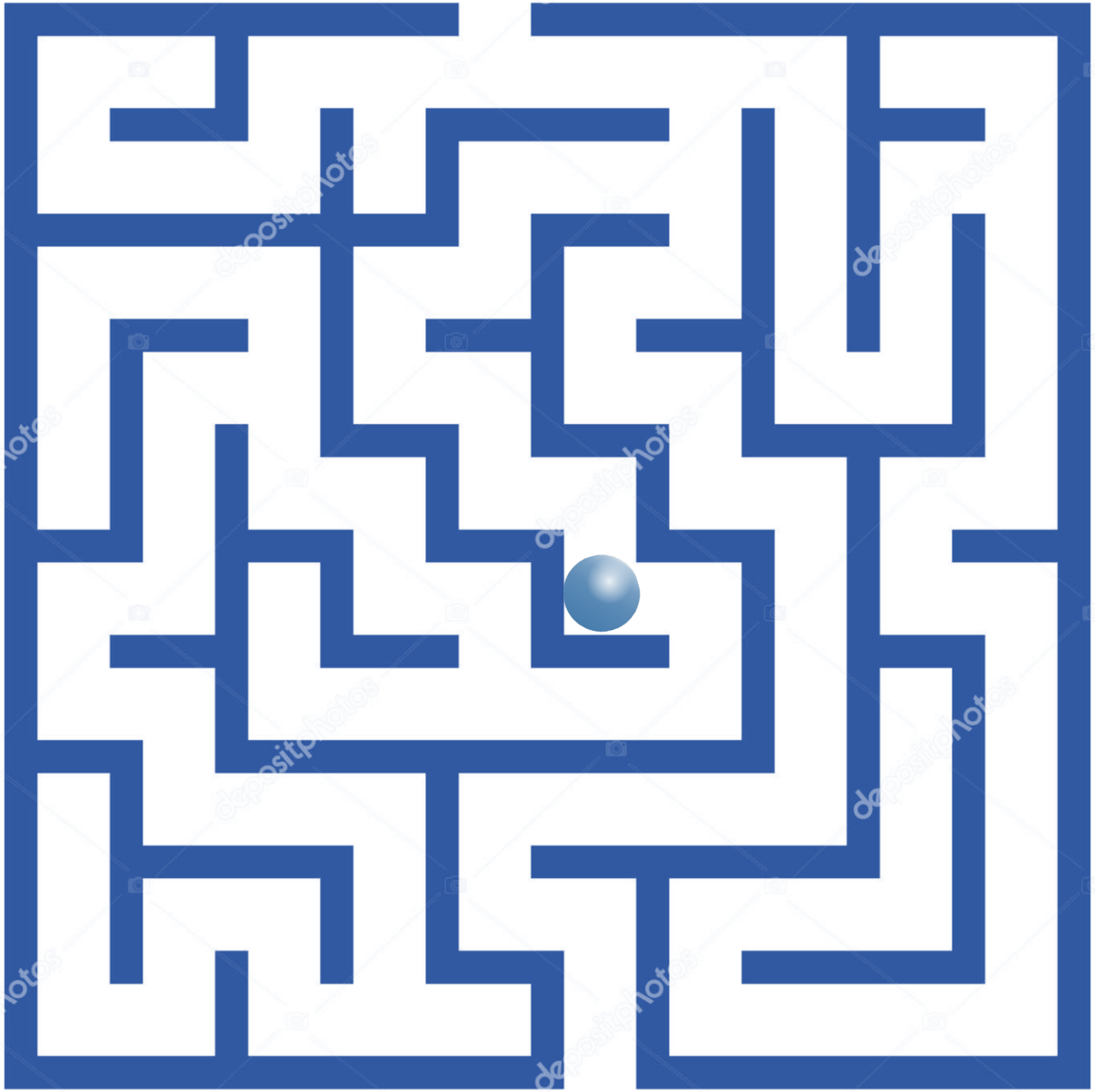
CLASSICAL COMPUTER





CLASSICAL COMPUTER

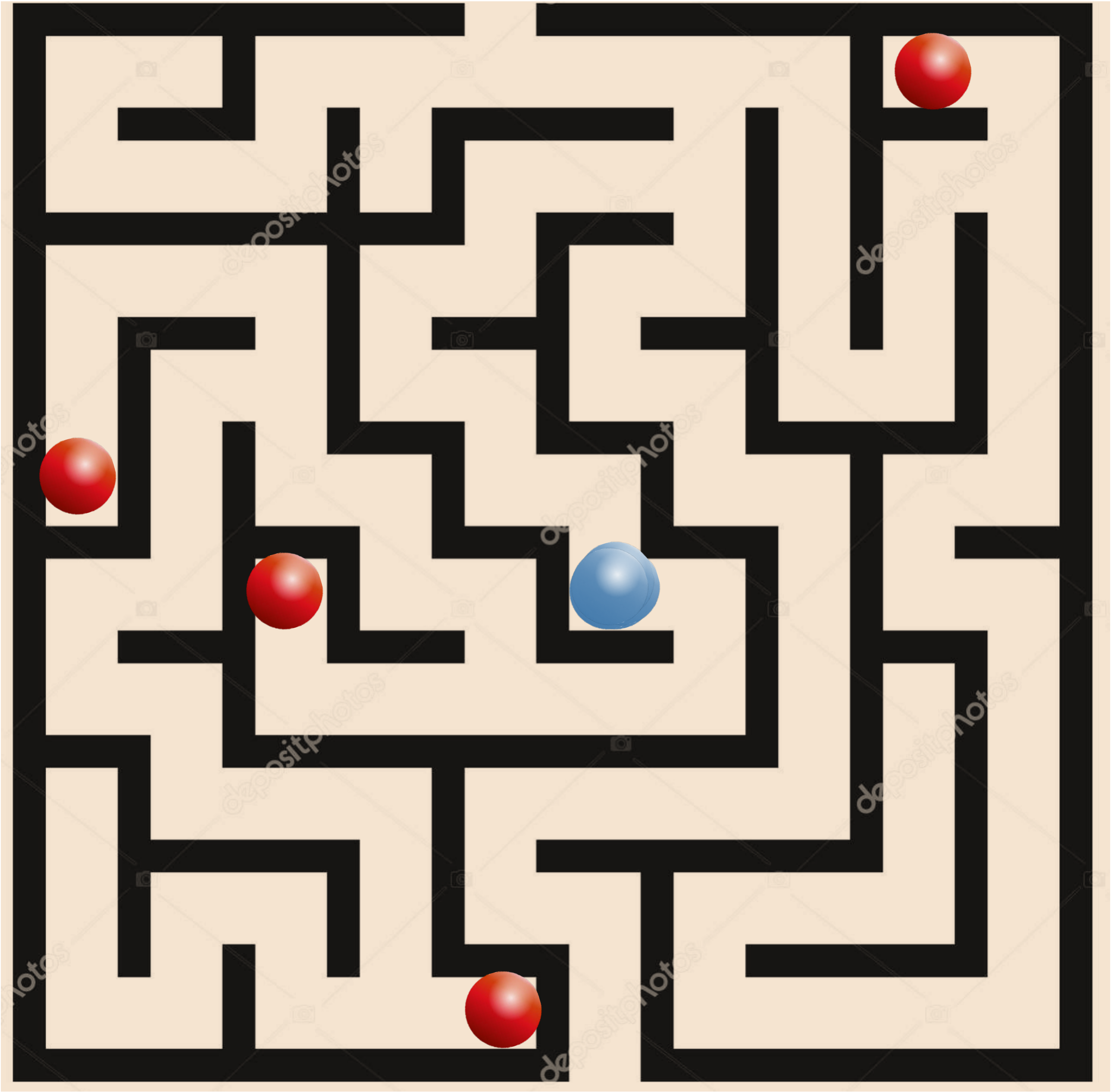




Quantum Computing

Quantum Computing

QUANTUM COMPUTER



Complexity theory

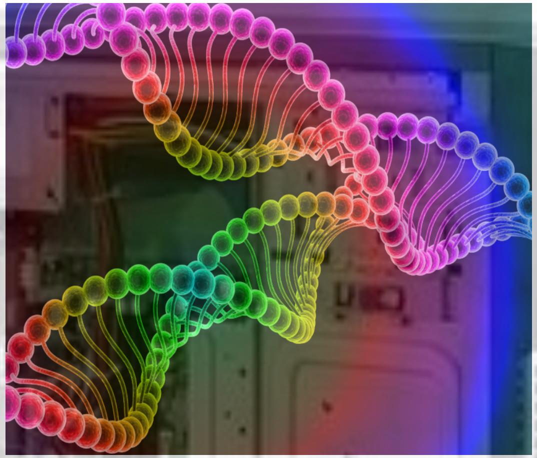
- Study of the computational effort required to run any algorithm. Usually given in terms of runtime/resources as a function of input size.
- By considering the best possible algorithm to solve a given problem, we can also study the computational effort inherent in solving this problem.
- It is useful to compare complexity of some problems for digital (slightly depending on the theoretical model used) and quantum computers.
- **Digital** computers: use discrete variables but can be built with arbitrarily high precision and methods for detecting and correcting errors exist.
- **Analog** computers: are based on precise manipulations of continuously varying parameters. They may quickly solve problems that are intractable for digital computers, but they cannot be built to reach arbitrarily precision.
- A **quantum** computers tries to combine the robustness of a digital computer with the subtle manipulations of an analog computer (exploiting in some sense the wave-particle duality typical of Quantum Mechanics).

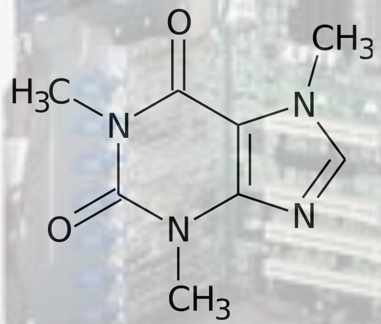
When to use a Quantum Computer

- To determine **global properties of a given function** (e.g. period or minimum). Rather then repeating the computation many times for a variety of different inputs, we can prepare a superposition of input states. By measuring the results we cannot access all of these states, but we can exploit interference to enhance the correct solution and infer the global property we require. E.g.: Grover's algorithm, $O(\sqrt{N})$ speedup.
- **Factoring** large numbers in primes. Shor's algorithm: super-polynomial speedup, from $O(e^{\sqrt[3]{n}})$ to $O(n^3)$.
- **Simulating quantum systems**, to design new materials, compute evolution of strongly interacting many-body systems, model molecules, drug design.
- **Optimization** problems: finance, protein-folding, traffic
- ……

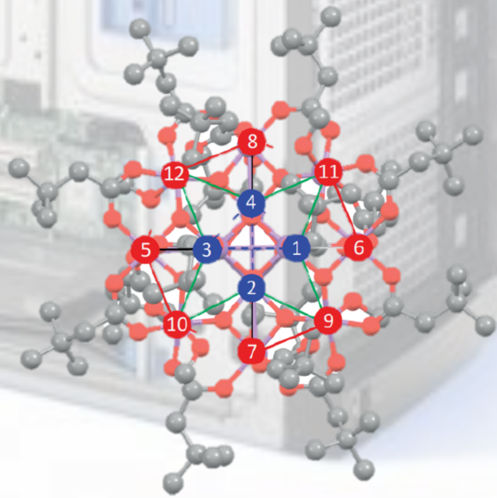
Quantum Computing

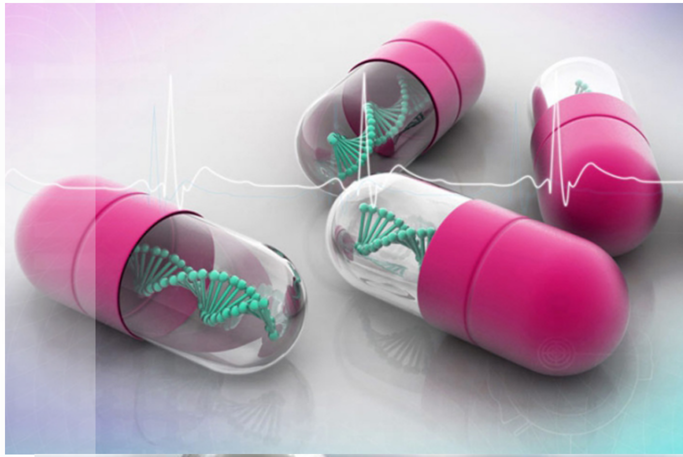
Understand → Design

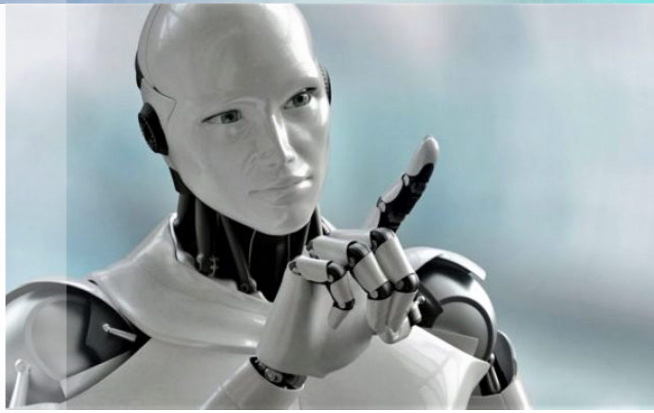




QC



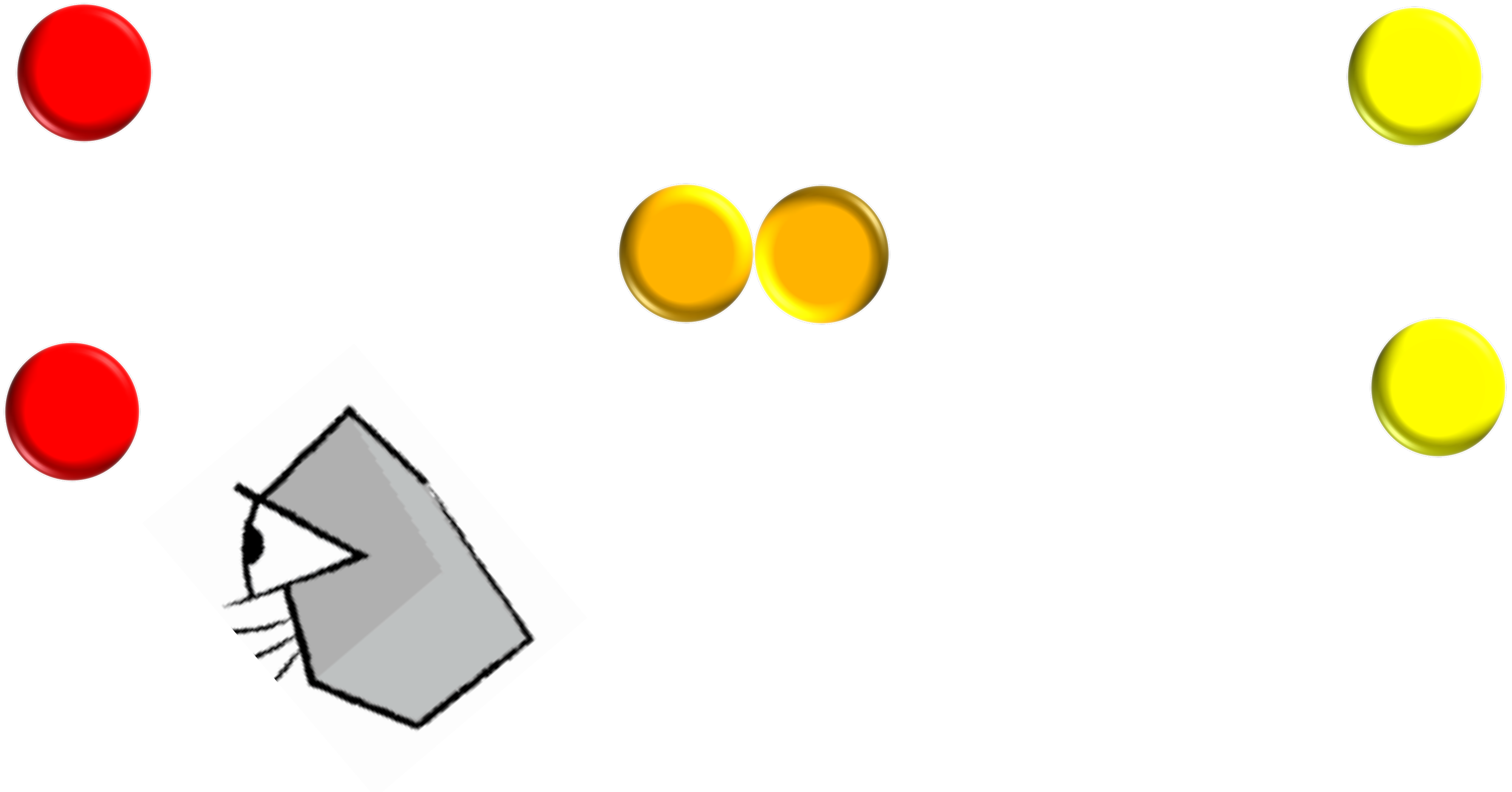




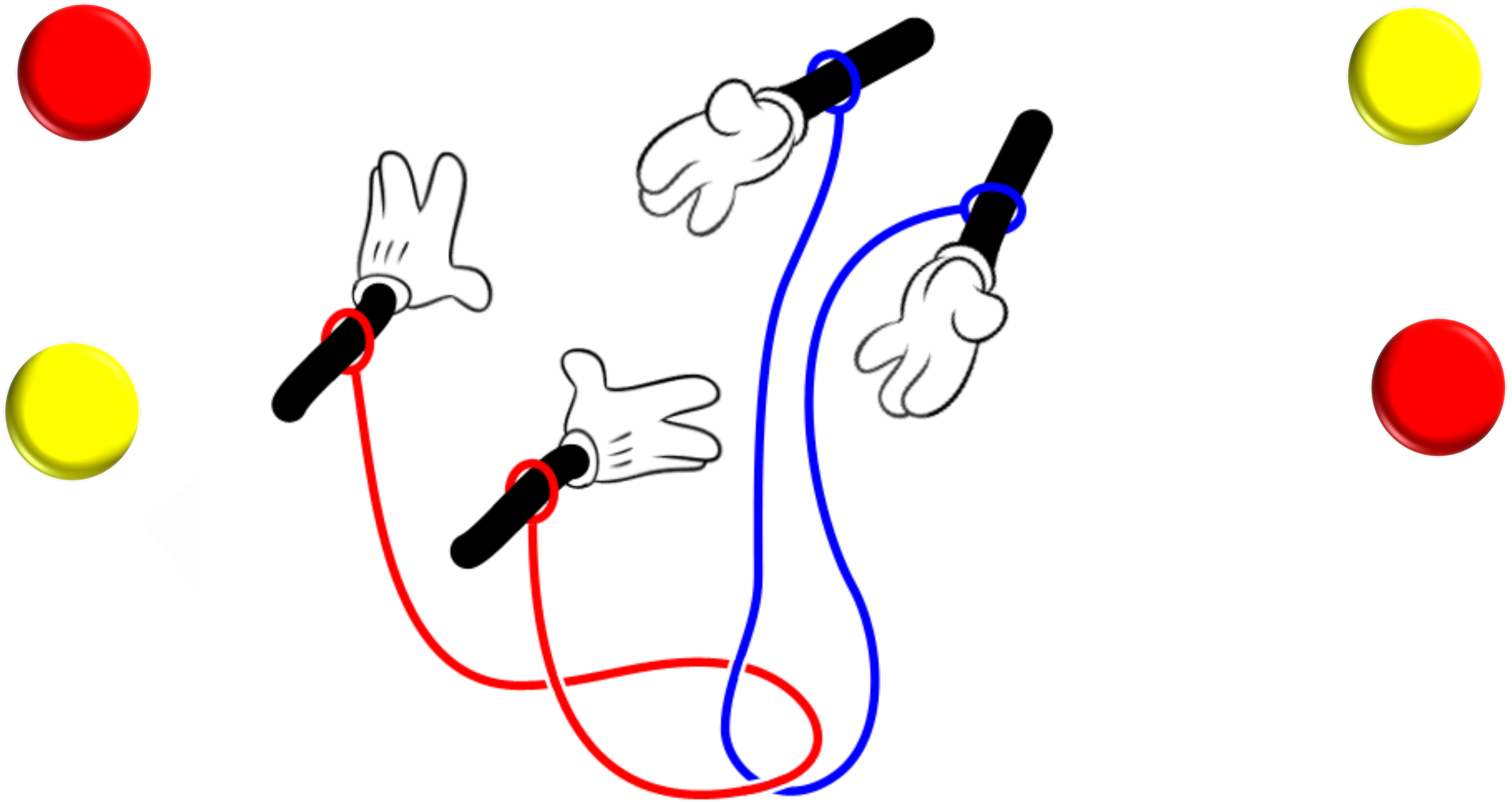
Unfortunately... we need some QM

Ingredients

Entanglement



Entanglement



Outline del corso

1. Prerequisites:
   I. the mathematical language (linear algebra)
   II. the programming language (Pyhton)
2. The Quantum Mechanical Tool-Box
3. Qubits
4. From one to multiple qubits: entangled states
5. Basic principles of Quantum Computing and Quantum Algorithms
6. Quantum Algorithms for Applications (including simulators)
7. From the code-world to reality: physical implementations, errors, decoherence, NISQs

Durante il corso useremo Qiskit, pacchetto Python per quantum-programmare e far girare I codici su simulatore o su hardware da remoto.

Testi consigliati

- M. Le Bellac, *A short introduction to Quantum Information and Quantum Computation*, Cambridge, UK (2006).
- P. Kaye, R. Laflamme, M. Mosca, *An introduction to Quantum Computing, Oxford University Press*, New York (2007).
- S. M. Barnett, *Quantum Information*, Oxford University Press, New York (2009).
- M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, New York (2000).
- A. Asfaw et al., https://qiskit.org/textbook/preface.html

Modalità esame e contatti

A. Orale tradizionale.

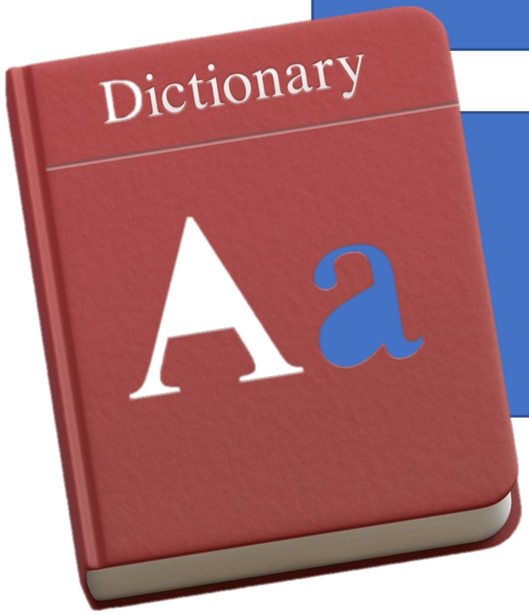
B. Progetto in Qiskit (simulatore) per risolvere un problema proof-of-principle (pochi qubit) che mostri uno speed-up quantistico. Breve relazione e discussione orale dei metodi utilizzati e dei risultati.

Mi trovate presso il Plesso di Fisica, previo contatto email alessandro.chiesa@unipr.it

- Lunedì 15-17
- Martedì 15-17

https://personale.unipr.it/it/ugovdocenti/person/110347

1. The mathematical language: Linear Algebra



Quantum Computing

UNIVERSITÀ DI PARMA

Hilbert spaces

A Hilbert space $\mathcal{H}$ is a **linear vector space** over the field $\mathbb{C}$ possessing an inner product which induces a norm and is complete with respect to this norm.

We use hereafter **Dirac notation**.

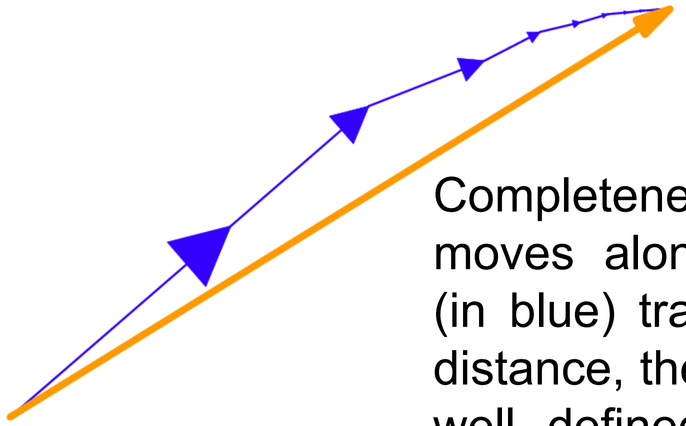
Linear superpositions of vectors still belong to $\mathcal{H}$

$$|v\rangle, |w\rangle \in \mathcal{H} \Rightarrow \alpha|v\rangle + \beta|w\rangle \in \mathcal{H}$$

Inner product: $\langle v|w\rangle \in \mathbb{C}$
linear map associating a complex number to each pair of elements $|v\rangle, |w\rangle \in \mathcal{H}$. Given $\alpha, \beta \in \mathbb{C}$ the following **properties** hold

- $\langle v|(\alpha|w_1\rangle + \beta|w_2\rangle) = \alpha\langle v|w_1\rangle + \beta\langle v|w_2\rangle$
- $\langle v|w\rangle = \langle w|v\rangle^*$
- $\langle v|v\rangle \geq 0$
- $\langle v|v\rangle = 0$ if and only if $|v\rangle = 0$

We then define the norm of state $|v\rangle$ as $\|v\| = \sqrt{\langle v|v\rangle}$.



Completeness: if a particle moves along the broken path (in blue) travelling a finite total distance, then the particle has a well defined net displacement (in orange)

Bra-kets and vectors

$$|v\rangle = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \qquad \Rightarrow \qquad \langle v| = |v\rangle^\dagger = \begin{pmatrix} v_1^* & v_2^* & \cdots & v_n^* \end{pmatrix}$$

$$|w\rangle = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}$$

Inner product $$\langle v|w\rangle = \begin{pmatrix} v_1^* & v_2^* & \cdots & v_n^* \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = v_1^* w_1 + v_2^* w_2 + \cdots + v_n^* w_n$$

Norm $$\||v\rangle\| = \sqrt{\langle v|v\rangle} = \sqrt{|v_1|^2 + |v_2|^2 + \cdots |v_n|^2}$$

Orthonormal basis sets

Two vectors $|v\rangle, |w\rangle \in \mathcal{H}$ are orthogonal if $\langle v|w\rangle = 0$.

Given a subspace $A \subseteq \mathcal{H}$, its orthogonal complement $A^{\perp}$ is the set of all vectors orthogonal to A.

If A is closed, the Hilbert space $\mathcal{H}$ is the direct sum of the two complementary closed spaces A and $A^{\perp}$, i.e. $\mathcal{H} = A \oplus A^{\perp}$ (Beppo-Levi theorem).

A set $U \subset \mathcal{H}$ of orthonormal vectors $|u_k\rangle$ (orthogonal and with unit norm) is complete if

$$\boxed{\sum_k |u_k\rangle\langle u_k| = \mathbb{I}} \qquad \text{i.e.} \qquad |v\rangle = \sum_k \langle u_k|v\rangle |u_k\rangle \quad \forall |v\rangle \in \mathcal{H}$$

COMPLETENESS RELATION

Therefore, U is a "good" basis set for $\mathcal{H}$. The size of U is the dimension of the Hilbert space.

Examples ($d = 2$)

$$U = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \quad \Rightarrow \quad \begin{pmatrix} a \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |v\rangle$$

$$U = \left\{ \underset{u_0}{\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}}, \underset{u_1}{\begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}} \right\}$$

$$\langle u_0|v\rangle = \frac{a+b}{\sqrt{2}} \qquad \langle u_1|v\rangle = \frac{a-b}{\sqrt{2}}$$

$$|v\rangle = \frac{a+b}{\sqrt{2}}|u_0\rangle + \frac{a-b}{\sqrt{2}}|u_1\rangle$$

Linear Operators and matrices

Linear operator $A\colon \mathcal{H} \to \mathcal{H}$ $\quad A(\alpha|v\rangle + \beta|w\rangle) = \alpha A|v\rangle + \beta A|w\rangle$

Limited if $\exists M \in \mathbb{R}$ s.t. $\||A|v\rangle\| \le M\||v\rangle\|\ \forall |v\rangle \in \mathcal{H}$ Then $\|A\| \doteq \sup_{|v\rangle \neq 0} \frac{\|A|v\rangle\|}{\||v\rangle\|}$

Matrix representation $|w\rangle = A|v\rangle \to |w_i\rangle = \sum_j A_{ij}|v_j\rangle$

Outer product Given $|v\rangle \in V$, $|w\rangle \in W$ Define $U\colon V \to W$

$U = |w\rangle\langle v|$ whose action is defined by $(|w\rangle\langle v|)|v'\rangle = |w\rangle\langle v|v'\rangle = \langle v|v'\rangle|w\rangle$

Recall the **completeness** relation:
given an orthonormal basis set $|k\rangle$ for the Hilbert space $\mathcal{H}$, any vector $|v\rangle \in \mathcal{H}$ can be written as $|v\rangle = \sum_k v_k|k\rangle$, with complex coefficients $v_k = \langle k|v\rangle$. Hence $|v\rangle = \sum_k \langle k|v\rangle|k\rangle = \sum_k |k\rangle\langle k|v\rangle$.
Since this equality holds $\forall|v\rangle$, we get $\boxed{\sum_k |k\rangle\langle k| = \mathbb{I},}$ i.e. the completeness relation.

We can use the completeness relation to obtain the outer product representation of an operator A:

$$A = \mathbb{I}_W A \mathbb{I}_V = \sum_{j,k} |w_j\rangle\langle w_j|A|v_k\rangle\langle v_k| = \sum_{j,k} \langle w_j|A|v_k\rangle|w_j\rangle\langle v_k| = \sum_{j,k} A_{jk}|w_j\rangle\langle v_k|$$

UNIVERSITÀ DI PARMA

Quantum Computing

Some useful operators

Given an operator A acting in the Hilbert space $\mathcal{H}$, there exist a unique operator $A^\dagger$ such that

$$\forall |v\rangle, |w\rangle \in \mathcal{H} \qquad (|v\rangle, A|w\rangle) = \left(A^\dagger|v\rangle, |w\rangle\right)$$

We call $A^\dagger$ the **adjoint** of A.

It is easy to see that $(AB)^\dagger = B^\dagger A^\dagger$. By convention $|v\rangle^\dagger = \langle v| \Rightarrow (A|v\rangle)^\dagger = \langle v|A^\dagger$

In a matrix representation, $\quad A^\dagger = (A^*)^T$

A is **Hermitian** or self-adjoint if $\quad A^\dagger = A$

Let $\{|1\rangle, \dots, |d\rangle\}$ be an orthonormal basis set for the Hilbert space $\mathcal{H}$ of dimension d and let V be a subspace of $\mathcal{H}$ spanned by the orthonormal basis set $\{|1\rangle, \dots, |n\rangle\}$, with $n < d$. Then

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & \\ & & & \ddots \; 0 \end{pmatrix} = P \equiv \sum_{k=1}^{n} |k\rangle\langle k|$$

Is the **projector** onto the subspace V. We can check that it is

- Hermitian ($P^\dagger = P$)
- Idem-potent $P^2 = P$

$$P^2 = \sum_{k,j} |k\rangle\overbrace{\langle k|j\rangle}^{\delta_{kj}}\langle j| = \sum_k |k\rangle\langle k| = P$$

The orthogonal complement of P is the operator $Q = \mathbb{I} - P$. Using the completeness relation, we can check that

$$Q \equiv \sum_{k=n+1}^{d} |k\rangle\langle k| = \begin{pmatrix} 0 & & & & \\ & 0 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix}$$

The vector space spanned by Q is the orthogonal complement of V.

$$P + Q = \mathbb{I}$$

Some useful operators

Normal operator $A^\dagger A = AA^\dagger$

Unitary operator $U^\dagger U = UU^\dagger = \mathbb{I}$

Unitary operator preserve norm and inner products:

If U is invertible, $U^\dagger = U^{-1}$

$$(U|v\rangle, U|w\rangle) = \langle v|U^\dagger U|w\rangle = \langle v|\mathbb{I}\,|w\rangle = \langle v|w\rangle$$

$\langle v|U^\dagger U|v\rangle = \langle v|v\rangle$

Outer product representation (for any two orthonormal basis sets $|u_k\rangle$ and $|v_k\rangle$)

$$U = \sum_k |u_k\rangle\langle v_k|$$

This matrix represents the basis transformation from $|v_k\rangle$ to $|u_k\rangle$

Pauli matrices

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

are **Hermitian and unitary**

Eigenvalues and eigenvectors

Eigenvalue equation $A|u\rangle = \lambda|u\rangle$

Complex eigenvalue

Eigenvector

Eigenvalues can be found by solving the characteristic equation. $\det|A - \lambda\mathbb{I}| = 0$

The set of (discrete) eigenvalues λ is the **spectrum** of A.

Hermitian operators are characterized by:

- **real eigenvalues** and
- **eigenvectors** corresponding to different eigenvalues are **orthogonal**

Diagonal (outer product) representation of A (discrete spectrum): $\Lambda = \sum_k \lambda_k P_k = \sum_k \lambda_k |u_k\rangle\langle u_k|$

This is an orthonormal decomposition into orthonormal eigenspaces spanned by eigenvectors $|u_k\rangle$

Given the unitary matrix V whose columns represent the eigenvectors: $\Lambda = V^\dagger A V$

Change of basis: given the unitary matrix $U = \sum_k |u_k\rangle\langle v_k|$ $A_u = U^\dagger A_v U$ Operator A written in the new basis $|u_k\rangle$

Example: Pauli matrices

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad |Z - \lambda\mathbb{I}| = \begin{vmatrix} 1-\lambda & 0 \\ 0 & -1-\lambda \end{vmatrix} = -(1-\lambda)(1+\lambda)$$

$$|Z - \lambda\mathbb{I}| = 0 \Longrightarrow (1-\lambda)(1+\lambda) = 0 \Longrightarrow \lambda = \pm 1 \qquad |u_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |u_{-1}\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad |X - \lambda\mathbb{I}| = \begin{vmatrix} -\lambda & 1 \\ 1 & -\lambda \end{vmatrix} = \lambda^2 - 1$$

$$|X - \lambda\mathbb{I}| = 0 \Longrightarrow \lambda^2 - 1 = 0 \Longrightarrow \lambda = \pm 1 \qquad |u_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad |u_{-1}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

The eigenvalues of unitary matrices are complex numbers of modulus 1. Indeed

$$U|\phi\rangle = \lambda|\phi\rangle \Longrightarrow \langle\phi|U^\dagger = \lambda^*\langle\phi| \Longrightarrow \langle\phi|U^\dagger U|\phi\rangle = \lambda^*\lambda \Longrightarrow \lambda^*\lambda = 1$$

$U|\phi\rangle = \lambda|\phi\rangle$ $\qquad \langle\phi|U^\dagger U|\phi\rangle = \langle\phi|\phi\rangle$

$\langle\phi|U^\dagger = \lambda^*\langle\phi|$ $\qquad \lambda^*\lambda\langle\phi|\phi\rangle =$ $\qquad \lambda^*\lambda = 1$

$|\lambda|^2 = 1$

Operator functions

$\sigma_x = X, \sigma_y = Y$

Commutator $[A,B] = AB - BA$ $\qquad [\sigma_\alpha, \sigma_\beta] = 2i\varepsilon_{\alpha\beta\gamma}\sigma_\gamma$

Anti-commutator $\{A,B\} = AB + BA$ $\qquad [X,Y] = XY - YX = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} - \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 2i & 0 \\ 0 & -2i \end{pmatrix} = 2iZ$

Verify the following identities: $\qquad [Z,X] = 2iY$

$$AB = \frac{\{A,B\} + [A,B]}{2} \qquad [A,B]^\dagger = [B^\dagger, A^\dagger] \qquad \{\sigma_\alpha, \sigma_\beta\} = 0$$

$XY + YX = 0$

Simultaneous diagonalization theorem:

$[A,B] = 0 \Leftrightarrow$ there exist a basis of simultaneous eigenvectors for A and B

Trace $\qquad \mathrm{Tr}A = \sum_i A_{ii}$

- Cyclic $\mathrm{Tr}[ABC] = \mathrm{Tr}[CAB] = \mathrm{Tr}[BCA]$
- Linear $\mathrm{Tr}[aA + bB] = a\mathrm{Tr}[A] + \mathrm{bTr}[B]$

$$\mathrm{Tr}\,[\mathrm{A}|\psi\rangle\langle\psi|] = \sum_i \langle i|A|\psi\rangle\langle\psi|i\rangle = \underbrace{\sum_i \langle\psi|i\rangle\langle i|}_{=\mathbb{I}}A|\psi\rangle = \langle\psi|A|\psi\rangle$$

Matrix exponential

Given a Hermitian limited operator H, the operator $e^{iHt} = \sum_{n=0}^{\infty} \frac{i^n t^n}{n!} H^n = U$ is unitary.

Indeed, $U^\dagger = e^{-iH^\dagger t} = e^{-iHt}$. Hence $U^\dagger U = e^{-iHt} e^{iHt} = \mathbb{I}$

Pauli matrices $\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$$h = a_1 X + a_2 Y + a_3 Z = \begin{pmatrix} a_3 & a_1 - i a_2 \\ a_1 + i a_2 & -a_3 \end{pmatrix}$$

$a_1 = \mathrm{Tr}(Xh)/2$ $a_2 = \mathrm{Tr}(Yh)/2$ $a_3 = \mathrm{Tr}(Zh)/2$

$\mathrm{Tr}(h) = 0$

$a_i \in \mathbb{R}$

$h^2 = a^2 \mathbb{I} \Rightarrow h^{2n} = a^{2n} \mathbb{I}$, $h^{2n+1} = a^{2n} h$ $a^2 = a_1^2 + a_2^2 + a_3^2$

$$\Rightarrow \quad e^{ih} = \sum_{n=0}^{\infty} \frac{(ih)^{2n}}{(2n)!} + \frac{(ih)^{2n+1}}{(2n+1)!} = \sum_{n=0}^{\infty} \frac{(h)^{2n}}{(2n)!} (-1)^n + i \sum_{n=0}^{\infty} \frac{(h)^{2n+1}}{(2n+1)!} (-1)^n$$

$$= \mathbb{I} \underbrace{\sum_{n=0}^{\infty} \frac{(-1)^n a^{2n}}{(2n)!}}_{\cos a} + ih \underbrace{\sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} a^{2n}}_{\sin a / a}$$

$$\Rightarrow \quad e^{ih} = \mathbb{I} \cos a + ih \frac{\sin a}{a}$$

Exercise

We can easily find eigenvalues and eigenvectors of the generic Hermitian zero-trace matrix h. These are

$$\lambda_\pm = \pm a = \pm\sqrt{a_1^2 + a_2^2 + a_3^2} \qquad |\phi_\pm\rangle = \begin{pmatrix} \dfrac{\pm(a_1 - ia_2)}{\sqrt{2a(a \mp a_3)}} \\ \sqrt{\dfrac{a \mp a_3}{2a}} \end{pmatrix}$$

The most general Hermitian matrix H of order 2 can be decomposed into Pauli matrices as follows:

Hilbert-Schmidt inner products on operators: $(A, B) = \mathrm{Tr}[A^\dagger B]$

$$H = \begin{pmatrix} a_0 + a_3 & a_1 - ia_2 \\ a_1 + ia_2 & a_0 - a_3 \end{pmatrix}$$

$$a_0 = (\mathrm{I}, \mathrm{H})/\|I\|^2 = \mathrm{Tr}(H)/2$$

$$a_1 = \mathrm{Tr}(XH)/2$$

$$a_2 = \mathrm{Tr}(YH)/2$$

$$a_3 = \mathrm{Tr}(ZH)/2$$

Exercise: Suzuki-Trotter expansion

- Show that, given two non-commuting operators A, B with $[A, B] \neq 0$
$$e^{x(A+B)} = e^{xA}e^{xB} + O(x^2)$$

- Show that the decomposition $e^{x(A+B)} \approx e^{xB/2}e^{xA}e^{xB/2}$ provides a better approximation.

Hint: expand $e^{x(A+B)} = \mathbb{I} + x(A+B) + \frac{1}{2}x^2(A+B)^2 + O(x^3)$ *and compare it with the product of the separate expansions of* e^{xA} *and* e^{xB}

Remember this for quantum simulations https://arxiv.org/pdf/math-ph/0506007v1.pdf

2. The Quantum Mechanical Tool-Box

Quantum Computing

UNIVERSITÀ DI PARMA

The postulates

1. *The state of a quantum physical system is completely specified by its state vector of unit norm, indicated by the ket $|\psi\rangle \in \mathcal{H}$ (Hilbert space).*

Since $\mathcal{H}$ is a linear vector space, given two normalized vectors $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$

$$|\psi\rangle = \alpha|\psi_1\rangle + \beta|\psi_2\rangle \quad (\text{with } |\alpha|^2 + |\beta|^2 = 1)$$

still belongs to $\mathcal{H}$ and is a possible state vector of the system.

An equivalent representation is given in terms of the bra

$$\langle\psi| = \alpha^*\langle\psi_1| + \beta^*\langle\psi_2|$$

The postulates

2. *Let $|\psi\rangle$ be the state vector of a micro-system and $|\phi\rangle$ another state within the same Hilbert space. Then the probability amplitude to find $|\psi\rangle$ in $|\phi\rangle$ is the complex number $\langle\phi|\psi\rangle$ and the relative probability is $|\langle\phi|\psi\rangle|^2$.*

Being all the states normalized, we find

$$0 \leq |\langle\phi|\psi\rangle|^2 \leq 1$$

The postulates

3. *We can associate to each observable $\mathcal{A}$ an Hermitian operator A acting on the Hilbert space $\mathcal{H}$. The spectrum of A constitutes the range of possible values of the observable.*

Spectral decomposition of A: $A = \sum_k a_k |k\rangle\langle k|$ with non-degenerate a_k eigenvalues

In a measurement of the observable $\mathcal{A}$ for a system described by state vector $|\psi\rangle$, we will find the result a_k with probability $p_k = |\langle k|\psi\rangle|^2$. That is, if we consider N copies of the physical system (always prepared in state $|\psi\rangle$) our measurement will give us the result a_k for a number of times close to $N|\langle k|\psi\rangle|^2$ in the limit $N \to \infty$.

In such limit, the **expectation value** of $\mathcal{A}$ on state $|\psi\rangle$ is given by

$$\langle A\rangle_\psi = \langle\psi|A|\psi\rangle = \sum_k a_k \langle\psi|k\rangle\langle k|\psi\rangle = \sum_k a_k p_k$$

Degenerate eigenvalues

If the observable $\mathcal{A}$ has degenerate eigenvalues, each eigenvalue a_k corresponds to a subspace spanned by (ortho-normalized) eigenvectors

$$|k,l\rangle, \qquad l = 1, 2, \ldots, g(k)$$

with $g(k)$ the degeneracy of eigenvalue a_k.

The probability $P(a_k) = \sum_{l=1}^{g(k)} |\langle\psi|k,l\rangle|^2 = \langle\psi|P_k|\psi\rangle$

$$P_k = \sum_{l=1}^{g(k)} |k,l\rangle\langle k,l|$$

$$P_\psi = |\psi\rangle\langle\psi| \qquad \langle A\rangle_\psi = \langle\psi|A|\psi\rangle = \mathrm{Tr}[AP_\psi] \qquad p(a_k) = \mathrm{Tr}[P_k P_\psi]$$

The postulates

4. *After a measurements of the observable $\mathcal{A}$ with outcome a_k the state of the system is projected onto the corresponding subspace.*

$$|\psi\rangle \longrightarrow \frac{P_k|\psi\rangle}{||P_k|\psi\rangle||}$$

Hence a repetition of the same measurement yields a_k with probability 1.

Compatible observables $\Longleftrightarrow$ $[A, B] = 0$ $\Longleftrightarrow$ A, B have a common eigenbasis

Complete set of commuting observables (CSCO): set of hermitian operators characterized by a non-degenerate complete set of orthonormal eigenvectors

$$p(A = a_k, B = b_l) = \sum_{m=1}^{g(k,l)} |\langle k, l, m|\psi\rangle|^2 = \langle\psi|P_{k,l}|\psi\rangle \qquad P_{k,l} = \sum_m |k, l, m\rangle\langle k, l, m|$$

The eigenvectors of a non-degenerate set of eigenvalues of a CSCO form a basis of the Hilbert space

The postulates

5. *The time-evolution of a closed quantum system is described by a unitary transformation.*

$$|\psi(t)\rangle = U(t, t_0)|\psi(t_0)\rangle$$

5. *The time-evolution of a closed quantum system is described by the Schrödinger equation*

$$i\hbar \frac{d|\psi(t)\rangle}{dt} = H|\psi(t)\rangle$$

Hamiltonian of the closed system (hermitian operator).
It completely determines the dynamics of the system.

Quantum Computing

Dynamics

We can write an analogous differential equation for the time evolution operator:

$$i\hbar \frac{d}{dt} U(t, t_0) = H(t) U(t, t_0) \qquad U(t_0, t_0) = \mathbb{I}$$

For time-independent Hamiltonian $\frac{\partial H}{\partial t} = 0 \Longrightarrow U(t, t_0) = e^{-\frac{iH(t-t_0)}{\hbar}} = U(t - t_0)$

$$|\psi(t)\rangle = U\,|\psi(t_0)\rangle \Longrightarrow$$

$$\langle A(t)\rangle_\psi = \langle \psi(t)|A|\psi(t)\rangle = \big(\langle \psi(t_0)|U^\dagger\big) A \big(U|\psi(t_0)\rangle\big)$$

Operator fixed,
Evolution of the ket (Schrödinger picture)

$$= \left\langle \psi(t_0) \middle| U^\dagger A U \middle| \psi(t_0) \right\rangle$$

Evolution of the operator,
Ket fixed (Heisenberg picture)

A is a **constant** of motion if

$$\frac{d}{dt}\langle \psi(t)|A|\psi(t)\rangle = 0 \quad \forall |\psi(t_0)\rangle \quad \Longrightarrow \quad [A, H] + i\hbar \frac{\partial A(t)}{\partial t} = 0$$

In that case, its eigenvalues and probability distributions are independent of time.

Time evolution, time independent Hamiltonian

$$H = \sum_k E_k |\phi_k\rangle\langle\phi_k|$$ Spectral decomposition of the Hamiltonian

$$|\psi(0)\rangle = \sum_k |\phi_k\rangle\langle\phi_k|\psi(0)\rangle \Rightarrow \sum_k \alpha_k |\phi_k\rangle \qquad \alpha_k = \langle\phi_k|\psi(0)\rangle$$

$$|\psi(t)\rangle = e^{-\frac{iHt}{\hbar}}|\psi(0)\rangle = \sum_k \alpha_k e^{-\frac{iE_k t}{\hbar}}|\phi_k\rangle = \sum_k \boxed{c_k(t)}|\phi_k\rangle$$

$$c_k(t) = \langle\phi_k|\psi(0)\rangle e^{-\frac{iE_k t}{\hbar}}$$

$$|\psi(0)\rangle = |\phi_k\rangle \;\Longrightarrow\; |\psi(t)\rangle = e^{-\frac{iE_k t}{\hbar}}|\phi_k\rangle \;\Longrightarrow\; |\langle\psi(0)|\psi(t)\rangle|^2 = 1$$

Eigenstates of H are stationary (overall phase is irrelevant)

Exercise

Given the Hamiltonian and three observables of a physical system

$$H = w\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad A = a\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \qquad B = b\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad C = c\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

1. Determine which observables are constant of motion
2. A measurement of C at time $t = 0$ gives the result 0. Which is the result of a measurement of A at time $t > 0$?
3. Determine three different CSCO.

Exercise: spin precession

$$H = \frac{\Delta}{2}\sigma_z = \begin{pmatrix} \frac{\Delta}{2} & 0 \\ 0 & -\frac{\Delta}{2} \end{pmatrix} = \frac{\Delta}{2}|0\rangle\langle 0| - \frac{\Delta}{2}|1\rangle\langle 1|$$

$$|\psi(0)\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|\psi(t)\rangle = e^{-iHt/\hbar}|\psi(0)\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} e^{-i\Delta t/2\hbar} \\ e^{i\Delta t/2\hbar} \end{pmatrix} = \frac{1}{\sqrt{2}}\left(e^{-i\Delta t/2\hbar}|0\rangle + e^{i\Delta t/2\hbar}|1\rangle\right)$$

$$S_z = (|0\rangle\langle 0| - |1\rangle\langle 1|)/2 \qquad \Rightarrow \langle\psi(t)|S_z|\psi(t)\rangle = 0$$

$$S_x = (|0\rangle\langle 1| + |1\rangle\langle 0|)/2 \qquad \Rightarrow \langle\psi(t)|S_x|\psi(t)\rangle = \frac{1}{2}\cos\omega t$$

Check that $\langle\psi(t)|S_y|\psi(t)\rangle = \frac{1}{2}\sin\omega t$

The spin (prepared along x) precedes about the magnetic field (z axis) with $\omega = \Delta/\hbar$

Exercise: paramagnetic resonance (Rabi problem)

$$H = \frac{1}{2}\begin{pmatrix} -\Delta & g\, e^{i\omega t} \\ g\, e^{-i\omega t} & \Delta \end{pmatrix} = -\frac{\Delta}{2}\sigma_z + \frac{g}{2}\left(|0\rangle\langle 1|\, e^{i\omega t} + |1\rangle\langle 0|\, e^{-i\omega t}\right)$$

Pulse at frequency $\omega \neq \Delta/\hbar$

$$|\psi(0)\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

We look for a solution of the form

$$|\psi(t)\rangle = \begin{pmatrix} a(t) \\ b(t) \end{pmatrix} = \begin{pmatrix} \alpha(t)\, e^{i\omega t/2} \\ \beta(t)\, e^{-i\omega t/2} \end{pmatrix}$$

$$\frac{d}{dt}|\psi(t)\rangle = \begin{pmatrix} \dot{a}(t) \\ \dot{b}(t) \end{pmatrix} = \begin{pmatrix} [\dot{\alpha}\,(t) + \frac{i\omega}{2}]\, e^{\frac{i\omega t}{2}} \\ [\dot{\beta}(t) - \frac{i\omega}{2}]\, e^{-i\omega t/2} \end{pmatrix}$$

$$H|\psi(t)\rangle = \begin{pmatrix} [-\alpha(t)\Delta + \beta(t) g]/2\, e^{i\omega t/2} \\ [\alpha(t) g + \beta(t)\Delta]/2\, e^{-i\omega t/2} \end{pmatrix}$$

The Schrödinger equation $i\hbar \frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle$ becomes $i\hbar \frac{d}{dt}|\tilde{\psi}\,(t)\rangle = \tilde{H}|\psi(t)\rangle$

$$\tilde{H} = \frac{1}{2}\begin{pmatrix} \hbar\omega - \Delta & g \\ g & -\hbar\omega + \Delta \end{pmatrix} \qquad |\tilde{\psi}\,(t)\rangle = \begin{pmatrix} \alpha(t) \\ \beta(t) \end{pmatrix}$$

Effective time-independent Hamiltonian

Exercise: paramagnetic resonance (Rabi problem)

$$\tilde{H} = \frac{1}{2}\begin{pmatrix} \hbar\omega - \Delta & g \\ g & -\hbar\omega + \Delta \end{pmatrix}$$

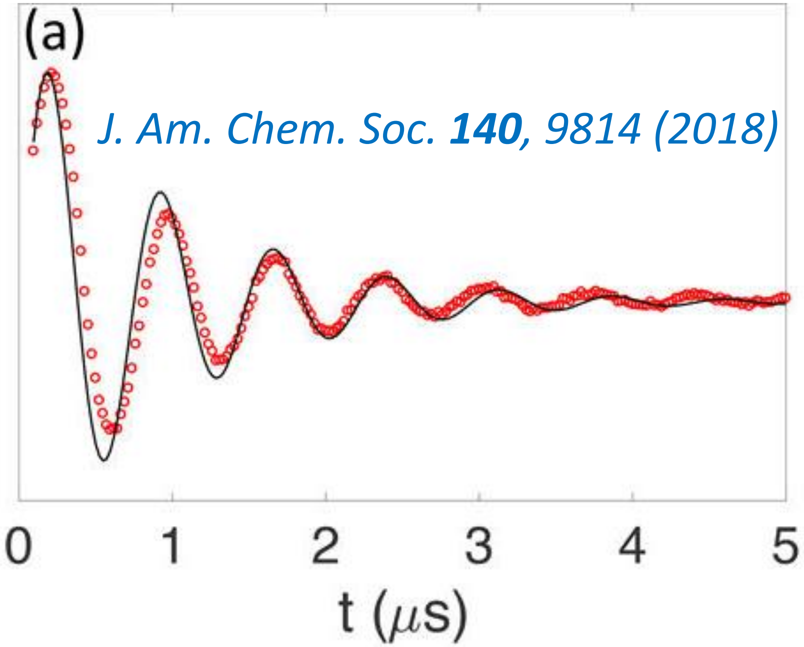
On resonance ($\hbar\omega = \Delta$) this implements a **rotation** about x

$$\tilde{H} = \frac{1}{2}\begin{pmatrix} 0 & g \\ g & 0 \end{pmatrix} \qquad U = e^{i\tilde{H}t} = \begin{pmatrix} \cos\Omega t & -i\sin\Omega t \\ -i\sin\Omega t & \cos\Omega t \end{pmatrix} \qquad \Omega = g/2\hbar$$

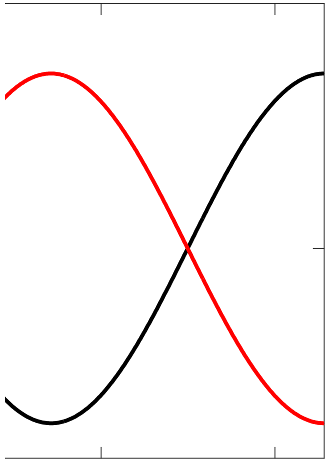
Out of resonance $\quad |\beta(t)|^2 = \dfrac{g^2/4\hbar^2}{\Omega^2}\sin^2\Omega\, t$

$$\Omega = \sqrt{\frac{g^2}{4\hbar^2} + \frac{(\omega - \Delta/\hbar)^2}{4}}$$

Rabi frequency



C. Alabiso



relativistica, 7.15

Additional problems

C. Alabiso, A. Chiesa, *Problemi di meccanica quantistica non relativistica*, Springer-Verlag (Milano, 2013)

Es.: 7.3, 9.4, 9.29, 9.30, 11.4, 11.38, 11.49

Uncertainty principle

$$\Delta A^2 = \langle\psi|(A-\langle A\rangle)^2|\psi\rangle = \langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2 \qquad \Delta A = \sqrt{\Delta A^2}$$ uncertainty

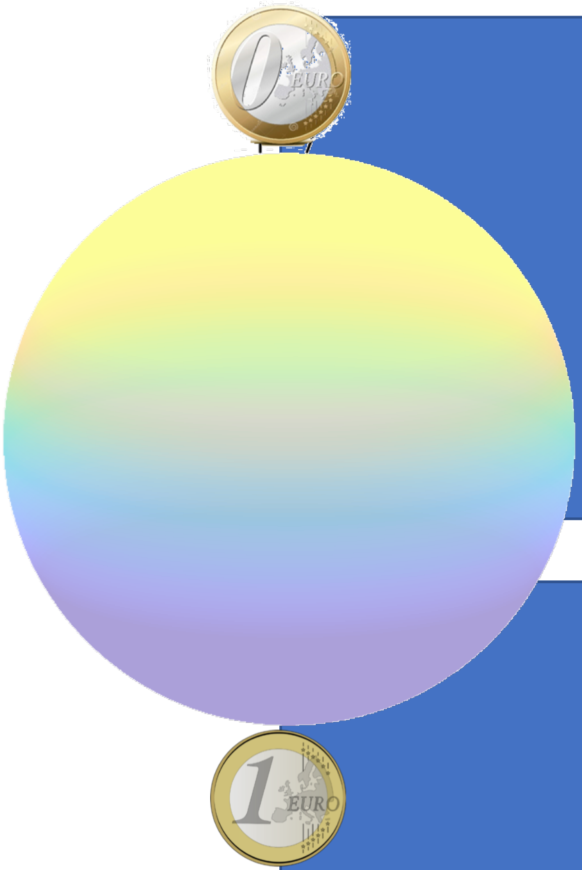
$$\Delta A\,\Delta B \geq \frac{1}{2}|\langle[A,B]\rangle|$$

***Heisenberg principle**: if we prepare a large number of quantum systems in identical states and then we perform measurements of A on some systems and of B on some others, there is a lower bound on the product of the standard deviations of A and B. This limits our possible simultaneous knowledge of incompatible observables.*

Let's consider two incompatible observables A, B such that $[A,B] = iC \neq 0$ ($C^\dagger = C$)

$$|\psi\rangle = |0\rangle \qquad [X,Y] = 2iZ \Longrightarrow \Delta X\,\Delta Y \geq |\langle Z\rangle| = 1 \Longrightarrow \qquad \Delta X, \Delta Y > 0$$

(We can easily check that $\Delta X^2 = \Delta Y^2 = 1$)



3. Qubits

Quantum Computing

UNIVERSITÀ DI PARMA

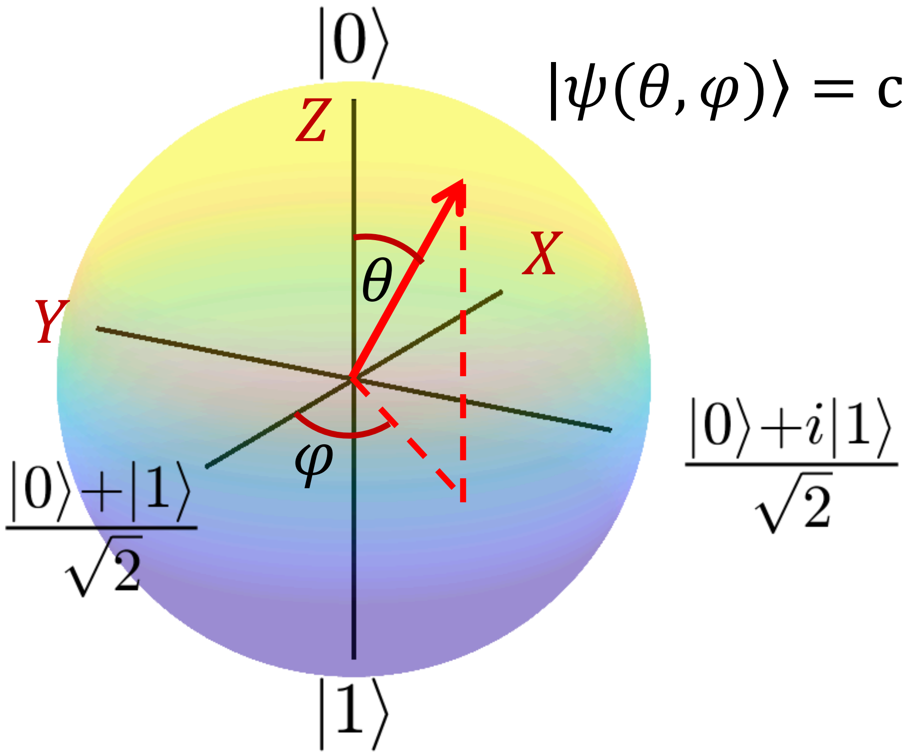
Qubit states

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \quad \text{BASIS}$$

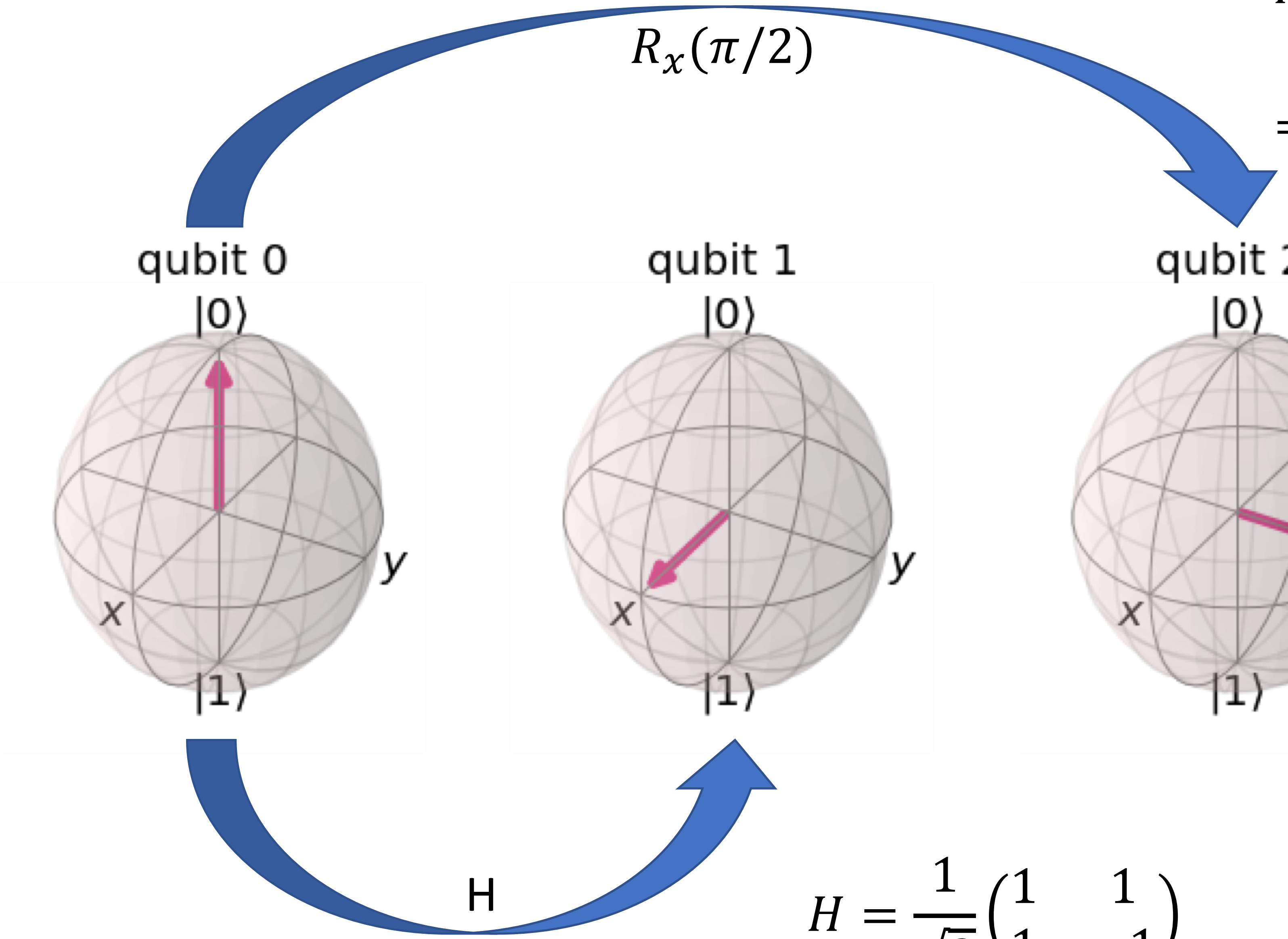
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha\\\beta\end{pmatrix}$$

$$\alpha, \beta \in \mathbb{C}$$
$$|\alpha|^2 + |\beta|^2 = 1$$

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



- The surface of this sphere is a valid Hilbert space
- Unitary operators (preserving the norm) induce rotations on the Bloch sphere



$$R_x(\vartheta) = e^{-i\vartheta X/2} = \begin{pmatrix} \cos\frac{\vartheta}{2} & -i\sin\frac{\vartheta}{2} \\ -i\sin\frac{\vartheta}{2} & \cos\frac{\vartheta}{2} \end{pmatrix}$$

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

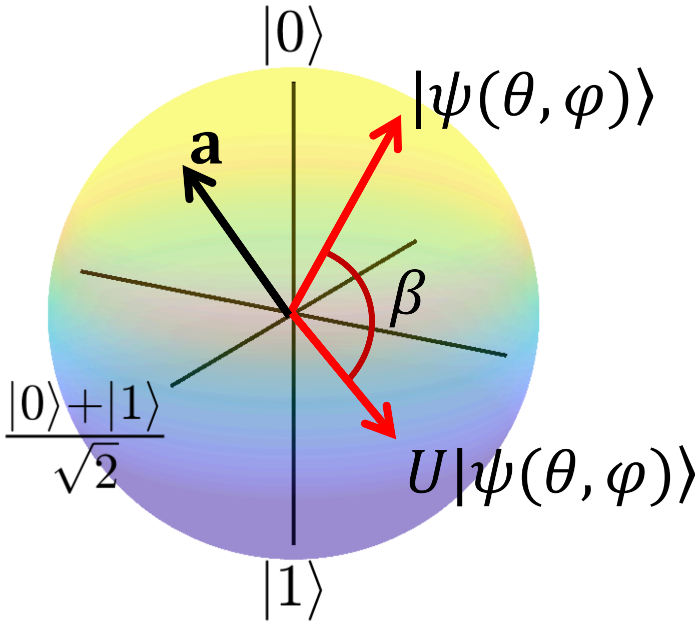
Single-qubit gates

$$U = e^{i(\alpha\mathbb{I}+\beta\,\mathbf{a}\cdot\boldsymbol{\sigma}/2)} = e^{i\alpha}\left(\cos\frac{\beta}{2}\mathbb{I} + i\sin\frac{\beta}{2}\mathbf{a}\cdot\boldsymbol{\sigma}\right)$$

General unitary transformation:
Rotation of β about axis $\mathbf{a}$.

Decomposition in Euler angles:

$$U = e^{i\alpha}e^{i\xi Z/2}e^{i\mu Y/2}e^{i\gamma Z/2}$$



$$R_\alpha(\vartheta) = e^{-i\vartheta\sigma_\alpha/2}\begin{cases} R_x(\vartheta) = \begin{pmatrix} \cos\vartheta/2 & -i\sin\vartheta/2 \\ -i\sin\vartheta/2 & \cos\vartheta/2 \end{pmatrix} \\ R_y(\vartheta) = \begin{pmatrix} \cos\vartheta/2 & -\sin\vartheta/2 \\ \sin\vartheta/2 & \cos\vartheta/2 \end{pmatrix} \\ R_z(\vartheta) = \begin{pmatrix} e^{-i\vartheta/2} & 0 \\ 0 & e^{i\vartheta/2} \end{pmatrix} = e^{-i\vartheta/2}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\vartheta} \end{pmatrix} \end{cases}$$

QISKIT

$$U_1(\lambda) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{pmatrix} = e^{-\frac{i\lambda}{2}} R_z(\lambda) \propto R_z(\lambda)$$

$$U_2(\phi, \lambda) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -e^{i\lambda} \\ e^{i\phi} & e^{i(\phi+\lambda)} \end{pmatrix}$$

$$H = U_2(0, \pi)$$

$$U_3(\theta, \phi, \lambda) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} e^{i\lambda} \\ \sin\frac{\theta}{2} e^{i\phi} & \cos\frac{\theta}{2} e^{i(\phi+\lambda)} \end{pmatrix}$$

$$R_x(\theta) = U_3(\theta, -\pi/2, \pi/2)$$

$$R_y(\theta) = U_3(\theta, 0,0)$$

$$R_z(\lambda) \propto U_3(0,0, \lambda)$$

Measurements

Let's consider the pure state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

- **Z-basis measurement**: $p_0 = |\alpha|^2, \quad p_1 = |\beta|^2 = 1 - |\alpha|^2$. $\langle Z \rangle = p_0 - p_1$
- **X-basis measurement**: first apply H, then measure

$$|\psi_X\rangle = H|\psi\rangle = \alpha\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

$$p_0 = \left|\frac{\alpha+\beta}{\sqrt{2}}\right|^2 = \frac{1}{2}(|\alpha|^2 + \alpha\beta^* + \alpha^*\beta + |\beta|^2)$$

$$p_1 = \left|\frac{\alpha-\beta}{\sqrt{2}}\right|^2 = \frac{1}{2}(|\alpha|^2 - \alpha\beta^* - \alpha^*\beta + |\beta|^2)$$

$$p_0 - p_1 = \alpha\beta^* + \alpha^*\beta = \\ = \langle X \rangle = \langle\psi|X|\psi\rangle$$

Hence we call this X-basis measurement.

How can we get Y-basis measurements?

State tomography

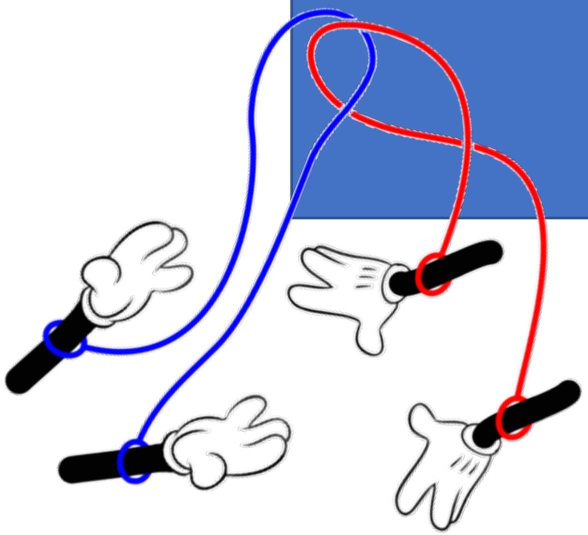
Let's consider the pure state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} = \begin{pmatrix} |\alpha|^2 & \mathrm{Re}[\alpha\beta^*] + i\mathrm{Im}[\alpha\beta^*] \\ \mathrm{Re}[\alpha\beta^*] - i\mathrm{Im}[\alpha\beta^*] & 1 - |\alpha|^2 \end{pmatrix}$$

- 3 Independent elements to be determined for full state tomography
- Diagonal elements from Z-basis measurements
- Real part of the off diagonal element by X-basis measurement: $\langle X \rangle = 2\mathrm{Re}[\alpha\beta^*]$
- Imaginary part of the off diagonal element by Y-basis measurement: $\langle Y \rangle = 2i\mathrm{Im}[\alpha\beta^*]$
- You can try with Qiskit!

4. Multiple qubits & Entanglement

Quantum Computing



UNIVERSITÀ
DI PARMA

Composite systems: tensor products

The state of two independent qubits can be written as a tensor (Kronecker) product:

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

The state of n independent qubits can be written as $|\psi\rangle = |q_0\rangle \otimes \cdots \otimes |q_n\rangle$. The resulting vector belongs to an Hilbert space of dimension $\boldsymbol{d = 2^n}$.

Single qubit gates can be expressed as tensor product

$$A_p = \mathbb{I} \otimes \cdots \mathbb{I} \otimes \underset{\substack{\uparrow \\ p^{\text{th}}\text{ qubit}}}{A} \otimes \mathbb{I} \otimes \cdots \mathbb{I}$$

product state

$$A_p(|q_0\rangle \otimes \cdots |q_p\rangle \cdots \otimes |q_n\rangle) = |q_0\rangle \otimes \cdots (A\overset{\substack{p^{\text{th}}\text{ qubit} \\ \downarrow}}{|q_p\rangle}) \cdots \otimes |q_n\rangle$$

Entangling gates

$$X_A(\,|0\rangle \otimes |0\rangle) = (X\,|0\rangle) \otimes |0\rangle = \;|1\rangle \otimes |0\rangle \equiv \;|10\rangle$$

$$X_A Y_B(\,|0\rangle \otimes |0\rangle) = (X\,|0\rangle) \otimes (Y\,|0\rangle) = \;|1\rangle \otimes i|1\rangle \equiv i|11\rangle$$

$$H_A(\,|0\rangle \otimes |0\rangle) = (H\,|0\rangle) \otimes |0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle \equiv \frac{|00\rangle + |10\rangle}{\sqrt{2}}$$ Product state

CNOT	$\vert 00\rangle$	$\vert 01\rangle$	$\vert 10\rangle$	$\vert 11\rangle$
$\langle 00\vert$	1	0	0	0
$\langle 01\vert$	0	1	0	0
$\langle 10\vert$	0	0	0	1
$\langle 11\vert$	0	0	1	0

$$\frac{|00\rangle + |10\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

product entangled

It is still a 2-qubit state but cannot be written as product.
Instead, it is a superposition of product states

Entangled states

$$|\psi\rangle = \sum_k a_k |\psi_0^k\rangle \otimes |\psi_1^k\rangle \otimes \cdots \otimes |\psi_n^k\rangle$$

Not all multi-qubit states can be written as product states. For the superposition principle, this is also a possible n-qubits state

$$\langle\psi|A_p|\psi\rangle = \sum_k \sum_j a_k\, a_j^* \left\langle \psi_0^j \cdots \psi_p^j \cdots \psi_d^j \middle| A_p \middle| \psi_0^k \cdots \psi_p^k \cdots \psi_n^k \right\rangle = \sum_k |a_k|^2 \left\langle \psi_p^k \middle| A \middle| \psi_p^k \right\rangle$$

2-qubit states which cannot be written as tensor product are called **entangled**.
If $|\psi\rangle$ is entangled, qubit j cannot be in a definite quantum state $|\psi_j\rangle$. For instance

$$|\psi\rangle = \frac{|0_A 1_B\rangle + |1_A 0_B\rangle}{\sqrt{2}} \qquad \langle M_A\rangle_\psi = \langle\psi|M\otimes\mathbb{I}|\psi\rangle = \frac{1}{2}(\langle 0|M|0\rangle + \langle 1|M|1\rangle)$$

There is no state $|\psi_A\rangle = \alpha|0\rangle + \beta|1\rangle$ such that $\langle M_A\rangle_\psi = \langle\psi_A|M|\psi_A\rangle$. Indeed,

$$\langle\psi_A|M|\psi_A\rangle = |\alpha|^2\langle 0|M|0\rangle + \alpha\beta^*\langle 1|M|0\rangle + \beta\alpha^*\langle 0|M|1\rangle + |\beta|^2\langle 1|M|1\rangle \quad \neq \quad \langle M_A\rangle_\psi$$

The state of qubit A is an incoherent mixture, not a linear superposition.

UNIVERSITÀ DI PARMA

Quantum Computing

$$|\psi\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \qquad \langle\psi| M \otimes \mathbb{1} |\psi\rangle =$$

$$= \frac{1}{2}\left(\langle 01| + \langle 10|\right)\left(M \otimes \mathbb{1}\right)\left(|01\rangle + |10\rangle\right) =$$

$$= \frac{1}{2}\Big(\langle 01| M \otimes \mathbb{1} |01\rangle + \langle 01| M \otimes \mathbb{1} |10\rangle + \langle 10| M \otimes \mathbb{1} |01\rangle$$

$$+ \langle 10| M \otimes \mathbb{1} |10\rangle\Big) =$$

$$= \frac{1}{2}\Big(\langle 0|M|0\rangle\langle 1|1\rangle + \cancel{\langle 0|M|1\rangle\langle 1|0\rangle}$$

$$+ \cancel{\langle 1|M|0\rangle\langle 0|1\rangle} + \langle 1|M|1\rangle\langle 0|0\rangle\Big)$$

Exercise: exchange interaction

$X_1 \otimes X_2 + Y_1 \otimes Y_2$

$$H = J\left(s_{1x}\, s_{2x} + s_{1y}\, s_{2y}\right)$$

$S_x = \frac{X}{2}$ $S_y = \frac{Y}{2}$

autostati $J > 0$ $\leftarrow$ $\underline{H = J\mathbf{s}_1 \cdot \mathbf{s}_2}$

$|0\rangle = \frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}}$ $|\uparrow\uparrow\rangle, |\downarrow\downarrow\rangle, \frac{|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle}{\sqrt{2}}$ degeneri

- Determine eigenvalues and eigenvectors.
- Compute the time evolution for a system initialized in $|\uparrow\uparrow\rangle$. Autostato
- Compute the time evolution for a system initialized in $|\uparrow\downarrow\rangle$.

Quantum no-cloning theorem

Goal: copy the **unknown** pure state $|\chi\rangle$ into slot $|s\rangle$ by means of a unitary operator U_{copy} :

$$|\chi\rangle\otimes|s\rangle \xrightarrow{U_{\text{copy}}} U_{\text{copy}}(|\chi\rangle\otimes|s\rangle) = |\chi\rangle\otimes|\chi\rangle$$

IMPOSSIBLE

$$|\chi\rangle\otimes|0\rangle = (\alpha|0\rangle + \beta|1\rangle)\otimes|0\rangle = \alpha|00\rangle + \beta|10\rangle \xrightarrow{U_{\text{CNOT}}} \alpha|00\rangle + \beta|11\rangle$$ **ENTANGLED**

$$\neq |\chi\rangle\otimes|\chi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$$ **NON-ENTANGLED**

PROOF: Suppose there exist an universal operator able to copy two unknown quantum states

$$U_{\text{copy}}|\chi_1\otimes s\rangle = |\chi_1\otimes\chi_1\rangle$$

$$U_{\text{copy}}|\chi_2\otimes s\rangle = |\chi_2\otimes\chi_2\rangle$$

We now evaluate the scalar product $a = \langle\chi_1\otimes\phi|U_{\text{copy}}^{\dagger}U_{\text{copy}}|\chi_2\otimes\phi\rangle$ in two different ways:

1. $a = \langle\chi_1\otimes\phi|\chi_2\otimes\phi\rangle = \langle\chi_1|\chi_2\rangle$
2. $a = \langle\chi_1\otimes\chi_1|\chi_2\otimes\chi_2\rangle = (\langle\chi_1|\chi_2\rangle)^2$

As a result, either $|\chi_1\rangle \equiv |\chi_2\rangle$ or $\langle\chi_1|\chi_2\rangle = 0 \Longrightarrow$ we cannot clone a superposition of the two.

Universality

Quantum Computing

Digital computer

- Converts sets of input bit strings to sets of output bit strings
- *Universality* = ability to realize any Boolean function on an arbitrary bit string
- *Universal gate set*: combination of NOT and any two-bit gate

Quantum Computer

- Converts sets of orthogonal input states to orthogonal output states
- *Universality* = capability to obtain any unitary on an arbitrary number of qubits
- *Universal gate set*: combination of single-qubit gates and a universal 2-qubit gate

Universality

- Special interesting case: input and output states represent real physical systems, described by a given Hamiltonian. H
- In that case the unitary would correspond to the time evolution of the system under investigation.

$U = e^{-iHt}$ $\quad U|\psi_0\rangle \rightarrow |\psi(t)\rangle$

- Implementing any unitary would mean **SIMULATE ANY QUANTUM TIME EVOLUTION** and would have crucial applications in the study and design of new materials (we will come back to this point in the Chapter 6 on Applications, *Quantum Simulation* section).

Clifford gates

Clifford gates: transform Paulis into Paulis $\quad U: P \longrightarrow UPU^\dagger \quad$ Conjugation by unitary

$$H = |+\rangle\langle 0| + |-\rangle\langle 1| = |0\rangle\langle +| + |1\rangle\langle -|$$

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \qquad X = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$R_z(\pi/2) = S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$HXH = Z$$
$$HZH = X$$
$$HYH = -Y$$

$$SXS^\dagger = Y$$
$$SYS^\dagger = -X$$
$$SZS^\dagger = Z$$

It transforms the eigenstates of P but not the eigenvalues (all Paulis share the same set of eigenvalues)

$$XZX = -Z$$
$$XYX = -Y$$
$$XXX = X$$

Paulis are Clifford

Multi-qubit Clifford gates: transform tensor products of Paulis into other tensor products of Paulis

$$CX(X \otimes \mathbb{I})CX = X \otimes X \qquad CX = (Z\otimes\mathbb{I} - Z\otimes X + \mathbb{I}\otimes X + \mathbb{I})/2$$

Non-Clifford gates

$H\ R_z(\theta) H = R_x(\theta)$

$$R_x(\vartheta) = e^{-i\vartheta X/2} \xrightarrow{\text{Conjugation}} UR_x(\vartheta)U^\dagger = e^{-i\vartheta UXU^\dagger/2}$$

Clifford gates can be used to expand the power of non-Clifford gates: here we have changed the rotation axis. Similarly:

$$CX(R_x(\vartheta)\otimes\mathbb{I})CX = CX\left(e^{-i\vartheta X\otimes\mathbb{I}/2}\right)CX = e^{-i\vartheta CX(X\otimes\mathbb{I})CX/2} = e^{-i\vartheta(X\otimes X)/2}$$

Conjugation by CNOT

$$(\mathbb{I}\otimes H)e^{-i\vartheta(X\otimes X)/2}(\mathbb{I}\otimes H) = e^{-i\vartheta(X\otimes HXH)/2} = e^{-i\vartheta(X\otimes Z)/2}$$

Conjugation by single-qubit gates

Combining 1 and 2-qubits Cliffords with R_x we can implement a large set of operations
The technique can be extended to many-qubit interactions (see notebook)

Proving Universality

We split the problem. First, suppose we wish to implement

$$U = e^{i(aX+bZ)}$$

But we are only able to implement $\quad R_x(\theta) = e^{iX\theta/2} \quad\quad R_z(\theta) = e^{iZ\theta/2}$

Unfortunately $\quad U = \underline{e^{i(aX+bZ)} \neq e^{iaX}e^{ibZ}} = R_x(2a)R_z(2b)$

However, $\quad U = \lim_{N\to\infty}\left(e^{iaX/N}e^{ibZ/N}\right)^N \quad \Longrightarrow \quad e^{iaX/N}e^{ibZ/N} \approx e^{i(aX+bZ)/N}$

with the error scaling as $1/N^2$

U can be approximated arbitrary well by using a sufficient number of slices N

Universality

The same method can be applied to multi-qubit unitaries. For instance

$$U = e^{i(aX\otimes X\otimes X + bZ\otimes Z)}$$

We have shown that we can implement both $e^{iaX\otimes X\otimes X}$ and $e^{ibZ\otimes Z}$ (by decomposing them in terms of elementary gates). However, since $[XXX, ZZ] \neq 0$, we need to resort to the "**slice**" technique (a.k.a. *Suzuki-Trotter* decomposition) introduced before

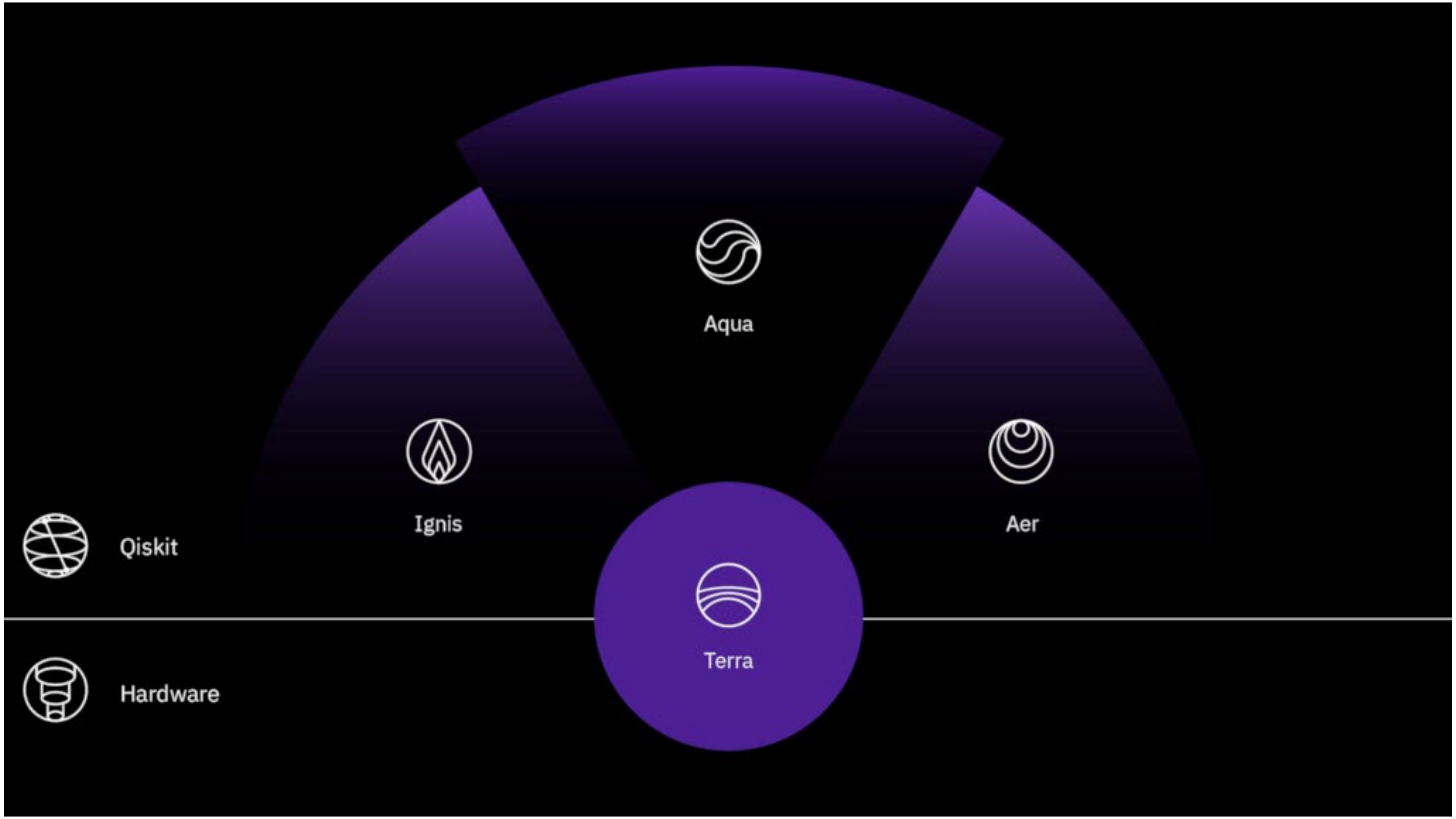
$$\left(e^{iaXXX/N} e^{ibZZ/N}\right)^N \approx U$$

By increasing N we get an arbitrarily accurate decomposition

The same method works on an arbitrary number of qubits and of terms in the exponential, provided they can be decomposed into Pauli matrices. Since all matrices can be expressed in this way, this proves that **we can implement any unitary using 1 and 2 qubit gates**.

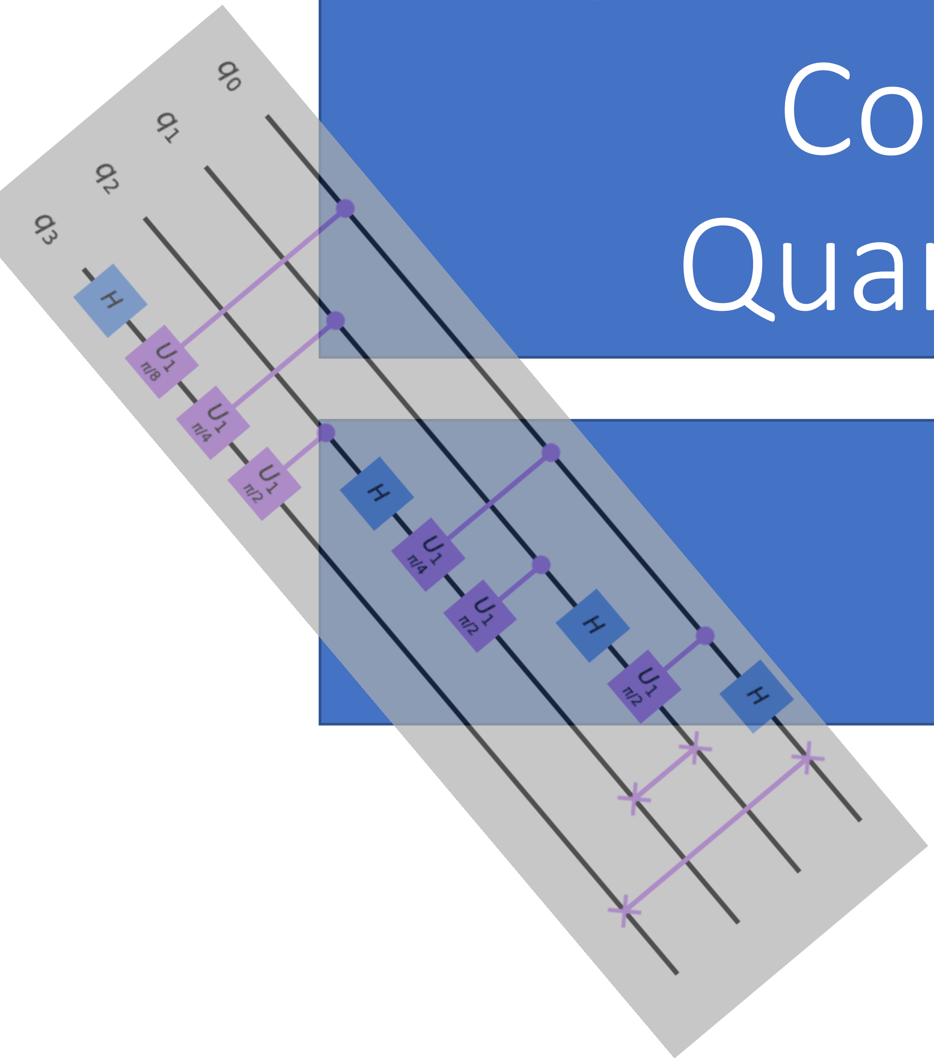
Increasing the number of terms increases the complexity of the method polynomially.

QISKIT



https://qiskit.org/documentation/

5. Principles of Quantum Computation and Quantum Algorithms



Quantum Computing

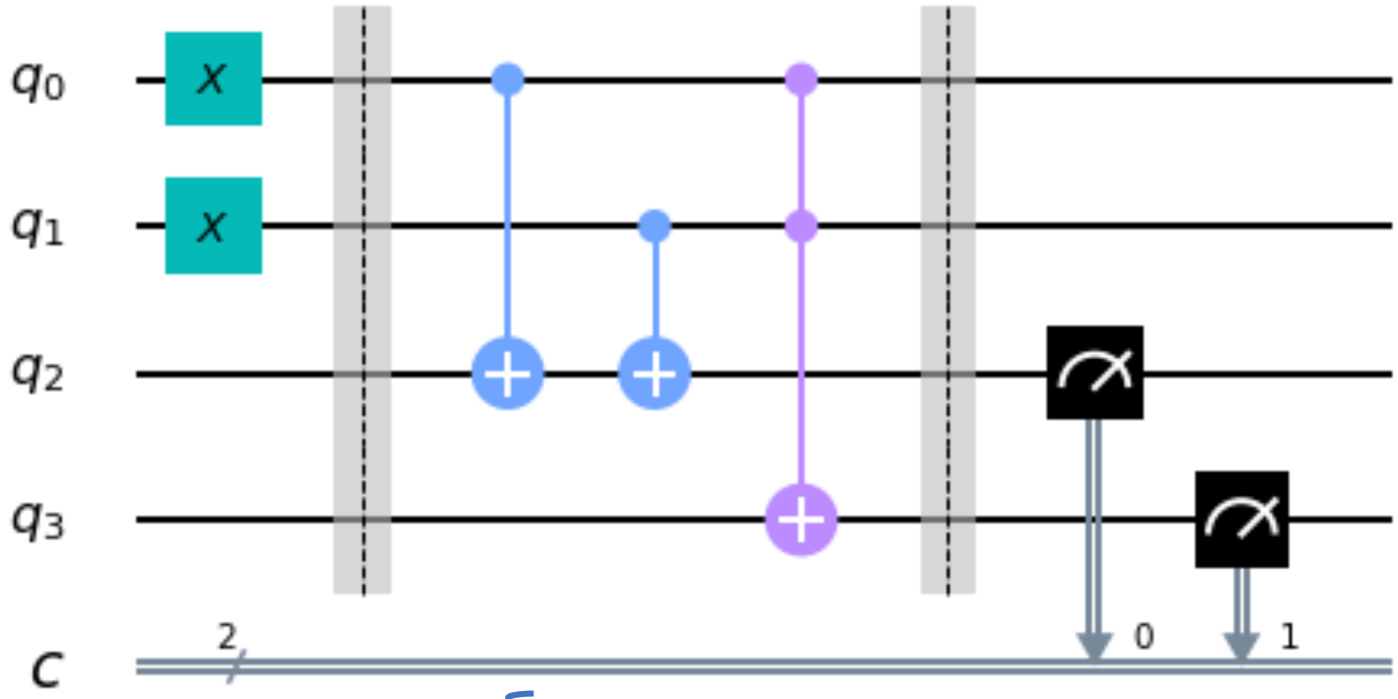
UNIVERSITÀ
DI PARMA

Quantum circuits

Initialization

Algorithm (sequence of unitary gates)

Measurement



Main differences from Classical Computer:

1. Inputs can be prepared in any superposition state
2. Quantum gates are unitary operators
3. Any measurement modifies the state of the qubits. You cannot simply stop, check and restart

Reversible calculation

Most logic gates are irreversible, because they correspond to a transformation 2 bits → 1 bit and the final state of a single bit does not allow to reconstruct the initial 2-bit state. E.g.:

XOR	
00	0
01	1
10	1
11	0

Equivalent reversible operation

CNOT	
00	0**0**
01	0**1**
10	1**1**
11	1**0**

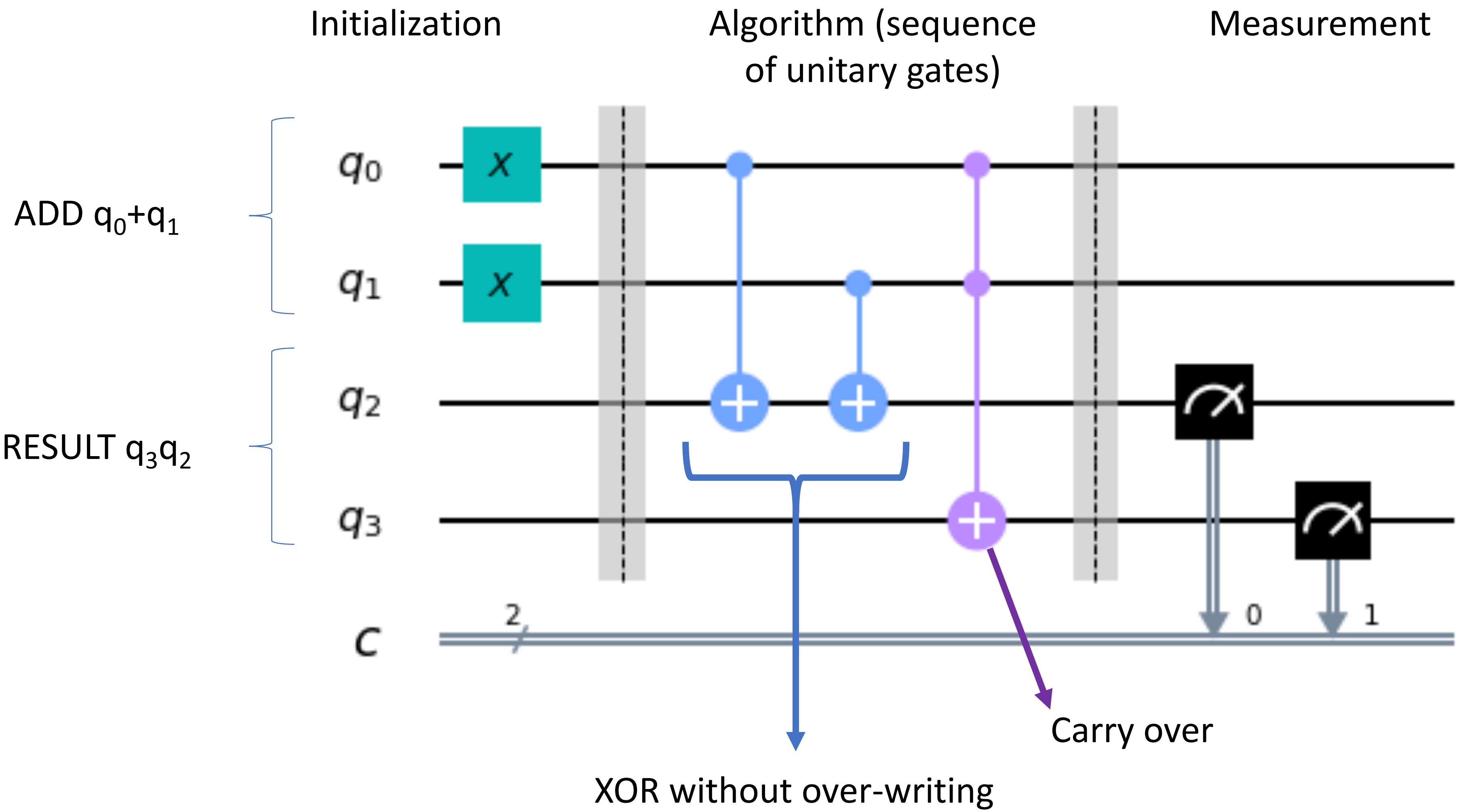
Any **irreversible** computation can be transformed into a **reversible** computation (usually by adding some extra lines to the circuit).

$$(x, y) \rightarrow (x, x \oplus y)$$

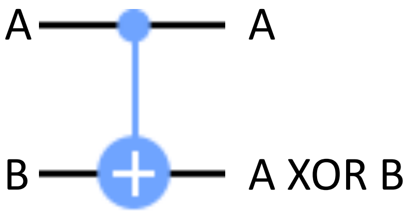
Using the CNOT and single-bit gates we can obtain linear Boolean functions.
The Toffoli gate (non-linear) allows us to reproduce reversibly all classical Boolean functions.

$$(x, y, z) \rightarrow (x, y, z \oplus xy)$$

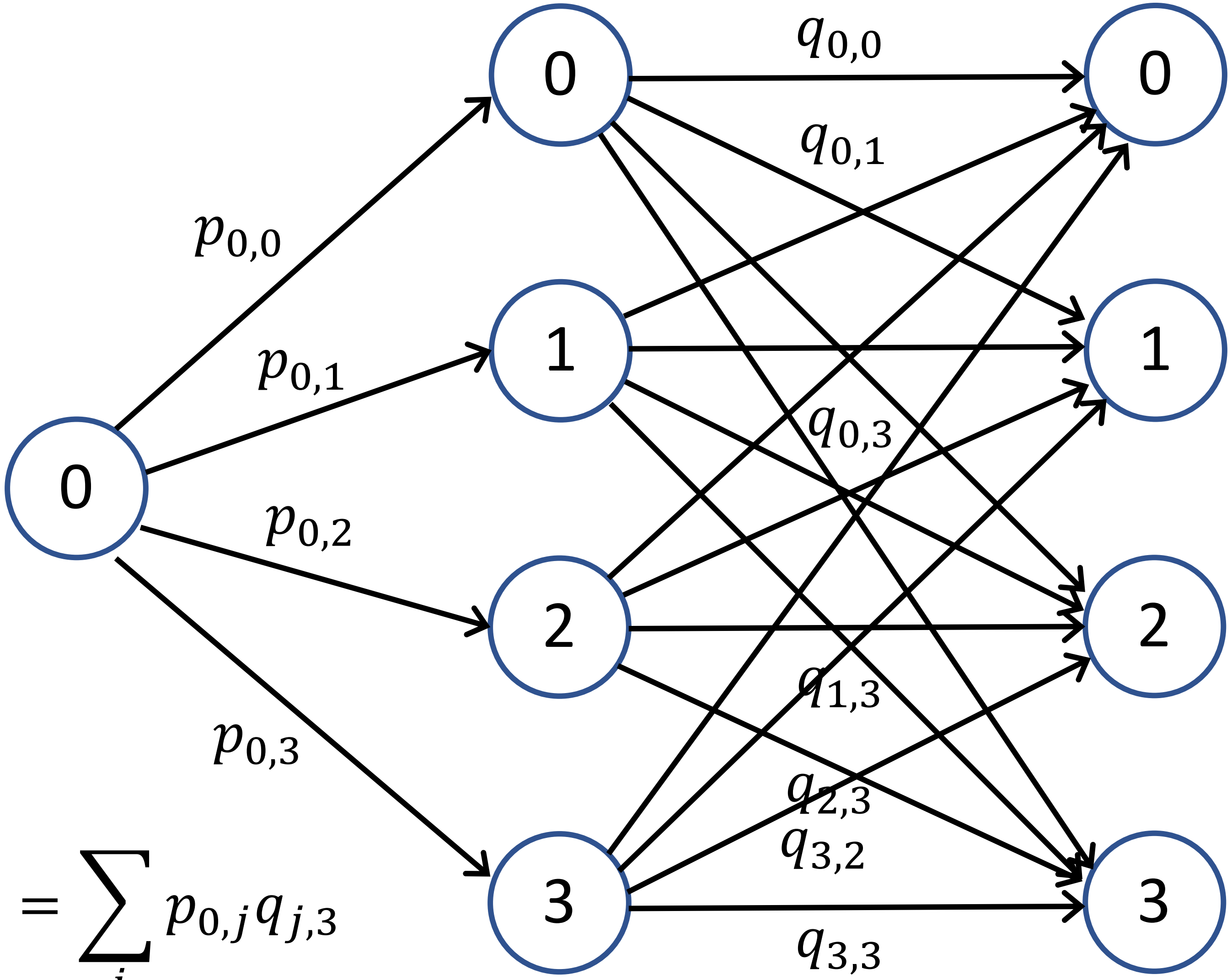
Adder circuit on Qiskit



q_0	q_1	q_0+q_1
0	0	00
0	1	01
1	0	01
1	1	10

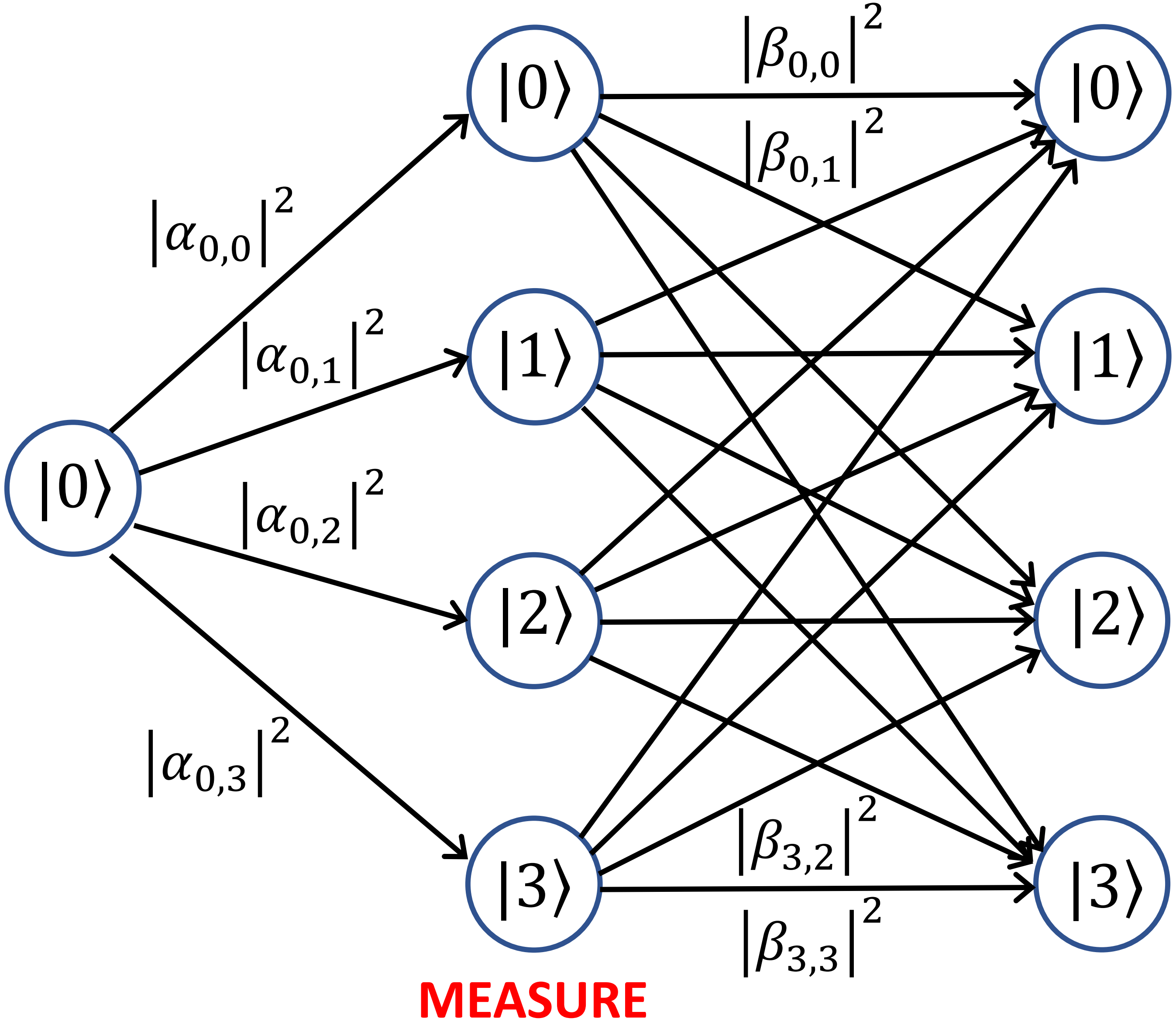


Probabilistic vs. Quantum Algorithms



$$P(\text{fin}=3)=\sum_j p_{0,j}q_{j,3}$$

Probabilistic vs. Quantum Algorithms



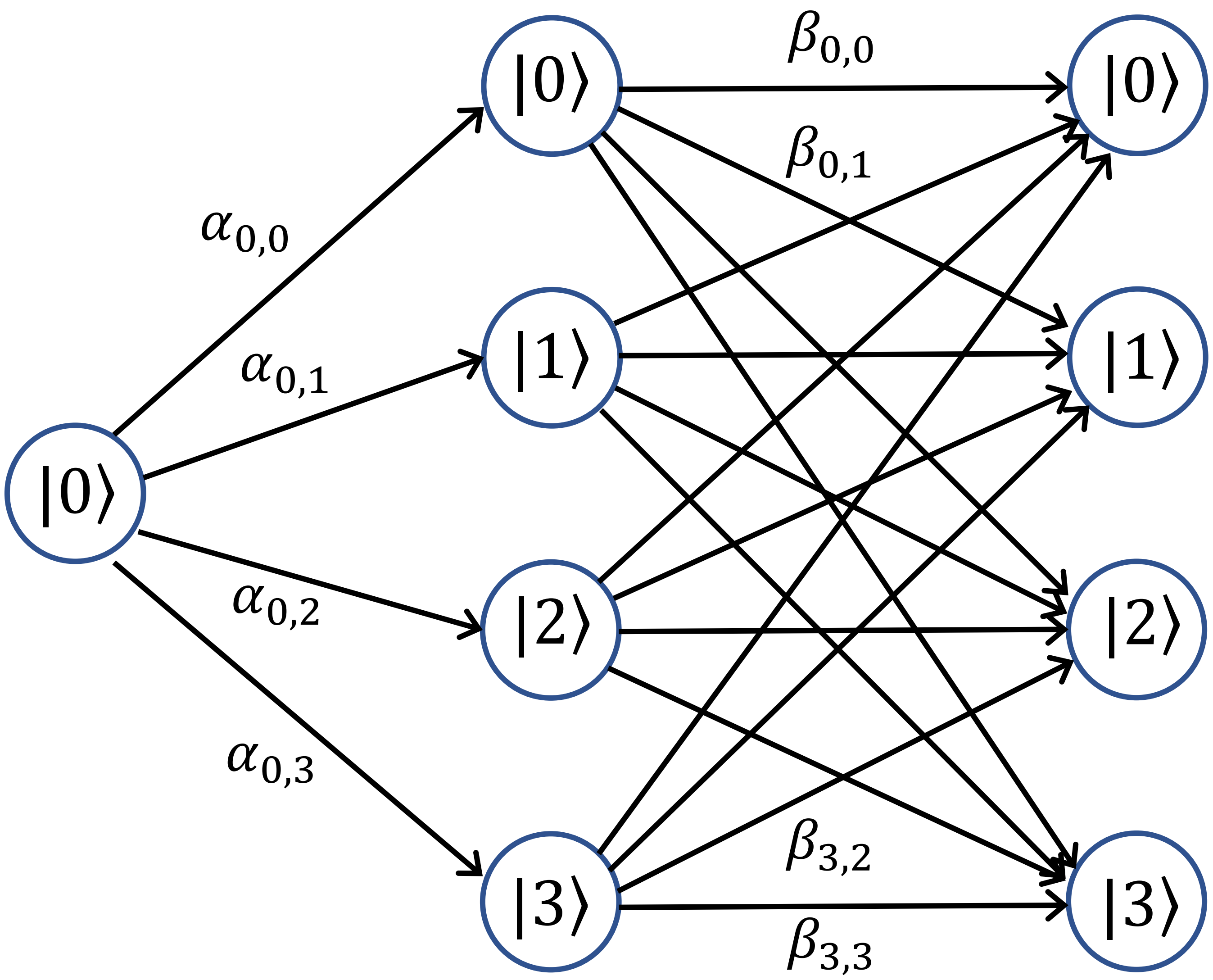
$$p_{0,j} = |\alpha_{0,j}|^2$$

$$q_{j,k} = |\beta_{j,k}|^2$$

$$P(\text{fin} = 3) = \sum_j |\alpha_{0,j}|^2 |\beta_{j,3}|^2$$

$$= \sum_j |\alpha_{0,j}\beta_{j,3}|^2$$

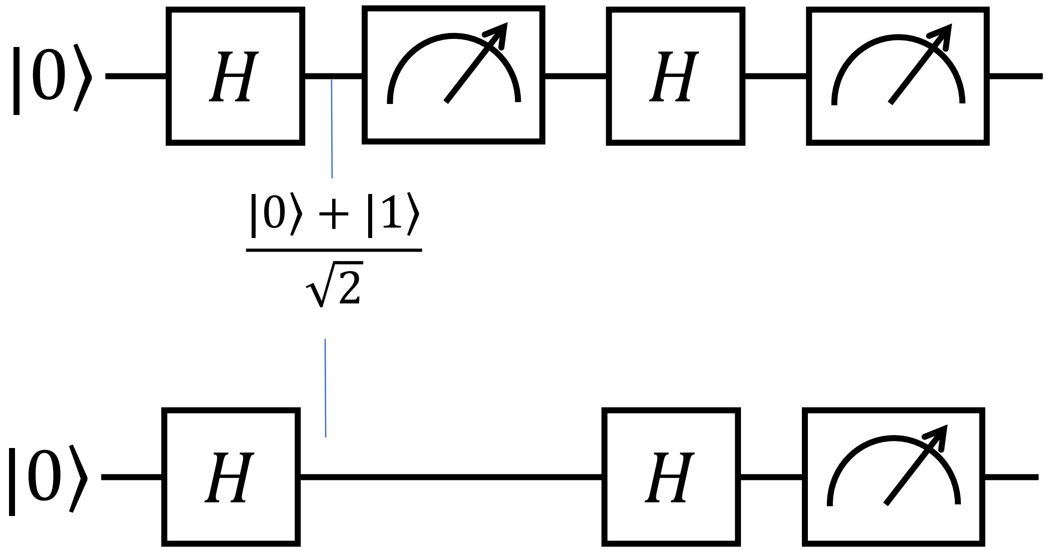
Fully quantum computation



$$P(\text{fin} = 3) = \left|\sum_j \alpha_{0,j}\beta_{j,k}\right|^2 \neq \sum_j \left|\alpha_{0,j}\beta_{j,k}\right|^2$$

INTERFERENCE

A circuit with quantum interference



No quantum interference: we finally get either $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ or $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ with 0.5 probability

Quantum interference: we finally get $|0\rangle$ with probability 1.

- Classical probabilistic algorithms can always be easily simulated by quantum algorithms.
- Classical probabilistic algorithms can also efficiently simulate quantum algorithms with small amount of entanglement (Gottesmann-Knill th.)

P. Kaye, R. Laflamme, M. Mosca, *An introduction to Quantum Computing, Oxford University Press*

Principles of Quantum Computation

A quantum processor would produce the transformation

$$|x\rangle \rightarrow U|x\rangle = |f(x)\rangle$$

desired binary number $\leq 2^n - 1$
(n is the number of qubits)

any function of x, $0 \leq f(x) \leq 2^n - 1$

However, this is not true for all functions. Indeed, unitary transformations preserve the overlap between any pair of states. Hence, given two input states $|x_1\rangle \neq |x_2\rangle$ such that $|f(x_1)\rangle = |f(x_2)\rangle$

$$|\langle f(x_1)|f(x_2)\rangle| = 1 \qquad\qquad 0 = \langle x_1|x_2\rangle = \left\langle x_1 U^\dagger \middle| U x_2\right\rangle$$

$$\Longrightarrow U|x\rangle \neq |f(x)\rangle \qquad \text{at least for some } x$$

To **reversibly** compute **any** function, we introduce a second bit string (initialized in $|y\rangle$), so that the processor performs the transformation

$$|x\rangle \otimes |y\rangle \longrightarrow U|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle$$

Now $|x_1\rangle \otimes |y \oplus f(x_1)\rangle$ and $|x_2\rangle \otimes |y \oplus f(x_2)\rangle$ are orthogonal even if $f(x_1) = f(x_2)$.

String of bits in which each bit is determined by modulo 2 addition of the bit strings y and $f(x)$

Principles of Quantum Computation

If $y = 0$ a measurement of the final state of the second string of qubits directly returns $f(x)$

$$|x\rangle = \mathrm{H}^{\otimes n}|0\rangle^{\otimes n} = 2^{-n/2}(|0\rangle + |1\rangle)\otimes(|0\rangle + |1\rangle)\otimes\cdots\otimes(|0\rangle + |1\rangle) = 2^{-n/2}\sum_{\nu=0}^{2^n-1}|\nu\rangle$$

$$U|x\rangle\otimes|0\rangle = 2^{-n/2}\sum_{\nu=0}^{2^n-1}|\nu\rangle\otimes|f(\nu)\rangle$$

Highly entangled output

The **single** quantum processor **computes simultaneously** the values of $f(\nu)$ for **all** ν, in the sense that states corresponding to all of these values are present in the transformed state

Origin of the **quantum speed-up**: performing U with an array of quantum gates requires a time that is polynomial in n. The prepared state, however, contains a superposition of 2^n values, so our processor has performed an exponential (in n) number of calculations in a polynomial time. We can expect, at least for some problems, an exponential speed up using a quantum computer.

Phase kick-back

$$\text{CNOT}: |0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \longrightarrow |0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$\text{CNOT}: |1\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \longrightarrow -|1\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ is an eigenstate of X gate with eigenvalue -1. The resulting phase can be moved in front of the control qubit (Note that in the Hadamard gate the role of control and target are swapped).

$$\text{CNOT}: |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \longrightarrow (-1)^x |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \qquad x \in \{0,1\}$$

$$\text{CNOT}: (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \longrightarrow (\alpha|0\rangle - \beta|1\rangle) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Z gate on the control qubit

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

$$\boxed{U|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}} = |x\rangle \otimes \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} = \begin{cases} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} & f(x) = 0 \\ -|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} & f(x) = 1 \end{cases} \boxed{= (-1)^{f(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}}$$

Phase kick-back

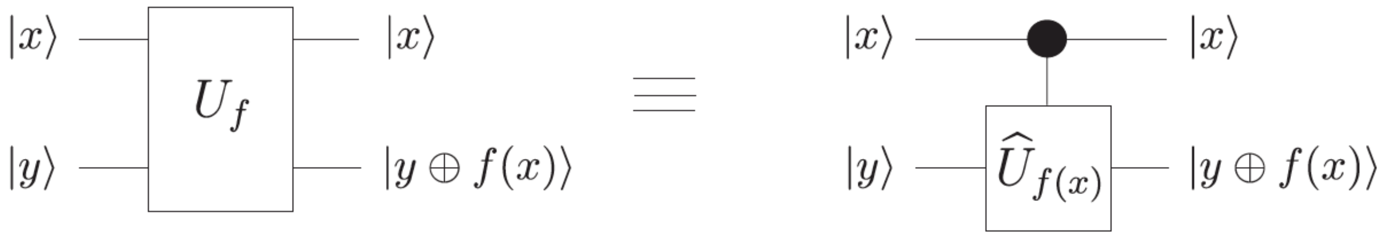


Fig. 6.6 The 2-qubit gate $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$ can be thought of as a 1-qubit gate $\widehat{U}_{f(x)}$ acting on the second qubit, controlled by the first qubit.

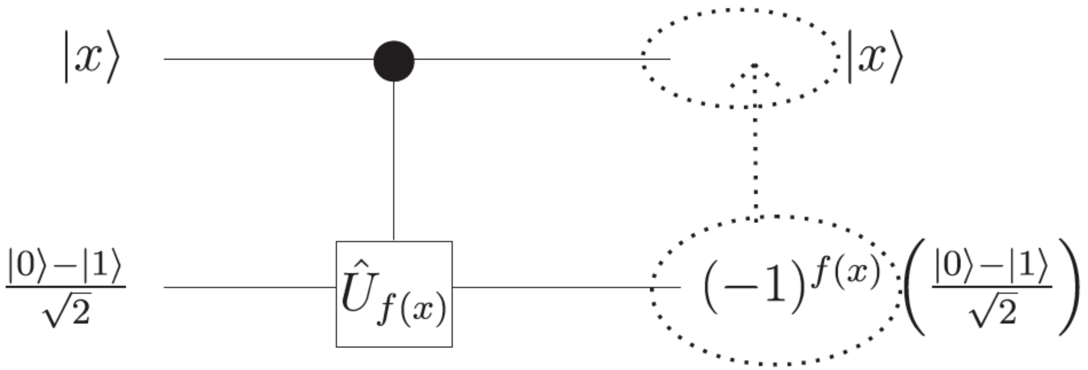
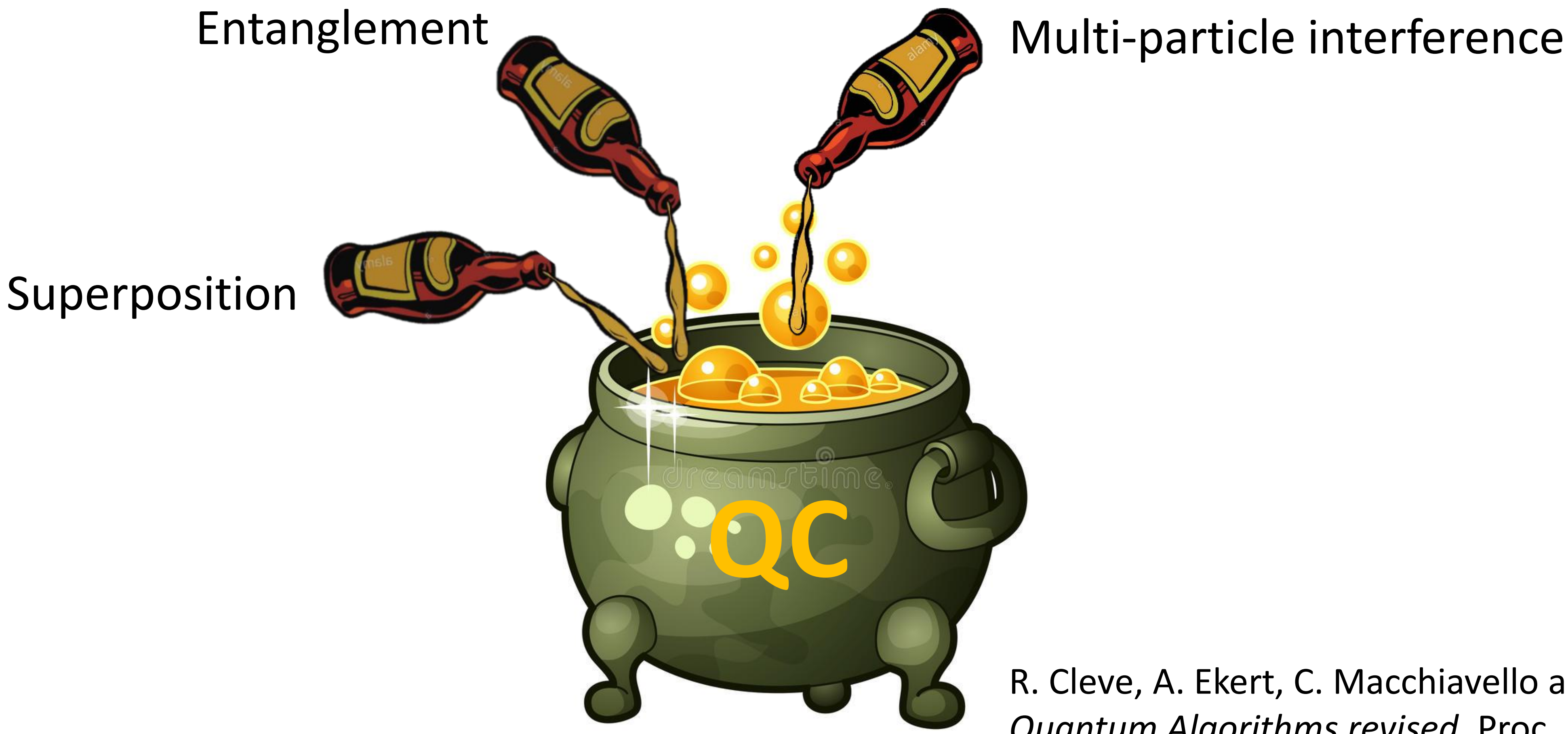


Fig. 6.7 The state $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ of the target register is an eigenstate of $\hat{U}_{f(x)}$. The eigenvalue $(-1)^{f(x)}$ can be 'kicked back' in front of the target register.

P. Kaye, R. Laflamme, M. Mosca, *An introduction to Quantum Computing, Oxford University Press*

Basic Ingredients of Quantum Computation

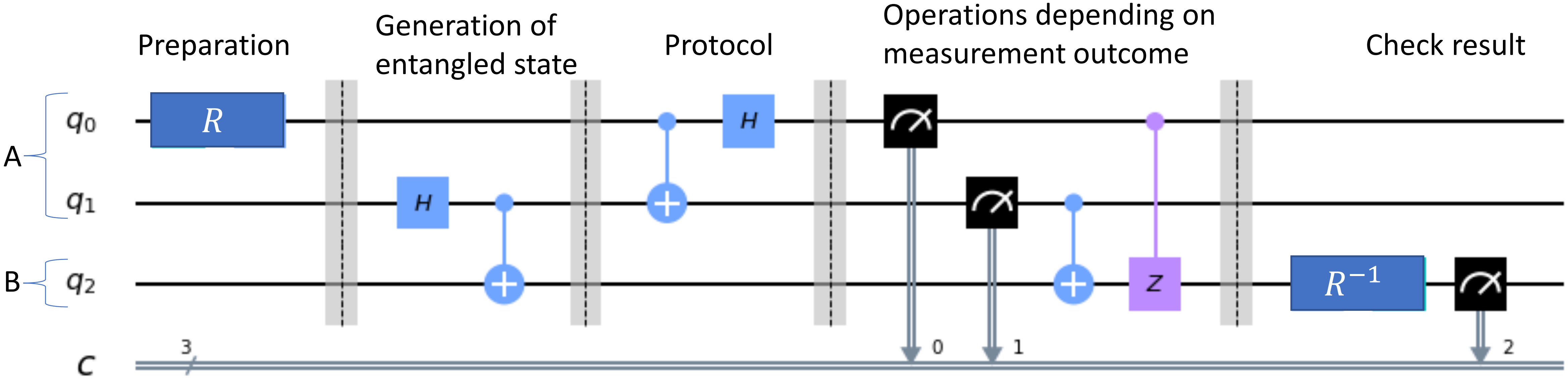


R. Cleve, A. Ekert, C. Macchiavello and M. Mosca, *Quantum Algorithms revised*, Proc. R. Soc. Lond. A (1998) 454, 339-354 (1998)

Quantum teleportation

The state of q_0 is transmitted from one location to another, with the help of classical communication and a Bell pair.

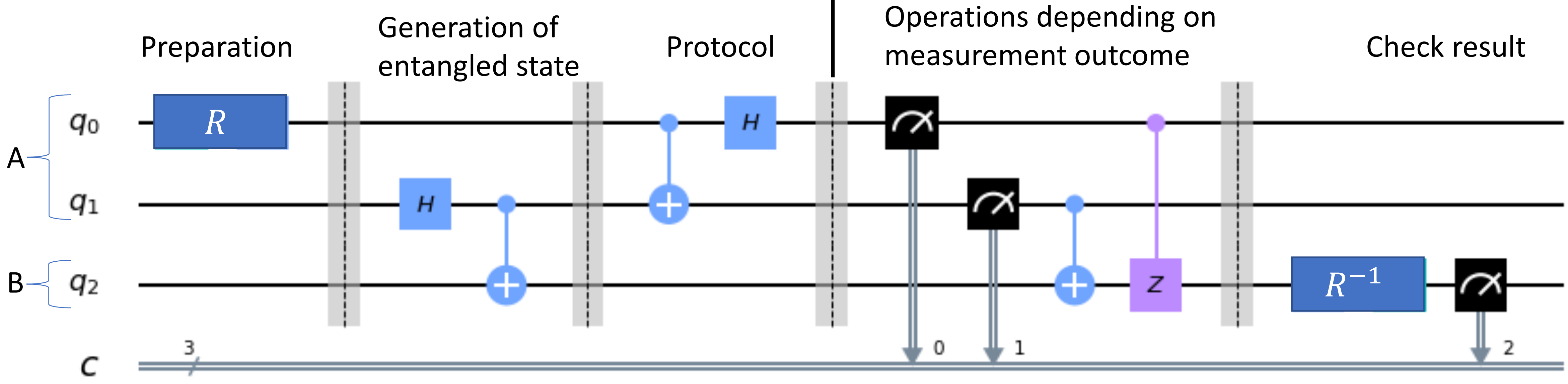
The protocol destroys the quantum state of a qubit in one location and recreates it on a qubit at a distant location, with the help of shared entanglement.



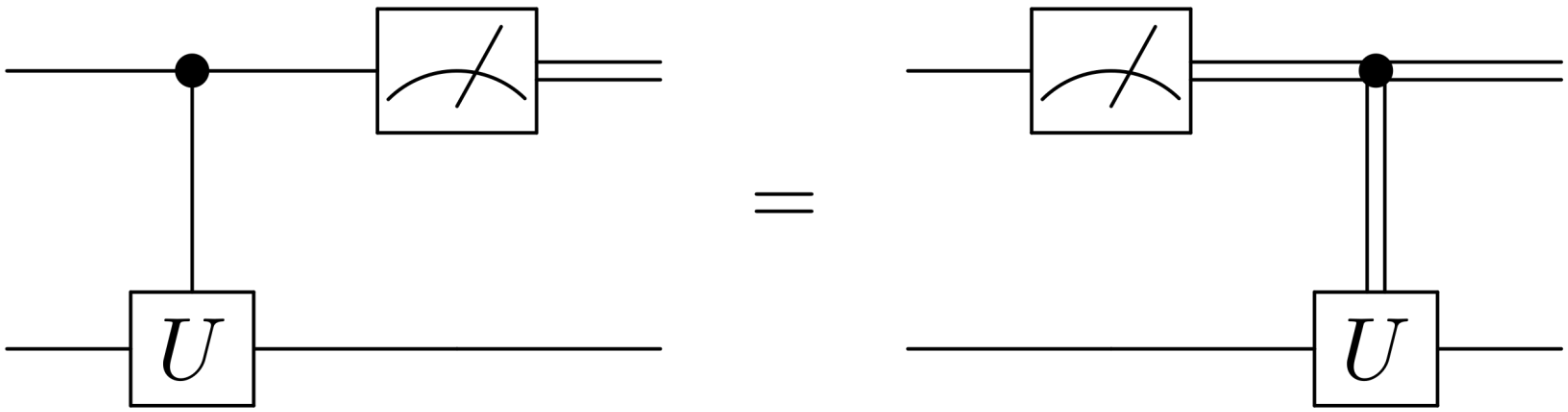
Quantum teleportation

$$
\begin{aligned}
\frac{1}{2}\big[&|00\rangle(\alpha|0\rangle+\beta|1\rangle) \xrightarrow{\quad\mathbb{I}\quad} |00\rangle(\alpha|0\rangle+\beta|1\rangle)\\
+&|01\rangle(\alpha|1\rangle+\beta|0\rangle) \xrightarrow{\quad X\quad} |01\rangle(\alpha|0\rangle+\beta|1\rangle)\\
+&|10\rangle(\alpha|0\rangle-\beta|1\rangle) \xrightarrow{\quad Z\quad} |10\rangle(\alpha|0\rangle+\beta|1\rangle)\\
+&|11\rangle(\alpha|1\rangle-\beta|0\rangle)\big] \xrightarrow{\quad ZX\quad} |11\rangle(\alpha|0\rangle+\beta|1\rangle)
\end{aligned}
$$

The protocol does not violate:
- No cloning theorem
- Special relativity



Deferred measurement principle



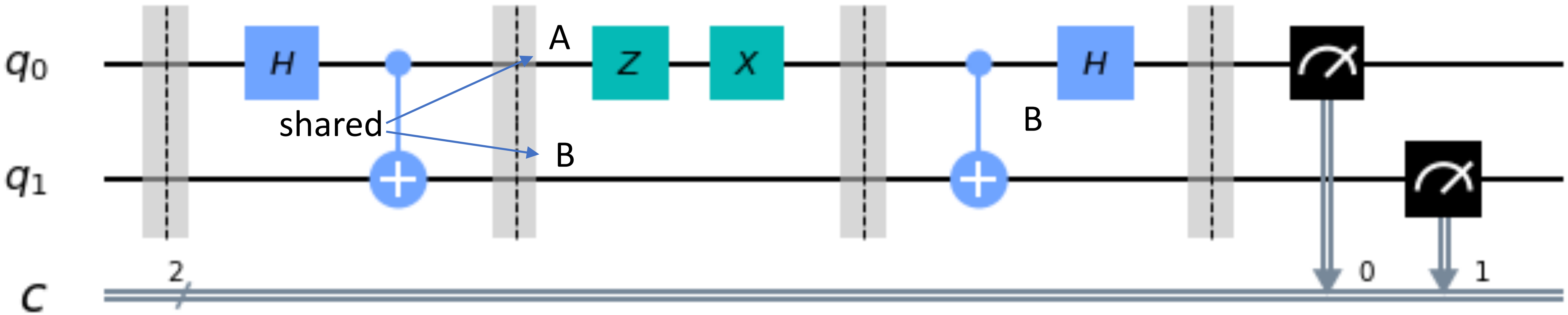
On the real hardware we cannot perform operations depending on a previous measurement outcome. But we can get the same result if we first perform a conditional gate and then we measure

Some drawbacks:

- By measuring early, we could reuse qubits or **reduce the time these qubits are in fragile superposition**.
- In quantum teleportation, the early measurement would have allowed us to transmit a qubit state **without a direct quantum communication channel** (much less stable than a classical one).
- Hence, in NISQ devices measuring earlier yields more reliable results (see e.g. VQE algorithm).

Superdense coding

Procedure that allows one to **send two classical bits** to another party **using just a single qubit** of communication.



Prepare $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

Encoding protocol on q_0

q_0 sent to B

Bell measurements

Teleportation	Superdense coding
Transmit 1 qubit using two c-bits	Transmit 2 c-bits using 1 qubit

Message	Gate	Output
00	I	$\|00\rangle + \|11\rangle$
01	X	$\|10\rangle + \|01\rangle$
10	Z	$\|00\rangle - \|11\rangle$
11	ZX	$\|10\rangle - \|01\rangle$

CNOT
$\|00\rangle + \|10\rangle$
$\|11\rangle + \|01\rangle$
$\|00\rangle - \|10\rangle$
$\|11\rangle - \|01\rangle$

H
$\|00\rangle$
$\|01\rangle$
$\|10\rangle$
$\|11\rangle$

Deutsch-Josza algorithm

First example of **quantum exponential speed-up.** Problem: given a Boolean function

f returns the same result for all inputs

$$f:\ \{0,1\}^n \rightarrow \{0,1\}$$

f returns 0 for half of the 2^n possible inputs, 1 for the others

Establish whether f is *constant* or *balanced*. On a classical computer you need to evaluate f an exponential ($2^{n-1}+1$) number of times to get a certain result

On a quantum computer a **single evaluation** is sufficient. **Exponential speed-up!**

In the worst case we need to evaluate f for half +1 of the possible inputs

We need **two registers**:

A. An n −qubit register initialized in $|+\rangle_A^{\otimes n} = H^{\otimes n}|0\rangle_A$
B. A single-qubit register initialized in $|-\rangle_B = H|1\rangle_B = HX|0\rangle_B$

Oracle: black-box performing the transformation U_f: $|x\rangle_A|y\rangle_B \rightarrow |x\rangle_A|y\oplus f(x)\rangle_B$

f-controlled-NOT

X-basis measurement (i.e. Hadamard followed by Z-measurement) of the first register

Deutsch's algorithm: how it works

Let's start from $n = 1$: $|x\rangle_A \frac{|0\rangle_B - |1\rangle_B}{\sqrt{2}}$

$$\Big\downarrow U_f$$

$$|x\rangle_A \frac{|f(x)\rangle_B - |1 \oplus f(x)\rangle_B}{\sqrt{2}} = (-1)^{f(x)} |x\rangle_A \frac{|0\rangle_B - |1\rangle_B}{\sqrt{2}}$$

$$\longrightarrow \frac{1}{2}\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right]_A \otimes (|0\rangle - |1\rangle)_B$$

constant $f(0) = f(1)$

$$\frac{1}{2}(|0\rangle + |1\rangle)_A \otimes (|0\rangle - |1\rangle)_B$$

$f(0) \neq f(1)$ balanced

$$\frac{1}{2}(|0\rangle - |1\rangle)_A \otimes (|0\rangle - |1\rangle)_B$$

$$\Big\downarrow H_A$$

$$|0\rangle_A \frac{|0\rangle_B - |1\rangle_B}{\sqrt{2}} \qquad |1\rangle_A \frac{|0\rangle_B - |1\rangle_B}{\sqrt{2}}$$

Measuring A gives the answer

Deutsch-Josza algorithm

$$H^{\otimes n}|0\rangle_A = 2^{-n/2}\sum_{x=0}^{2^n-1}|x\rangle_A \Longrightarrow$$

Initial state

$$2^{-(n+1)/2}\sum_{x=0}^{2^n-1}|x\rangle_A\otimes(|0\rangle-|1\rangle)_B$$

$$\xrightarrow{U_f} \quad 2^{-(n+1)/2}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle_A\otimes(|0\rangle-|1\rangle)_B$$

f constant

$$2^{-(n+1)/2}\sum_{x=0}^{2^n-1}|x\rangle_A\otimes(|0\rangle-|1\rangle)_B$$

Up to a global phase

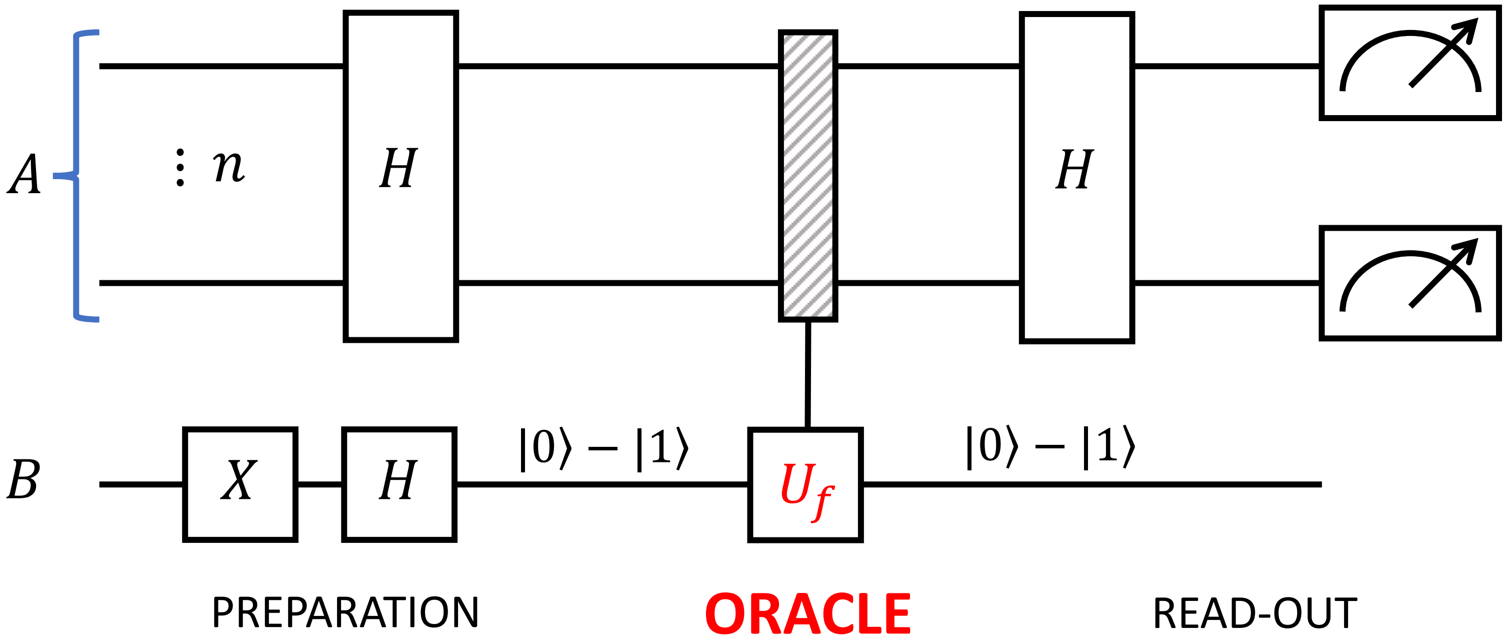
$$\Big\downarrow H_A^{\otimes n}$$

$$|0\cdots0\rangle_A\frac{|0\rangle_B-|1\rangle_B}{\sqrt{2}}$$

f balanced

Orthogonal state (negative phase added to half of the states)

Deutsch-Josza algorithm: general structure



n −qubit Hadamard: $|x\rangle \xrightarrow{H} \sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}\,|y\rangle$

$x \cdot y = (x_1 \wedge y_1)\oplus(x_2 \wedge y_2)\oplus\cdots\oplus(x_n \wedge y_n)$ Scalar product modulo 2

At the end of the algorithm $\sum_{x,y=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot y}|y\rangle\,(|0\rangle - |1\rangle)$ $P_{|0\rangle^{\otimes n}} = \left|\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\right|^2 = \begin{cases} 1 & \text{constant} \\ 0 & \text{balanced} \end{cases}$

Bernstein-Vazirani algorithm

PROBLEM:

Given a black-box function $f_s(x) = x \cdot s \pmod 2$ we aim to determine the string s

Classically, this requires querying the oracle n times.

QUANTUM SOLUTION:

The DJ circuit (register A) can be used to determine the bit string s of the hidden function:

$$f_s(x) = x \cdot s \pmod 2 = (x_1 \wedge s_1) \oplus (x_2 \wedge s_2) \oplus \cdots \oplus (x_n \wedge s_n)$$

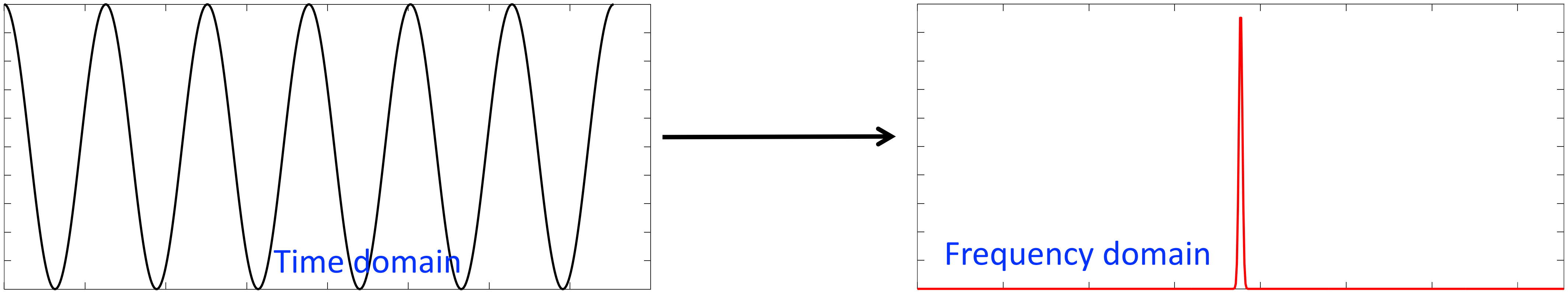
$$|0\rangle \xrightarrow{H^{\otimes n}} 2^{-n/2} \sum_{x \in \{0,1\}^n} |x\rangle \xrightarrow{f_s(x)} 2^{-n/2} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot s} |x\rangle \xrightarrow{H^{\otimes n}} |s\rangle$$

Quantum Fourier Transform

Physicists often solve problems by ***transforming*** it into another problem for which a solution is known. A few such transformations appear so often and in so many different contexts that these transformations are studied for their own sake.

Some of these transformations can be computed **much faster on a quantum computer** than on a classical computer and fast algorithms were constructed to achieve this goal.

One such transformation is the *discrete **Fourier** transform.*



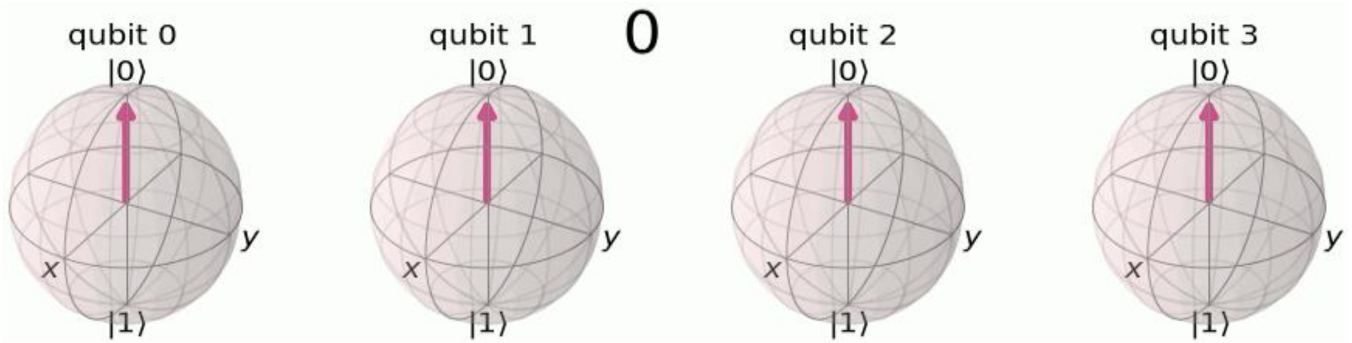
Quantum Fourier Transform

$$U_N^{QFT} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{2\pi i xy/N} |y\rangle\langle x| \qquad N = 2^n$$

$$|x\rangle = \sum_{i=0}^{N-1} x_i |i\rangle$$

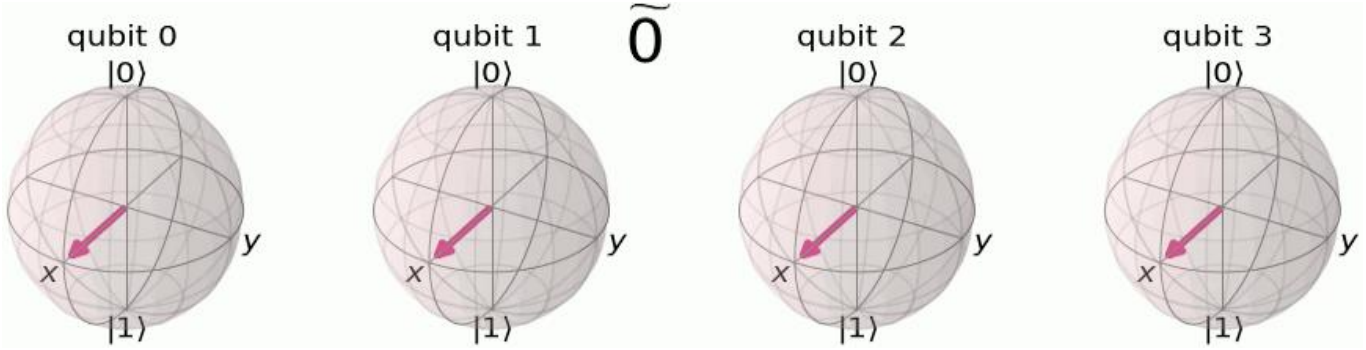
$$\Big\downarrow \mathcal{F}_N$$

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i xy/N} |y\rangle$$



Z basis

Highest frequency



Fourier basis

Highest frequency

$\tilde{x}$ dictates the angle at which each qubit is rotated around the Z-axis.

Quantum Computing

UNIVERSITÀ DI PARMA

Quantum Computing

Quantum Fourier Transform

$$y=\sum_{k=0}^{n-1} y_k 2^k = 2^n \sum_{k=0}^{n-1} y_k 2^{k-n} = 2^n \sum_{j=1}^{n} y_j 2^{-j} \Rightarrow \frac{y}{2^n} = \sum_{j=1}^{n} \frac{y_j}{2^j}$$

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y/N} |y\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x \sum_{j=1}^{n} y_j/2^j} |y_1 \dots y_n\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{j=1}^{n} e^{2\pi i x y_j/2^j} |y_1 \dots y_n\rangle$$

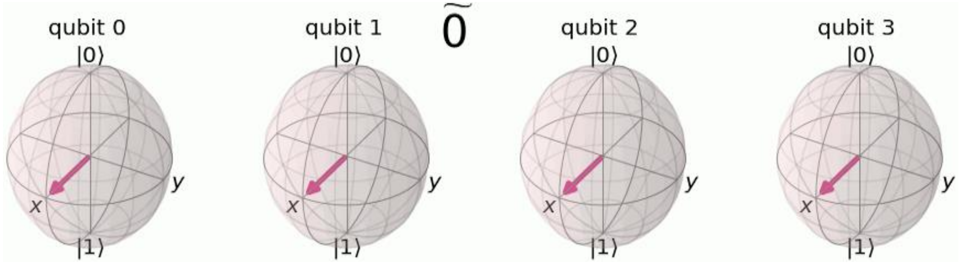
$$\sum_{y=0}^{N-1} |y\rangle = \sum_{y_1=0}^{1} \sum_{y_2=0}^{1} \cdots \sum_{y_n=0}^{1} |y_1 \dots y_n\rangle$$

$|\tilde{x}\rangle$ is **unentangled**. However, the phases depend on the state encoded in the whole y

$$\Rightarrow |\tilde{x}\rangle = \frac{1}{\sqrt{N}} \left(|0\rangle + e^{\frac{2\pi}{2} i x} |1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi}{2^2} i x} |1\rangle\right) \otimes \dots \otimes \left(|0\rangle + e^{\frac{2\pi}{2^n} i x} |1\rangle\right)$$

The circuit **requires also controlled gates**

On each qubit, the exponent contains the rotation frequency



1-qubit QFT

$N = 2$

$$|x\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \qquad \tilde{\alpha} = \frac{1}{\sqrt{2}}\left(\alpha\, e^{2\pi i 0\times 0/2} + \beta e^{2\pi i 1\times 0/2}\right) = \frac{\alpha+\beta}{\sqrt{2}}$$

$$|\tilde{x}\rangle = \begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} \qquad \tilde{\beta} = \frac{1}{\sqrt{2}}\left(\alpha\, e^{2\pi i 0\times 1/2} + \beta e^{2\pi i 1\times 1/2}\right) = \frac{\alpha-\beta}{\sqrt{2}}$$

$$U_2^{QFT}|x\rangle = \tilde{\alpha}|0\rangle + \tilde{\beta}|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle \qquad U_2^{QFT} = H$$

Circuit for the QFT

We use 2 gates:
- Single-qubit $\quad H|x_k\rangle = |0\rangle + \exp\frac{2\pi i x_k}{2}|1\rangle$
- Two-qubit $C\varphi_k$ $\quad C\varphi_{k\to j}|1x_j\rangle = \exp\frac{2\pi i}{2^k}x_j\,|1x_j\rangle \qquad C\varphi_k|0x_j\rangle = |0x_j\rangle$

1. Hadamard on the first qubit H_1: $\quad H_1|x_1x_2\ldots x_n\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\frac{2\pi i x_1}{2}|1\rangle\right)\otimes|x_2\ldots x_n\rangle$
2. $C\varphi_{2\to 1}: \longrightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left(\frac{2\pi i}{2}x_1 + \frac{2\pi i}{2^2}x_2\right)|1\rangle\right)\otimes|x_2\ldots x_n\rangle$
3. $C\varphi_{n\to 1}: \longrightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left(\frac{2\pi i}{2}x_1 + \frac{2\pi i}{2^2}x_2 + \cdots + \frac{2\pi i}{2^n}x_n\right)|1\rangle\right)\otimes|x_2\ldots x_n\rangle$
$$= \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\frac{2\pi i x}{2^n}|1\rangle\right)\otimes|x_2\ldots x_n\rangle$$
4. Repeat by starting with H_2 and then $C\varphi_{3\to 2}$ ... $C\varphi_{n\to 2}$

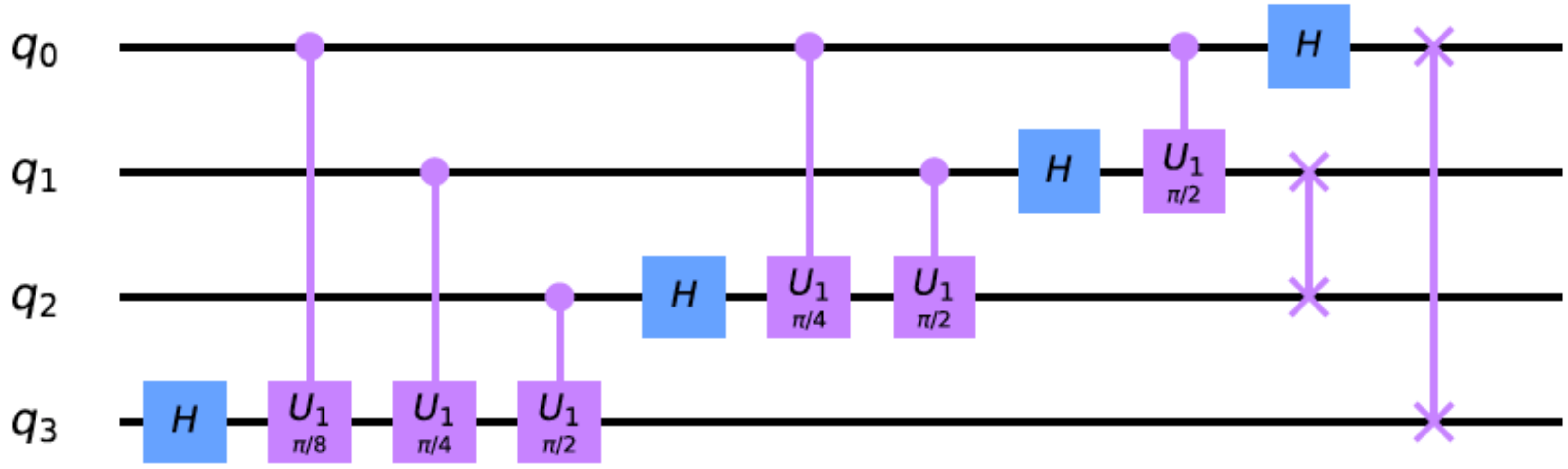
$$\longrightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\frac{2\pi i x}{2^n}|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + \exp\frac{2\pi i x}{2^{n-1}}|1\rangle\right)\otimes\ldots\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + \exp\frac{2\pi i x}{2^1}|1\rangle\right)$$

QFT: Scaling of resources

qubit	H	$C\varphi$	$SWAPs$
1	1	$n-1$	
2	1	$n-2$	
3	1	$n-3$	
…			
n	1	0	
TOTAL	n	$n(n-1)/2$	$n/2$

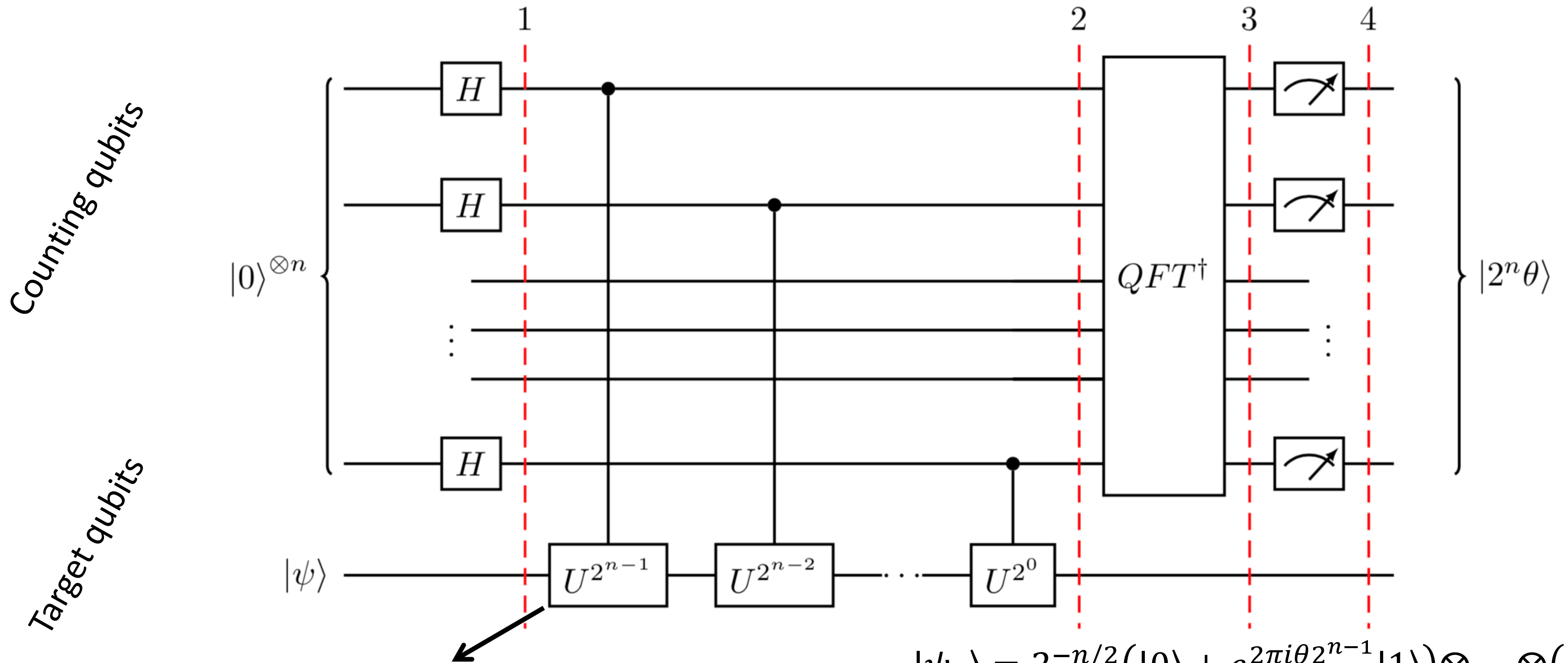
Total number of gates: $n(n+2)/2$

The best **classical** algorithm (Fast Fourier Transform) requires an **exponential number of gates**.



Quantum Phase Estimation

PROBLEM: Given a unitary operator U, estimate θ in $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$



$U^{2^k}|\psi\rangle = e^{2\pi i\theta 2^k}|\psi\rangle$

$$|\psi_2\rangle = 2^{-n/2}\left(|0\rangle + e^{2\pi i\theta 2^{n-1}}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{2\pi i\theta 2^1}|1\rangle\right)$$
$$\otimes\left(|0\rangle + e^{2\pi i\theta 2^0}|1\rangle\right)\otimes|\psi\rangle = 2^{-n/2}\sum_{m=0}^{2^n-1} e^{2\pi i\theta m}|m\rangle\otimes|\psi\rangle$$

… remember the QFT

$$|\psi_2\rangle = 2^{-n/2}\left(|0\rangle + e^{2\pi i\theta 2^{n-1}}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{2\pi i\theta 2^{1}}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i\theta 2^{0}}|1\rangle\right)\otimes|\psi\rangle =$$

$$= 2^{-n/2}\left(|0\rangle + e^{2\pi i x/2}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{2\pi i x/2^{n-1}}|1\rangle\right)\otimes\left(|0\rangle + e^{\frac{2\pi i x}{2^n}}|1\rangle\right)\otimes|\psi\rangle = U_{QFT}|x\rangle\otimes|\psi\rangle$$

$x = 2^n\theta$

$$|\psi_2\rangle = 2^{-n/2}\sum_{m=0}^{2^n-1} e^{2\pi i\theta m}\,|m\rangle\otimes|\psi\rangle \xrightarrow{U_{QFT}^{\dagger}} 2^{-n}\sum_{x=0}^{2^n-1}\sum_{m=0}^{2^n-1} e^{-\frac{2\pi i m}{2^n}(x-2^n\theta)}\,|x\rangle\otimes|\psi\rangle$$

This expression peaks close to $x = 2^n\theta$.

For integer $2^n\theta$, measuring the first register (counting qubits) exactly gives θ. Otherwise (see notebook) we can obtain a good approximation.

QPE is a **fundamental subroutine** in many Quantum Algorithms.

If we prepare the target register in a state $|\xi\rangle = \sum_n c_n|\psi_n\rangle$ (with $U|\psi_n\rangle = e^{i2\pi\theta_n}|\psi_n\rangle$), by measuring the counting register we get a good estimate of θ_n with probability $|c_n|^2$.

Example on qiskit: estimating π by QPE

$$QPE(U, |0\rangle_n, |\psi\rangle_m) = |\tilde{\theta}\rangle_n |\psi\rangle_m \qquad U|\psi\rangle_m = e^{i2\pi\theta} |\psi\rangle_m$$

Binary approximation to $2^n\theta$

$$U = u_1(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \qquad |\psi\rangle_1 = |1\rangle \qquad u_1(\varphi)|1\rangle = e^{i\varphi}|1\rangle$$

From QPE we measure an estimate of $x = 2^n\theta$. Hence, $\theta = \frac{x}{2^n}$

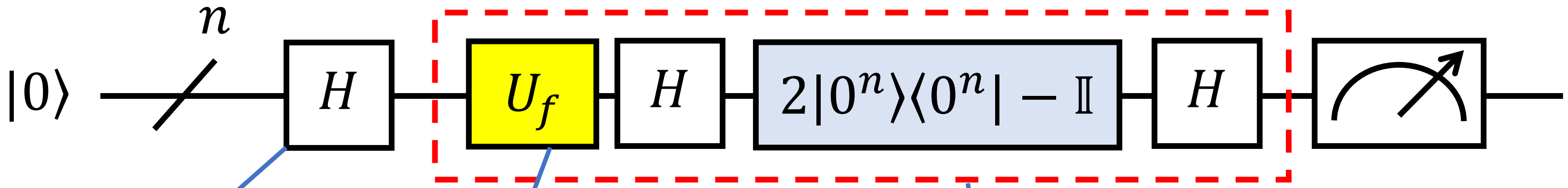
Here we have chosen $\varphi = 2\pi\theta = 1 \Longrightarrow \pi = \frac{\varphi}{2\theta} = \frac{2^n}{2x} = \frac{2^{n-1}}{x}$

Grover's algorithm

PROBLEM: **search** in an unstructured data-base.

BASIC **TRICK**: **Amplitude amplification** (used in many algorithms)

Quadratic advantage compared to classical counterpart. (Classically you would need on average $N/2$ trials)



Repeat $O(\sqrt{N})$ times

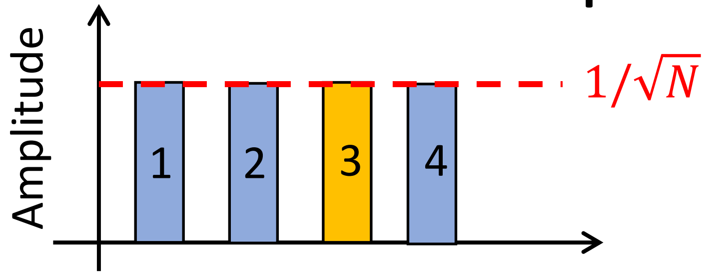
Prepare in uniform superposition
$|s\rangle = H^{\otimes n}|0\rangle$

Oracle function:
$$U_f|x\rangle = (-1)^{f(x)}|x\rangle$$
$$f(x) = \begin{cases} 0 & x \neq a \\ 1 & x = a \end{cases}$$

Amplitude amplification:
$$U_s = 2|s\rangle\langle s| - \mathbb{I} = H^{\otimes n}(2|0^n\rangle\langle 0^n| - \mathbb{I})H^{\otimes n}$$

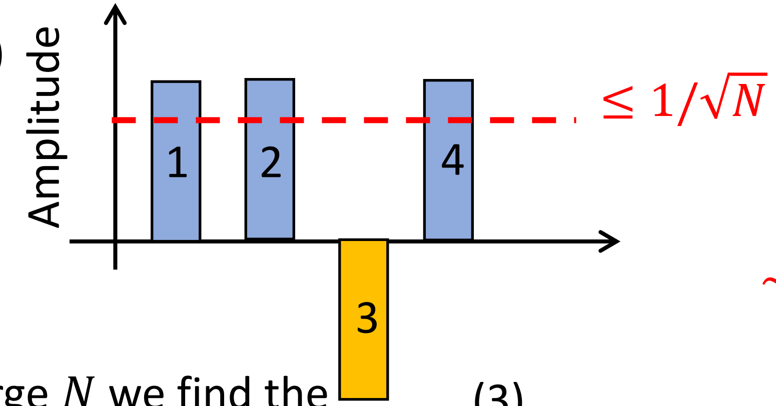
Amplitude amplification

(1)



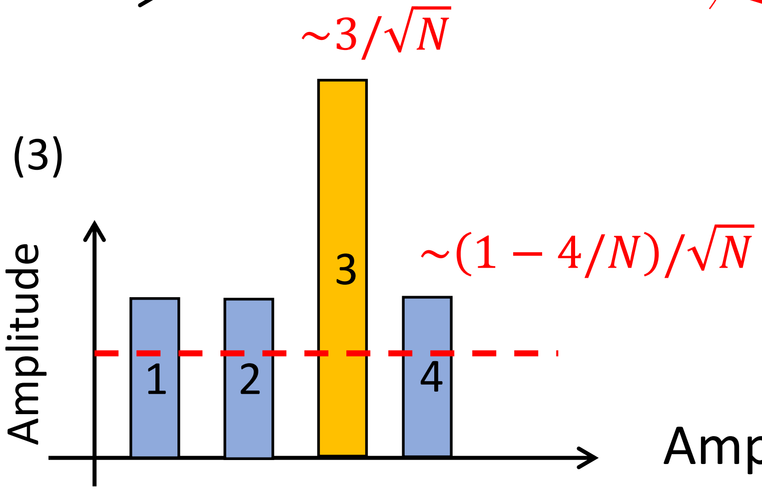
We start from a uniform superposition $|s\rangle = H^{\otimes n}|0\rangle$

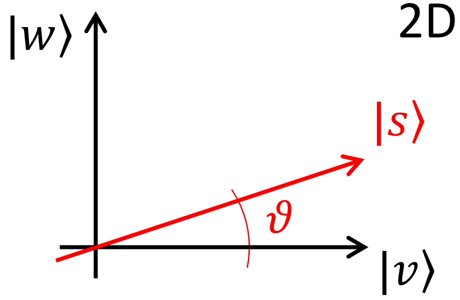
(2)



For large N we find the required element in the database with high probability using $\approx \frac{\pi}{4}\sqrt{N}$ queries of the oracle (Barnett)

(3)

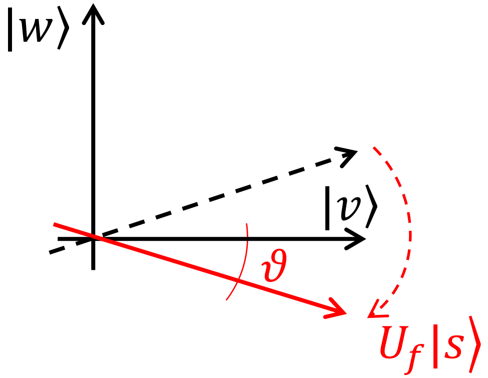




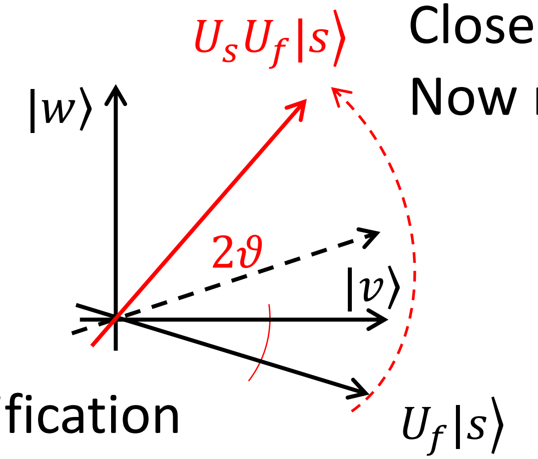
2D space spanned by vectors $|w\rangle$ and $|v\rangle$

$$|s\rangle = \sin\vartheta\,|w\rangle + \cos\vartheta\,|v\rangle,$$

$$\sin\vartheta = \langle s|w\rangle = 1/\sqrt{N}$$



Oracle function



Closer to $|w\rangle$! Now repeat!

Amplitude amplification

Example: $N = 4$

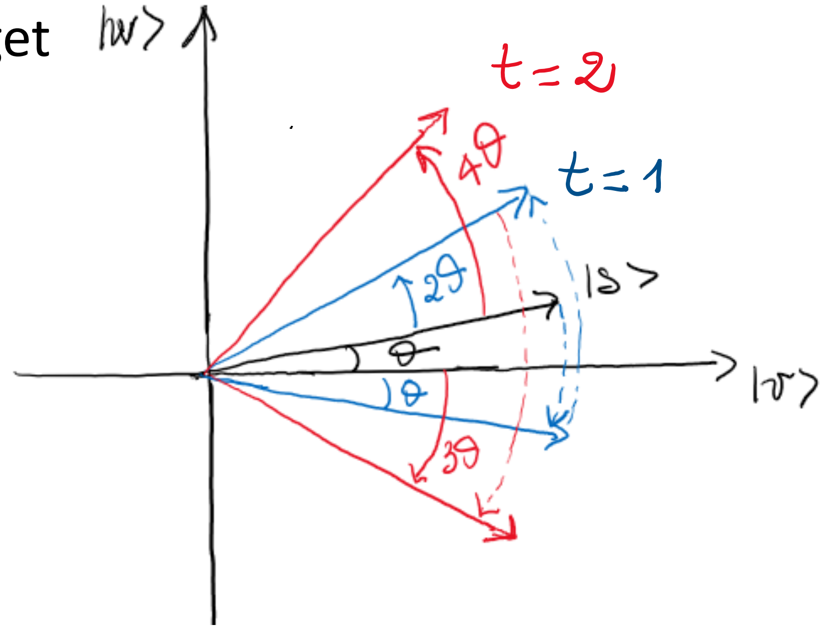
After n applications of the Grover's circuit (oracle+diffuser) we get

$$|\psi\rangle = (U_s U_f)^t \, |s\rangle = \sin\theta_t \, |w\rangle + \cos\theta_t |v\,\rangle$$

$$\theta_t = (2t+1)\theta$$

For $N = 4$, $\theta = \arcsin\frac{1}{2} = \frac{\pi}{6}$

To obtain $|w\rangle$, $\theta_t = \frac{\pi}{2}$ and hence after $t = 1$ we'll find the searched element. In general we need $\sim\sqrt{N}$ rotations.



e.g. $|w\rangle = |11\rangle$

$$U_f = U_{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$Z_1 Z_2 U_{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = 2|00\rangle\langle 00| - \mathbb{I}$$

6. Quantum Algorithms for Applications

Quantum Computing

UNIVERSITÀ
DI PARMA

Finding the period of a periodic function

FT: from times to frequencies $\Longrightarrow$ Determine the period of a periodic function $f(x)$!

Classical computer : we need to **evaluate** $f(x)$ **many times**, until we find two identical values

Quantum computer:

$$\frac{1}{\sqrt{N}}\sum_{a=0}^{N-1}|a\rangle \otimes |0\rangle \longrightarrow |\psi_0\rangle = \frac{1}{\sqrt{N}}\sum_{a=0}^{N-1}|a\rangle \otimes |f(a)\rangle$$

This register encodes all the value of $f(a)$, correlated with the inputs a. Hence, the information on the period is present in such a superposition state.

Measure the second register and find $f(a_0)$, i.e.

$$|\mathbb{I} \otimes f(a_0)\rangle\langle\mathbb{I} \otimes f(a_0)|\psi_0\rangle = [|a_0\rangle + |a_0 + T\rangle + |a_0 + 2T\rangle + \cdots] \otimes |f(a_0)\rangle$$

The first register is therefore projected onto the state $|\psi\rangle = \sqrt{\frac{T}{N}}\sum_{m=0}^{\frac{N}{T}-1}|a_0 + mT\rangle$ $\qquad 0 \leq a_0 \leq T-1$

$\Big\downarrow U_{QFT}$

where $b = lN/T$ $\qquad U_{QFT}|\psi\rangle = \sqrt{\frac{T}{N}}\sum_{m=0}^{\frac{N}{T}-1}\frac{1}{\sqrt{N}}\sum_{b=0}^{N-1}e^{i2\pi(a_0+mT)b/N}\,|b\rangle = \frac{1}{\sqrt{T}}\sum_{l=0}^{T-1}e^{i2\pi a_0 l/T}\,|lN/T\rangle$

Finding the period of a periodic function

$$U_{QFT}|\psi\rangle = \sqrt{\frac{T}{N}} \sum_{m=0}^{\frac{N}{T}-1} \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} e^{i2\pi(a_0+mT)b/N}\,|b\rangle = \frac{1}{\sqrt{T}} \sum_{l=0}^{T-1} e^{i2\pi a_0 l/T}\,|lN/T\rangle$$

If we measure the first register, we get one of the values

$$b = \frac{lN}{T} \qquad l = 0, \dots, T-1$$

If l and T are relatively prime, the simplified fraction gives the value of T

$$\frac{b}{N} = \frac{l}{T}$$

What happens if we use the QFT to find the period of a periodic function in which a value of f appears twice in a single period?

Shor's algorithm

Problem: finding prime factors of a given number N

We select a random integer $y < N$ relatively prime to N. (If not, we have already found a factor of N). We then define

$$f(a) = y^a \bmod N$$

Note that $f(0) = 1$. We seek the smallest subsequent T such that $f(T) = 1$:

$$f(T) = y^T \bmod N = 1$$

T is the period of f. Having T, with some algebra we determine a factor of N:

$$(y^T - 1) \bmod N = 0$$

$$\left(y^{T/2} + 1\right)\left(y^{T/2} - 1\right) \bmod N = 0$$

$$\left(y^{T/2} + 1\right)\left(y^{T/2} - 1\right) = \lambda N$$

For some integer λ

Ex : $2^0 \bmod 15 = 1$
$2^1 \bmod 15 = 2$
$2^2 \bmod 15 = 4$
$2^3 \bmod 15 = 8$
$2^4 \bmod 15 = 1$

$T = 4$
$y^{T/2} + 1 = 5$
$y^{T/2} - 1 = 3$

If T is not even, we must try again with a different value of y

Shor's algorithm: quantum advantage

Best known classical algorithm for factoring a large n-bit number N is **super-polynomial** in n (i.e. not bounded by any polynomial)

The hard step is the **FT**, which can be performed in a **polynomial (rather than exponential)** time on a quantum computer.

Hence, factoring using a quantum processor can also be done in a polynomial time.

Shor's algorithm: implementation

Use **quantum phase estimation** on the unitary operator $U|y\rangle = |ay \bmod N\rangle$

$a = 3, N = 14$ $\boxed{T = 6}$

Repeated applications of U
(each time we multiply by $a \bmod N$)

$$U|1\rangle = |3\rangle$$
$$U^2|1\rangle = |9\rangle$$
$$U^3|1\rangle = |13\rangle$$
$$U^4|1\rangle = |11\rangle$$
$$U^5|1\rangle = |5\rangle$$
$$U^6|1\rangle = |1\rangle$$

A superposition of the states in this cycle is an eigenstate of U with eigenvalue 1

$$|\xi_0\rangle = \frac{1}{\sqrt{6}}[|1\rangle + |3\rangle + |9\rangle + |13\rangle + |11\rangle + |5\rangle]$$

$$|\xi_0\rangle = \frac{1}{\sqrt{T}}\sum_{k=0}^{T-1}|a^k \bmod N\rangle$$

$$U|\xi_0\rangle = \frac{1}{\sqrt{6}}[|3\rangle + |9\rangle + |13\rangle + |11\rangle + |5\rangle + |1\rangle] = |\xi_0\rangle$$

$$|\xi_1\rangle = \frac{1}{\sqrt{T}}\sum_{k=0}^{T-1} e^{-\frac{2\pi i k}{T}}|a^k \bmod N\rangle$$

$$|\xi_1\rangle = \frac{1}{\sqrt{6}}\left[|1\rangle + e^{-\frac{2\pi i}{6}}|3\rangle + e^{-\frac{4\pi i}{6}}|9\rangle + e^{-\frac{6\pi i}{6}}|13\rangle + e^{-\frac{8\pi i}{6}}|11\rangle + e^{-\frac{10\pi i}{6}}|5\rangle\right]$$

$$U|\xi_1\rangle = e^{\frac{2\pi i}{T}}|\xi_1\rangle$$

$$U|\xi_1\rangle = \frac{1}{\sqrt{6}}\left[|3\rangle + e^{-\frac{2\pi i}{6}}|9\rangle + e^{-\frac{4\pi i}{6}}|13\rangle + e^{-\frac{6\pi i}{6}}|11\rangle + e^{-\frac{8\pi i}{6}}|5\rangle + e^{-\frac{10\pi i}{6}}|1\rangle\right]$$

$$= e^{\frac{2\pi i}{6}}\frac{1}{\sqrt{6}}\left[e^{-\frac{2\pi i}{6}}|3\rangle + e^{-\frac{4\pi i}{6}}|9\rangle + e^{-\frac{6\pi i}{6}}|13\rangle + e^{-\frac{8\pi i}{6}}|11\rangle + e^{-\frac{10\pi i}{6}}|5\rangle + e^{-\frac{12\pi i}{6}}|1\rangle\right] = e^{\frac{2\pi i}{6}}|\xi_1\rangle$$

Shor’s algorithm: implementation

$$|\xi_s\rangle = \frac{1}{\sqrt{T}}\sum_{k=0}^{T-1} e^{-\frac{2\pi i s k}{T}} |a^k \bmod N\rangle \qquad U|\xi_s\rangle = e^{\frac{2\pi i s}{T}}|\xi_s\rangle$$

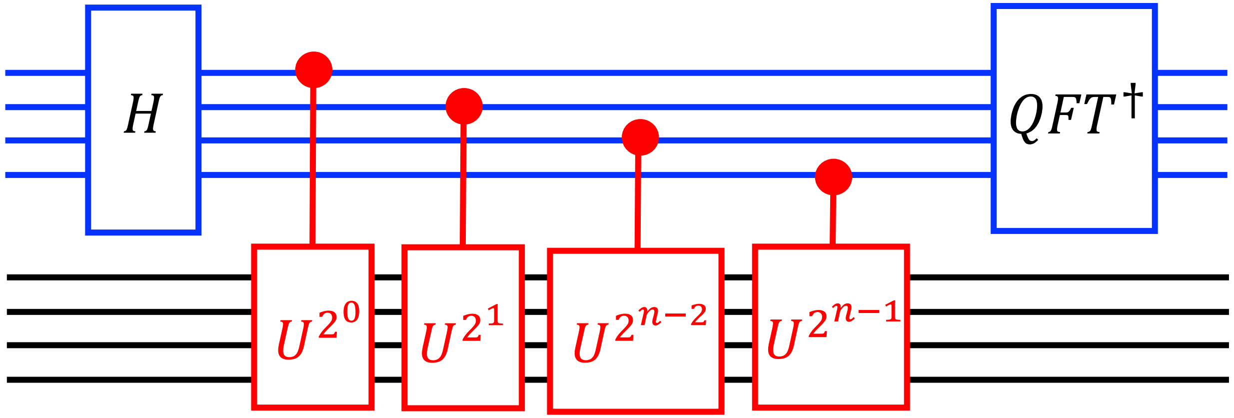
We thus get a unique eigenstate for each ingeter $s \in [0, T-1]$

$$\frac{1}{\sqrt{T}}\sum_{s=0}^{T-1} |\xi_s\rangle = |1\rangle$$

The computational basis state $|1\rangle$ is a superposition of these eigenstates.

Hence by **QPE** we will measure a phase s/T for a random integer $s \in [0, T-1]$

$$|1\rangle = \frac{1}{\sqrt{T}}[|\xi_0\rangle + |\xi_1\rangle + \dots + |\xi_{T-1}\rangle]$$



$$\frac{1}{\sqrt{T}}[|2^n 1/T\rangle + |2^n 2/T\rangle + \dots + |2^n (T-1)/T\rangle]$$

Quantum Computing

Solving linear systems (HHL)

PROBLEM: given $A \in \mathbb{C}^{N\times N}$ $\vec{b} \in \mathbb{C}^N$ **find** $\vec{x} \in \mathbb{C}^N$ $A\vec{x} = \vec{b}$

The system is s-sparse if A has at most s non-zero entries per rows or column.

On a classical computer we can solve an s-sparse system of size N in $O(Nsk\log(1/\epsilon))$ time by the conjugate gradient method, being ϵ the error of the approximation and k the condition number of the system.

HHL [A. W. Harrow, A. Hassidim, S. Lloyd, Phys. Rev. Lett. **103**, 150502 (2009)] algorithm estimates the solution in $O(\log(N)s^2k^2/\epsilon)$ time

- **Exponential advantage**
- We do not find the full solution, but only **approximate** functions of the solution vector
- We assume A Hermitian and efficient oracles for loading the data

Map to quantum states

$\vec{x} \rightarrow |x\rangle$ $\vec{b} \rightarrow |b\rangle$ $\vec{x}, \vec{b}$ must be normalized

$$A|x\rangle = |b\rangle$$

$$A = \sum_{j=0}^{N-1} \lambda_j |u_j\rangle\langle u_j| \qquad \lambda_j \in \mathbb{R}$$

Spectral decomposition

$$A^{-1} = \sum_{j=0}^{N-1} \lambda_j^{-1} |u_j\rangle\langle u_j|$$

$$|b\rangle = \sum_{j=0}^{N-1} b_j |u_j\rangle \qquad b_j \in \mathbb{C}$$

Representation of $|b\rangle$ on A eigenbasis.

$$|x\rangle = A^{-1}|b\rangle = \sum_{j=0}^{N-1} \lambda_j^{-1} b_j |u_j\rangle$$

Implicit normalisation

HHL algorithm

3 registers: $\begin{cases} n_l: & \text{Binary representation of the eigenvalues of } A \\ n_b: & \text{Vector solution. Hereafter } N = 2^{n_b}. \\ n_a: & \text{Ancilla qubit} \end{cases}$

1. Load the data $|b\rangle \in \mathbb{C}^{\mathrm{N}}$ $|0\rangle_{n_b} \to |b\rangle_{n_b}$

Normalisation constant

2. Apply QPE to $U = e^{-iAt} = \sum_{j=0}^{N-1} \mathrm{e}^{-\mathrm{i}\lambda_j t} |u_j\rangle\langle u_j|$ $\Rightarrow$ $\sum_{j=0}^{N-1} b_j |\lambda_j\rangle_{n_l} |u_j\rangle_{n_b}$

3. Add an ancilla qubit and apply a rotation conditioned on $|\lambda_j\rangle$ $\Rightarrow$ $\sum_{j=0}^{N-1} b_j |\lambda_j\rangle_{n_l} |u_j\rangle_{n_b} \left(\sqrt{1 - \frac{c^2}{\lambda_j^2}} |0\rangle + \frac{c}{\lambda_j} |1\rangle \right)$

4. Apply $QPE^\dagger$. Neglecting possible errors in the QPE $\Rightarrow$ $\sum_{j=0}^{N-1} b_j |0\rangle_{n_l} |u_j\rangle_{n_b} \left(\sqrt{1 - \frac{c^2}{\lambda_j^2}} |0\rangle + \frac{c}{\lambda_j} |1\rangle \right)$

5. Measure ancilla. If we find $|1\rangle$ $\Rightarrow$ $\sum_{j=0}^{N-1} \frac{b_j}{\lambda_j} |0\rangle_{n_l} |u_j\rangle_{n_b}$ Apart from a normalization

which corresponds (apart from a factor) to the solution.

QPE within HHL

$$QPE(U, |0\rangle_n, |\psi\rangle_m) = |\tilde{\theta}\rangle_n |\psi\rangle_m \qquad U|\psi\rangle_m = e^{i2\pi\theta}\, |\psi\rangle_m$$

Binary approximation to $2^n\theta$

Within HHL $\qquad U = e^{iAt} = \sum_{j=0}^{N-1} e^{i\lambda_j t} |u_j\rangle\langle u_j|$

$$QPE\left(e^{iAt}, |0\rangle_{n_l}, |u_j\rangle_{n_b}\right) = |\tilde{\lambda}_j\rangle_{n_l} |u_j\rangle_{n_b}$$

$\tilde{\lambda}_j$ is a n_l–bit binary approximation to $2^{n_l} \frac{\lambda_j t}{2\pi}$

If λ_j can be represented exactly with n_l bits

$$QPE\left(e^{iA2\pi}, \sum_{j=0}^{N-1} b_j\, |0\rangle_{n_l} |u_j\rangle_{n_b}\right) = \sum_{j=0}^{N-1} b_j\, |\lambda_j\rangle_{n_l}\, |u_j\rangle_{n_b}$$

Otherwise we obtain an approximation

Example: HHL on 4 qubits

$$A = \begin{pmatrix} 1 & -1/3 \\ -1/3 & 1 \end{pmatrix} \qquad |b\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$n_b = 1$ to represent $|b\rangle$ and then the solution
$n_l = 2$ qubits to store the eigenvalues of A
$n_a = 1$ to store if the conditional rotation (and hence the algorithm) was successful

QPE gives a binary approximation (on an n_l-bit string) to $2^{n_l} \frac{\lambda_j t}{2\pi}$. Hence, if we set $t = 2\pi \frac{3}{8}$ we get

$$\lambda_1 = \frac{2}{3} \qquad \lambda_2 = \frac{4}{3}$$

$$\frac{\lambda_1 t}{2\pi} = \frac{1}{4} \longrightarrow |01\rangle_{n_l} \qquad \frac{\lambda_2 t}{2\pi} = \frac{1}{2} \longrightarrow |10\rangle_{n_l}$$

Rescaled eigenvalues. We choose this value of t to simplify the problem and get the exact result from QPE.

Eigenvectors of A: $\quad |u_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad |u_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$

$$|b\rangle = |0\rangle = \frac{1}{\sqrt{2}}(|u_1\rangle + |u_2\rangle)$$

Note that we do not need to know eigenvalues and eigenvectors [$\mathcal{O}(N)$ problem]

Example: HHL on 4 qubits

Initial state $$|\psi\rangle = |0\rangle_{n_l}|0\rangle_{n_b}|0\rangle_a = |0\rangle_{n_l}\frac{1}{\sqrt{2}}\left(|u_1\rangle_{n_b} + |u_2\rangle_{n_b}\right)|0\rangle_a$$

$$\Big\downarrow QPE$$

$$\frac{1}{\sqrt{2}}\left(|01\rangle_{n_l}|u_1\rangle_{n_b} + |10\rangle_{n_l}|u_2\rangle_{n_b}\right)|0\rangle_a$$

$$\Big\downarrow$$

Conditioned rotation of the ancilla ($c = 3/8$ to compensate rescaling of the eigenvalues)

$$\frac{1}{\sqrt{2}}|01\rangle_{n_l}|u_1\rangle_{n_b}\left(\sqrt{1-\frac{(3/8)^2}{(1/4)^2}}|0\rangle_a + \frac{(3/8)}{(1/4)}|1\rangle_a\right) + \frac{1}{\sqrt{2}}|10\rangle_{n_l}|u_2\rangle_{n_b}\left(\sqrt{1-\frac{(3/8)^2}{(1/2)^2}}|0\rangle_a + \frac{(3/8)}{(1/2)}|1\rangle_a\right)$$

$$\Big\downarrow QPE^\dagger$$

$$\frac{1}{\sqrt{2}}|00\rangle_{n_l}|u_1\rangle_{n_b}\left(\sqrt{1-\frac{9}{4}}|0\rangle_a + \frac{3}{2}|1\rangle_a\right) + \frac{1}{\sqrt{2}}|00\rangle_{n_l}|u_2\rangle_{n_b}\left(\sqrt{1-\frac{9}{16}}|0\rangle_a + \frac{3}{4}|1\rangle_a\right)$$

$$\Big\downarrow$$

Project onto $|1\rangle_a$

$$\propto |00\rangle_{n_l}\left(2|u_1\rangle_{n_b} + |u_2\rangle_{n_b}\right)|1\rangle_a = |00\rangle_{n_l}\left(3|0\rangle_{n_b} + |1\rangle_{n_b}\right)|1\rangle_a$$

Which is the correct solution

Hybrid algorithms: VQE

Findind the **minimum or maximum eigenvalue** is important in many problems: e.g. determine the results of internet search engines, designing new materials and drugs, calculating physical properties.

This problem is very hard for a classical computer.

QPE: exponential speed-up, but to estimate the eigenvalue with precision ϵ it requires $\mathcal{O}(1/\epsilon)$ noiseless operations, during which the QC must remain **coherent**.

The hybrid algorithm Variational Quantum Eigensolver (VQE) provides an interesting alternative, offering an exponential speedup in evaluating the expectation value of a given Hamiltonian, compared to classical exact diagonalization.

The algorithm is **hybrid** because it combines a quantum and a classical part. This **reduces the coherence requirements** and allows us to implement it efficiently on NISQs.

Variational theorem

We consider a Hamiltonian H and its spectral decomposition:

$$H = \sum_k E_k |\phi_k\rangle\langle\phi_k|$$

The expectation value of H on an arbitrary state $|\psi\rangle$ is given by $\langle H\rangle_\psi = \langle\psi|H|\psi\rangle$

Which can be re-written as $\langle H\rangle_\psi = \langle\psi|H|\psi\rangle = \sum_k E_k \langle\psi|\phi_k\rangle\langle\phi_k|\psi\rangle = \sum_k E_k |\langle\phi_k|\psi\rangle|^2$

Hence, the expectation value of H on a given state $|\psi\rangle$ is a linear combination of its eigenvalues with **POSITIVE** weights.

$$\boxed{E_{min} \leq \langle H\rangle_\psi = \sum_k E_k |\langle\phi_k|\psi\rangle|^2}$$

We can use this result to obtain an **approximation** of the **ground state** of a given Hamiltonian

And this value is minimized by $|\psi_{min}\rangle$ such that $H|\psi_{min}\rangle = E_{min}|\psi_{min}\rangle$

Variational Quantum Eigensolver

Quantum Computing

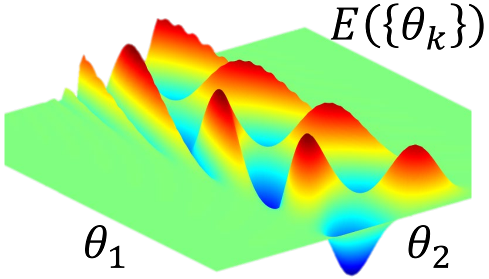
QUANTUM HARDWARE

1. Generate a variational ansatz depending on a set of parameters $|\psi(\{\theta_k\})\rangle$

2. Evaluate the expectation value of the Hamiltonian as a linear combination of Pauli products (local measurements)

CLASSICAL

3. Combine measurement results and optimize using a classical algorithm to explore the energy surface



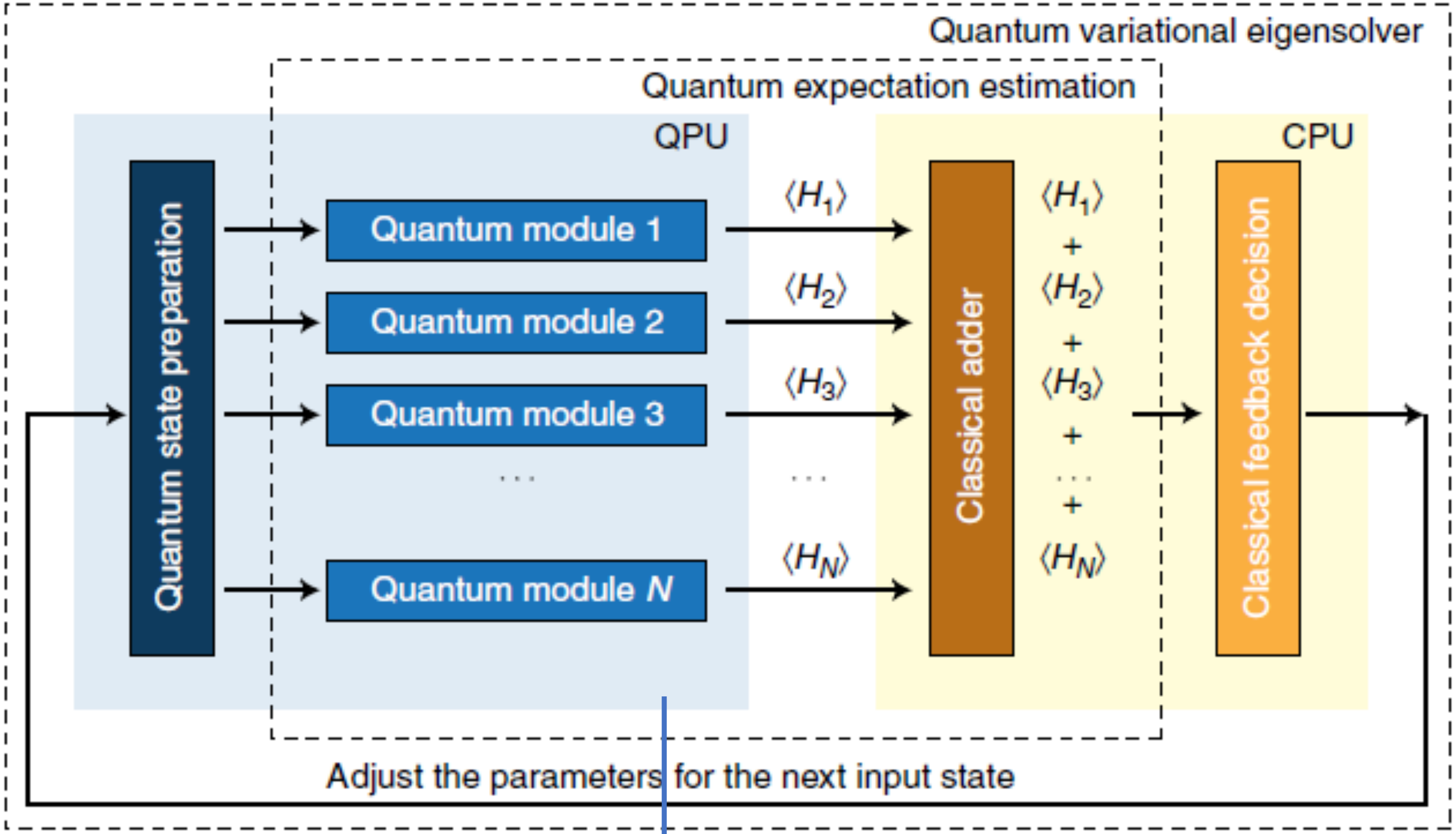
Repeat until convergence (energy variation below a threshold)

$$E(\{\theta_k\}) = \frac{\langle\psi(\{\theta_k\})|H|\psi(\{\theta_k\})\rangle}{\langle\psi(\{\theta_k\})|\psi(\{\theta_k\})\rangle}$$
$$= \sum_j \frac{\langle\psi(\{\theta_k\})|H_j|\psi(\{\theta_k\})\rangle}{\langle\psi(\{\theta_k\})|\psi(\{\theta_k\})\rangle}$$

Any hermitian Hamiltonian can be expressed as a **combination of tensor products of Paulis**.

Since the expectation value is linear, we can evaluate all these terms separately, by **local measurements** on each qubit performed in parallel.

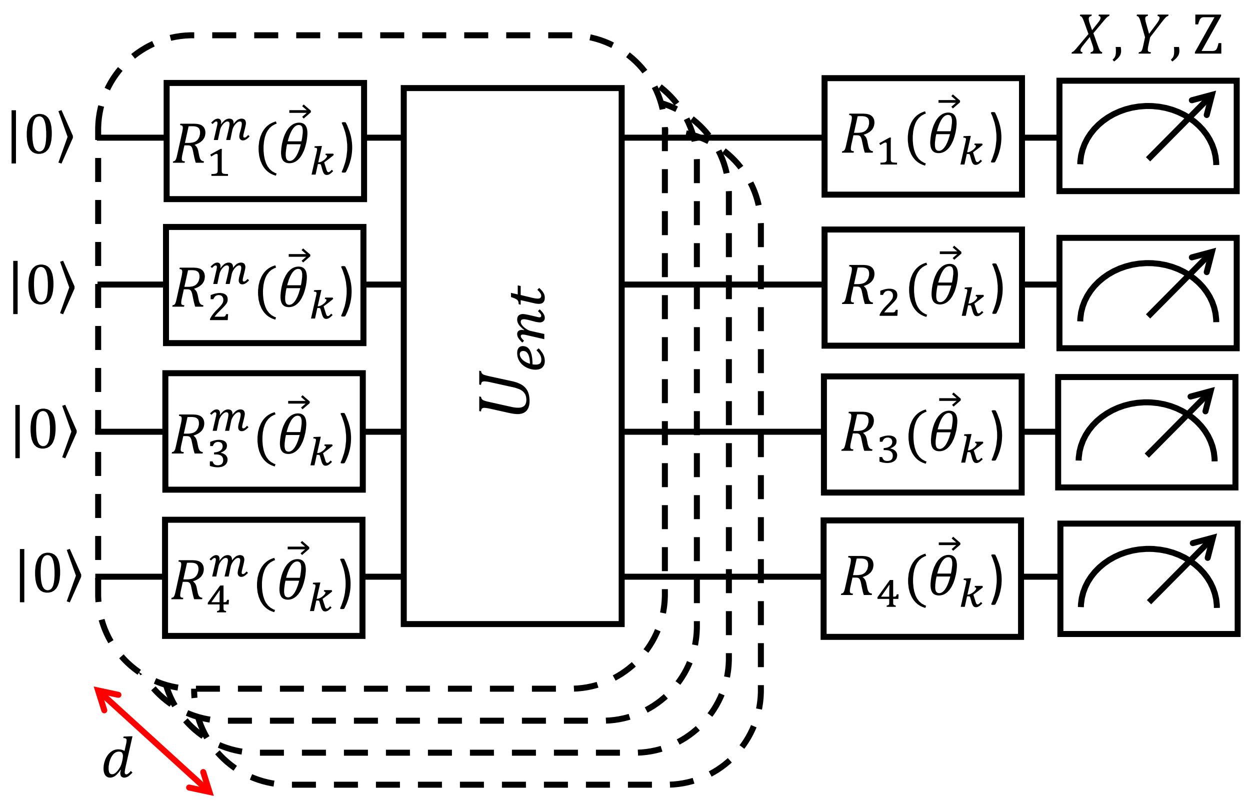
Variational Quantum Eigensolver



A. Peruzzo et al., Nature Commun. **5**, 4213 (2014)

$$H = H_1 + H_2 + \cdots H_N \Rightarrow \langle H \rangle = \langle H_1 \rangle + \langle H_2 \rangle + \cdots \langle H_N \rangle$$

Preparation of the variational ansatz



Generate ansatz $|\psi(\{\theta_k\})\rangle$

Uses layers of rotations (depending on some parameters) and entangling gates to generate the variational ansatz

A. Kandala et al., Nature **242**, 549 (2017)

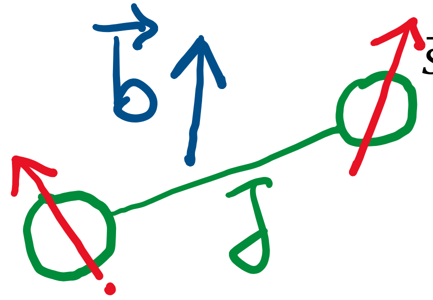
Example: VQE on a spin dimer

Spin systems are an **ideal test-bed** for a quantum hardware

$$H = J_x X_1 X_2 + J_y Y_1 Y_2 + J_z Z_1 Z_2 + b(Z_1 + Z_2)$$

The Hamiltonian (and hence its expectation value) is already a sum of products of Paulis

$$\langle\psi|H|\psi\rangle$$
$$= J_x\langle\psi|X_1X_2|\psi\rangle + J_y\langle\psi|Y_1Y_2|\psi\rangle + J_z\langle\psi|Z_1Z_2|\psi\rangle$$
$$+ b\langle\psi|Z_1|\psi\rangle + b\langle\psi|Z_2|\psi\rangle$$

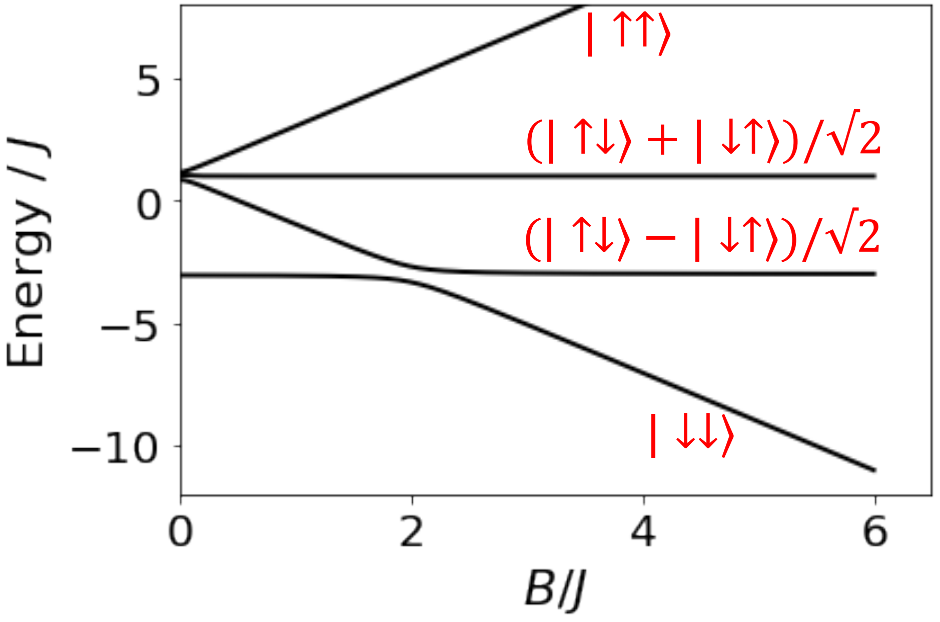


$\vec{s}_2 = {(X_2, Y_2, Z_2)}/{2}$

$\vec{s}_1 = {(X_1, Y_1, Z_1)}/{2}$

In this simple example we can compare the solution by exact diagonalization with that found using the VQE algorithm and calculate the final **fidelity** (i.e. 'closeness' of two states)

$$\mathcal{F} = \left|\langle\psi_0|\psi(\{\tilde{\theta}_k\})\rangle\right|$$



We can also compute some **observables** (e.g. magnetization) on the **final ground state**

$$\langle\psi(\{\tilde{\theta}_k\})|M_z|\psi(\{\tilde{\theta}_k\})\rangle = \langle\psi(\{\tilde{\theta}_k\})|(Z_1 + Z_2)|\psi(\{\tilde{\theta}_k\})\rangle/2$$

Example: VQE on a spin dimer

$$\langle\psi(\{\tilde\theta_k\})|M_z|\psi(\{\tilde\theta_k\})\rangle = \langle\psi(\{\tilde\theta_k\})|(Z_1+Z_2)|\psi(\{\tilde\theta_k\})\rangle/2$$

$$|\psi(\{\tilde\theta_k\})\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$\begin{aligned}
\langle\psi(\{\tilde\theta_k\})|(Z_1+Z_2)|\psi(\{\tilde\theta_k\})\rangle &= \langle\psi(\{\tilde\theta_k\})|Z_1|\psi(\{\tilde\theta_k\})\rangle + \langle\psi(\{\tilde\theta_k\})|Z_2|\psi(\{\tilde\theta_k\})\rangle \\
&= |\alpha_{00}|^2\langle 00|Z_1|00\rangle + |\alpha_{01}|^2\langle 01|Z_1|01\rangle + |\alpha_{10}|^2\langle 10|Z_1|10\rangle + |\alpha_{11}|^2\langle 11|Z_1|11\rangle \\
&+ |\alpha_{00}|^2\langle 00|Z_2|00\rangle + |\alpha_{01}|^2\langle 01|Z_2|01\rangle + |\alpha_{10}|^2\langle 10|Z_2|10\rangle + |\alpha_{11}|^2\langle 11|Z_2|11\rangle
\end{aligned}$$

$$\begin{aligned}
&= |\alpha_{00}|^2\langle 0|Z_1|0\rangle + |\alpha_{01}|^2\langle 0|Z_1|0\rangle + |\alpha_{10}|^2\langle 1|Z_1|1\rangle + |\alpha_{11}|^2\langle 1|Z_1|1\rangle \\
&+ |\alpha_{00}|^2\langle 0|Z_2|0\rangle + |\alpha_{01}|^2\langle 1|Z_2|1\rangle + |\alpha_{10}|^2\langle 0|Z_2|0\rangle + |\alpha_{11}|^2\langle 1|Z_2|1\rangle \\
&= |\alpha_{00}|^2 + |\alpha_{01}|^2 - |\alpha_{10}|^2 - |\alpha_{11}|^2 + |\alpha_{00}|^2 - |\alpha_{01}|^2 + |\alpha_{10}|^2 - |\alpha_{11}|^2 \\
&= 2(|\alpha_{00}|^2 - |\alpha_{11}|^2)
\end{aligned}$$

Example: spin dimer

If $J_x = J_y = J_z = J$ (isotropic exchange interaction) the solution is analytic, but it requires a bit of Quantum Mechanics.

$\vec{S} = \vec{s}_1 + \vec{s}_2$

$s_1 = s_2 = 1/2$

$S = |s_1 - s_2|, \dots, s_1 + s_2$

$M = -S, \dots, S$

We can rewrite $H = H_1 + H_2$, with

$$H_1 = J(X_1X_2 + Y_1Y_2 + Z_1Z_2) = 2J\, 2\vec{s}_1 \cdot \vec{s}_2 = 2J(S^2 - s_1^2 - s_2^2)$$

$$H_2 = b(Z_1 + Z_2) = 2b\, S_z$$

$[H_1, H_2] = 0$

$$S^2|S,M\rangle = S(S+1)|S,M\rangle$$

$$S_z|S,M\rangle = M|S,M\rangle$$

$$H_1|S,M\rangle = 2J[S(S+1) - s_1(s_1+1) - s_2(s_2+1)]|S,M\rangle = 2J[S(S+1) - 3/2]|S,M\rangle$$

$$H_2|S,M\rangle = 2bM\,|S,M\rangle$$

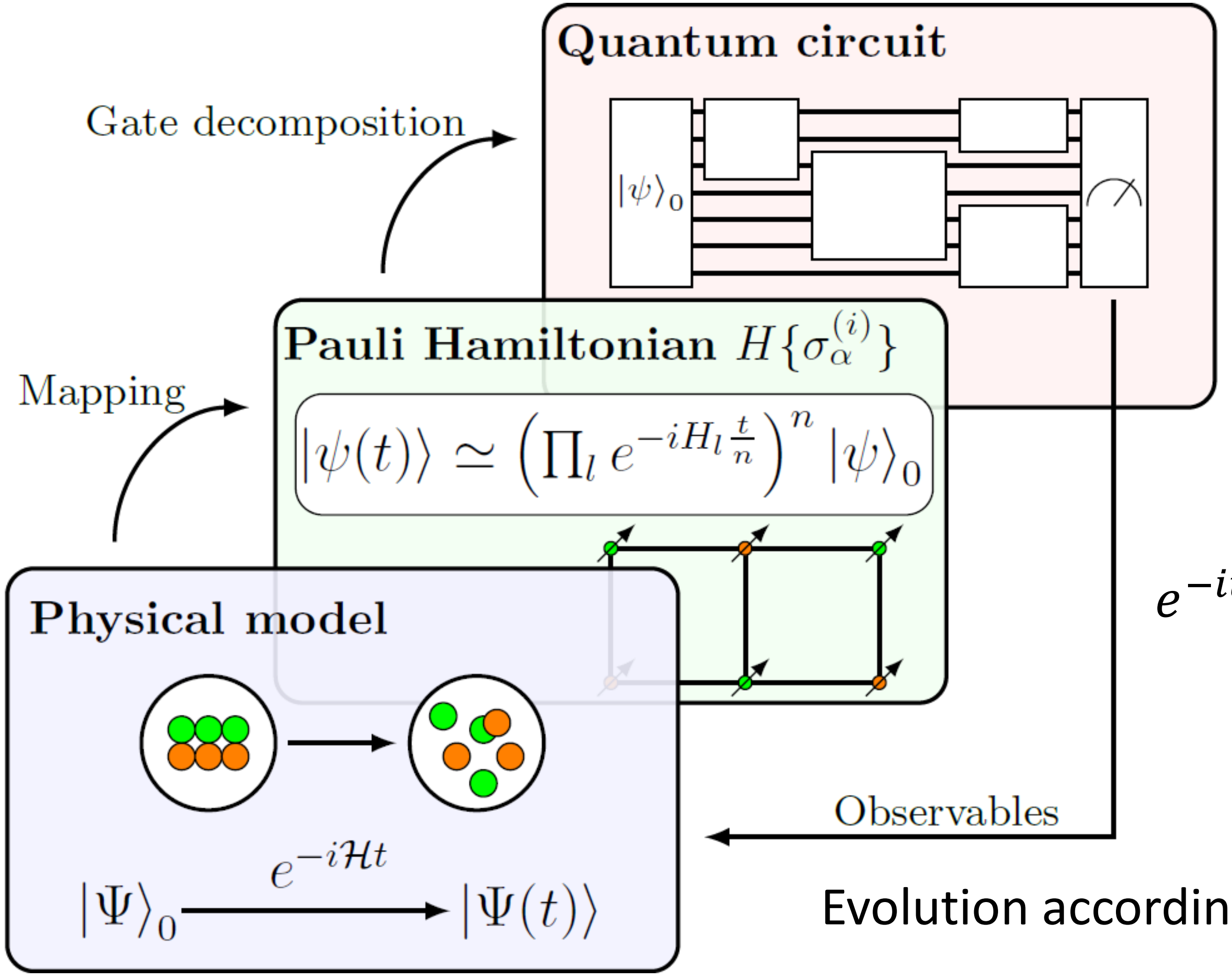
$$(H_1+H_2)|S,M\rangle = [2bM + 2JS(S+1) - 3J]|S,M\rangle$$

$\vert S=1, M=1\rangle$	$J+2b$
$\vert S=1, M=0\rangle$	J
$\vert S=1, M=-1\rangle$	$J-2b$
$\vert S=0\rangle$	$-3J$

$S = 1$
split by b

Two multiplets separated by $4J$

Quantum Simulation



Compute **observables**

$$A(t) = \langle\psi(t)|A|\psi(t)\rangle$$

Suzuki-Trotter approximation

$$e^{-it/\hbar \sum_l H_l}|\psi(0)\rangle \approx \left(\prod_l e^{-\frac{iH_l t}{\hbar n}}\right)^n |\psi(0)\rangle$$

$$\mathcal{H} = \sum_l H_l \qquad [H_l, H_k] \neq 0$$

Evolution according to target Hamiltonian $\mathcal{H}$

S. Lloyd, Science **273**, 1073 (1996)

F. Tacchino et al., https://arxiv.org/pdf/1907.03505.pdf Adv. Quant. Technol. 1900052 (2019)

Optimizing the digitalization

In the **NISQ** (noisy-intermediate scale quantum computing) era
each operation is error-prone

By increasing the circuit depth we increase the error probability.

Trade-off **Targeted error mitigation strategies**

N Trotter steps

$\tau = t/N$

$\tau' < \tau$

$N' > N$

$\tau'' < \tau'$

$N'' > N'$

Too many
noisy gates

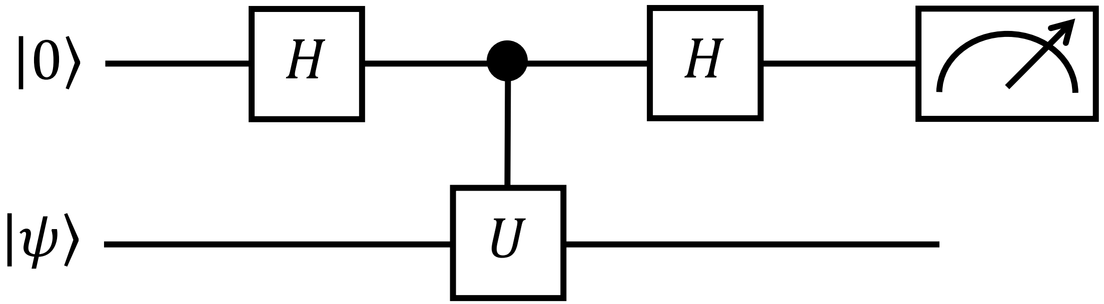
Coarse discretization

Good simulation

Simulator fails

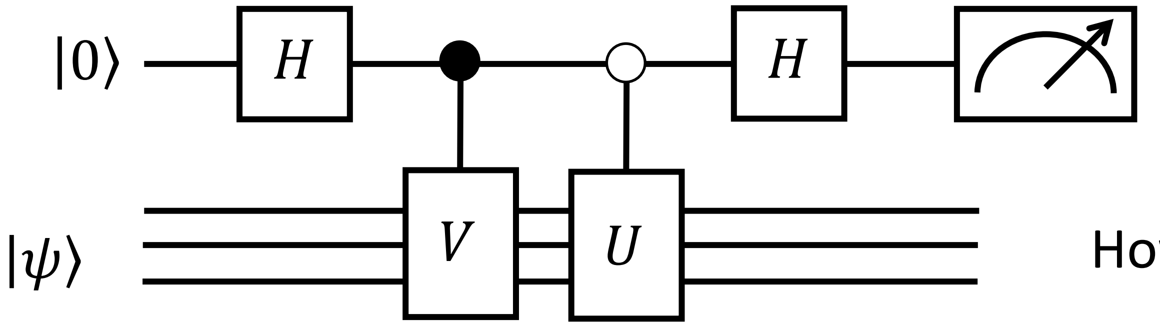
Quantum Simulation: Hadamard test

Compute observables and/or correlation functions using an ancilla for the Hadamard test:



$P_0 - P_1 = \mathrm{Re}\langle U\rangle_\psi$

Check this identity



$P_0 - P_1 = \mathrm{Re}\left\langle U^\dagger V\right\rangle_\psi$

How can you compute the imaginary part $\mathrm{Im}\langle U\rangle_\psi$?

R. Somma et al., Phys. Rev A **65**, 042323 (2002).

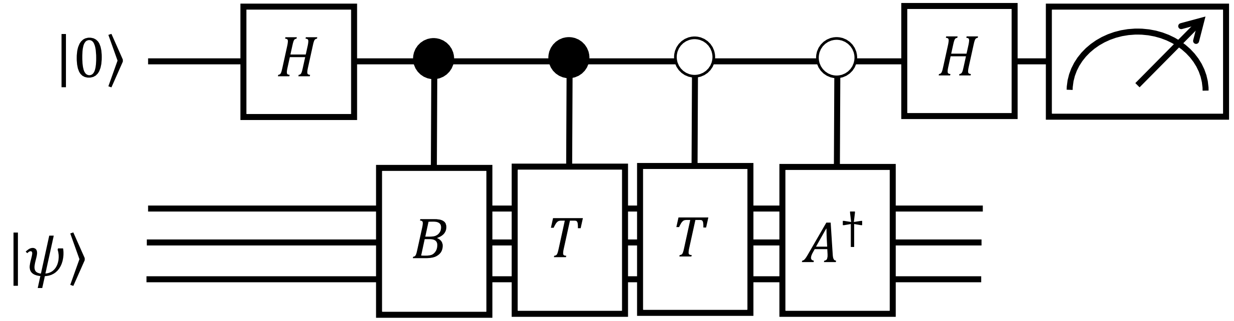
Quantum Simulation: correlation functions

It is often useful in Physics to compute dynamical **correlation functions,** i.e.

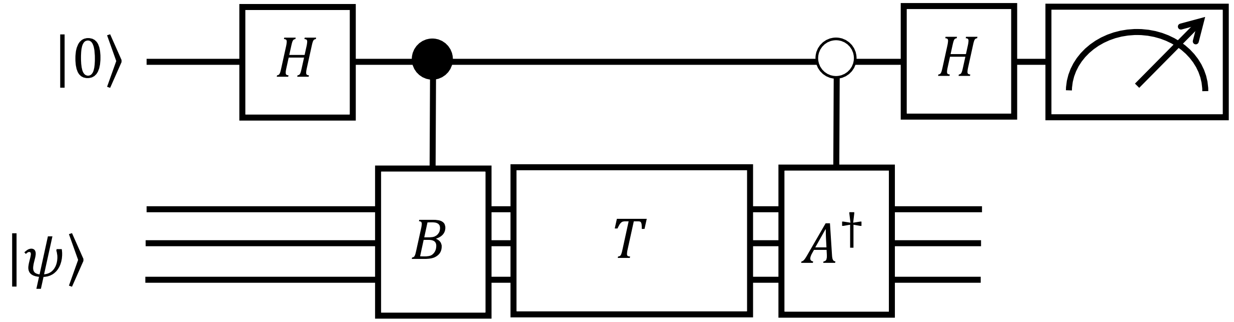
$$\langle\psi|A(t)B(0)|\psi\rangle = \langle\psi|T^\dagger A T B|\psi\rangle$$

As before, with $U^\dagger = T^\dagger A$ and $V = TB$

$$T = e^{-i\mathcal{H}t}$$



$$P_0 - P_1 = \mathrm{Re}\langle A(t)B\rangle_\psi$$



R. Somma et al., Phys. Rev A **65**, 042323 (2002).
A. Chiesa et al., Nature Phys. **15**, 455 (2019).

Quantum Approximate Optimization

Goal: minimize or maximize a function $C(x)$ subject to $x \in S$

Cost, distance, length of a trip, weight, processing time, energy consumption, number of objects

Profit, yield, efficiency, utility, capacity, number of results

Binary combinatorial problems

$$C(x) = \sum_{(Q,\bar{Q})\subset[n]} w_{(Q,\bar{Q})} \prod_{i\in Q} x_i \prod_{j\in\bar{Q}} (1 - x_j)$$

n bit strings $x \in \{0,1\}^n$

$x_i \in \{0,1\}$ $\quad w_{(Q,\bar{Q})} \in \mathbb{R}$

Map to diagonal Hamiltonian in the computational basis $\quad H = \sum_{x\in\{0,1\}^n} C(x)\, |x\rangle\langle x| \quad |x\rangle \in \mathbb{C}^{2^n}$

If $C(x)$ only has at most weight k terms (terms with at most k bits), this diagonal Hamiltonian is the sum of weight k Z operators.

Quantum Approximate Optimization

$$H = \sum_{(Q,\bar{Q})\subset[n]} w_{(Q,\bar{Q})} \frac{1}{2^{|Q|+|\bar{Q}|}} \prod_{i\in Q}(1-Z_i) \prod_{j\in\bar{Q}}(1-Z_j)$$

$$H = \sum_{k=0}^{m} C_k$$

We assume only a m (polynomial in n) w are non-zero

$$B = \sum_{i=1}^{n} X_i$$

$$\left|\psi_p\left(\vec{\gamma},\vec{\beta}\right)\right\rangle = e^{-i\beta_p B} e^{-i\gamma_p H} \ \cdots e^{-i\beta_1 B} e^{-i\gamma_1 H} |+\rangle^n$$

Ansatz obtained by combining *p* alternating evolutions of H and B

$$F_p\left(\vec{\gamma},\vec{\beta}\right) = \left\langle\psi_p\left(\vec{\gamma},\vec{\beta}\right)\left|H\right|\psi_p\left(\vec{\gamma},\vec{\beta}\right)\right\rangle = \sum_k \left\langle\psi_p\left(\vec{\gamma},\vec{\beta}\right)\left|C_k\right|\psi_p\left(\vec{\gamma},\vec{\beta}\right)\right\rangle$$

To be minimized, as in VQE

E. Farhi, J. Goldstone, and S. Gutmann, arXiv:1411.4028 (2014)

Quantum Image Processing

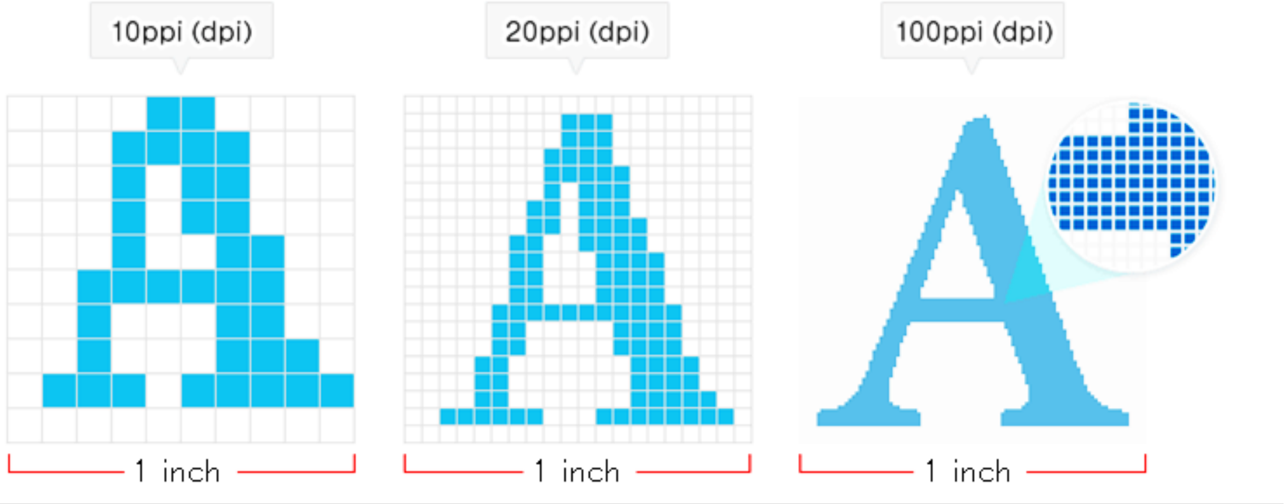
Various applications:

- Visual recognition
- Video analysis
- Optical character recognition (OCR)
- Movement detection

We focus on:

- Image encoding
- Edge detection

- Efficiency decreases by:
  - Increasing image size
  - Increasing image resolution (dpi: dots per inch, ppi: pixels per inch)



Flexible Representation of Quantum Images

$$|I(\theta)\rangle = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} (\cos\theta_i\, |0\rangle + \sin\theta_i\, |1\rangle) \otimes |i\rangle$$

$$\theta_i \in \left[0, \frac{\pi}{2}\right], i = 0,1,\cdots,2^{2n}-1$$

- Created for black and white images is easily generalised for color images.

Requirements:
$2n+1$ qubits are needed to encode a square $2^n \times 2^n$ gray tones image. Gray tones must be encoded from 0 to $\frac{\pi}{2}$.

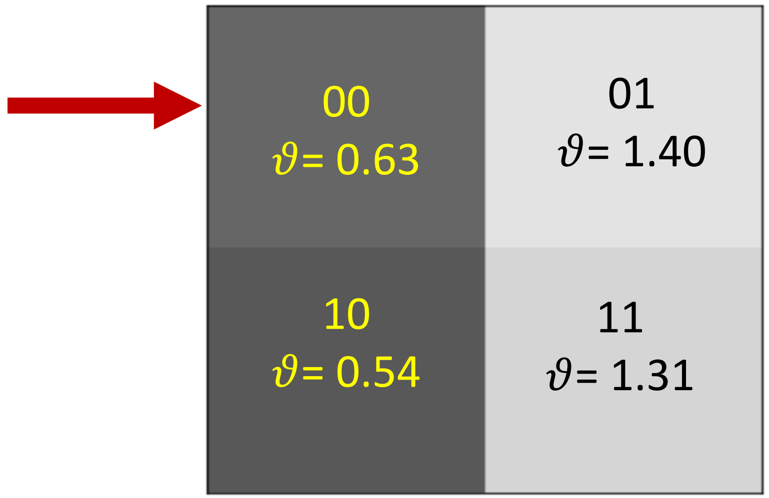
Superposition state:

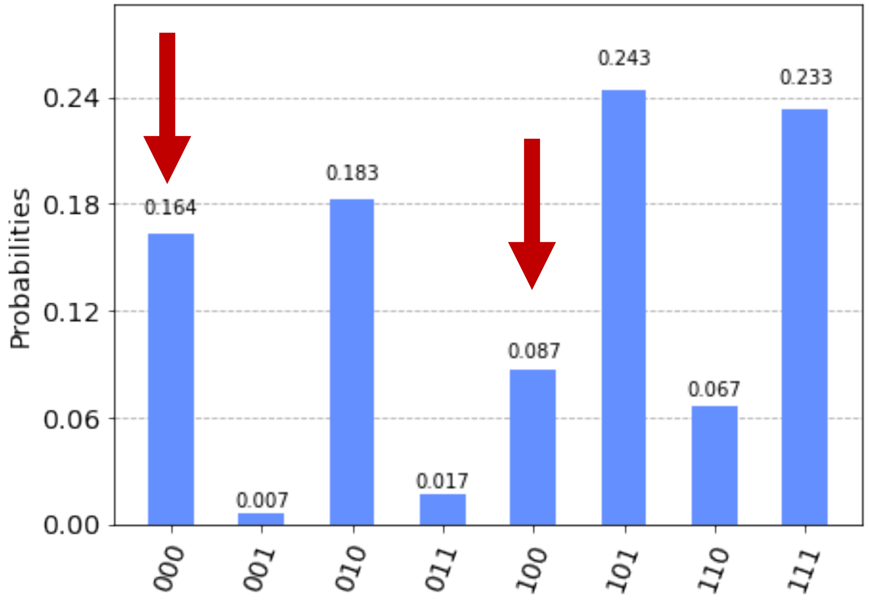
$$|H\rangle = \frac{1}{2^n}\, |0\rangle \otimes H^{\otimes 2n}|0\rangle$$

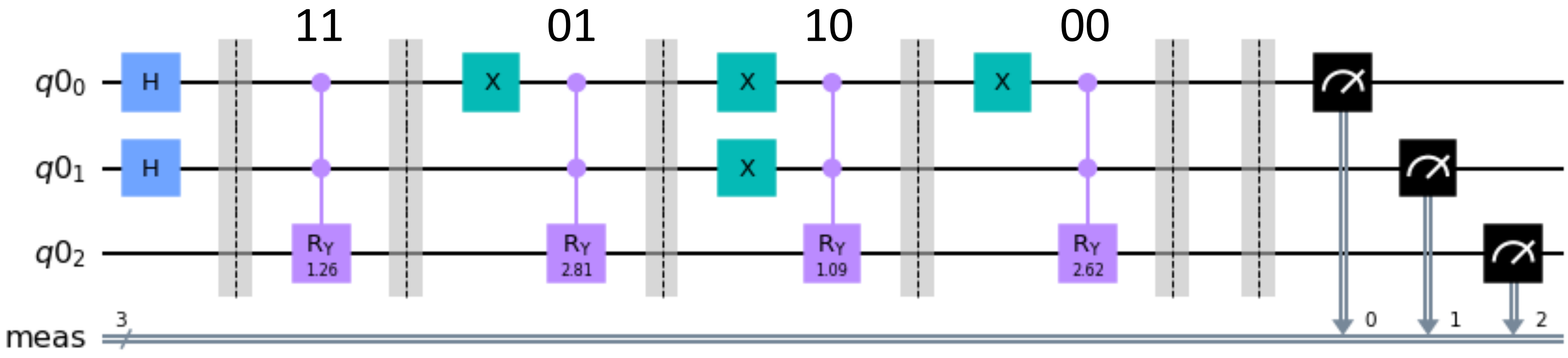
Encoding gray tones: Applying Multi Control Ry gates (MCRY)

$$C^{2n}\left(R_y(2\theta_i)\right) |H\rangle = |I(\theta)\rangle$$

Flexible Representation of Quantum Images







Novel Enhanced Quantum Representation

$$|I\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^{2n}-1} \sum_{X=0}^{2^{2n}-1} |\otimes_{i=0}^{q-1}\rangle |C_{XY}^{i}\rangle |YX\rangle$$

$$i = 0,1, \cdots, 7$$

- Quadradic speedup of the time complexity to prepare the NEQR quantum image with respect to FRQI.
- Accurate image retrieval after measurement, as opposed to probabilistic as for FRQI
- Complex operations can be achieved

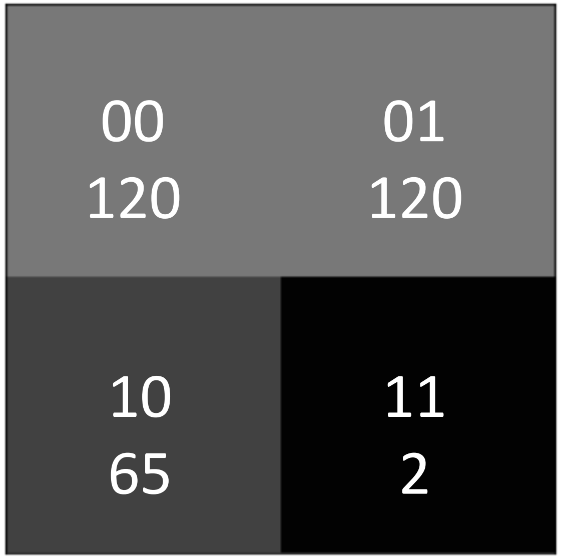
Requirements:
$2n + m$ qubits are needed to encode a square $2^n \times 2^n$ image. The various shades of gray intensity must be encoded in m bits.

Superposition state:

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

Encoding gray tones: Applying Multi Control X gates (MCX)

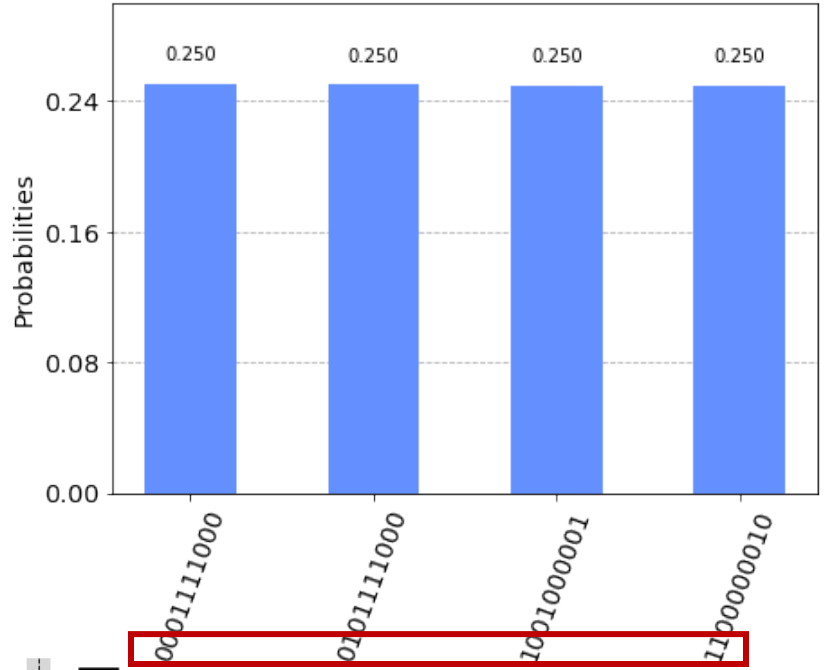
$$C^{2n}(X)\,|H\rangle = |I\rangle$$

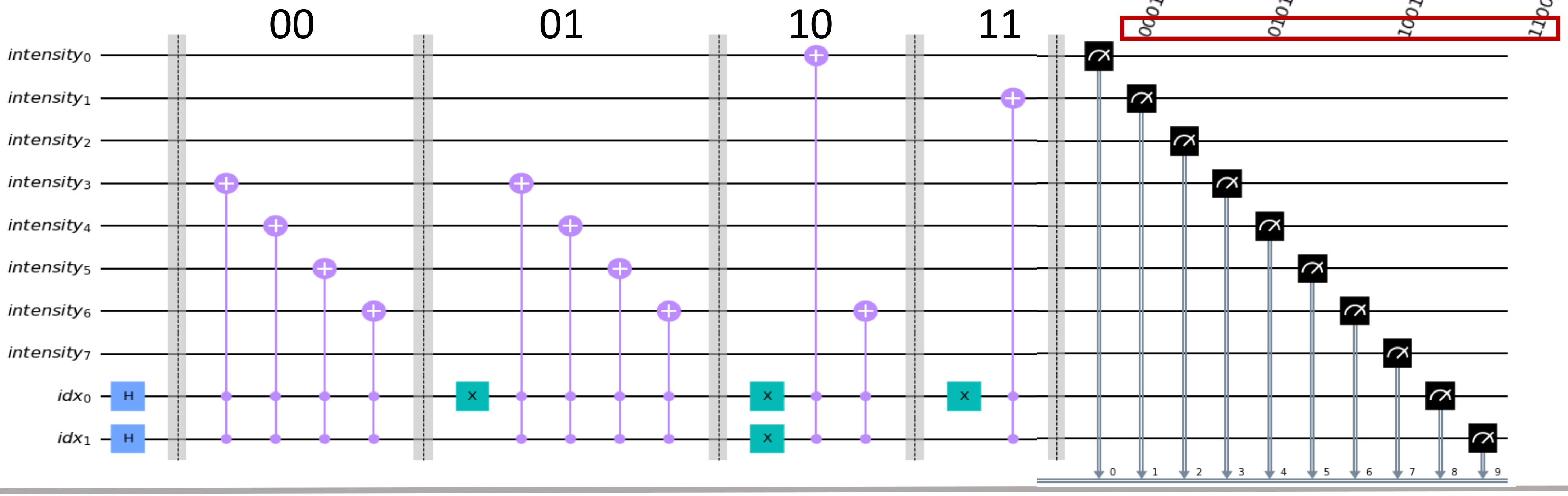


$$120 = 2^6 + 2^5 + 2^4 + 2^3$$

$$65 = 2^6 + 2^0$$

$$2 = 2^1$$

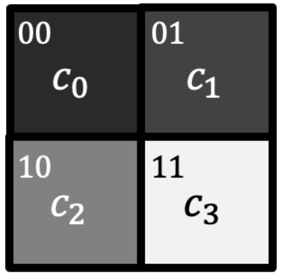




Edge detection

An edge is a change on image intensity, and it is usually gradual on a certain number of pixels

$$|\mathrm{Img}\rangle = \sum_{i=0}^{2^n-1} c_i \, |i\rangle$$



$$|\mathrm{Img}\rangle \otimes \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} c_0 \\ c_0 \\ c_1 \\ c_1 \\ c_2 \\ c_2 \\ \vdots \\ c_{N-2} \\ c_{N-2} \\ c_{N-1} \\ c_{N-1} \end{bmatrix}$$

Add an ancilla

$$D_{2^{n+1}} = \begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}$$

Decrement gate

$$(I_{2^n} \otimes H) \cdot \begin{bmatrix} c_0 \\ c_1 \\ c_1 \\ c_2 \\ c_2 \\ c_3 \\ \vdots \\ c_{N-2} \\ c_{N-1} \\ c_{N-1} \\ c_0 \end{bmatrix} \rightarrow \begin{bmatrix} c_0 + c_1 \\ c_0 - c_1 \\ c_1 + c_2 \\ c_1 - c_2 \\ c_2 + c_3 \\ c_2 - c_3 \\ \vdots \\ c_{N-2} + c_{N-1} \\ c_{N-2} - c_{N-1} \\ c_{N-1} + c_0 \\ c_{N-1} - c_0 \end{bmatrix}$$

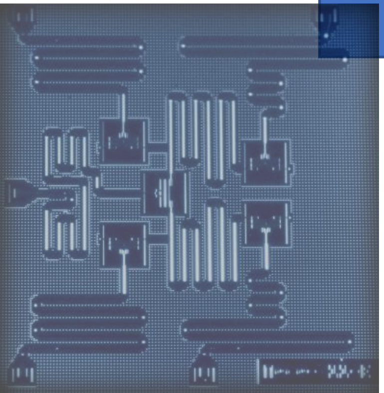
Gradient

Phys. Rev. X **7**, 031041 (2017)

https://journals.aps.org/prx/abstract/10.1103/PhysRevX.7.031041

7. From the code-world to reality: physical implementation

Quantum Computing



UNIVERSITÀ DI PARMA

Requirements: DiVincenzo criteria

1. A **scalable** system with well characterized **qubits**
2. The ability to **initialize** the system in a simple fiducial state, such as $|00\cdots 0\rangle$
3. **Long decoherence times**, much longer than the gate operation time
4. A **universal set** of quantum gates
5. A qubit-specific **measurement** capability

https://arxiv.org/abs/quant-ph/0002077

Examples of architectures

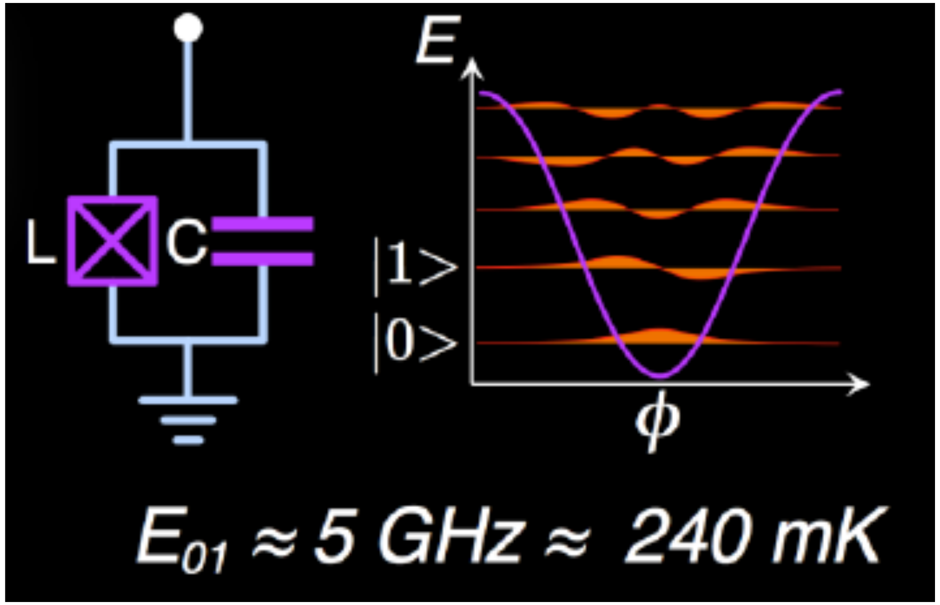
Trapped-ions quantum computer

https://ionq.com/technology

Superconducting circuits

https://www.rigetti.com/

https://www.ibm.com/quantum-computing/learn/what-is-ibm-q/

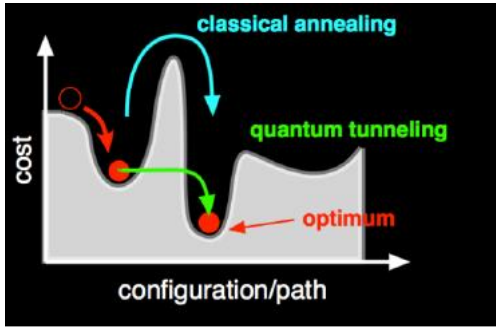


Steps of development

Quantum Annealer

- Optimization problems

- No clear quantum advantage
- Large number of noisy qubits



Approximate NISQ QC

- Material discovery
- Quantum chemistry
- Quantum simulation
- Optimization

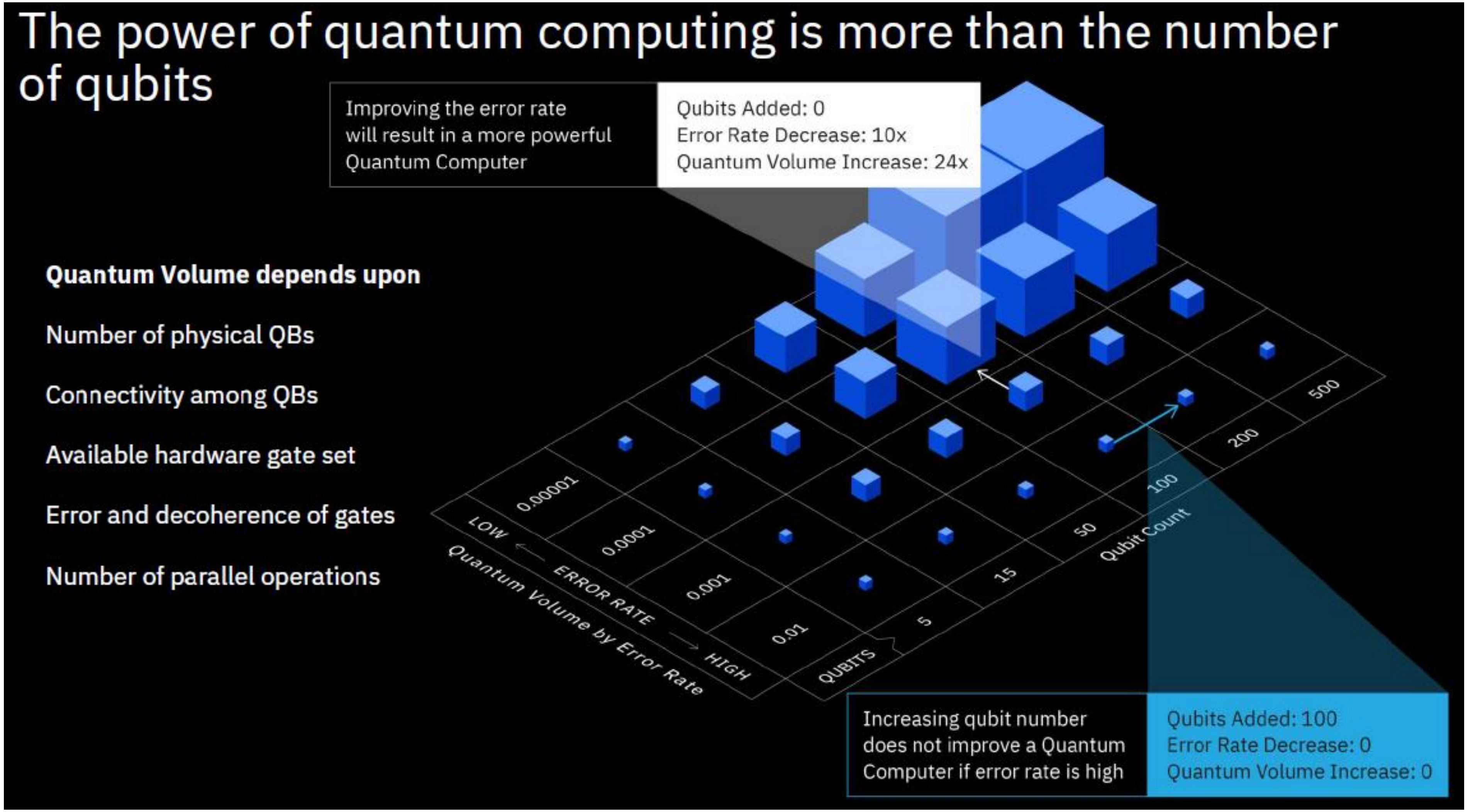
- Hybrid quantum-classical approach
- Good advantage with 50-100 qubits
- Need to **understand and mitigate errors**

Fault-tolerant Universal QC

- Arbitrary quantum algorithms:
  Binary combinatorial problems
  Cryptography
  Digital quantum simulation

- Quantum error correction needed
- Significant hardware overhead

Quantum Volume



Mixed states

Sometimes we do **not** have **enough information** to specify the state vector of a quantum system (e.g. in presence of **environmental decoherence**), but we know the probabilities $\mathcal{P}_n$ to be in a state $|\psi_n\rangle$. We can then express the mean value of an operator A as

$$\bar{A} = \sum_n \mathcal{P}_n \langle \psi_n | A | \psi_n \rangle$$

Different from the expectation value $\langle \psi | A | \psi \rangle$, in which case we **know** precisely $|\psi\rangle$

Density operator $\rho = \sum_n \mathcal{P}_n \, |\psi_n\rangle\langle\psi_n|$ $\xrightarrow[\mathcal{P}_n = \delta_{nk}]{}$ $\rho = |\psi_k\rangle\langle\psi_k|$

mixed state — **pure** state $|\psi_k\rangle$

$$\boxed{\mathrm{Tr}[\rho A]} = \sum_m \langle \psi_m | \textstyle\sum_n \mathcal{P}_n \, |\psi_n\rangle\langle\psi_n| A |\psi_m\rangle =$$
$$= \textstyle\sum_{n,m} \mathcal{P}_n \langle \psi_m | \psi_n \rangle \langle \psi_n | A | \psi_m \rangle =$$
$$= \textstyle\sum_n \mathcal{P}_n \langle \psi_n | A | \psi_n \rangle = \boxed{\bar{A}}$$

Properties of the density operator:

- $\mathrm{Tr}[\rho] = \sum_n \mathcal{P}_n = 1$
- Positive: $\langle \chi | \rho | \chi \rangle = \sum_n \mathcal{P}_n \, |\langle \chi | \psi_n \rangle|^2 \geq 0$
- For **pure** states $\mathrm{Tr}[\rho^2] = 1$

Density operator

The postulates of quantum mechanics can be re-formulated in terms of the density operator. Density operators allow us to describe **ensembles of quantum states**. This is particularly useful if

(i) the state of the system is unknown

(ii) we aim to describe a subsystem of a composite quantum system (see chapter 4).

In a closed quantum system, the time evolution of ρ is described by the unitary operator $U(t, t_0)$. Indeed,

$$\rho(t_0) = \sum_n \mathcal{P}_n \, |\psi_n(t_0)\rangle\langle\psi_n(t_0)|$$

$$\rho(t) = \sum_n \mathcal{P}_n \, U(t,t_0)|\psi_n(t_0)\rangle\langle\psi_n(t_0)|U^\dagger(t,t_0) = U(t,t_0)\rho(t_0)U^\dagger(t,t_0)$$

$$\frac{d\rho(t)}{dt} = -\frac{i}{\hbar}[H, \rho(t)]$$

Density operator

Quantum measurements are described by a set of measurement operators P_k projecting the state of the system onto subspaces corresponding to the measurement outcomes a_k. The probability that the result a_k occurs is given by

$$p_k = \mathrm{Tr}[P_k \rho]$$

And the state of the system after the measurement is $$\frac{P_k \rho P_k^\dagger}{\mathrm{Tr}[P_k \rho]}$$

with measurement (projector) operators satisfying the completeness relation $\sum_k P_k^\dagger P_k = \mathbb{I}$

We have introduced two completely different time evolutions for the quantum system: measurements induce an instantaneous, irreversible projection of the state, whereas the dynamics described by Schrödinger equation is unitary and reversible.

Partial trace

It is not possible to describe part of a physical system by as state vector.
Let AB be a composite quantum system consisting of two subsystems A and B and described by state operator ρ^{AB} in state space $\mathcal{H}_A \otimes \mathcal{H}_B$. If $\mathcal{M}$ is an observable on subsystem A represented by the operator $M = M_A \otimes \mathbb{I}_B$

$$\langle M \rangle = \mathrm{Tr}[\rho^{AB} M] = \sum_{ij \in A} \sum_{\mu\nu \in B} \langle i, \mu | \rho^{AB} | j, \nu \rangle \underbrace{\langle j, \nu | M_A \otimes \mathbb{I}_B | i, \mu \rangle}_{\langle j | M_A | i \rangle \delta_{\mu\nu}} = \sum_{ij \in A} \sum_{\mu \in B} \langle j | M_A | i \rangle \langle i, \mu | \rho^{AB} | j, \mu \rangle$$

$$\langle i | \rho^A | j \rangle = \sum_{\mu \in B} \langle i, \mu | \rho^{AB} | j, \mu \rangle \qquad \rho^A = \mathrm{Tr}_B[\rho^{AB}] \qquad \Longrightarrow \langle M \rangle = \mathrm{Tr}[\rho^A M_A]$$

Reduced density operator

Partial trace with respect to B

Decoherence

$$|\Psi\rangle = \alpha|0_A 1_B\rangle + \beta|1_A 0_B\rangle \qquad \rho^A = \mathrm{Tr}_B|\Psi\rangle\langle\Psi| = |\alpha|^2\,|0_A\rangle\langle 0_A| + |\beta|^2\,|1_A\rangle\langle 1_A| = \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix}$$

All information about phases of complex numbers α, β lost!

if a pair of states of the system of interest becomes correlated with mutually orthogonal states of another system, then all the phase coherence between the orthogonal states of the first system is lost $\Rightarrow$ **DECOHERENCE**

REMARKS:

1. In another basis set ρ^A could be not diagonal. Try to write it in the basis $|\pm_A\rangle = (|0_A\rangle \pm |1_A\rangle)/\sqrt{2}$
2. Phase information is only **locally** lost.
3. Coherences can be dynamically recovered, unless we lose control on some of the quantum variables, e.g. if one subsystem is an environment containing many degrees of freedom.

Decoherence

We can model the interaction of the quantum system with the environment by adding a term to the equation of motion for ρ:

$$\frac{d\rho(t)}{dt} = -\frac{i}{\hbar}[H,\rho(t)] + \mathcal{D}[\rho]$$

Here $\rho = \mathrm{Tr}_E \rho^{SE}$ is the **REDUCED** density matrix on the system, having traced the environmental degrees of freedom.

Unitary evolution

Non-unitary evolution due to system-environment interaction

It makes our computer **QUANTUM**

HARMFUL: It destroys the quantumness of our computer on a time-scale set by the *decoherence time*

It must be reduced as much as possible on devices

Phase damping channel

$$|0_A 0_E\rangle \longrightarrow \sqrt{1-p}|0_A 0_E\rangle + \sqrt{p}|0_A 1_E\rangle = |0_A\rangle \otimes \left(\sqrt{1-p}|0_E\rangle + \sqrt{p}|1_E\rangle\right)$$

$$|1_A 0_E\rangle \longrightarrow \sqrt{1-p}|1_A 0_E\rangle + \sqrt{p}|1_A 2_E\rangle = |1_A\rangle \otimes \left(\sqrt{1-p}|0_E\rangle + \sqrt{p}|2_E\rangle\right)$$

The state of the qubit does not change, but the state of the environment changes depending on the state of the qubit. $|0_A\rangle$ and $|1_A\rangle$ do not become entangled with the environment (pointer states) but a superposition does.

$$|\Psi\rangle = (\alpha|0_A\rangle + \beta|1_A\rangle) \otimes |0_E\rangle \longrightarrow \rho_0^A = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^* & |\beta|^2 \end{pmatrix}$$

$$U: \mathcal{H}_A \otimes \mathcal{H}_E \rightarrow \mathcal{H}_A \otimes \mathcal{H}_E \qquad U|\Psi\rangle = \alpha\sqrt{1-p}|0_A 0_E\rangle + \alpha\sqrt{p}|0_A 1_E\rangle + \beta\sqrt{1-p}|1_A 0_E\rangle + \beta\sqrt{p}|1_A 2_E\rangle$$

$$\rho^A = \mathrm{Tr}_E\left[U|\Psi\rangle\langle\Psi|U^\dagger\right] = |\alpha|^2|0_A\rangle\langle 0_A| + |\beta|^2|1_A\rangle\langle 1_A| + \alpha\beta^*(1-p)|0_A\rangle\langle 1_A| + \mathrm{h.c.}$$

$$\rho^A = \begin{pmatrix} |\alpha|^2 & \alpha\beta^*(1-p) \\ \beta\alpha^*(1-p) & |\beta|^2 \end{pmatrix} = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* e^{-t/T_2} \\ \beta\alpha^* e^{-t/T_2} & |\beta|^2 \end{pmatrix} \xrightarrow[t\to\infty]{} \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix}$$

$$p = (1 - e^{-t/T_2})$$

Decoherence time

Quantum operations

In general we cannot describe incoherent processes by unitary matrices acting on the whole Hilbert space, but we need to focus on a rather small subsystem described by a reduced density matrix. Within this framework, the evolution of ρ at discrete time steps can be given expressed by the quantum operation

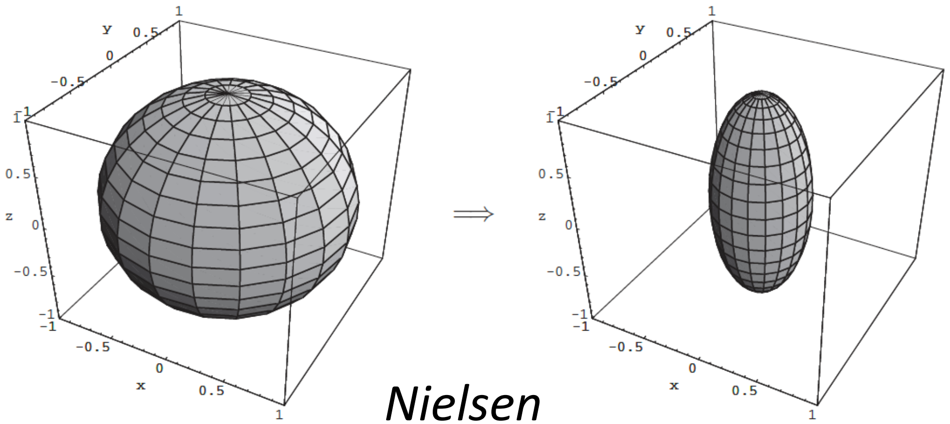
$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger \qquad \sum_k E_k E_k^\dagger = \mathbb{I}$$

Kraus operators, which can be expressed in terms of Paulis

Example: **phase flip** $E_0 = \sqrt{1-p}\,\mathbb{I}$ $\qquad E_1 = \sqrt{p}\,Z$

$$\rho \rightarrow \mathcal{E}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger = (1-p)\rho + pZ\rho Z$$

You can check this is equivalent to the previous slide calculation (continuous phase damping, with $1-2p = e^{-t/T_2}$).
The corresponding Bloch vector is projected along z

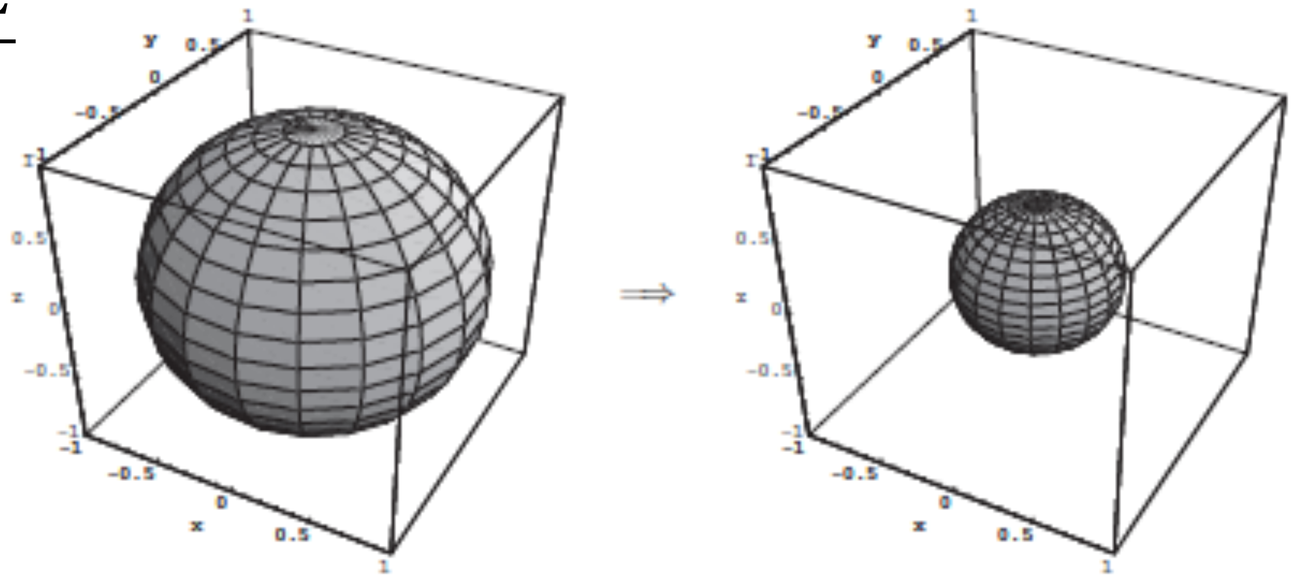


Nielsen

Depolarizing channel

$$\mathcal{E}(\rho) = (1-p)\rho + p\frac{\mathbb{I}}{2}$$
$$= (1-p)\rho + p\frac{\rho + X\rho X + Y\rho Y + Z\rho Z}{4}$$
$$= \left(1 - \frac{3p}{4}\right)\rho + p\frac{X\rho X + Y\rho Y + Z\rho Z}{4}$$

Uniform Pauli error channel



$$\mathcal{E}(\rho) = (1-p)\rho + p\frac{\mathbb{I}}{2^n}$$

On n qubits

M. A. Nielsen, I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000)

Relaxation

Amplitude damping (i.e. relaxation at $T = 0$) approximately modeled by

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix} \qquad E_1 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}$$

$$\rho \to \mathcal{E}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger$$

Decay of excited diagonal state with rate $1 - p = e^{-t/T_1}$

$$\rho(t) = \begin{pmatrix} 1 - |\beta|^2(1-p) & \alpha\beta^*\sqrt{1-p} \\ \beta\alpha^*\sqrt{1-p} & |\beta|^2(1-p) \end{pmatrix} = \begin{pmatrix} 1 - |\beta|^2 e^{-t/T_1} & \alpha\beta^* e^{-t/2T_1} \\ \beta\alpha^* e^{-t/2T_1} & |\beta|^2 e^{-t/T_1} \end{pmatrix} \xrightarrow[t \to \infty]{} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Bloch sphere for mixed states

An arbitrary density matrix for a qubit in a mixed state can be written as

$$\rho = \frac{\mathbb{I} + \mathbf{r}\cdot\boldsymbol{\sigma}}{2} \qquad \text{with } \mathbf{r} = (u, v, w),\ \boldsymbol{\sigma} = (X, Y, Z) \qquad \|\mathbf{r}\|^2 = u^2 + v^2 + w^2 \le 1$$

Bloch vector for state ρ

$\mathrm{Tr}\rho = 1$ ✔

$$\mathrm{Tr}\rho^2 = \frac{1}{2}(1 + \|\mathbf{r}\|^2)$$

Pure state $\|\mathbf{r}\|^2 = 1$

Mixed state $\|\mathbf{r}\|^2 < 1$

Maximally mixed: $\|\mathbf{r}\|^2 = 0$

If we diagonlize ρ we get:

$$\rho = \frac{1}{2}(1 + \|\mathbf{r}\|)|\rho_+\rangle\langle\rho_+| + \frac{1}{2}(1 - \|\mathbf{r}\|)|\rho_-\rangle\langle\rho_-|$$

It reduces to the pure state $\rho = |\rho_+\rangle\langle\rho_+|$ if $\|\mathbf{r}\| = 1$.

Decoherence = shrinking of Bloch sphere (see Nielsen, Chuang section 8.3)

Qiskit: noise models

Errors

Systematic (unitary) errors

Reduced by calibrating the hardware

Gate errors

Depolarizing channel

Increases with number of operations (circuit depth)

Relaxation and dephasing

Modeled by T_1 and T_2 dechorence times

Increases with time

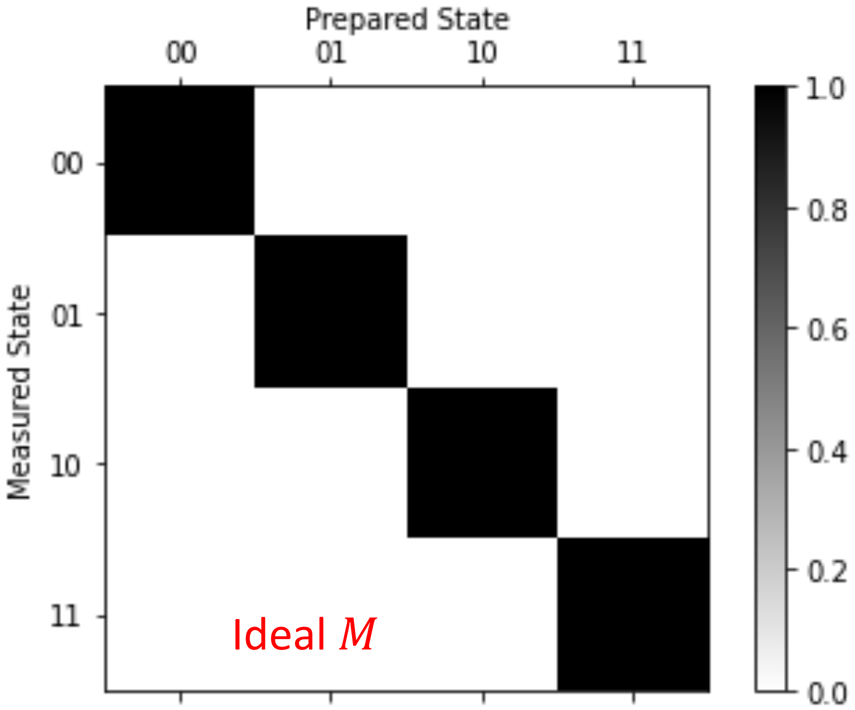
Measurement errors

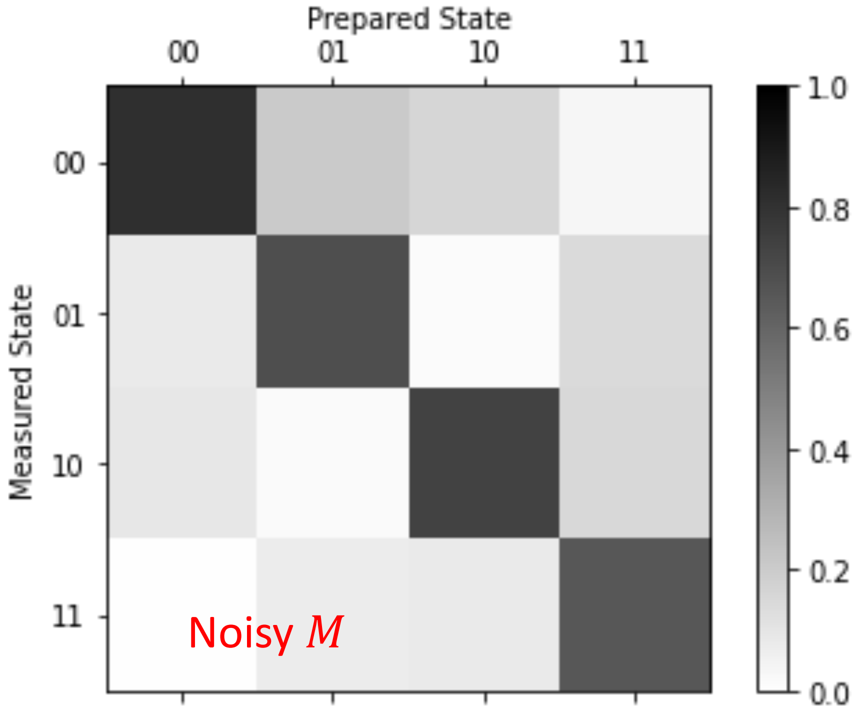
Assignement error at the qubit readout. Modeled by a deformation of the ideal projectors $P_0 = |0\rangle\langle 0|$, $P_1 = |1\rangle\langle 1|$

$$\pi_0 = (1-p)\ P_0 + p\ P_1$$
$$\pi_1 = (1-p)\ P_1 + p\ P_0$$

Error mitigation: measurement errors

The effect of noise occurring during computation can be complex. A simpler form of noise occurs during final readout. We can compute a **calibration matrix** $\langle y|M|x\rangle$ containing the probability of measuring output $|y\rangle$ for a bit string prepared in state $|x\rangle$ and then use it to **correct the output** C of a calculation.



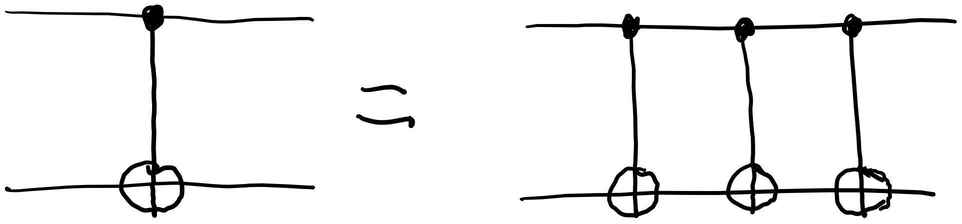


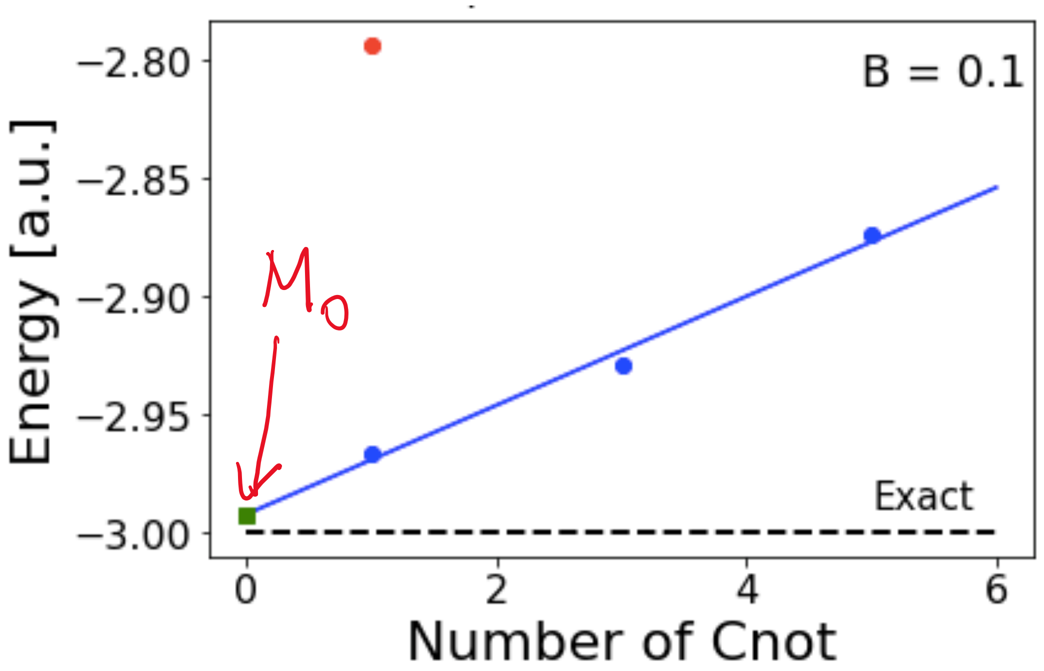
$$C_{noisy} = M\, C_{ideal} \quad \rightarrow \quad C_{ideal} = M^{-1}\, C_{noisy}$$

Error mitigation: gate errors

Extrapolation to zero noise

$$M(\lambda) = M_0 + \sum_k a_k \lambda^k$$





The expectation value of a given observable can be expressed in a power series of a noise parameter λ. Often the behavior is approximately linear and hence we can extract the zero-noise expectation value M_0 by linear extrapolation.

Quantum Error Correction

“We have learned that it is possible to fight entanglement with entanglement”

John Preskill

Example: three-qubit **bit-flip repetition code**

We can detect bit flip error on any of the three qubits by parity measurements of Z_1Z_2 and Z_2Z_3
Parity measurements can be implemented by two *additional ancillae* (Rep. Prog. Phys. **76**, 076001)
These measurement detect errors while **preserving the superposition**.
Two or more errors are not corrected.

Initial state $(\alpha|0\rangle + \beta|1\rangle) \otimes |00\rangle$

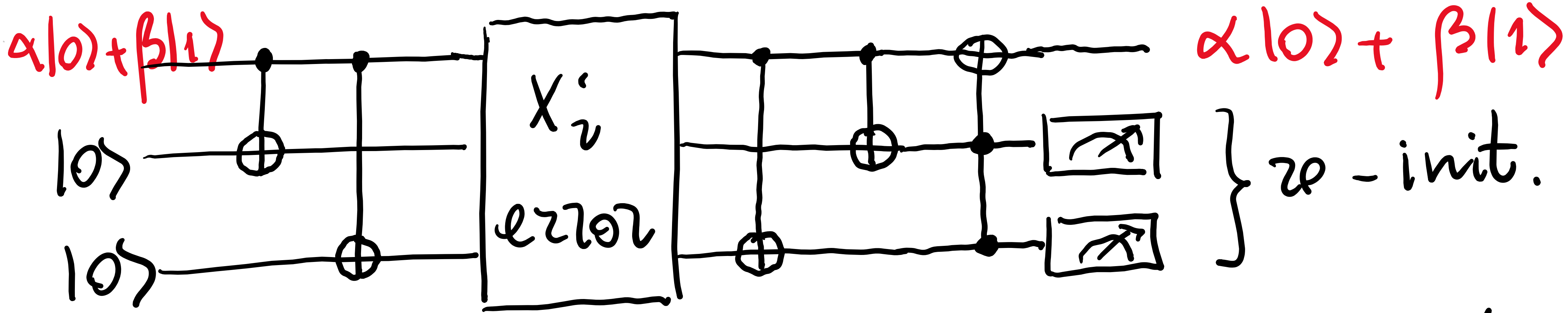
Encoding $\downarrow$

$\alpha|000\rangle + \beta|111\rangle \longrightarrow$

Output	$\langle Z_1Z_2\rangle$	$\langle Z_2Z_3\rangle$	Error
$\alpha\|000\rangle + \beta\|111\rangle$	1	1	No
$\alpha\|100\rangle + \beta\|011\rangle$	-1	1	1°
$\alpha\|010\rangle + \beta\|101\rangle$	-1	-1	2°
$\alpha\|001\rangle + \beta\|110\rangle$	1	-1	3°

Design a circuit
- to encode the protected state
- Correct the state of the 1° qubit without parity checks

3-qubit bit-flip repetition code



- This circuit detects an X error on any of the 3 qubits but corrects only the 1st one
- It can be adapted to correct Z errors
- It preserves superposition of the 1st qubit

Qubit calibration using Pulse