Istituto Nazionale di Fisica Nucleare
Sezione di Bologna

GGI School on
"Quantum Computation and Sensing"

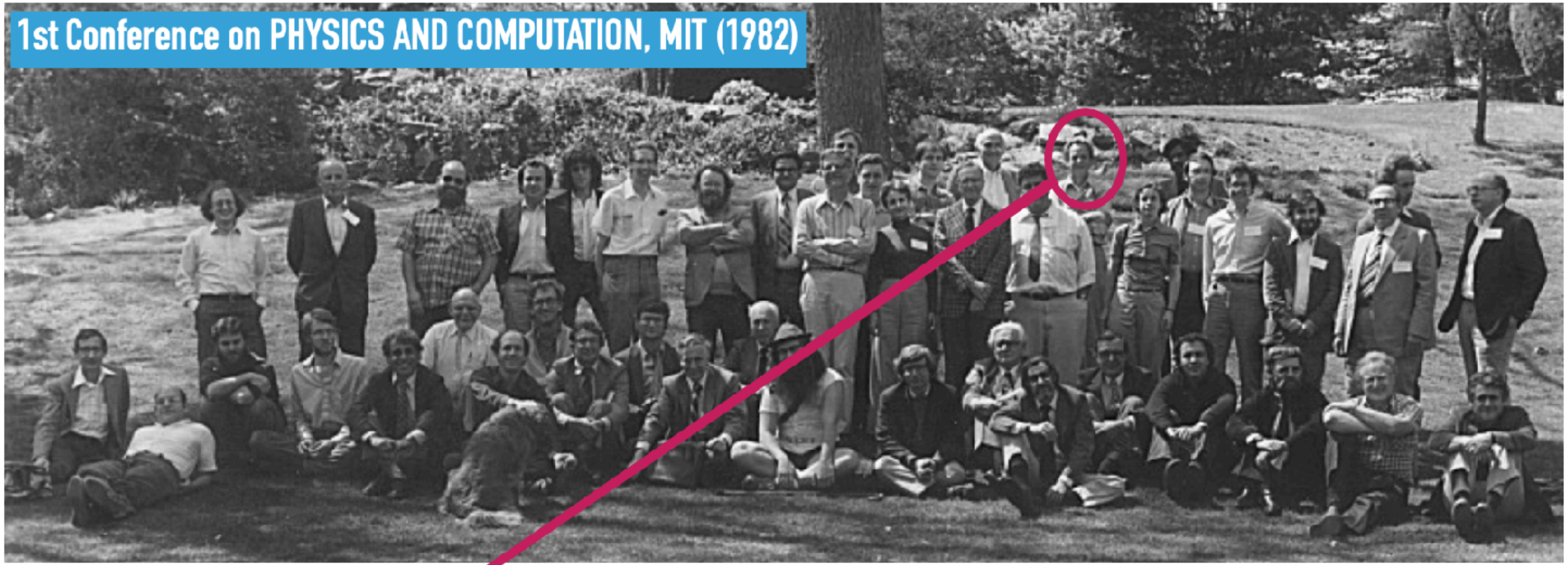
Quantum Algorithms and Protocols

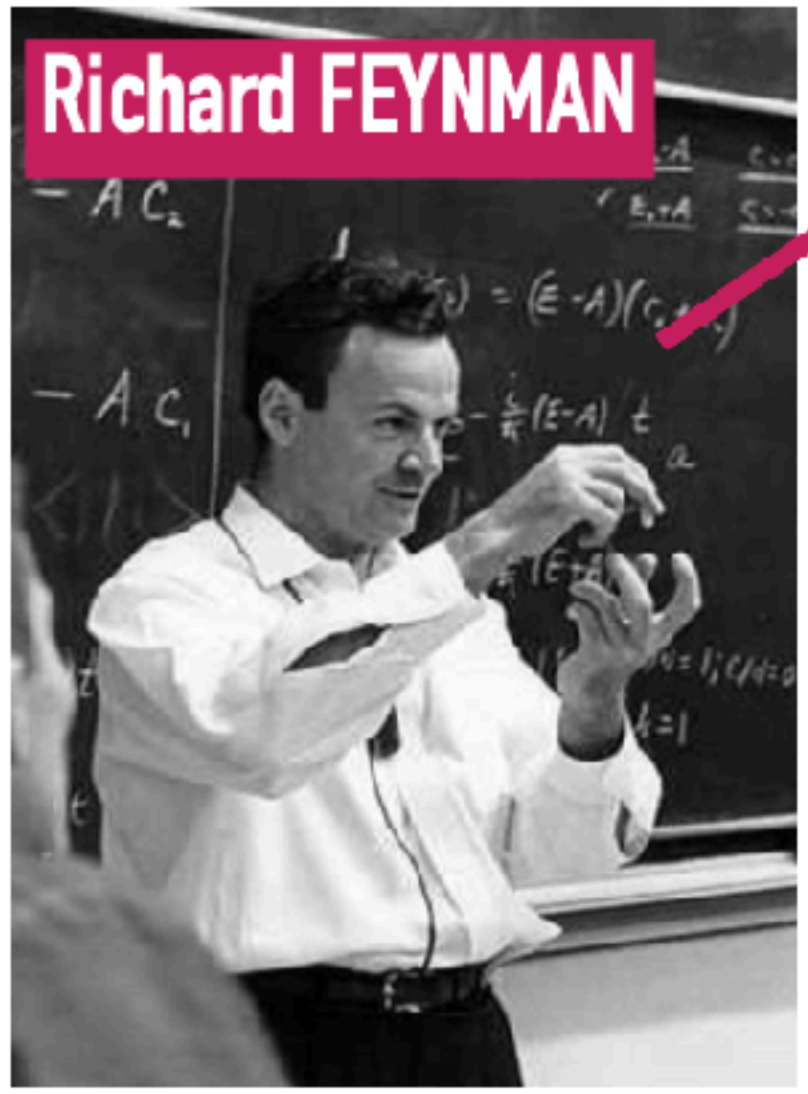
LECTURE 1

Elisa Ercolessi

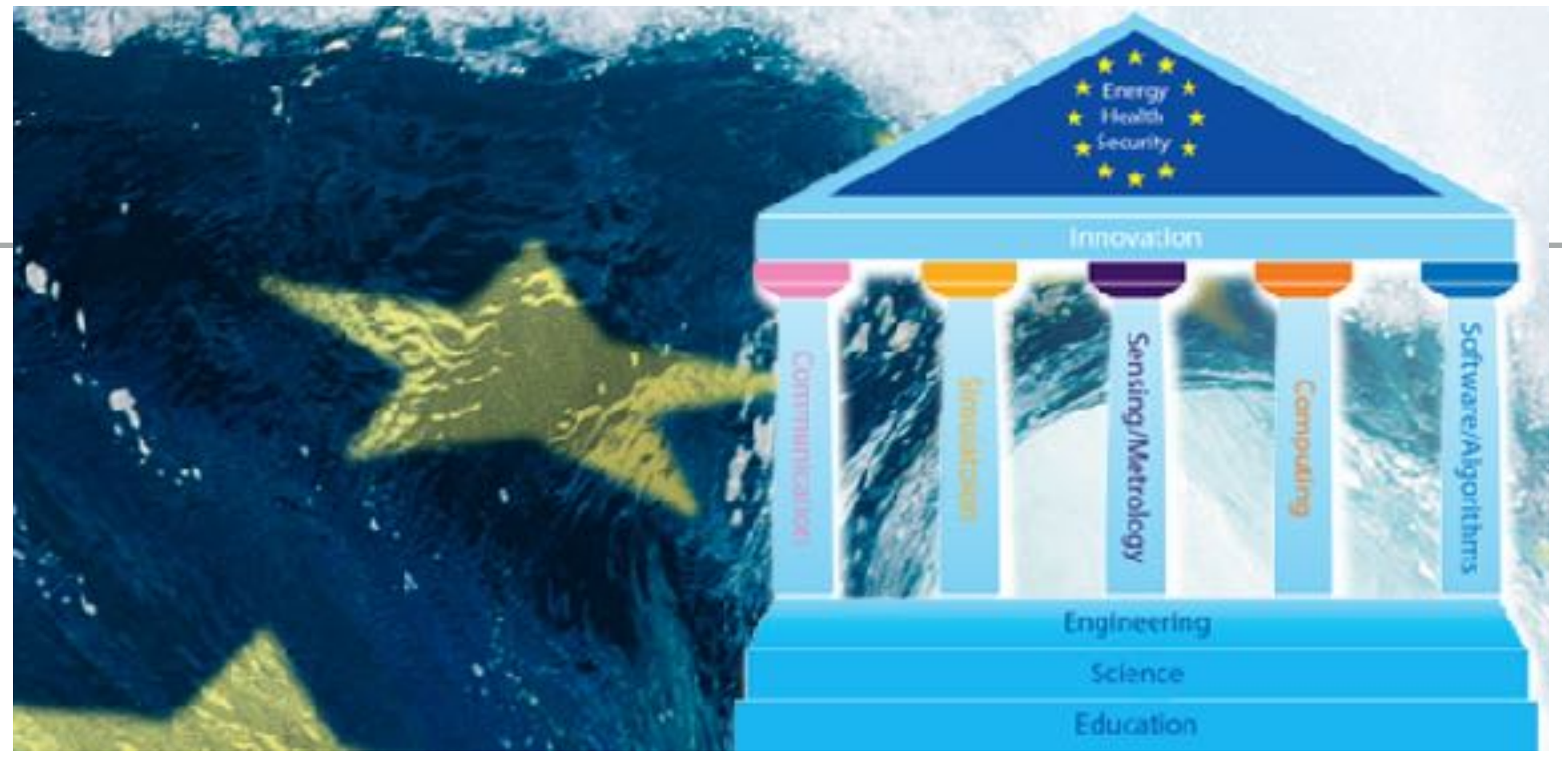
Theory and Phenomenology of Fundamental Interactions
UNIVERSITY AND INFN · BOLOGNA

QUANTUM COMPUTERS

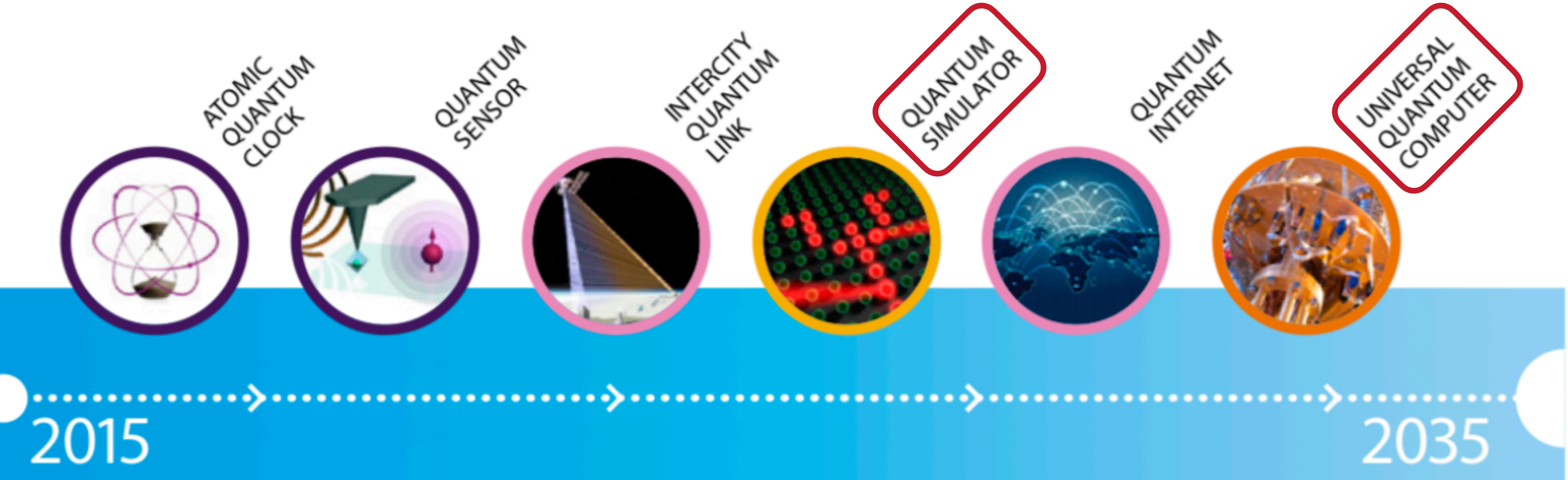




"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."
(Richard Feynman, 1982)



- Quantum theory is (almost) a century old:
  Heisenberg 1925, Schroedinger 1926
- The most debated and challenged, but also the most confirmed physical theory
- Modern every-day and advanced technology is based on quantum effects
- We are now in the era of a second quantum revolution:
  fundamentals of quantum theory are used to enhance technology



EUROPEAN
QUANTUM
FLAGSHIP

Antikythera Mechanism
(I century bc)

FERMIAC (1946)

WIND GALLERY

ENIAC (1946)

IBM PC (1981)

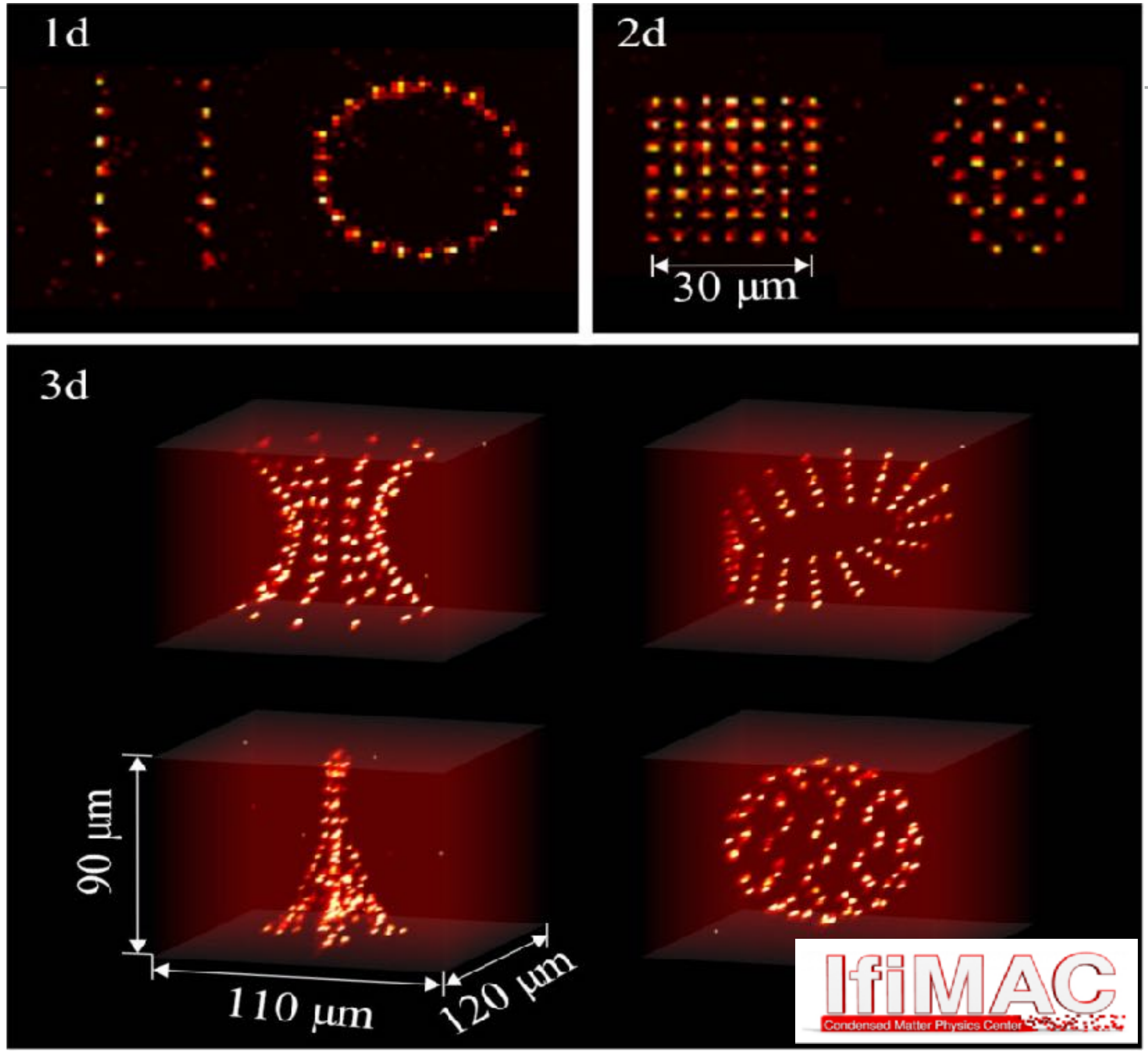
IBM
supercomputer (2018)

QUANTUM SIMULATORS

Manipulation of single cold atoms/ions, trapped in an optical potential

- Versatility:

- different geometries
- different "hopping" velocities
- tunable interactions
- internal degrees of freedom
- different statistics (bosonic, fermonic, ...)



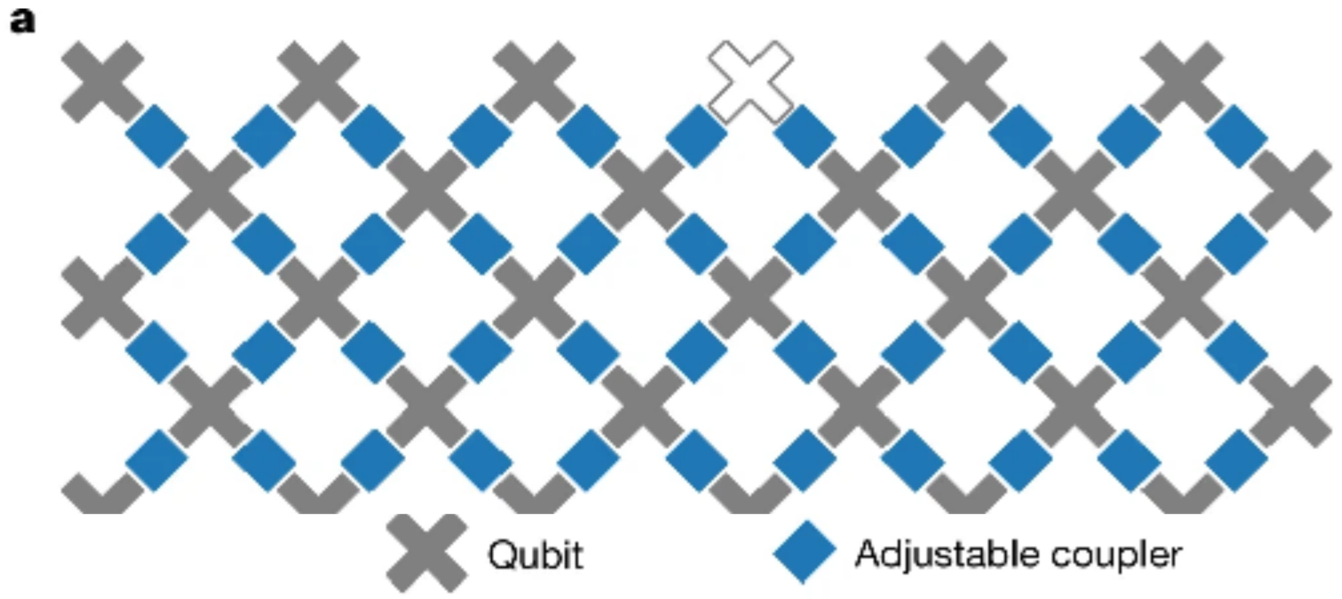
Wide range of models can be simulated:

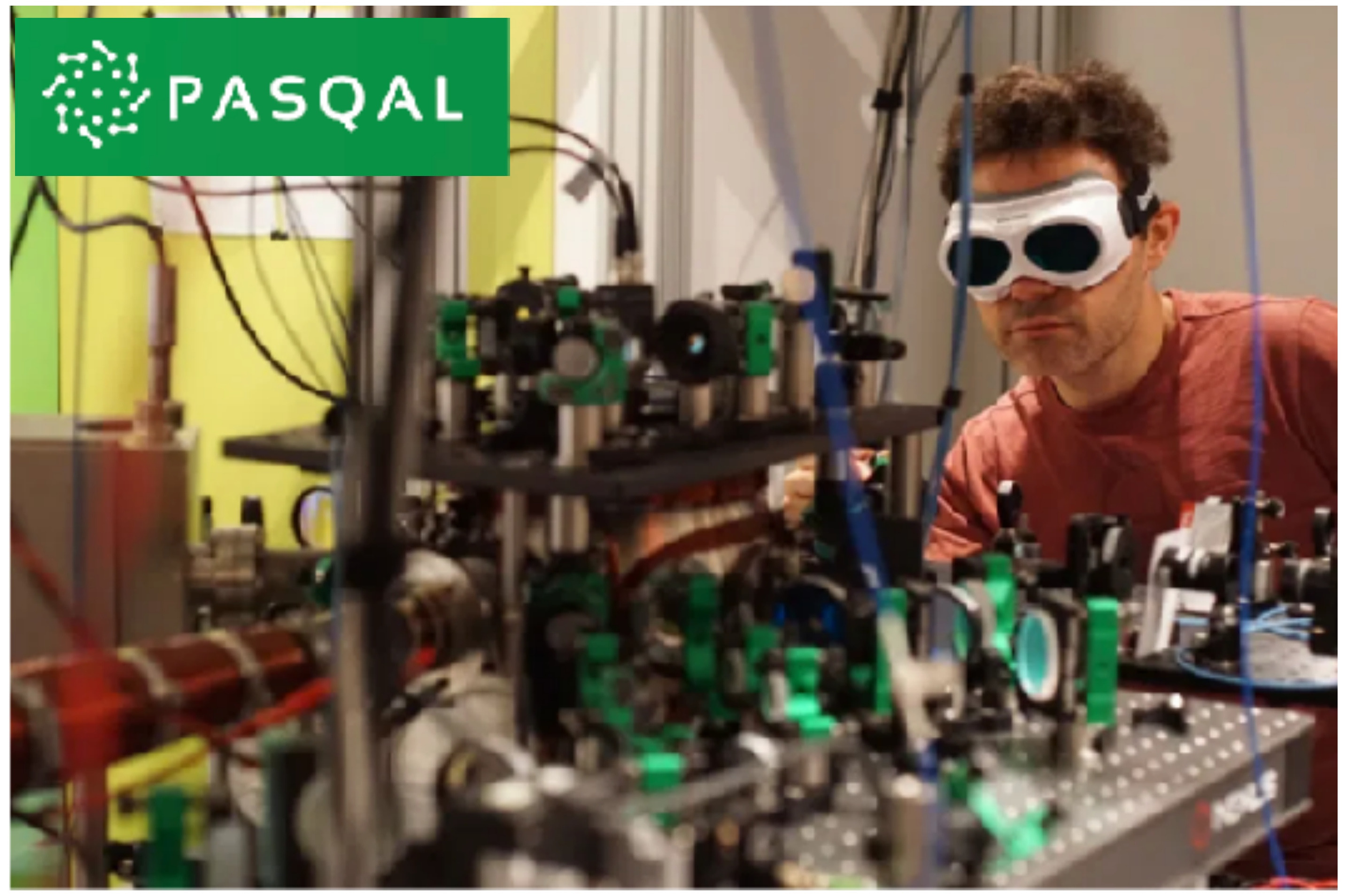
- condensed matter systems
- fundamental interactions (particles and gravity)

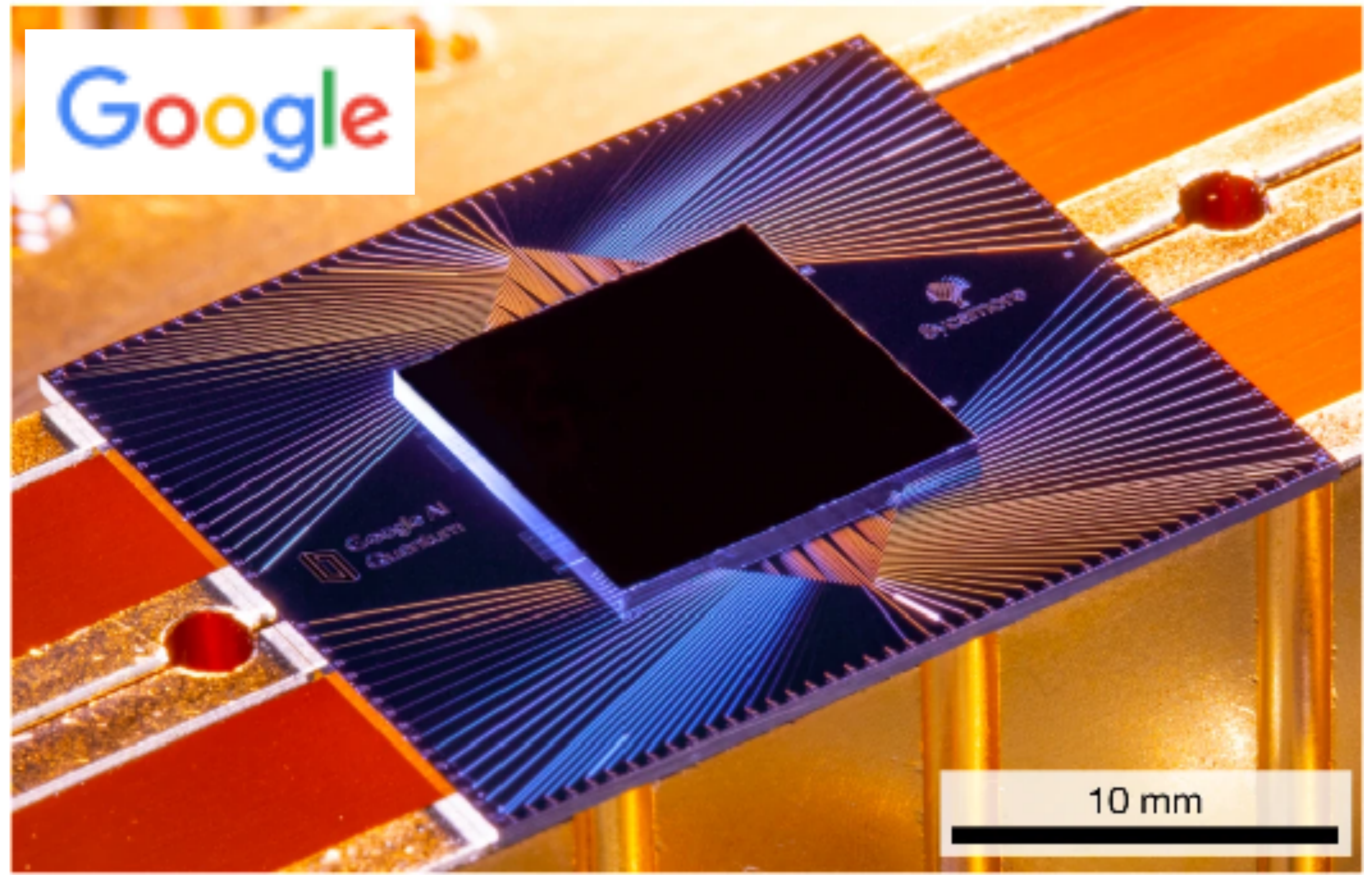
Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, […] John M. Martinis

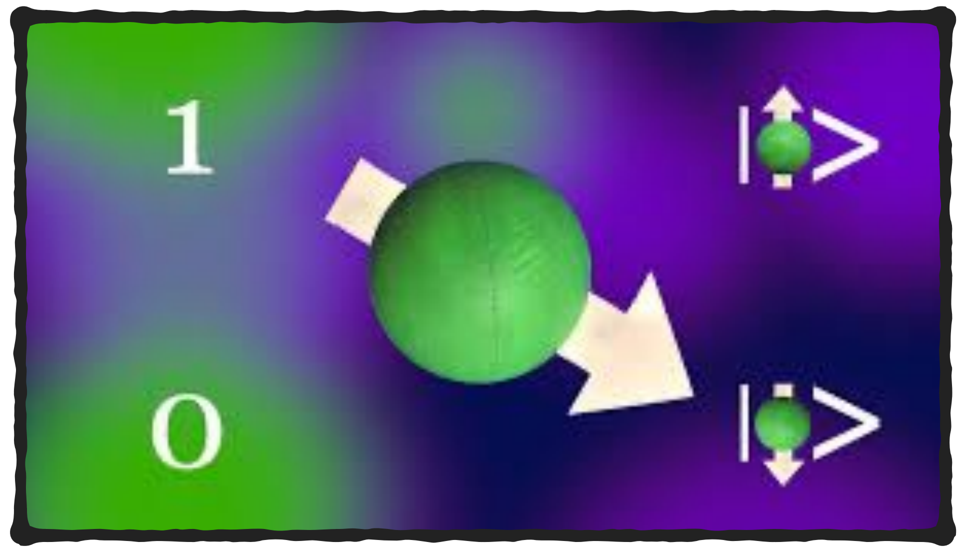
Nature **574**, 505–510(2019) | Cite this article







- How we describe the states of one or more qubits

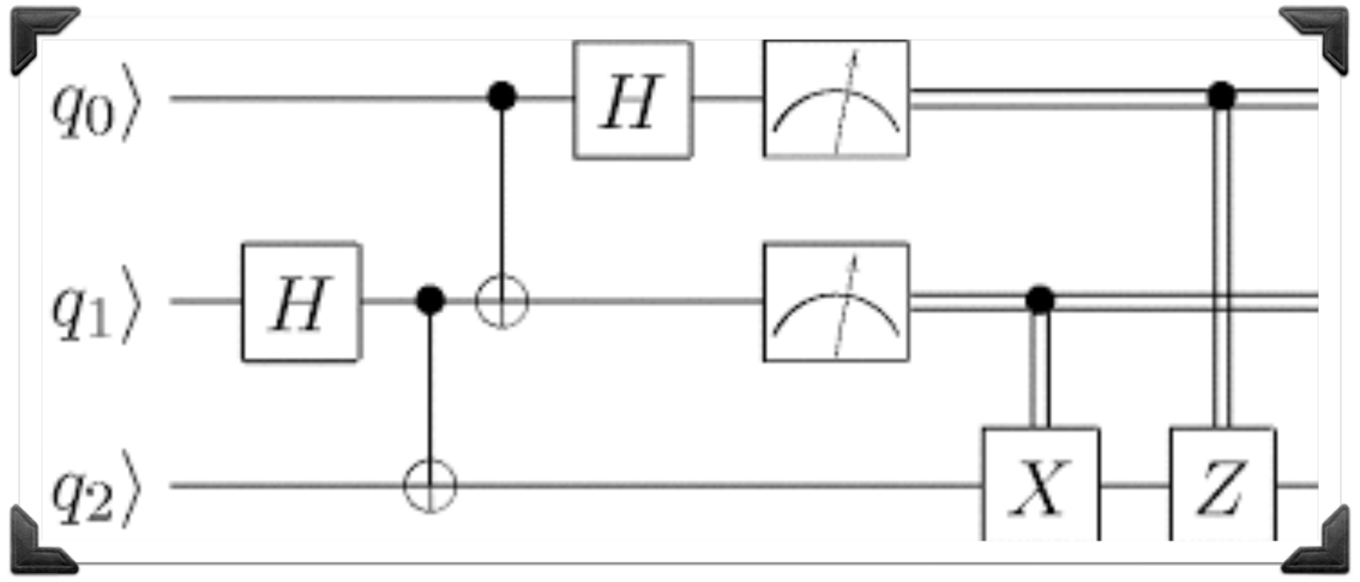


- Basic principles for quantum objects:

  linear superposition & *entanglement*

- How we change the state of a qubit:

  quantum gates and some examples of *algorithms*



- Open systems: decoherence and channels

- A *pure state* is a ray in a Hilbert space

$$[\,|\psi\rangle]_{\sim}$$

$|\psi\rangle \in \mathscr{H}$

probabilistic interpretation:

$\langle\psi|\psi\rangle = 1 \quad |\psi\rangle \sim e^{i\alpha}|\psi\rangle$

A *mixed state* is an ensemble $\{|\psi_j\rangle, p_j\}_j$ where $\{|\psi_j\rangle\}$ represent a set of possible states that can occur with probabilities $p_j \quad (0 \leq p_j \leq 1\,;\, \sum_j p_j = 1)$

A state can be represented in terms of a *density matrix*

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$$

- bounded, $\|\rho\| \leq 1$
- self-adjoint, $\rho^\dagger = \rho$
- definite positive, $\rho > 0$
- unit trace, $Tr[\rho] = 1$
- $\rho^2 = \rho \ iff \ \rho \ pure$

* An *observable* A is a self-adjoint operator on $\mathscr{H}$

$$A = \sum_n \lambda_n P_n \qquad A\,|\psi_n\rangle = \lambda_n |\psi_n\rangle \; with \; \{\,|\psi_n\rangle\}_n \; o.n.set, \;\; P_n = \rho_n = |\psi_n\rangle\langle\psi_n|$$

Given a state ρ, the expectation value (average) of A on ρ is $\langle A \rangle = Tr[\rho\, A]$

For a pure state $\rho = |\psi\rangle\langle\psi|$ with $|\psi\rangle = \sum_n c_n |\psi_n\rangle$: $\langle A \rangle = \sum_n |c_n|^2 \lambda_n$

* The *measurement* of $A = \sum_n \lambda_n P_n$ on a state $|\psi\rangle = \sum_n c_n |\psi_n\rangle$ is

- probabilistic $\quad outcomes: \; \lambda_n \quad probabilities: \; p_n = |c_n|^2 = \langle\psi|P_n|\psi\rangle$
- destructive $\quad$ the state has collapsed $\quad |\psi_n\rangle = P_n|\psi_n\rangle / \langle\psi|P_n|\psi\rangle^{1/2}$

- A *(closed) system* evolves according to Schroedinger equation

$$i\hbar\frac{\partial}{\partial t}|\psi\rangle = H|\psi\rangle$$

It generates a *unitary evolution*:

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle$$

$$\rho(t)\rangle = U(t)\rho(0)U(t)^\dagger$$

$$U(t)^\dagger = U(t)^{-1} = U(-t) \qquad H\ t - independent \Rightarrow U(t) = e^{-itH/\hbar}$$

- The Hilbert space of a composite system is $\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2$

- Simplest quantum system:

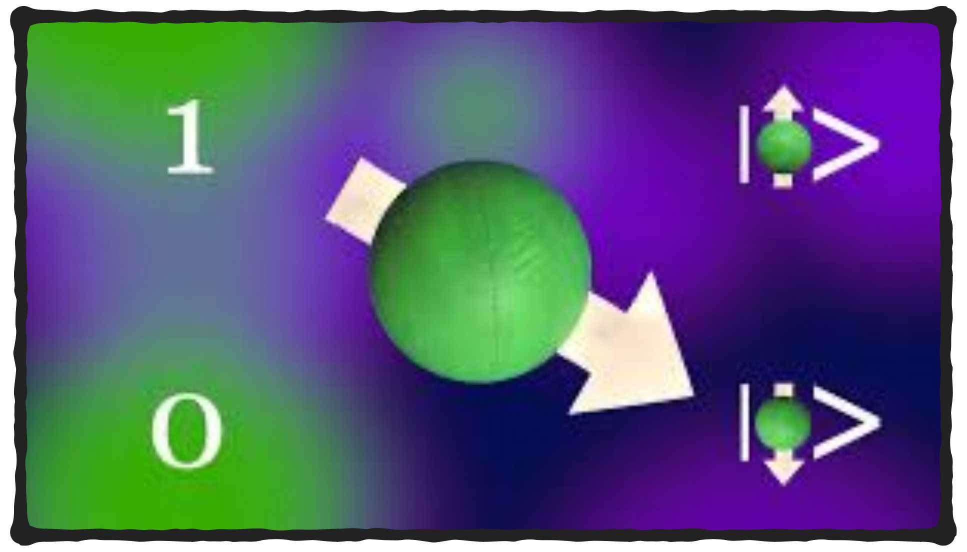
  two-level system

C-BIT	Q-BIT
0	|0>
1	|1>

- Superposition principle: generic state of a qubit

$$|Q\rangle = a|0\rangle + b|1\rangle = a\begin{pmatrix} 1 \\ 0 \end{pmatrix} + b\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

$$a, b \in \mathbb{C}$$
$$|a|^2 + |b|^2 = 1$$



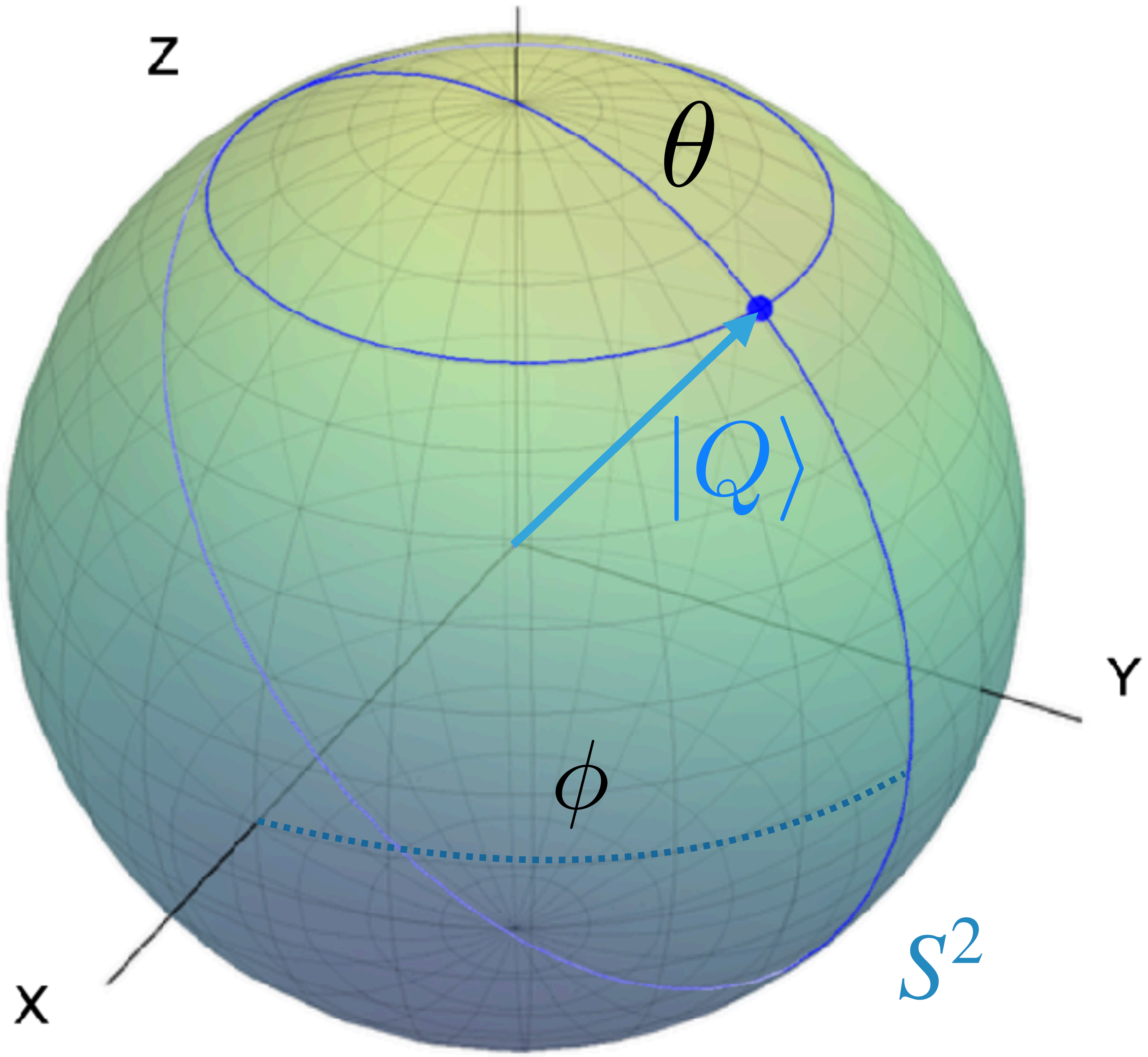
Examples: - two-levels in an atom
- particle with spin s=½
- states of polarisation of photon

- In general:

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

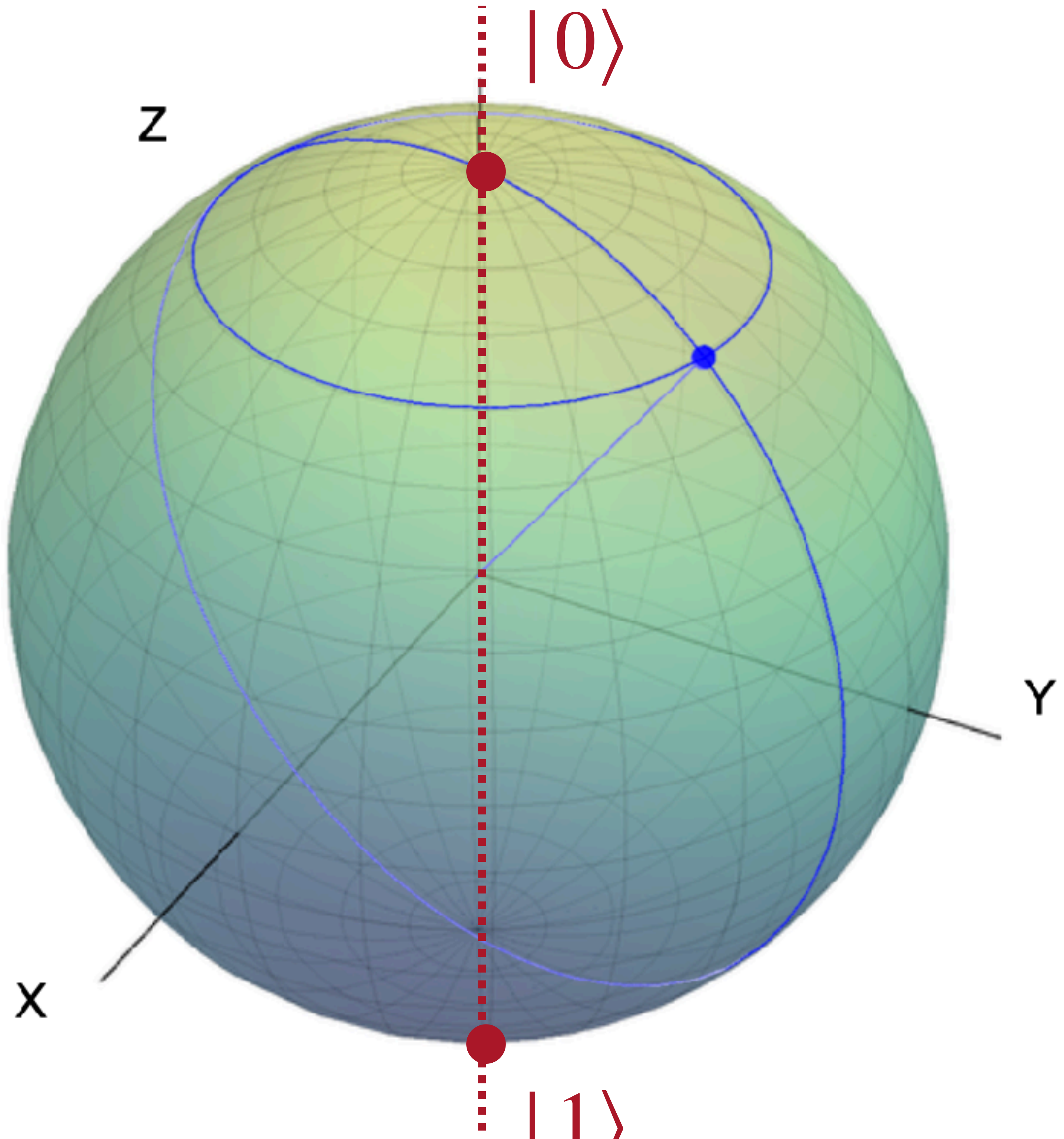
$$= \begin{pmatrix} \cos\theta/2 \\ e^{i\phi}\sin\theta/2 \end{pmatrix}$$

$\theta \in [0,\pi]\,,\, \phi \in [0,2\pi]$



Bloch sphere

$|0\rangle$

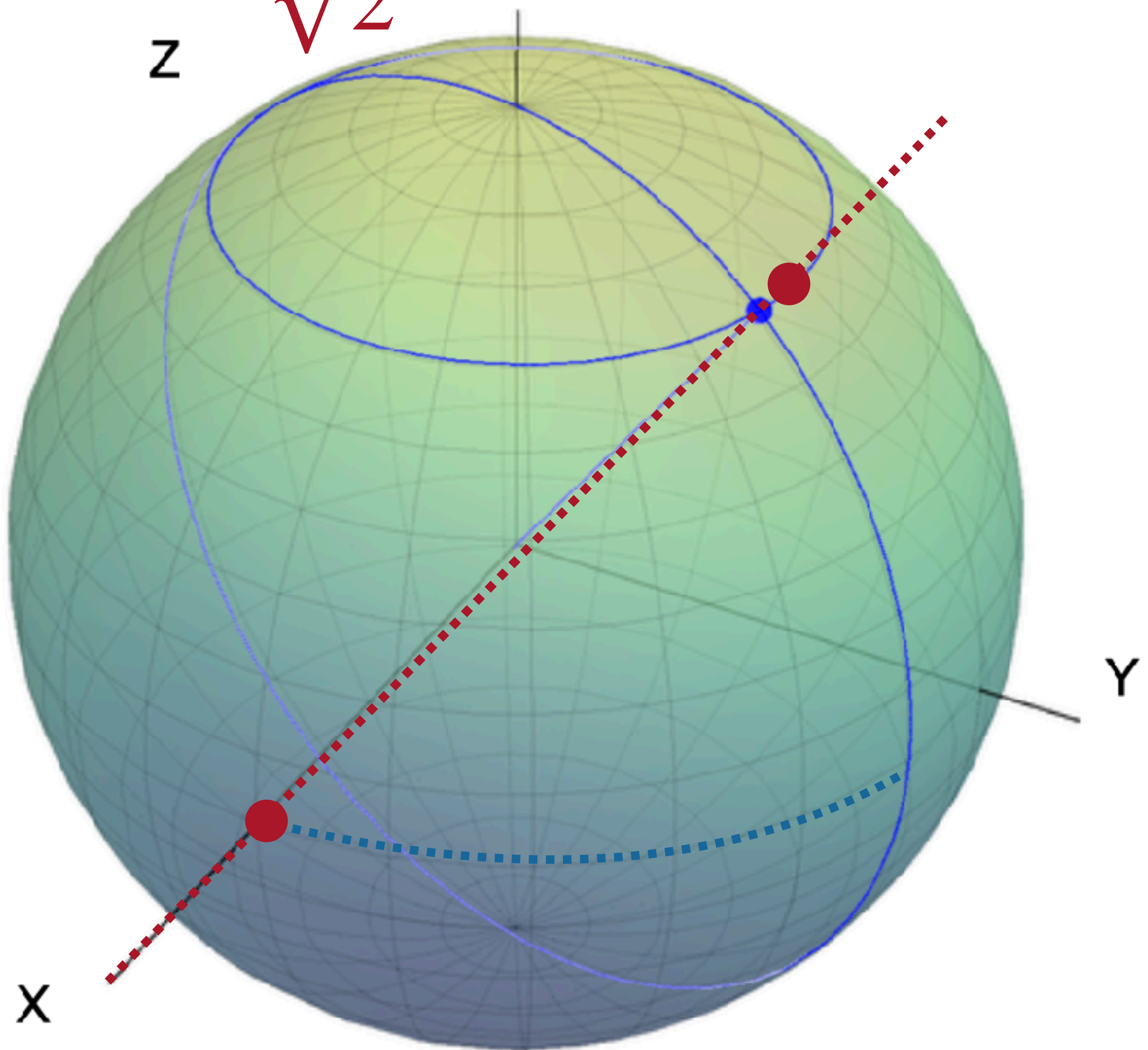


$|1\rangle$

Z-basis

(computational basis)

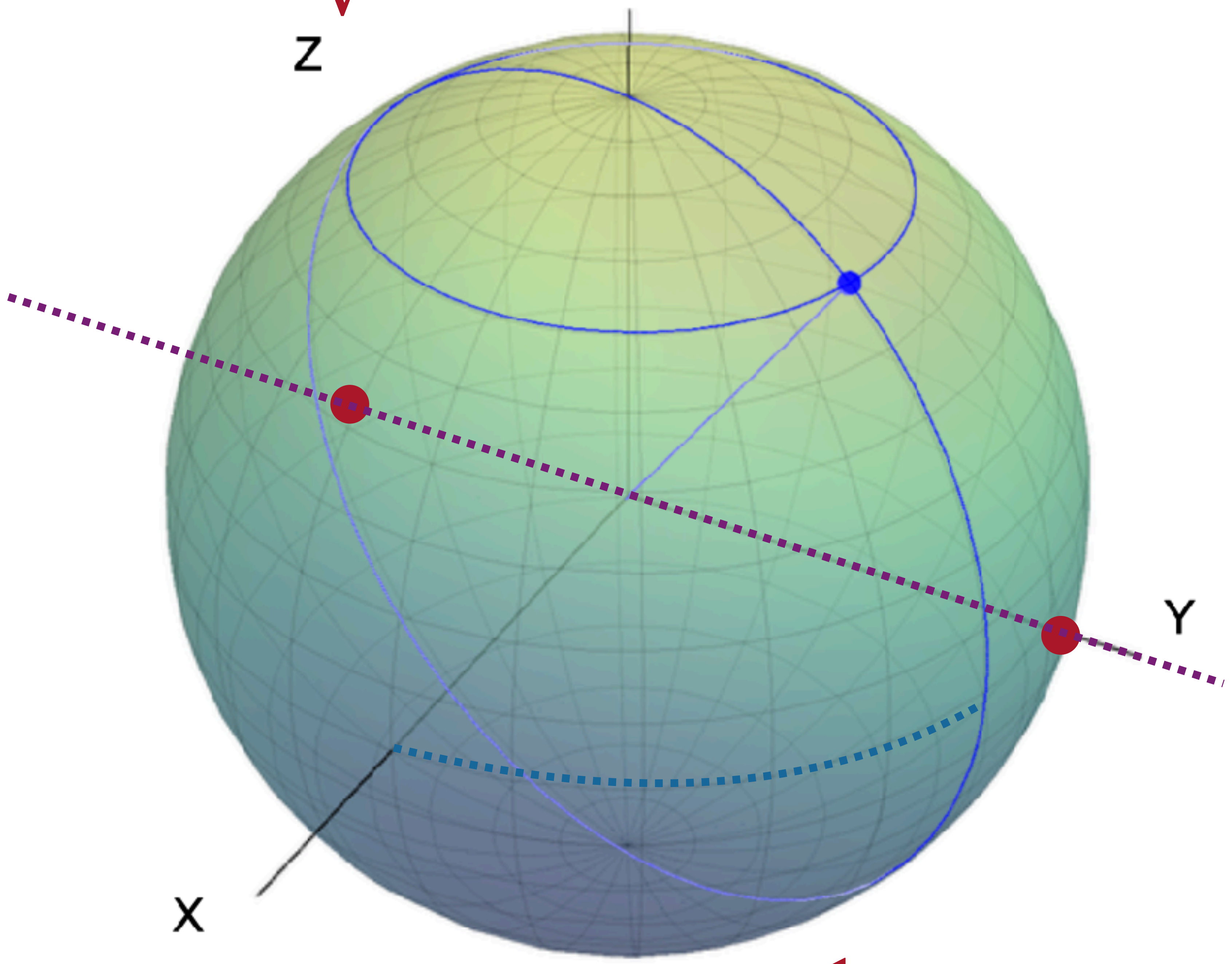
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



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

X-basis

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



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

Y-basis

- Pure density matrix of a qubit:

$$|Q\rangle = a|0\rangle + b|1\rangle$$

$$\rho_Q = \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix}$$

quantum mixture

- Mixed density matrix of a qubit:

e.g. $\{(|0\rangle, |a|^2), |1\rangle, |b|^2)\}$

$$\rho_Q = \begin{pmatrix} |a|^2 & 0 \\ 0 & |b|^2 \end{pmatrix}$$

classical mixture

- Pauli matrices

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_z|0,1\rangle = \pm|0,1\rangle \qquad \sigma_x|\pm\rangle = \pm|\pm\rangle \qquad \sigma_y|\pm\rangle_y = \pm|\pm\rangle_y$$

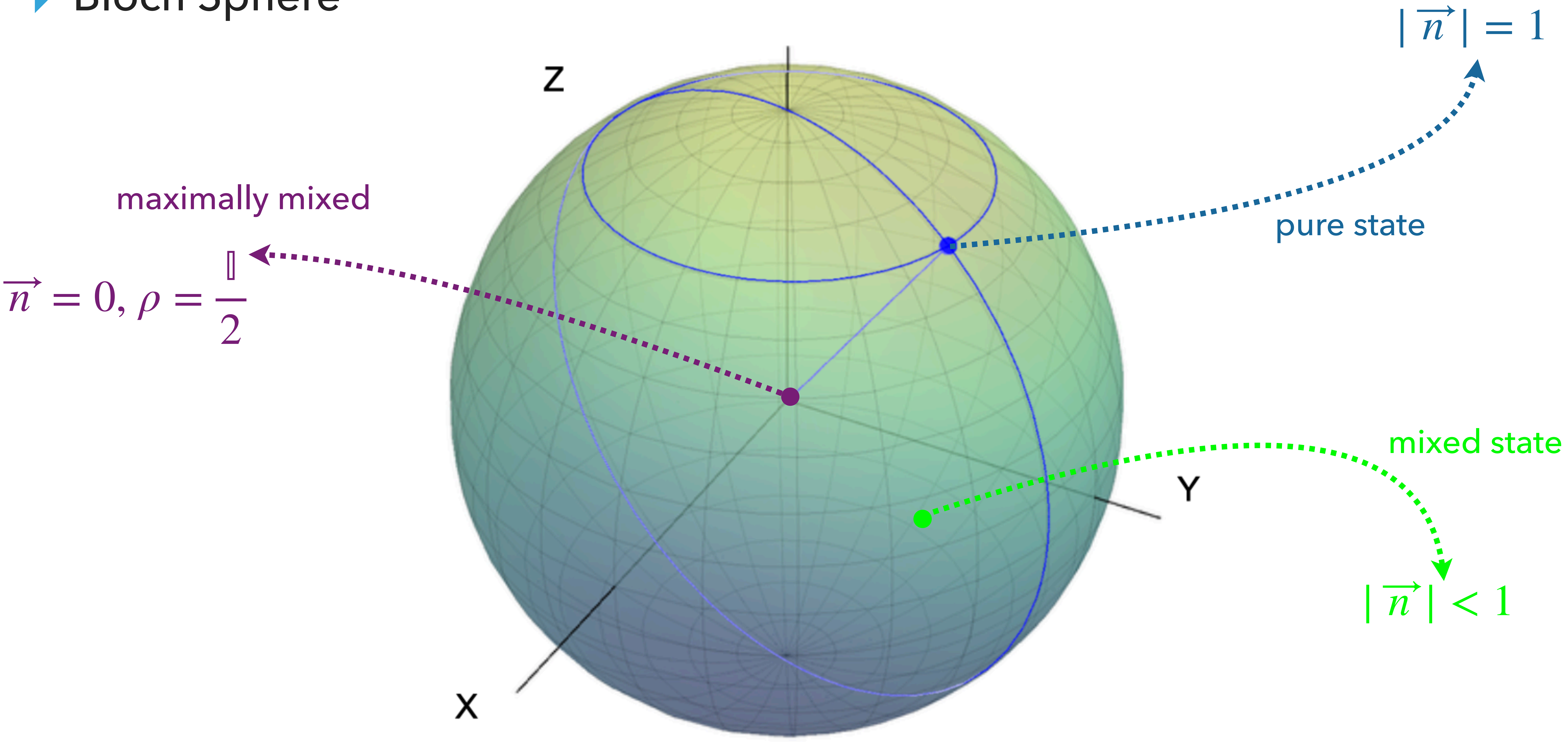
(Together with identity, they form a basis for all self-adjoint matrices (observables).

In particular any density matrix of a single qubit can be written as

$$\rho = \frac{\mathbb{1}}{2} + \frac{1}{2}\vec{n}\cdot\vec{\sigma} \qquad \vec{n} = (n_x, n_y, n_z)$$

$$with \quad |\vec{n}|^2 \leq 1$$

- Bloch Sphere



- The physical meaning of the coefficients a, b is linked to measurements

  We can devise a measurement to establish whether a qubit is in the state 0 or 1:

  the result of this measurement is a classical bit

- If the qubit is in superposition state $|Q\rangle = a|0\rangle + b|1\rangle$

  the outcome is:

  - probabilistic

  - destructive

outcome	probability	state after
0	$p_0 = \|a\|^2$	$\|0\rangle$
1	$p_1 = \|b\|^2$	$\|1\rangle$

- Linear and unitary transformation, i.e. a 2x2 rotation matrix

  that moves one point on the surface if the Bloch sphere to another point on it,

$$|Q\rangle = a|0\rangle + b|1\rangle \xrightarrow{\text{U}} |Q'\rangle = a'|0\rangle + b'|1\rangle$$

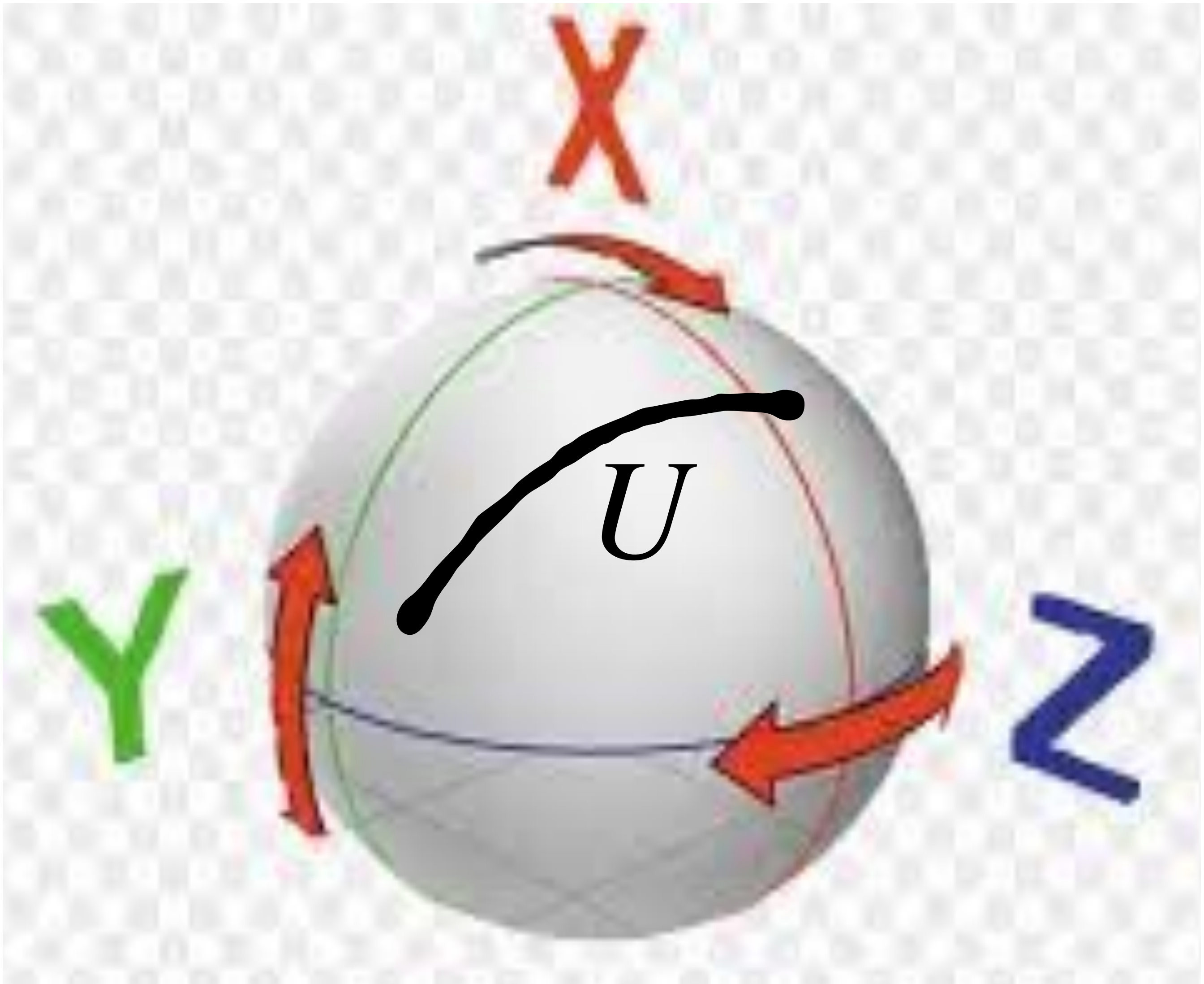
$$\begin{pmatrix} a \\ b \end{pmatrix} \rightarrow \begin{pmatrix} a' \\ b' \end{pmatrix} = U \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

with $U U^\dagger = U^\dagger \, U = \mathbb{I}$

Remark: since U is unitary, it is <u>reversible</u> with $U^{-1} = U^\dagger$.

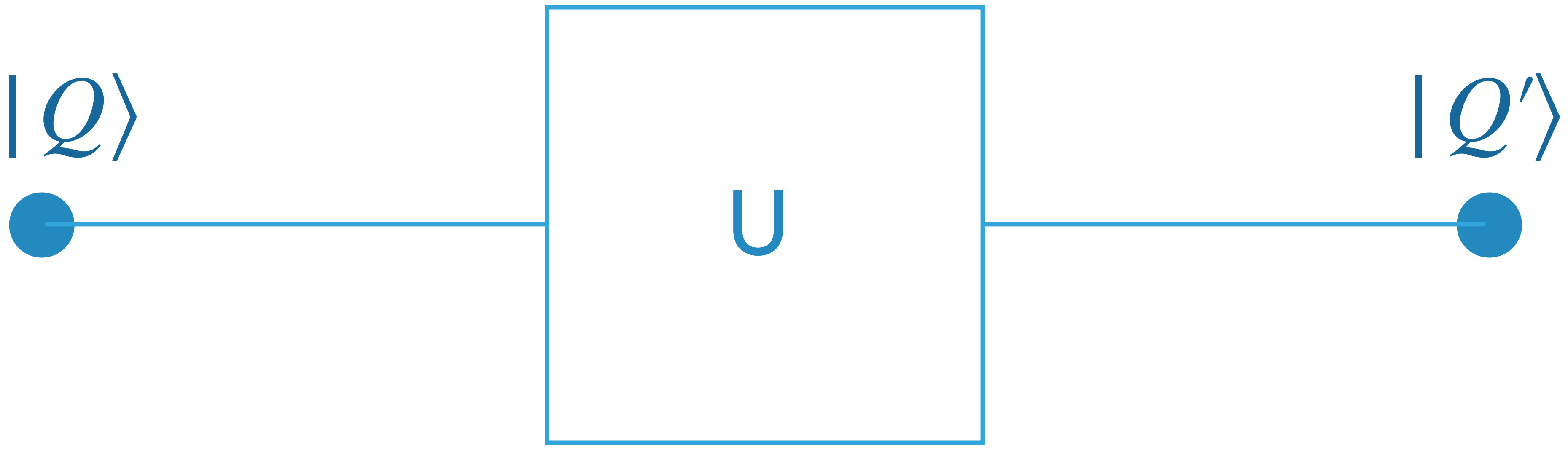
- (Unitary) Evolution operator

which is a rotation of time (angle) t about the axis $\hat{n}$



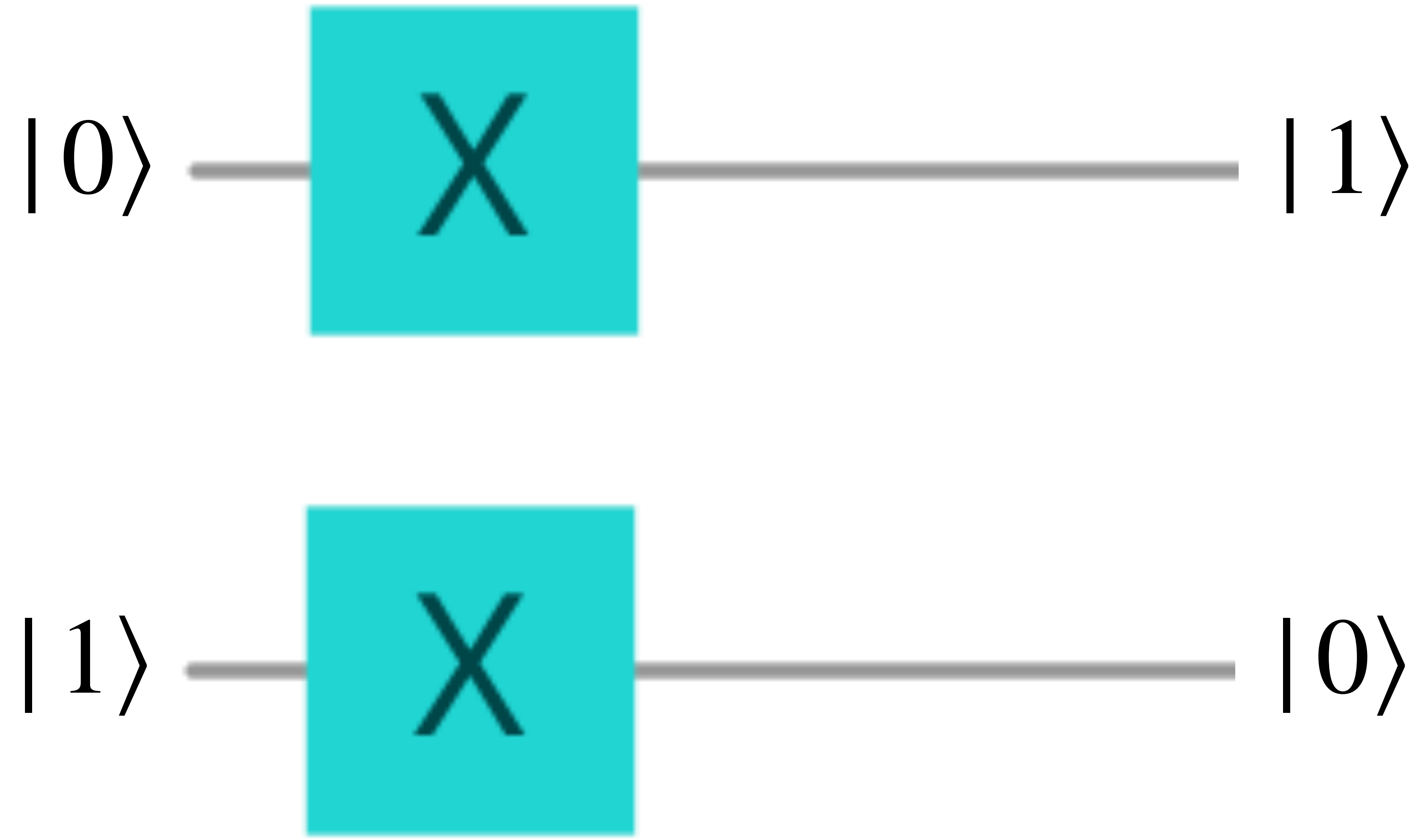
$$U = e^{it\,\hat{n}\cdot\vec{\sigma}} = \cos t\,\mathbb{I} + \sin t\,\hat{n}\cdot\vec{\sigma}$$

as it follows from the algebra $(\sigma_j)^2 = \mathbb{I}\,,\ [\sigma_i, \sigma_j] = 2i\epsilon_{ijk}\sigma_k$

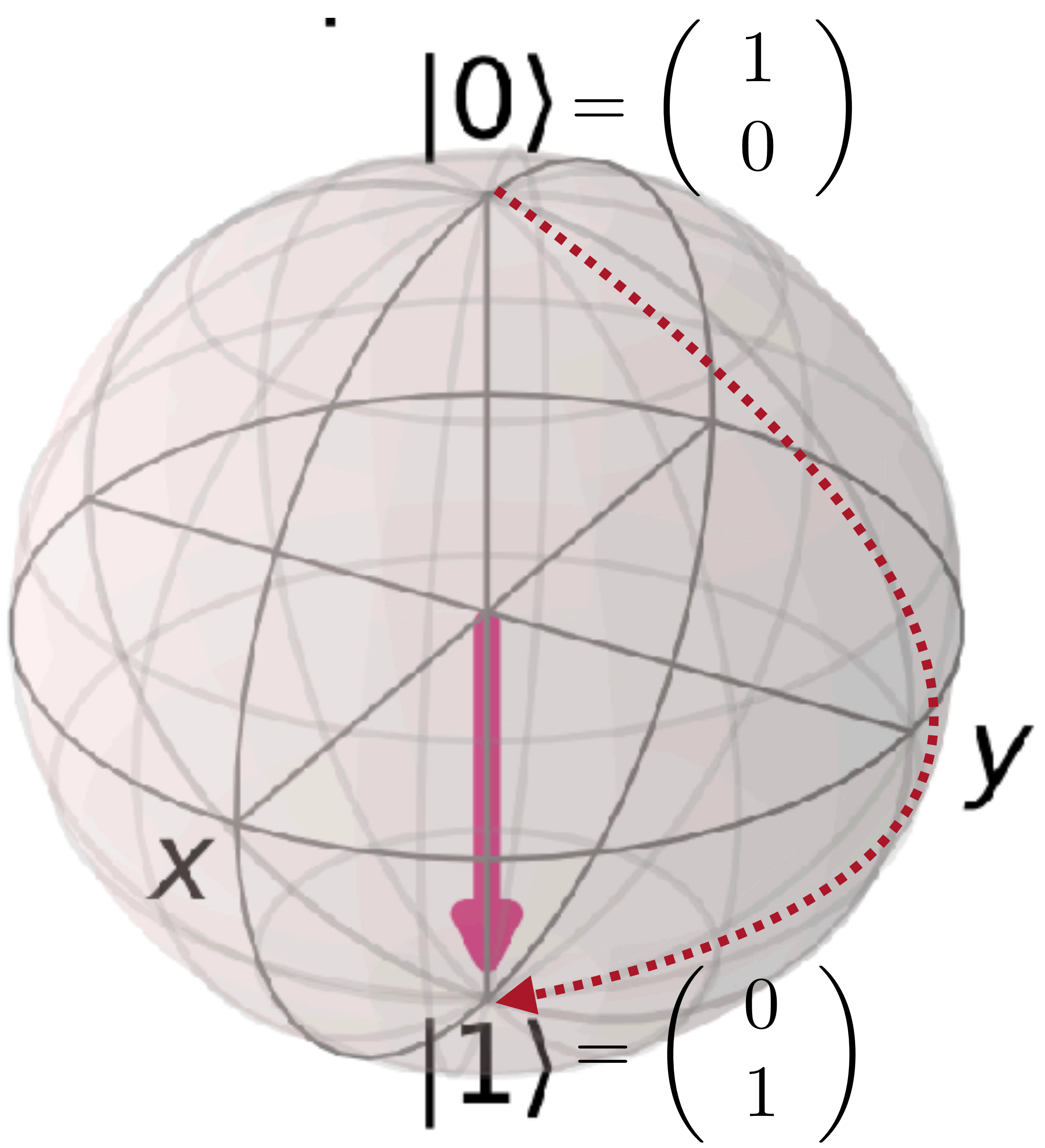


- X GATE

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



Geometrically,
it is a rotation
of π about the x-axis



- It gives the **NOT** gate: $|0\rangle \leftrightarrow |1\rangle$

IN	OUT
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$

- On a generic qubit:

$$|Q\rangle = a|0\rangle + b|1\rangle \mapsto |Q'\rangle = b|0\rangle + a|1\rangle$$

- Notice that $X^2 = I$.

- Y and Z GATES

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

IN	OUT
$\|0\rangle$	$i\|1\rangle$
$\|1\rangle$	$-i\|0\rangle$

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

IN	OUT
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$-\|1\rangle$

Geometrically, they represent a rotation of π about the y-axis and z-axis.

Also notice that: $Y^2 = Z^2 = I$.

- The Pauli matrices X, Y, Z (and the identity $\mathbb{I}$) generate all possible rotations. An arbitrary rotation can be achieved by the transformation:

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

- $\sqrt{NOT}$ GATE

$$\sqrt{NOT} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

$$since \quad (\sqrt{NOT})^2 = X$$

Classically such a gate does not exist.

- R(ϕ) GATE: it inserts a phase difference

$$R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

EXAMPLE of simple circuit

$|IN\rangle = |0\rangle$

$|IN\rangle = |1\rangle$

$|OUT\rangle = -e^{i\phi}|1\rangle$

$|OUT\rangle = |0\rangle$

In matrix notation:

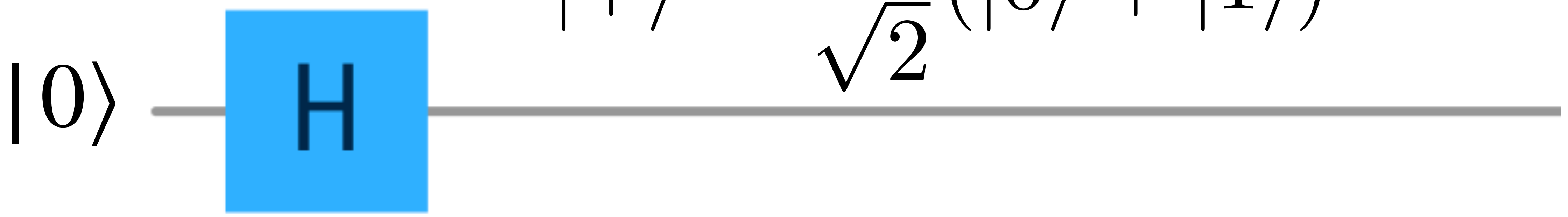
$$ZRX = \begin{pmatrix} 0 & 1 \\ -e^{i\phi} & 0 \end{pmatrix}$$

- Hadamard GATE: used to create superpositions

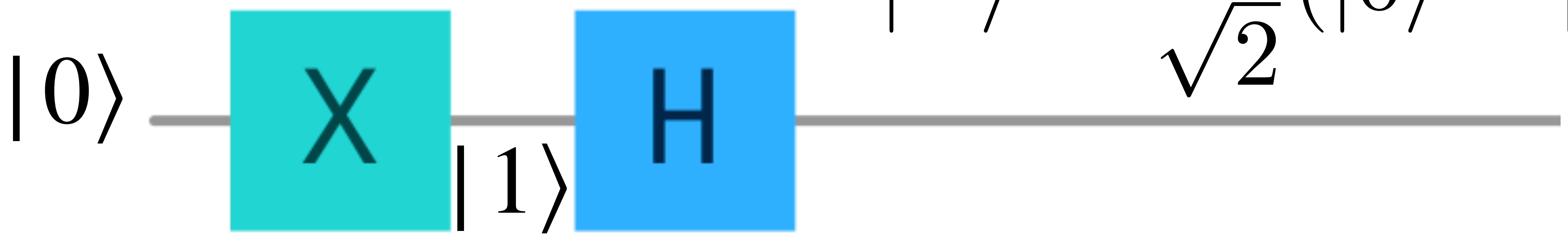
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Notice that $H^2 = I$.

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



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



EXERCISE

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

(up to a total phase, this is a rotation of $\phi/2$)

- EXERCISE: to achieve a given result, the circuit can be written in many ways

$$HZH = X$$

$$ZHZZ = ZH$$

$$HZ = XH$$

$$\dots$$

PROBLEM. How to optimise the explicit realisation of a given algorithm or protocol?