Principles of Quantum Mechanics and Quantum Computing

Antoine (Jack) Jacquier

(Imperial College London)

January 16, 2025

Overview

Q mechanics or Q computing?

Q mechanics is a *framework* for the development of Physics theories, as originally proposed mid-1920s by N. Bohr$^{\aleph}$, L. de Broglie$^{\aleph}$, M. Born$^{\aleph}$, W. Heisenberg$^{\aleph}$, W. Pauli$^{\aleph}$, E. Schrödinger$^{\aleph}$, P. Dirac$^{\aleph}$.
The mathematics of Q mechanics allow for more general *computation*:

- more general definition of the *memory state* compared to classical computing;
- wider range of *transformations / evolution* of memory states.

Q mechanics or Q computing?

Q mechanics is a *framework* for the development of Physics theories, as originally proposed mid-1920s by N. Bohr$^{\aleph}$, L. de Broglie$^{\aleph}$, M. Born$^{\aleph}$, W. Heisenberg$^{\aleph}$, W. Pauli$^{\aleph}$, E. Schrödinger$^{\aleph}$, P. Dirac$^{\aleph}$.
The mathematics of Q mechanics allow for more general *computation*:

- more general definition of the *memory state* compared to classical computing;
- wider range of *transformations / evolution* of memory states.

Why haven't we used this computation framework until now?
To perform Q computation efficiently we need actual Q mechanical systems, only proposed in the 1980s by P. Benioff, R. Feynman$^{\aleph}$, Y. Manin.
Q algorithms can be run on classical computers, but require enormous amount of memory, so that exponential gains in computing power are offset by exponential memory requirements.

Principles of Quantum Mechanics

Postulate 1 – Statics

Associated to any physical system is a complex inner product space (Hilbert space) known as the state space of the system. The system is completely described at any given point in time by its state vector, which is a unit vector in its state space.
State space: complex Hilbert space $\mathfrak{H} = \mathbb{C}^N$.
For $\mathrm{u}, \mathrm{v} \in \mathfrak{H}$, (*: complex conjugacy), with Dirac's notations

$$\text{(ket)} \quad |\mathrm{u}\rangle := \begin{pmatrix} u_0 \\ \vdots \\ u_{N-1} \end{pmatrix} \in \mathfrak{H},$$

$$\text{(bra)} \quad \langle \mathrm{u}| := \left(u_0^*, \ldots, u_{N-1}^*\right) \in \mathfrak{H}^*,$$

$$\text{(braket)} \quad \langle \mathrm{u}|\mathrm{v}\rangle := \sum_{i=0}^{N-1} u_i^* v_i \in \mathbb{C}.$$

Inner product

Standard computational basis vectors in $\mathbb{C}^N$:

$$|0\rangle = \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}, \quad |1\rangle = \begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix}, \quad \ldots \quad |N-1\rangle = \begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix}.$$

For two quantum states

$$|\mathrm{u}\rangle = \sum_{i=0}^{N-1} u_i |i\rangle \qquad \text{and} \qquad |\mathrm{v}\rangle = \sum_{i=0}^{N-1} v_i |i\rangle,$$

the inner product is

$$\langle \mathrm{u}|\mathrm{v}\rangle = \sum_i u_i^* v_i. \tag{1}$$

Quantum binary digit – Qubit

The Q-mechanics version of a bit, a *qubit*, is a Q mechanical two-state system. Its state can be represented mathematically by a unit vector in $\mathbb{C}^2$ and can thus in a superposition of basis states.
Any vector $|\mathrm{v}\rangle \in \mathbb{C}^2$ can be represented as a linear combination

$$|\mathrm{v}\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha \begin{pmatrix}1\\ 0\end{pmatrix} + \beta \begin{pmatrix}0\\ 1\end{pmatrix} = \alpha |0\rangle + \beta |1\rangle .$$

Since the state vector is a unit vector, the coefficients (*probability amplitudes*) $\alpha, \beta \in \mathbb{C}$ must satisfy

$$|\alpha|^2 + |\beta|^2 = \alpha^*\alpha + \beta^*\beta = 1.$$

A qubit can exist in a superposition of basis states but, once *measured*, its state *collapses* to $|0\rangle$ or $|1\rangle$, with respective probability $|\alpha|^2$ and $|\beta|^2$.

Quantum logic gates

A quantum logic gate allows to transform a qubit, i.e. to rotate it on the unit sphere. It generalises classical operations. It can be represented as a unitary matrix in $\mathbb{C}^2$ ($\mathtt{G}^\dagger\mathtt{G} = \mathtt{G}\mathtt{G}^\dagger = \mathtt{I}$).

Example: There is no Boolean function φ such that applied twice to a classical bit would result in a NOT gate: $\varphi(\varphi(0)) = 1$ and $\varphi(\varphi(1)) = 0$. In Q computing, let

$$\mathtt{G} := \frac{1}{2}\begin{pmatrix} 1+\mathrm{i} & 1-\mathrm{i} \\ 1-\mathrm{i} & 1+\mathrm{i} \end{pmatrix},$$

Then

$$\mathtt{G}^2 = \frac{1}{4}\begin{pmatrix} (1+\mathrm{i})^2 + (1-\mathrm{i})^2 & 2(1+\mathrm{i})(1-\mathrm{i}) \\ 2(1+\mathrm{i})(1-\mathrm{i}) & (1+\mathrm{i})^2 + (1-\mathrm{i})^2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

so that

$$\mathtt{G}^2 |0\rangle = \mathtt{G}^2 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \quad \text{and} \quad \mathtt{G}^2 |1\rangle = \mathtt{G}^2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle .$$

Postulate 2 – Dynamics

The evolution of the closed Q *system is described by the Schrödinger equation*

$$\mathrm{i}\hbar\partial_t |\psi(t)\rangle = \mathcal{H} |\psi(t)\rangle ,$$

where $\hbar$ is Planck's constant and $\mathcal{H}$ is a time-independent Hermitian operator (Hamiltonian of the system).

Note that, for any $0 \le t_1 \le t_2$, Schrödinger's equation gives us

$$|\psi(t_2)\rangle = \mathcal{U}(t_1, t_2) |\psi(t_1)\rangle , \quad \mathcal{U}(t_1, t_2) = \exp\left\{\frac{-\mathrm{i}\mathcal{H}(t_2 - t_1)}{\hbar}\right\}.$$

Lemma: if $\mathcal{H}$ is Hermitian ($\mathcal{H}^\dagger := (\mathcal{H}^*)^\top = \mathcal{H}$) and $\alpha \in \mathbb{R}$, then $\exp\{i\alpha\mathcal{H}\}$ is unitary.

Unitary operators – Q logic gates

Unitary operators preserve the inner product and hence norms: given $|\mathrm{u}\rangle$ and $|\mathrm{v}\rangle$, and a unitary operator $\mathcal{U}$, then

$$\langle \mathcal{U}\mathrm{u}| \cdot |\mathcal{U}\mathrm{v}\rangle = (|\mathcal{U}\mathrm{u}\rangle)^\dagger \cdot |\mathcal{U}\mathrm{v}\rangle = \langle \mathrm{u}\mathcal{U}^\dagger| \cdot |\mathcal{U}\mathrm{v}\rangle = \langle \mathrm{u}| \mathcal{U}^\dagger \mathcal{U} |\mathrm{v}\rangle = \langle \mathrm{u}|\mathrm{v}\rangle .$$

In Q mechanics, all physical transformations (rotations, translations, time evolution) correspond to (unitary) maps from Q states to Q states.

Unitary operators can then be viewed as *Q logic gates* implementing Q computations.

Since unitary operators are *invertible* ($\mathcal{U}^{-1} = \mathcal{U}^\dagger$), Q computing is *reversible*.

Postulate 3 – Measurement

Quantum measurements are operators $\{\mathcal{M}_m\}$ acting on $\mathcal{H}$, where m refers to the possible measurement outcomes and such that $\sum_m \mathcal{M}_m^\dagger \mathcal{M}_m = \mathcal{I}$. If the state of the system is $|\psi\rangle$ before measurement then the probability that result m occurs is $\mathbb{P}_m = \langle\psi|\mathcal{M}_m^\dagger \mathcal{M}_m|\psi\rangle$. After measurement, the system collapses to

$$\frac{\mathcal{M}_m |\psi\rangle}{\sqrt{\langle\psi|\mathcal{M}_m^\dagger \mathcal{M}_m|\psi\rangle}}.$$

Example: $\mathcal{M}_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\mathcal{M}_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, so that $\mathcal{M}_0^2 = \mathcal{M}_0 = \mathcal{M}_0^\dagger$, $\mathcal{M}_1^2 = \mathcal{M}_1 = \mathcal{M}_1^\dagger$ and $\mathcal{M}_0^\dagger \mathcal{M}_0 + \mathcal{M}_1^\dagger \mathcal{M}_1 = \mathcal{I}$.
With $\psi = \alpha|0\rangle + \beta|1\rangle$, then

$$\mathbb{P}_0 = \langle\psi|\mathcal{M}_0^\dagger \mathcal{M}_0|\psi\rangle = \Big(\alpha^* \langle 0| + \beta^* \langle 1|\Big) |0\rangle\langle 0| \Big(\alpha|0\rangle + \beta|1\rangle\Big) = |\alpha|^2$$

$$\mathbb{P}_1 = \langle\psi|\mathcal{M}_1^\dagger \mathcal{M}_1|\psi\rangle = \Big(\alpha^* \langle 0| + \beta^* \langle 1|\Big) |0\rangle\langle 0| \Big(\alpha|0\rangle + \beta|1\rangle\Big) = |\beta|^2.$$

We need to perform measurement on the same `Q` state many times to generate good enough statistics (akin to Monte Carlo).

Spectral Theorem and Projective measurements

Spectral Theorem: *If $\mathcal{A}$ is Hermitian ($\mathcal{A} = \mathcal{A}^\dagger$), there exists an orthonormal basis consisting of eigenvectors of $\mathcal{A}$. Each eigenvalue is real.*

Projective measurement: *A* Hermitian operator $\mathcal{M}$ admits the spectral decomposition $\mathcal{M} = \sum m\mathcal{P}_m$, where $\mathcal{P}_m$ is the projection onto the eigenspace of $\mathcal{M}$ with eigenvalue m.

In this setup, we can compute ($\mathbb{P}_m$ is the probability of observing m)

$$\begin{aligned}\mathbb{E}[\mathcal{M}] = \sum_m m\mathbb{P}_m &= \sum_m m \langle\psi|\mathcal{P}_m^\dagger\mathcal{P}_m|\psi\rangle \\ &= \sum_m m \langle\psi|\mathcal{P}_m|\psi\rangle \\ &= \langle\psi| \sum_m m\mathcal{P}_m| \, |\psi\rangle \\ &= \langle\psi|\mathcal{M}|\psi\rangle .\end{aligned}$$

Postulate 4 – Composite Systems

The state space of a composite physical system is the tensor product of the state spaces of the individual component physical systems.
If one component physical system is in state $|\psi_1\rangle$ and a second component physical system is in state $|\psi_2\rangle$, then the state of the combined system is

$$|\psi_1\rangle \otimes |\psi_2\rangle .$$

Not all combined systems can be split into a tensor product of states of individual components. When this is not the case, the components are called *entangled*.

More formally, a two-qubit state $|\psi\rangle$ is called entangled if it cannot be written as the tensor product $|\psi_1\rangle \otimes |\psi_2\rangle$ for some $|\psi_1\rangle, |\psi_2\rangle$.

The power of entanglement

Consider an n-qubit system, where (recall) an individual qubit can be found, after measurement, in $|0\rangle$ or $|1\rangle$, i.e. we need to specify 2 probability amplitudes to describe the state of the qubit.

If all the qubits are independent, the quantum state can be represented as

$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle \,,$$

and we need to specify 2n probability amplitudes.

If all individual qubits are entangled (hence, there is no tensor product representation), we need to specify 2^n probability amplitudes.

Quantum Computing

A note on computational basis

The standard orthonormal basis $(|0\rangle, |1\rangle)$

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

is called the *computational basis*, but any pair of *linearly independent* vectors $|\mathrm{u}\rangle$ and $|\mathrm{v}\rangle$ from $\mathbb{C}^2$ can serve as a basis:

$$\alpha|0\rangle + \beta|1\rangle = \alpha'|\mathrm{u}\rangle + \beta'|\mathrm{v}\rangle,$$

for example, the Hadamard basis, $(|+\rangle, |-\rangle)$, with

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \quad \text{and} \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}. \qquad (2)$$

From 1-qubit to 2-qubit system

A 2-qubit system can be represented by a unit vector in $\mathbb{C}^{2^2}$, with orthonormal basis $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$, given by the *tensor/Kronecker products*

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Any 2-qubit quantum state can then be described by four probability amplitudes:

$$|\psi\rangle = \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle,$$

with $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$.

n-qubit system

More generally,

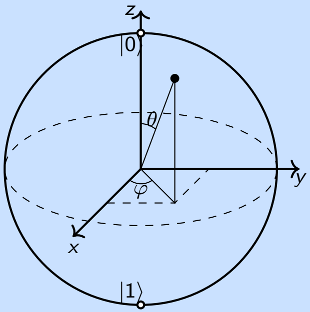
$$|0\rangle^{\otimes n} = \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{\text{n times}}$$

An n-qubit system can exist in any superposition of the 2^n basis states and requires 2^n probability amplitudes to be fully specified.

The Bloch sphere

Bloch$^{\aleph}$ *sphere*: every quantum state is uniquely (up to global phase) specified by $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi)$, so that, with $\alpha = \cos\left(\frac{\theta}{2}\right)$, $\beta = \mathrm{e}^{\mathrm{i}\varphi} \sin\left(\frac{\theta}{2}\right)$,

Canonical representation $$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \mathrm{e}^{\mathrm{i}\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \mathrm{e}^{\mathrm{i}\varphi}\sin\left(\frac{\theta}{2}\right) \end{pmatrix}.$$



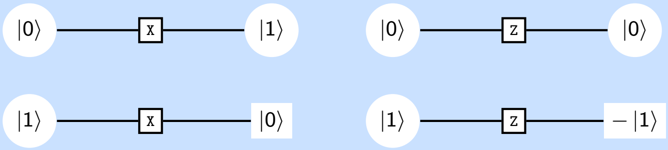
A unitary matrix can then be seen as a rotation operator, and the gate parameters are called *rotation angles*.

1-qubit logic gates

$$\mathtt{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathtt{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathtt{Y} = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad \mathtt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The $\mathtt{X}$ gate flips the bit (NOT gate); the $\mathtt{Z}$ gate flips the phase (PHASE gate):

$$\begin{aligned} \mathtt{X}\,|0\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} &&= \begin{pmatrix} 0 \\ 1 \end{pmatrix}, & \mathtt{X}\,|1\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} &&= \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \\ \mathtt{Z}\,|0\rangle &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} &&= \begin{pmatrix} 1 \\ 0 \end{pmatrix}, & \mathtt{Z}\,|1\rangle &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} &&= -\begin{pmatrix} 0 \\ 1 \end{pmatrix}. \end{aligned}$$



Graphical representation of $\mathtt{X}$ and $\mathtt{Z}$ gates.

Q operations

- $\mathtt{Q}$ Gate: reversible quantum circuit (unitary matrix: $\mathtt{U}\mathtt{U}^* = \mathtt{U}^*\mathtt{U} = \mathtt{I}$).
- Standard gates:

$$\mathtt{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathtt{Y} = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}, \quad \mathtt{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \mathtt{R}_y(\theta) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

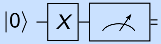
Q operations

- Q Gate: reversible quantum circuit (unitary matrix: $\mathtt{UU}^* = \mathtt{U}^*\mathtt{U} = \mathtt{I}$).
- Standard gates:

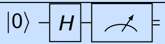
$$\mathtt{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathtt{Y} = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}, \quad \mathtt{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \mathtt{R}_y(\theta) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

- Examples:

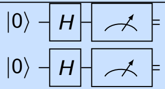
$$\mathtt{X}|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle .$$



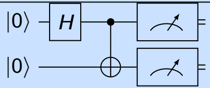
$$\mathtt{H}|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \quad \text{and} \quad \mathtt{H}|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$$



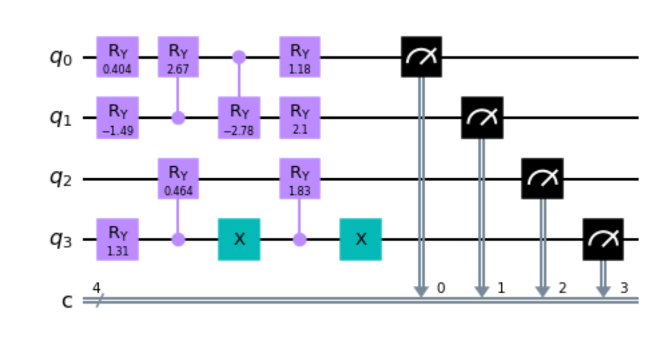
$$\mathtt{H}^{\otimes 2}|00\rangle = (\mathtt{H}|0\rangle) \otimes (\mathtt{H}|0\rangle) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$



$$_c\mathtt{X}\Big((\mathtt{H} \otimes \mathtt{I})|00\rangle\Big) = {}_c\mathtt{X}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle\right) = \frac{|0\rangle|0\rangle + |1\rangle\mathtt{X}|0\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \text{ (EPR)}$$



Example of a Q circuit

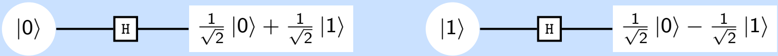


Superposition with Hadamard gate

The Hadamard gate $\mathtt{H}$ creates an equal superposition of $|0\rangle$ and $|1\rangle$ when applied to either state $|0\rangle$ or state $|1\rangle$:

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

$$\begin{aligned}
\mathtt{H}\,|0\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} &= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 0\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}0\\ 1\end{pmatrix} &= \frac{|0\rangle + |1\rangle}{\sqrt{2}},\\
\mathtt{H}\,|1\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} &= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 0\end{pmatrix} - \frac{1}{\sqrt{2}}\begin{pmatrix}0\\ 1\end{pmatrix} &= \frac{|0\rangle - |1\rangle}{\sqrt{2}}.
\end{aligned}$$



Circuit representation of the $\mathtt{H}$ gate.

Hadamard and phase shift gates

An immediate computation shows that $\mathtt{H}^{-1} = \mathtt{H}$, so that

$$|0\rangle \;—\; \boxed{\mathtt{H}} \;—\; \boxed{\mathtt{H}} \;—\; |0\rangle \qquad\qquad |1\rangle \;—\; \boxed{\mathtt{H}} \;—\; \boxed{\mathtt{H}} \;—\; |1\rangle$$

$\mathtt{H}$ gate applied twice.

Exciting example: Generating a uniform distribution

- 1 qubit, i.e. 2 values (discrete distribution over 2 points):

$$\mathtt{H}\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Exciting example: Generating a uniform distribution

- 1 qubit, i.e. 2 values (discrete distribution over 2 points):

$$\mathtt{H}\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

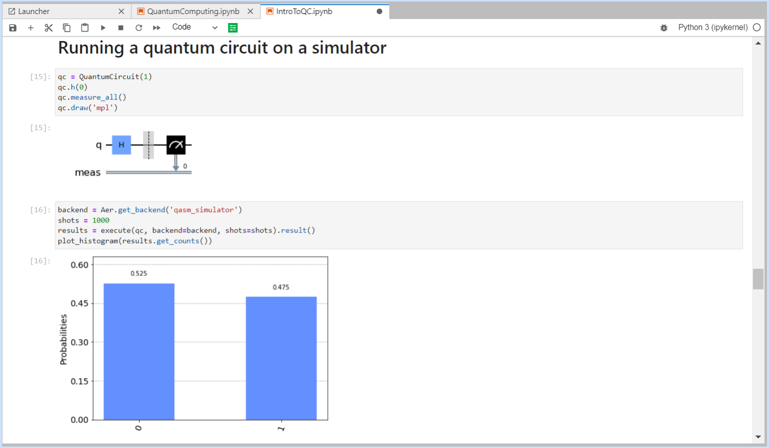
- n qubits, i.e. 2^n values (discrete distribution over 2^n points):

$$\begin{aligned}
\mathtt{H}^{\otimes n}\,|0\rangle^{\otimes n} &= \Big(\mathtt{H}\,|0\rangle\Big) \otimes \cdots \otimes \Big(\mathtt{H}\,|0\rangle\Big) \\
&= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \cdots \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{2^{n/2}}\Big(|0\rangle + |1\rangle\Big) \otimes \cdots \otimes \Big(|0\rangle + |1\rangle\Big) \\
&= \frac{1}{2^{n/2}}\Big(|0\cdots 0\rangle + |0\cdots 01\rangle + \cdots + |1\cdots 10\rangle + |1\cdots 1\rangle\Big) \\
&= \frac{1}{2^{n/2}}\sum_{i=0}^{2^n-1} |i\rangle\,.
\end{aligned}$$

Possible to code things up:

- Simulated quantum computer
- Actual (small-size) quantum computer

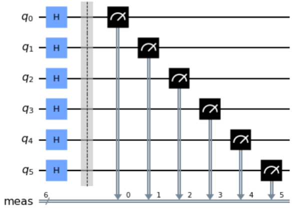
```
from qiskit import QuantumCircuit, Aer, execute
from qiskit.visualization import plot_histogram
```



6 qubits

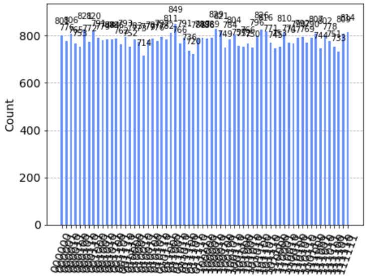
[10]:
```python
n = 6
qc = QuantumCircuit(n)
for i in range(n):
    qc.h(i)
qc.measure_all()
qc.draw('mpl')
```

[10]:



[11]:
```python
backend = Aer.get_backend('qasm_simulator')
shots = 50000
results = execute(qc, backend=backend, shots=shots).result()
plot_histogram(results.get_counts())
```

[11]:



Adjustable 1-qubit gates

Adjustable 1-qubit gates perform rotation of the qubit state around specific axis by an arbitrary angle θ and an arbitrary unitary gate $\mathtt{U}$

$$\mathtt{R}_{\mathtt{U}}(\theta) := \exp\left\{-\frac{\mathrm{i}\theta}{2}\mathtt{U}\right\}.$$

In particular,

$$\mathtt{R}_{\mathtt{X}}(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\mathrm{i}\sin\left(\frac{\theta}{2}\right) \\ -\mathrm{i}\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}, \qquad \mathtt{R}_{\mathtt{Y}}(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix},$$

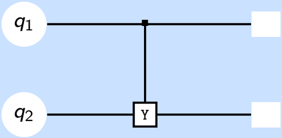
$$\mathtt{R}_{\mathtt{Z}}(\theta) = \begin{pmatrix} \exp\left(-\frac{\mathrm{i}\theta}{2}\right) & 0 \\ 0 & \exp\left(\frac{\mathrm{i}\theta}{2}\right) \end{pmatrix}.$$

so that

$$\begin{aligned}
\mathtt{R}_{\mathtt{X}}(\theta)\left|0\right\rangle &= \cos\left(\frac{\theta}{2}\right)\left|0\right\rangle - \mathrm{i}\sin\left(\frac{\theta}{2}\right)\left|1\right\rangle, & \mathtt{R}_{\mathtt{Y}}(\theta)\left|0\right\rangle &= \cos\left(\frac{\theta}{2}\right)\left|0\right\rangle + \sin\left(\frac{\theta}{2}\right)\left|1\right\rangle, \\
\mathtt{R}_{\mathtt{X}}(\theta)\left|1\right\rangle &= -\mathrm{i}\sin\left(\frac{\theta}{2}\right)\left|0\right\rangle + \cos\left(\frac{\theta}{2}\right)\left|1\right\rangle, & \mathtt{R}_{\mathtt{Y}}(\theta)\left|1\right\rangle &= -\sin\left(\frac{\theta}{2}\right)\left|0\right\rangle + \cos\left(\frac{\theta}{2}\right)\left|1\right\rangle, \\
\mathtt{R}_{\mathtt{Z}}(\theta)\left|0\right\rangle &= \exp\left(-\frac{\mathrm{i}\theta}{2}\right)\left|0\right\rangle, & \mathtt{R}_{\mathtt{Z}}(\theta)\left|1\right\rangle &= \exp\left(\frac{\mathrm{i}\theta}{2}\right)\left|1\right\rangle.
\end{aligned}$$

n-qubit gates

An n-qubit gate can be represented by $2^n \times 2^n$ unitary matrices. By acting on several qubits at the same time, it can be used to *entangle* them.
This is in particular the case with conditional operators, or *controlled* gates: the gate is applied to the *target qubit* only if the *control qubit* is in state $|1\rangle$.
For example, Controlled `Y` (`CY`) gate:



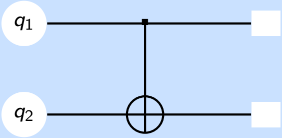
`CY` gate.

Controlled NOT (CNOT) gate

The CX gate is the controlled Pauli X (bit flip) gate, represented by

$$\mathtt{CNOT} \equiv \mathtt{CX} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

and has the circuit representation



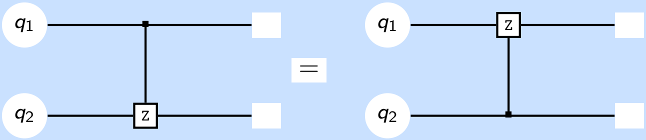
CX (CNOT) gate.

Controlled Z (CZ or CPHASE) gate

The CZ gate is the controlled Pauli Z (phase flip) gate, represented by

$$\mathtt{CPHASE} \equiv \mathtt{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{3}$$

In this particular case, the target and control qubits are interchangeable i.e.



CZ (CPHASE) gates.

Adjustable 2-qubit gates

An example of adjustable two-qubit gate is the XY gate, which is a rotation by some angle θ between the $|01\rangle$ and $|10\rangle$ states:

$$\mathtt{XY}(\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\left(\frac{\theta}{2}\right) & \mathrm{i}\sin\left(\frac{\theta}{2}\right) & 0 \\ 0 & \mathrm{i}\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4}$$

Lemma: For any unitary U, there exist $\alpha \in \mathbb{R}$ and $\theta_1, \theta_2, \theta_3 \in [0, \pi]$ such that

$$\mathtt{U} = \mathrm{e}^{\mathrm{i}\alpha}\mathtt{R}_{\mathtt{Z}}(\theta_1)\mathtt{R}_{\mathtt{Y}}(\theta_2)\mathtt{R}_{\mathtt{Z}}(\theta_3).$$

Entanglement

An n-qubit system can exist in any superposition of the 2^n basis states:

$$c_0 |00\dots00\rangle + c_1 |00\dots01\rangle + \dots + c_{2^n-1} |11\dots11\rangle, \quad \sum_{i=0}^{2^n-1} |c_i|^2 = 1.$$

If such a state can be represented as a tensor product of individual qubit states then the qubit states are *not entangled*.
For example:

$$\begin{aligned}&\frac{1}{4\sqrt{2}}\left(\sqrt{3}|000\rangle + |001\rangle + 3|010\rangle + \sqrt{3}|011\rangle + \sqrt{3}|100\rangle + |101\rangle + 3|110\rangle + \sqrt{3}|111\rangle\right)\\ &= \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \otimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right). \end{aligned} \tag{5}$$

An *entangled* state cannot be represented as a tensor product of individual qubit states.

Entanglement (continued)

For example, one cannot find $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ such that

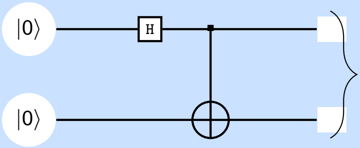
$$\frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) = (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle).$$

Entanglement allows us to encode much more information than with individual independent qubits. Most of the information in the state of a `Q` state is stored *non-locally* in the *correlations* between the qubit states.
This is one of the major features of `Q` computing vs classical computing.

Construction of entangled states

Qubit states can be entangled with the help of two-qubit gates.

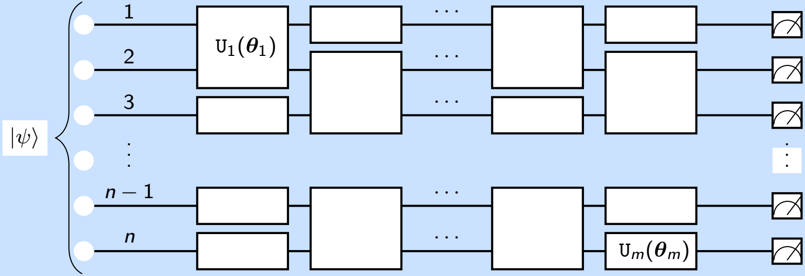
The entangled 2-qubit state above is one of the four maximally entangled *Bell* states, and can be constructed as



$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Bell circuit.

Parameterised Quantum Circuit



Schematic representation of the Parameterised Quantum Circuit.

A $\mathtt{Q}$ circuit consisting of a mix of fixed and adjustable gates transforms initial $\mathtt{Q}$ state, $|\psi\rangle$ into final $\mathtt{Q}$ state $|\psi'\rangle$ by applying a sequence of unitary operators:

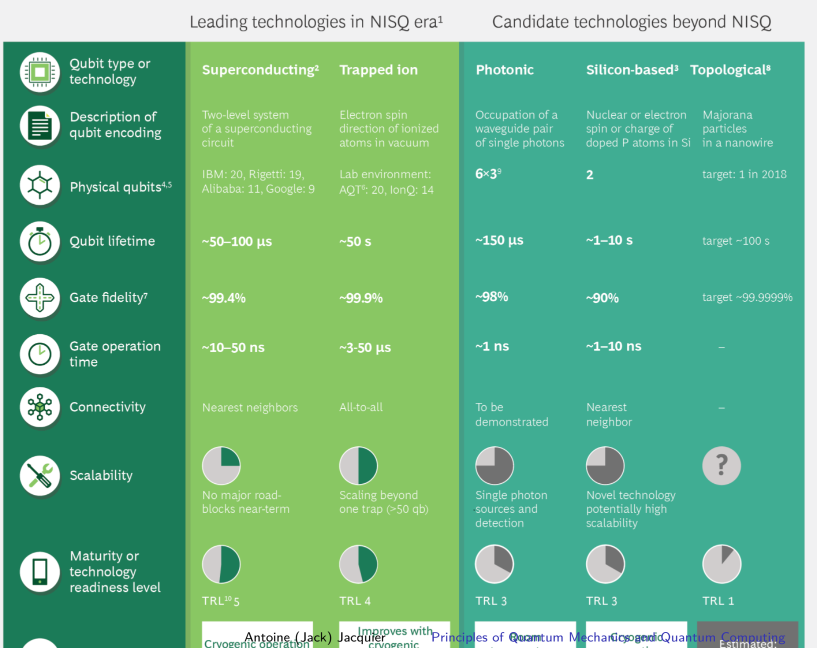
$$|\psi'\rangle = \mathtt{U}_m(\boldsymbol{\theta}_m)\dots\mathtt{U}_2(\boldsymbol{\theta}_2)\mathtt{U}_1(\boldsymbol{\theta}_1)\,|\psi\rangle\,. \tag{6}$$

Here, $\mathtt{U}_i$ and $\boldsymbol{\theta}_i$ denote, respectively, the individual gate i, $i=1,\dots,m$, and associated vector of gate parameters.

Is there any sense of reality here?

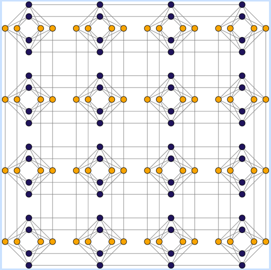
Two competing technologies:

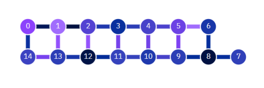
- Superconducting qubits: each qubit can interact with its nearest neighbour, limited decoherence time, needs super-cooling; `IBM`, `Google`, `AWS`, `Alibaba`, `Rigetti`, `Intel`, `D-Wave`.
- Ion trapped: ions trapped in electric fields, that can be *perturbed* by laser beams. `Quantinuum`, `IonQ` , `Quantum Factory` , `Alpine Quantum Technologies`, `eleQtron`, `Oxford Ionics`.

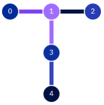


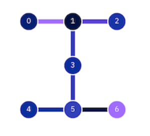
	Leading technologies in NISQ era[1]		Candidate technologies beyond NISQ		
Qubit type or technology	Superconducting[2]	Trapped ion	Photonic	Silicon-based[3]	Topological[8]
Description of qubit encoding	Two-level system of a superconducting circuit	Electron spin direction of ionized atoms in vacuum	Occupation of a waveguide pair of single photons	Nuclear or electron spin or charge of doped P atoms in Si	Majorana particles in a nanowire
Physical qubits[4,5]	IBM: 20, Rigetti: 19, Alibaba: 11, Google: 9	Lab environment: AQT[6]: 20, IonQ: 14	6×3[9]	2	target: 1 in 2018
Qubit lifetime	~50–100 µs	~50 s	~150 µs	~1–10 s	target ~100 s
Gate fidelity[7]	~99.4%	~99.9%	~98%	~90%	target ~99.9999%
Gate operation time	~10–50 ns	~3-50 µs	~1 ns	~1–10 ns	–
Connectivity	Nearest neighbors	All-to-all	To be demonstrated	Nearest neighbor	–
Scalability	No major road-blocks near-term	Scaling beyond one trap (>50 qb)	Single photon sources and detection	Novel technology potentially high scalability	?
Maturity or technology readiness level	TRL[10] 5	TRL 4	TRL 3	TRL 3	TRL 1
	Cryogenic operation	Improves with cryogenic		Cryogenic	Estimated:

Q Tech: interesting graph theoretic problems









Quantum timeline