Information quantique, calcul quantique : Une introduction pour le traitement du signal.

François CHAPEAU-BLONDEAU
LARIS, Université d'Angers, France.

"I believe that science is not simply a matter of exploring new horizons. One must also make the new knowledge readily available, and we have in this work a beautiful example of such a pedagogical effort."
Claude Cohen-Tannoudji, in foreword to the book "Introduction to Quantum Optics"
by G. Grynberg, A. Aspect, C. Fabre ; *Cambridge University Press* 2010.

A definition (at large)

To exploit quantum properties and phenomena
for information processing and computation.

Motivations for the quantic

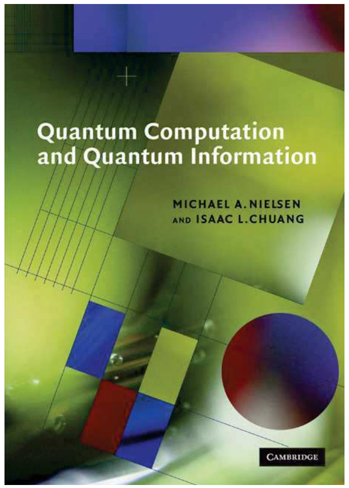
for information and computation :

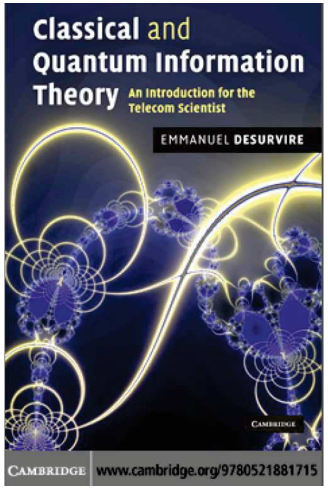
1) When using elementary systems (photons, electrons, atoms, ions, nanodevices, . . .).

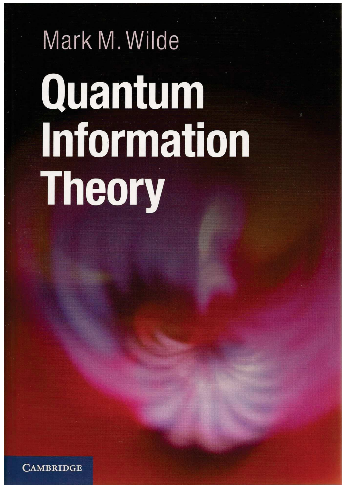
2) To benefit from purely quantum effects (parallelism, entanglement, . . .).

3) Recent field of research, rich of large potentialities (science & technology).

Some basic textbooks







M. Nielsen & I. Chuang
2000, 676 pages

E. Desurvire
2009, 691 pages

M. Wilde
2017, 757 pages

arXiv:1106.1445v8 [quant-ph] M. Wilde, "From classical to quantum Shannon theory", 774 pages.

Quantum system

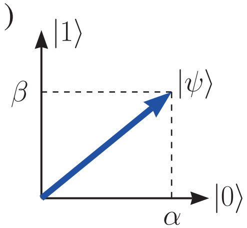
(1) State

Represented by a **state** vector $|\psi\rangle$

in a complex Hilbert space $\mathcal{H}$,
with unit norm $\langle\psi|\psi\rangle = ||\psi||^2 = 1$.

In dimension 2 : the qubit (photon, electron, atom, . . .)

State $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
in some orthonormal basis $\{|0\rangle\,, |1\rangle\}$ of $\mathcal{H}_2$,
with complex coordinates $\alpha, \beta \in \mathbb{C}$
such that $|\alpha|^2 + |\beta|^2 = \langle\psi|\psi\rangle = ||\psi||^2 = 1$.



$$|\psi\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}, \quad |\psi\rangle^\dagger = \langle\psi| = [\alpha^*, \beta^*] \quad \Longrightarrow \langle\psi|\psi\rangle = ||\psi||^2 = |\alpha|^2 + |\beta|^2 \text{ scalar.}$$

$$|\psi\rangle\langle\psi| = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}[\alpha^*, \beta^*] = \begin{bmatrix}\alpha\alpha^* & \alpha\beta^*\\ \alpha^*\beta & \beta\beta^*\end{bmatrix} = \Pi_\psi \text{ orthogonal projector on } |\psi\rangle.$$

Measurement of the qubit

(2) Measurement

When a qubit in state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
is measured in the orthonormal basis $\{|0\rangle\,, |1\rangle\}$,

$\Longrightarrow$ only 2 possible outcomes (Born rule) :

state $|0\rangle$ with probability $|\alpha|^2 = |\langle 0|\psi\rangle|^2 = \langle\psi|0\rangle\langle 0|\psi\rangle = \langle\psi|\Pi_0|\psi\rangle$, or

state $|1\rangle$ with probability $|\beta|^2 = |\langle 1|\psi\rangle|^2 = \langle\psi|1\rangle\langle 1|\psi\rangle = \langle\psi|\Pi_1|\psi\rangle$.

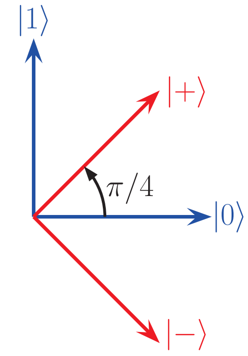
Quantum measurement : usually :

- a probabilistic process,
- as a destructive projection of the state $|\psi\rangle$ in an orthonormal basis,
- with statistics evaluable over repeated experiments with same preparation $|\psi\rangle$.

Hadamard basis

Another orthonormal basis of $\mathcal{H}_2$

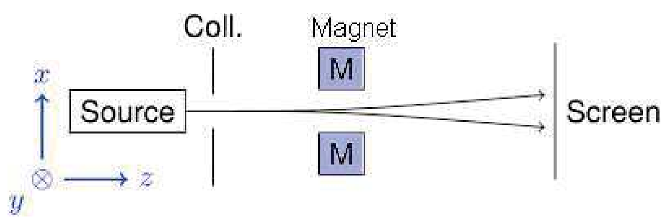
$$\left\{\,|+\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)\ ; \quad |-\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)\,\right\}.$$



$\Longleftrightarrow$ Computational orthonormal basis

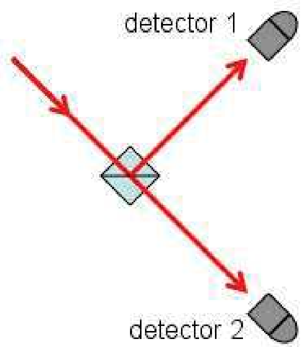
$$\left\{\,|0\rangle = \frac{1}{\sqrt{2}}\Big(|+\rangle + |-\rangle\Big)\ ; \quad |1\rangle = \frac{1}{\sqrt{2}}\Big(|+\rangle - |-\rangle\Big)\,\right\}.$$

Experiments



Stern-Gerlach apparatus for particles with two states of spin (electron, atom).

Two states of polarization of a photon :
(Nicol prism, Glan-Thompson,
polarizing beam splitter, . . .)

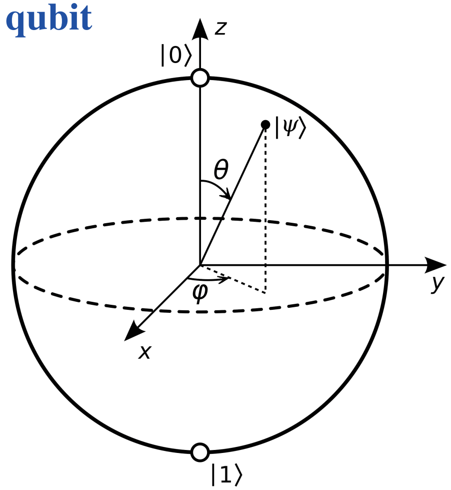


Bloch sphere representation of the qubit

Qubit in state
$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$.

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

with $\theta \in [0, \pi]\,$,
$\varphi \in [0, 2\pi[\,$.



Two states $\perp$ in $\mathcal{H}_2$ are antipodal on sphere.

As a quantum object,
the qubit has access to infinitely many configurations
via its two continuous degrees of freedom (θ, φ),
yet when it is measured it can only be found in one of two states.

In dimension N (finite) (extensible to infinite dimension)

State $|\psi\rangle = \sum_{n=1}^{N} \alpha_n |n\rangle$, in some orthonormal basis $\{|1\rangle, |2\rangle, \ldots |N\rangle\}$ of $\mathcal{H}_N$,

with $\alpha_n \in \mathbb{C}$, and $\sum_{n=1}^{N} |\alpha_n|^2 = \langle\psi|\psi\rangle = 1$.

Proba. $\Pr\{|n\rangle\} = |\alpha_n|^2$ in a projective measurement of $|\psi\rangle$ in basis $\{|n\rangle\}$.

Inner product $\langle k|\psi\rangle = \sum_{n=1}^{N} \alpha_n \overbrace{\langle k|n\rangle}^{\delta_{kn}} = \alpha_k$ coordinate.

$\mathsf{S} = \sum_{n=1}^{N} |n\rangle\langle n| = \mathrm{I}_N$ identity of $\mathcal{H}_N$ (closure or completeness relation),

since, $\forall |\psi\rangle : \mathsf{S}|\psi\rangle = \sum_{n=1}^{N} |n\rangle \overbrace{\langle n|\psi\rangle}^{\alpha_n} = \sum_{n=1}^{N} \alpha_n |n\rangle = |\psi\rangle \Longrightarrow \mathsf{S} = \mathrm{I}_N$.

Continuous infinite dimensional states

A particle moving in one dimension has a state $|\psi\rangle = \int_{-\infty}^{\infty} \psi(x)\,|x\rangle\,dx$ in an orthonormal basis $\{|x\rangle\}$ of a continuous infinite-dimensional Hilbert space $\mathcal{H}$.

The basis states $\{|x\rangle\}$ in $\mathcal{H}$ satisfy $\langle x|x'\rangle = \delta(x - x')$ (orthonormality),

$$\int_{-\infty}^{\infty} |x\rangle\langle x|\,dx = \mathrm{Id} \quad \text{(completeness).}$$

The coordinate $\mathbb{C} \ni \psi(x) = \langle x|\psi\rangle$ is the wave function, satisfying

$$1 = \int_{-\infty}^{\infty} |\psi(x)|^2 dx = \int_{-\infty}^{\infty} \psi^*(x)\,\psi(x)\,dx = \int_{-\infty}^{\infty} \langle\psi|x\rangle\langle x|\psi\rangle\,dx = \langle\psi|\psi\rangle\,,$$

with $|\psi(x)|^2$ the probability density for finding the particle at position x, when measuring the position of the particle.

Multiple qubits

A system (a word) of L qubits has a state in $\mathcal{H}_2^{\otimes L}$, a tensor-product vector space with dimension 2^L, and orthonormal basis $\{|x_1 x_2 \cdots x_L\rangle\}_{\vec{x} \in \{0,1\}^L}$.

Example $L = 2$:

Generally $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ (2^L coord.).

Or, as a special separable state ($2L$ coord.)

$$|\phi\rangle = \big(\alpha_1|0\rangle + \beta_1|1\rangle\big) \otimes \big(\alpha_2|0\rangle + \beta_2|1\rangle\big)$$
$$= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle\,.$$

A multipartite state which is not separable is entangled.

An entangled state behaves as a nonlocal whole : with no definite state for A and B separately, and what is done on one part may influence the other part instantly, no matter how distant they are.

Entangled states

- Example of a separable state of two qubits AB :

$$|AB\rangle = |+\rangle \otimes |+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) = \frac{1}{2}\big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\big).$$

When measured in the basis $\{|0\rangle, |1\rangle\}$, each qubit A and B can be found in state $|0\rangle$ or $|1\rangle$ independently with probability $1/2$.

$$\Pr\{A \text{ in } |0\rangle\} = \Pr\{|AB\rangle = |00\rangle\} + \Pr\{|AB\rangle = |01\rangle\} = 1/4 + 1/4 = 1/2.$$

- Example of an entangled state of two qubits AB :

$$|AB\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big). \qquad \Pr\{A \text{ in } |0\rangle\} = \Pr\{|AB\rangle = |00\rangle\} = 1/2.$$

When measured in the basis $\{|0\rangle, |1\rangle\}$, each qubit A and B can be found in state $|0\rangle$ or $|1\rangle$ with probability $1/2$ (randomly, no predetermination before measurement).

But if A is found in $|0\rangle$ necessarily B is found in $|0\rangle$,

and if A is found in $|1\rangle$ necessarily B is found in $|1\rangle$,

no matter how distant the two qubits are before measurement.

Futhermore, $|AB\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) = \frac{1}{\sqrt{2}}\Big(|{+}{+}\rangle + |{-}{-}\rangle\Big)$.

$\Longrightarrow \Pr\{A \text{ in } |+\rangle\} = \Pr\{|AB\rangle = |{+}{+}\rangle\} = 1/2$.

When measured in the basis $\{|+\rangle, |-\rangle\}$, each qubit A and B can be found in state $|+\rangle$ or $|-\rangle$ with probability $1/2$ (randomly, no predetermination before measurement).

But if A is found in $|+\rangle$ necessarily B is found in $|+\rangle$,
and if A is found in $|-\rangle$ necessarily B is found in $|-\rangle$,
no matter how distant the two qubits are before measurement.

Bell basis

A pair of qubits in $\mathcal{H}_2^{\otimes 2}$ is a quantum system with dimension $2^2 = 4$,
with original (computational) orthonormal basis $\Big\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\Big\}$.

Another orthonormal basis of $\mathcal{H}_2^{\otimes 2}$ is the Bell basis $\Big\{|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle\Big\}$:

$$\left\{\begin{array}{lcl} |\beta_{00}\rangle & = & \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) \\ |\beta_{01}\rangle & = & \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big) \\ |\beta_{10}\rangle & = & \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big) \\ |\beta_{11}\rangle & = & \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big) \end{array}\right. \Longleftrightarrow \left\{\begin{array}{lcl} |00\rangle & = & \frac{1}{\sqrt{2}}\Big(|\beta_{00}\rangle + |\beta_{10}\rangle\Big) \\ |01\rangle & = & \frac{1}{\sqrt{2}}\Big(|\beta_{01}\rangle + |\beta_{11}\rangle\Big) \\ |10\rangle & = & \frac{1}{\sqrt{2}}\Big(|\beta_{01}\rangle - |\beta_{11}\rangle\Big) \\ |11\rangle & = & \frac{1}{\sqrt{2}}\Big(|\beta_{00}\rangle - |\beta_{10}\rangle\Big) \end{array}\right.$$

Observables

For a quantum system in space $\mathcal{H}_N$ with dimension N,
a projective measurement is defined by an orthonormal basis $\{|1\rangle, \dots |N\rangle\}$ of $\mathcal{H}_N$,
and the N orthogonal projectors $|n\rangle\langle n|$, for $n = 1$ to N.

Also, any Hermitian (i.e. $\Omega = \Omega^\dagger$) operator Ω on $\mathcal{H}_N$,
has its eigenstates forming an orthonormal basis $\{|\omega_1\rangle, \dots |\omega_N\rangle\}$ of $\mathcal{H}_N$.
Therefore, any Hermitian operator Ω on $\mathcal{H}_N$ defines a valid measurement,
and has a spectral decomposition $\Omega = \sum_{n=1}^{N} \omega_n |\omega_n\rangle\langle\omega_n|$, with the real eigenvalues ω_n.

Also, any physical quantity measurable on a quantum system is represented in quantum theory by a Hermitian operator (an observable) Ω.

When system in state $|\psi\rangle$, measuring observable Ω is equivalent to performing a projective measurement in eigenbasis $\{|\omega_n\rangle\}$, with projectors $|\omega_n\rangle\langle\omega_n| = \Pi_n$, and yields the eigenvalue ω_n with probability $\Pr\{\omega_n\} = |\langle\omega_n|\psi\rangle|^2 = \langle\psi|\omega_n\rangle\langle\omega_n|\psi\rangle = \langle\psi|\Pi_n|\psi\rangle$.

The average is $\langle\Omega\rangle = \sum_n \omega_n \Pr\{\omega_n\} = \langle\psi|\Omega|\psi\rangle$.

Heisenberg uncertainty relation (1/2)

For two operators A and B : commutator $[\mathsf{A}, \mathsf{B}] = \mathsf{AB} - \mathsf{BA}$,
anticommutator $\{\mathsf{A}, \mathsf{B}\} = \mathsf{AB} + \mathsf{BA}$,
so that $\mathsf{AB} = \frac{1}{2}[\mathsf{A}, \mathsf{B}] + \frac{1}{2}\{\mathsf{A}, \mathsf{B}\}$.

When A and B Hermitian : $[\mathsf{A}, \mathsf{B}]$ is antiHermitian and $\{\mathsf{A}, \mathsf{B}\}$ is Hermitian,
and for any $|\psi\rangle$ then $\langle\psi|[\mathsf{A}, \mathsf{B}]|\psi\rangle \in i\mathbb{R}$ and $\langle\psi|\{\mathsf{A}, \mathsf{B}\}|\psi\rangle \in \mathbb{R}$; then

$$\langle\psi|\mathsf{AB}|\psi\rangle = \frac{1}{2}\underbrace{\langle\psi|[\mathsf{A}, \mathsf{B}]|\psi\rangle}_{\text{imaginary (part)}} + \frac{1}{2}\underbrace{\langle\psi|\{\mathsf{A}, \mathsf{B}\}|\psi\rangle}_{\text{real (part)}} \Longrightarrow \Big|\langle\psi|\mathsf{AB}|\psi\rangle\Big|^2 \geq \frac{1}{4}\Big|\langle\psi|[\mathsf{A}, \mathsf{B}]|\psi\rangle\Big|^2 ;$$

and for two vectors $\mathsf{A}|\psi\rangle$ and $\mathsf{B}|\psi\rangle$, the Cauchy-Schwarz inequality is

$$\Big|\langle\psi|\mathsf{AB}|\psi\rangle\Big|^2 \leq \langle\psi|\mathsf{A}^2|\psi\rangle\langle\psi|\mathsf{B}^2|\psi\rangle ,$$

so that $\langle\psi|\mathsf{A}^2|\psi\rangle\langle\psi|\mathsf{B}^2|\psi\rangle \geq \frac{1}{4}\Big|\langle\psi|[\mathsf{A}, \mathsf{B}]|\psi\rangle\Big|^2$.

Heisenberg uncertainty relation (2/2)

For two observables A and B measured in state $|\psi\rangle$:
the average (scalar) : $\langle \mathsf{A}\rangle = \langle\psi|\mathsf{A}|\psi\rangle$,
the centered or dispersion operator : $\widetilde{\mathsf{A}} = \mathsf{A} - \langle\mathsf{A}\rangle\, \mathrm{I}$,

$\Longrightarrow \left\langle \widetilde{\mathsf{A}}^2 \right\rangle = \langle \mathsf{A}^2\rangle - \langle\mathsf{A}\rangle^2$ scalar variance,

also $[\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}}] = [\mathsf{A}, \mathsf{B}]$.

Whence $\left\langle \widetilde{\mathsf{A}}^2 \right\rangle \left\langle \widetilde{\mathsf{B}}^2 \right\rangle \geq \dfrac{1}{4}\big|\langle[\mathsf{A},\mathsf{B}]\rangle\big|^2$ Heisenberg uncertainty relation ;

or with the scalar dispersions $\Delta A = \left(\langle\widetilde{\mathsf{A}}^2\rangle\right)^{1/2}$ and $\Delta B = \left(\langle\widetilde{\mathsf{B}}^2\rangle\right)^{1/2}$,

then $\Delta A\, \Delta B \geq \dfrac{1}{2}\big|\langle[\mathsf{A},\mathsf{B}]\rangle\big|$ Heisenberg uncertainty relation.

Computation on a qubit

(3) Evolution

Through a unitary (linear) operator U on $\mathcal{H}_2$ (a 2×2 matrix) : (i.e. $\mathsf{U}^{-1} = \mathsf{U}^\dagger$)

normalized vector $|\psi\rangle \in \mathcal{H}_2 \longrightarrow \mathsf{U}\,|\psi\rangle$ normalized vector $\in \mathcal{H}_2$.

$\equiv$ quantum gate
(always reversible)

input output

$$|\psi\rangle \longrightarrow \boxed{\mathrm{U}} \longrightarrow \mathrm{U}|\psi\rangle$$

Hadamard gate $\mathsf{H} = \dfrac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Identity gate $\mathrm{I}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

$\mathsf{H}^2 = \mathrm{I}_2 \Longleftrightarrow \mathsf{H}^{-1} = \mathsf{H} = \mathsf{H}^\dagger$ Hermitian unitary.

$\mathsf{H}\,|0\rangle = |+\rangle$ and $\mathsf{H}\,|1\rangle = |-\rangle$

$$\Longrightarrow \quad \mathsf{H}\,|x\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + (-1)^x\,|1\rangle\Big) = \frac{1}{\sqrt{2}}\sum_{z\in\{0,1\}} (-1)^{xz}\,|z\rangle \ , \quad \forall\, x \in \{0,1\}.$$

Pauli gates

$$\mathsf{X} = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \mathsf{Y} = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad \mathsf{Z} = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

$\mathsf{X}^2 = \mathsf{Y}^2 = \mathsf{Z}^2 = \mathrm{I}_2$. Hermitian unitary. $\mathsf{XY} = -\mathsf{YX} = i\mathsf{Z}$, $\mathsf{ZX} = i\mathsf{Y}$, etc.

$\left\{\mathrm{I}_2, \mathsf{X}, \mathsf{Y}, \mathsf{Z}\right\}$ a basis for operators on $\mathcal{H}_2$.

Hadamard gate $\mathsf{H} = \dfrac{1}{\sqrt{2}}\big(\mathsf{X} + \mathsf{Z}\big)$.

$\mathsf{X} = \sigma_x$ the inversion or Not quantum gate. $\mathsf{X}\,|0\rangle = |1\rangle$, $\mathsf{X}\,|1\rangle = |0\rangle$.

$$\mathsf{W} = \sqrt{\mathsf{X}} = \sqrt{\sigma_x} = \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} e^{i\pi/4} & e^{-i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4} \end{bmatrix} \Longrightarrow \mathsf{W}^2 = \mathsf{X}\ ,$$

square-root of Not, (or $\mathsf{W}^\dagger$), typically quantum gate (no classical analogue).

In general, the gates U and $e^{i\phi}\mathsf{U}$ lead to the same measurement statistics at the output, and are thus physically equivalent, in this respect.

Any single-qubit gate can always be expressed as $e^{i\phi}\mathsf{U}_\xi$ with

$$\mathsf{U}_\xi = \exp\left(-i\,\frac{\xi}{2}\vec{n}\cdot\vec{\sigma}\right) = \cos\left(\frac{\xi}{2}\right)\mathrm{I}_2 - i\sin\left(\frac{\xi}{2}\right)\vec{n}\cdot\vec{\sigma} \quad \in \mathrm{SU}(2)\ ,$$

with a formal "vector" of 2×2 matrices $\vec{\sigma} = [\sigma_x, \sigma_y, \sigma_z]$,

and $\vec{n} = [n_x, n_y, n_z]^\top$ a real unit vector of $\mathbb{R}^3 \Longrightarrow \det(\mathsf{U}_\xi) = 1$,

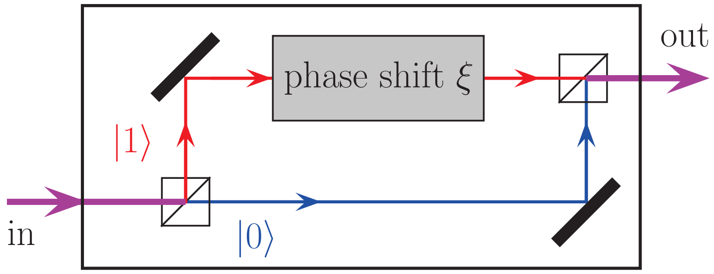
implementing in the Bloch sphere representation
a rotation of the qubit state of an angle ξ around the axis $\vec{n}$ in $\mathbb{R}^3$ $\in \mathrm{SO}(3)$.

Example : $\mathsf{W} = \sqrt{\sigma_\mathsf{x}} = e^{i\pi/4}\Big[\cos(\pi/4)\,\mathrm{I}_2 - i\sin(\pi/4)\,\sigma_x\Big]$, $(\xi = \pi/2,\ \vec{n} = \vec{e}_x)$.

An optical implementation

A one-qubit phase gate $\mathsf{U}_\xi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\xi} \end{bmatrix} = e^{i\xi/2} \exp(-i\xi\sigma_z/2)$

optically implemented by a Mach-Zehnder interferometer



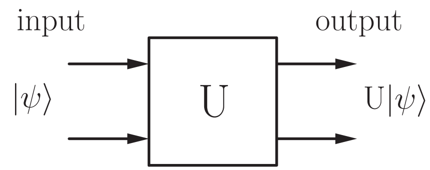
acting on individual photons with two states of polarization $|0\rangle$ and $|1\rangle$ which are selectively shifted in phase, to operate as well on any superposition $\alpha\,|0\rangle + \beta\,|1\rangle \longrightarrow \alpha\,|0\rangle + \beta e^{i\xi}\,|1\rangle$.

Computation on a pair of qubits

Through a unitary operator U on $\mathcal{H}_2^{\otimes 2}$ (a 4×4 matrix) :

normalized vector $|\psi\rangle \in \mathcal{H}_2^{\otimes 2} \longrightarrow \mathsf{U}\,|\psi\rangle$ normalized vector $\in \mathcal{H}_2^{\otimes 2}$.

$\equiv$ quantum gate
(always reversible)



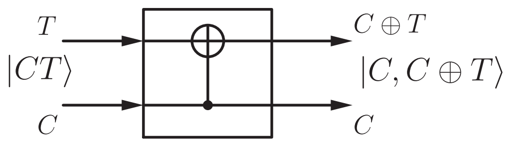
Completely defined for instance by the transformation of the four state vectors of the computational basis $\big\{|00\rangle\,, |01\rangle\,, |10\rangle\,, |11\rangle\big\}$.

But works equally on any linear superposition of quantum states
$\Longrightarrow$ quantum parallelism.

• Example : Controlled-Not gate

Via the XOR binary function : $a \oplus b = a$ when $b = 0$, or $= \overline{a}$ when $b = 1$;
invertible $a \oplus x = b \Longleftrightarrow x = a \oplus b = b \oplus a$.

Used to construct a unitary invertible quantum C-Not gate :
(T target, C control)



$|CT\rangle \longrightarrow |C, C \oplus T\rangle$
$|00\rangle \longrightarrow |00\rangle$
$|01\rangle \longrightarrow |01\rangle$
$|10\rangle \longrightarrow |11\rangle$
$|11\rangle \longrightarrow |10\rangle$

$$\mathsf{U} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$(\text{C-Not})^2 = \mathrm{I}_4 \Longleftrightarrow (\text{C-Not})^{-1} = \text{C-Not} = (\text{C-Not})^\dagger$ Hermitian unitary.

Computation on a system of L qubits

Through a unitary operator U on $\mathcal{H}_2^{\otimes L}$ (a $2^L \times 2^L$ matrix) :

normalized vector $|\psi\rangle \in \mathcal{H}_2^{\otimes L} \longrightarrow \mathsf{U}\,|\psi\rangle$ normalized vector $\in \mathcal{H}_2^{\otimes L}$.

$\equiv$ quantum gate : L input qubits $\xrightarrow{\mathsf{U}}$ L output qubits.

Completely defined for instance by the transformation of the 2^L state vectors of the computational basis ;
but works equally on any linear superposition of them (parallelism).

Universal set of gates :
Any L-qubit quantum gate or circuit U can always be obtained from two-qubit C-Not gates and single-qubit gates.
And in principle this ensures experimental realizability of any unitary U.

This provides a foundation for quantum computation.

Continuous-time evolution of a quantum system

By empirical postulation Schrödinger equation (for isolated systems) :

$$\frac{d}{dt}|\psi\rangle = -\frac{i}{\hbar}\mathsf{H}|\psi\rangle \Longrightarrow |\psi(t_2)\rangle = \underbrace{\exp\left(-\frac{i}{\hbar}\int_{t_1}^{t_2}\mathsf{H}dt\right)}_{\text{unitary } \mathsf{U}(t_2,t_1)}|\psi(t_1)\rangle = \mathsf{U}(t_2,t_1)|\psi(t_1)\rangle$$

Hermitian operator Hamiltonian H, or energy operator.

Conversely, postulating for $|\psi\rangle$ a linear unitary evolution $\mathsf{U}(t_2,t_1)$ between any two times t_1 and t_2, especially $|\psi(t+dt)\rangle = \mathsf{U}(t+dt,t)|\psi(t)\rangle$, recovers the Schrödinger equation.