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

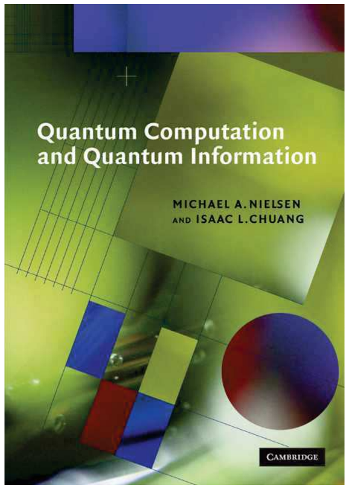
for information and computation :

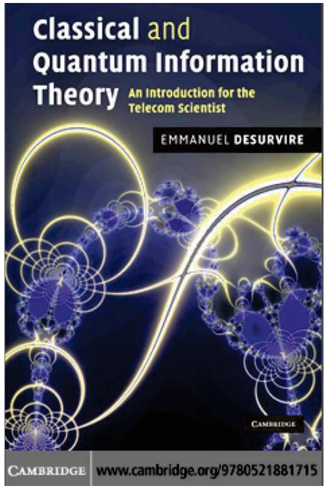
1) When using elementary systems (photons, electrons, atoms, ions, nanodevices, . . .).

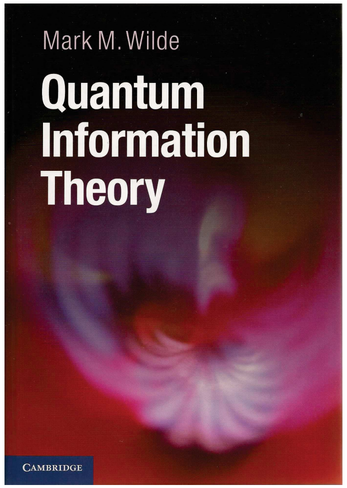
2) To benefit from purely quantum effects (parallelism, entanglement, . . .).

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

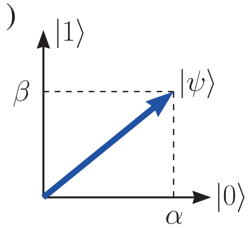
(1) State

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

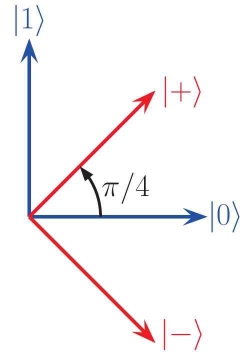
Quantum measurement : usually :

- 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 $\mathcal{H}_2$

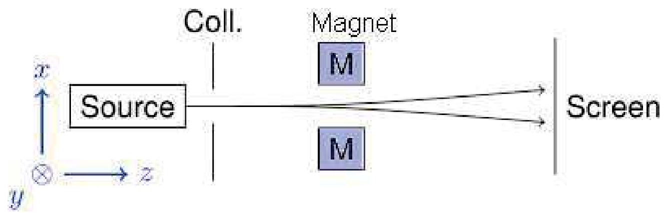
$$\left\{\,|+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)\;;\quad |-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)\right\}.$$



$\Longleftrightarrow$ Computational orthonormal basis

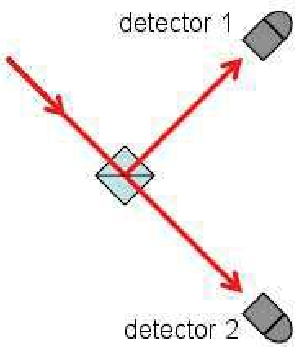
$$\left\{\,|0\rangle = \frac{1}{\sqrt{2}}\big(|+\rangle + |-\rangle\big)\;;\quad |1\rangle = \frac{1}{\sqrt{2}}\big(|+\rangle - |-\rangle\big)\right\}.$$

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, . . .)

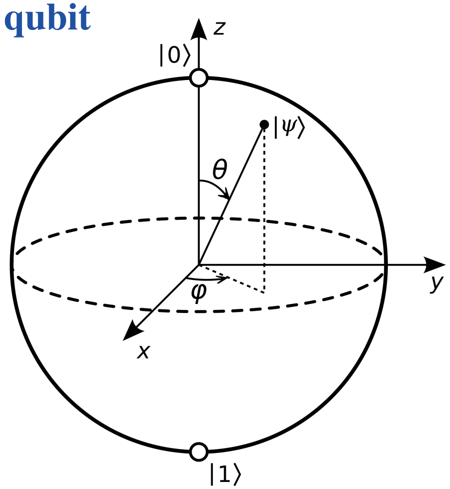


Bloch sphere representation of the qubit

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 $\{|1\rangle, |2\rangle, \dots |N\rangle\}$ 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 $\big\{|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle\big\}$:

$$\begin{cases} |\beta_{00}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \\ |\beta_{01}\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big) \\ |\beta_{10}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big) \\ |\beta_{11}\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big) \end{cases} \iff \begin{cases} |00\rangle = \frac{1}{\sqrt{2}}\big(|\beta_{00}\rangle + |\beta_{10}\rangle\big) \\ |01\rangle = \frac{1}{\sqrt{2}}\big(|\beta_{01}\rangle + |\beta_{11}\rangle\big) \\ |10\rangle = \frac{1}{\sqrt{2}}\big(|\beta_{01}\rangle - |\beta_{11}\rangle\big) \\ |11\rangle = \frac{1}{\sqrt{2}}\big(|\beta_{00}\rangle - |\beta_{10}\rangle\big) \end{cases}$$

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 $\left\langle \widetilde{\mathsf{A}}^2 \right\rangle \left\langle \widetilde{\mathsf{B}}^2 \right\rangle \geq \frac{1}{4} \left| \langle [\mathsf{A}, \mathsf{B}] \rangle \right|^2$ 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 $\Delta A \, \Delta B \geq \frac{1}{2} \left| \langle [\mathsf{A}, \mathsf{B}] \rangle \right|$ Heisenberg uncertainty relation.

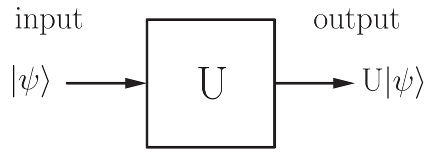
Computation on a qubit

(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 $\in \mathcal{H}_2$.

≡ quantum gate
(always reversible)



Hadamard gate $\mathsf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. 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

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

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

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

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

$\mathsf{X} = \sigma_x$ 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 $\mathbb{R}^3 \Longrightarrow \det(\mathsf{U}_\xi) = 1$,

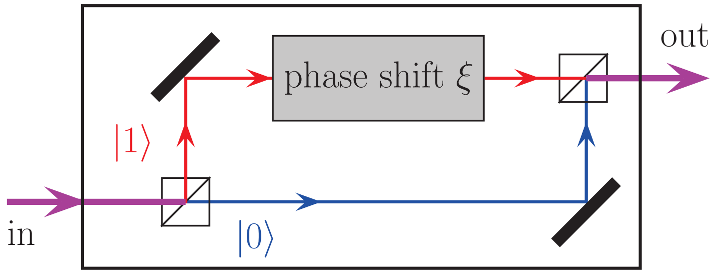
implementing in the Bloch sphere representation
a rotation of the qubit state of an angle ξ around the axis $\vec{n}$ in $\mathbb{R}^3$ $\in \mathrm{SO}(3)$.

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



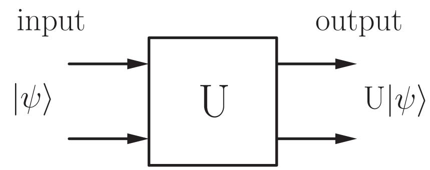
acting on individual photons with two states of polarization $|0\rangle$ and $|1\rangle$
which are selectively shifted in phase,
to operate as well on any superposition $\alpha_0 |0\rangle + \alpha_1 |1\rangle \longrightarrow \alpha_0 |0\rangle + \alpha_1 e^{i\xi} |1\rangle$.

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 $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

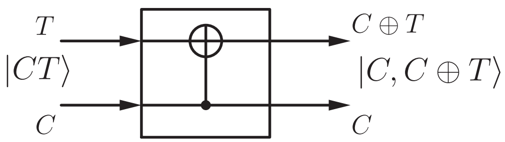
But works equally on any linear superposition of quantum states
$\Longrightarrow$ quantum parallelism.

• 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) :

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

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.

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

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

université angers

LARIS

"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.

Summary (so far) : Foundation on 3 general postulates or principles :

• **State :** Unit-norm vector $|\psi\rangle = \sum_{n=1}^{N}\alpha_n|n\rangle \in \mathcal{H}_N$ complex Hilbert space.
Realizable with L two-dimensional qubits, with $2^L \ge N$.
Multipartite states in tensor-product space $\Longrightarrow$ quantum entanglement.

• **Measurement :** Random and destructive, in $\mathcal{H}_N$ via
a set of M orthogonal projectors $\Pi_m = \Pi_m^\dagger\Pi_m$, satisfying $\sum_{m=1}^{M}\Pi_m = \mathrm{I}_N$,
with M outcomes of probability $P(m) = \bigl\|\Pi_m|\psi\rangle\bigr\|^2 = \langle\psi|\Pi_m|\psi\rangle$,
and post-measurement state $|\psi_{\text{post}}\rangle = \dfrac{\Pi_m|\psi\rangle}{\bigl\|\Pi_m|\psi\rangle\bigr\|}$.

• **Evolution :** Linear unitary : $|\psi\rangle \xrightarrow{\mathsf{U}} \mathsf{U}|\psi\rangle$
Realizable from one-qubit gates and the two-qubit C-Not gate.

In particular :

• **State :** $|\psi\rangle = \sum_{n=1}^{N}\alpha_n|n\rangle \Longrightarrow |\psi\rangle = \int_{-\infty}^{\infty}\psi(x)\,|x\rangle\,dx$ continuously infinite dimension. (p. 10)

• **Measurement** of $|AB\rangle = \frac{1}{\sqrt{2}}\bigl(|00\rangle + |11\rangle\bigr) = \frac{1}{\sqrt{2}}\bigl(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle\bigr) \in \mathcal{H}_2\otimes\mathcal{H}_2$ (p. 12)

$$\text{with}\ \begin{cases}\Pi_1 &= |00\rangle\langle 00| = |0\rangle\langle 0|\otimes|0\rangle\langle 0|\\ \Pi_2 &= |01\rangle\langle 01| = |0\rangle\langle 0|\otimes|1\rangle\langle 1|\\ \Pi_3 &= |10\rangle\langle 10| = |1\rangle\langle 1|\otimes|0\rangle\langle 0|\\ \Pi_4 &= |11\rangle\langle 11| = |1\rangle\langle 1|\otimes|1\rangle\langle 1|\end{cases} \Longrightarrow \sum_{m=1}^{4}\Pi_m = \mathrm{I}_4 = \mathrm{I}_2\otimes\mathrm{I}_2,$$

$$\text{or with}\ \begin{cases}\Pi_1' &= |0\rangle\langle 0|\otimes\mathrm{I}_2\\ \Pi_2' &= |1\rangle\langle 1|\otimes\mathrm{I}_2\end{cases} \Longrightarrow \sum_{m=1}^{2}\Pi_m' = \mathrm{I}_2\otimes\mathrm{I}_2 = \mathrm{I}_4.$$

• **Evolution :** $|\psi\rangle \xrightarrow{\mathsf{U}} \mathsf{U}|\psi\rangle \Longleftrightarrow \frac{d}{dt}|\psi\rangle = -\frac{i}{\hbar}\mathsf{H}\,|\psi\rangle \Longrightarrow |\psi(t_2)\rangle = \mathsf{U}(t_2,t_1)\,|\psi(t_1)\rangle$, (p. 25)

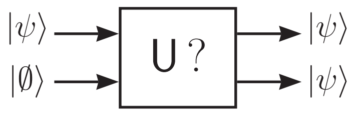
with $\mathsf{U}(t_2,t_1) = \exp\Bigl(-\frac{i}{\hbar}\int_{t_1}^{t_2}\mathsf{H}dt\Bigr)$. Trivial $\mathsf{H} = H_0\mathsf{Id} \Longrightarrow |\psi(t_2)\rangle = \exp\Bigl(-i\frac{H_0}{\hbar}(t_2-t_1)\Bigr)|\psi(t_1)\rangle$.

No cloning theorem (1982)

¿ Possibility of a circuit (a unitary U) that would take any state $|\psi\rangle$, associated with an auxiliary register $|\emptyset\rangle$, to transform the input $|\psi\rangle\,|\emptyset\rangle$ into the cloned output $|\psi\rangle\,|\psi\rangle$?

$$|\psi_1\rangle\,|\emptyset\rangle \xrightarrow{\ \mathsf{U}\ } \mathsf{U}(|\psi_1\rangle\,|\emptyset\rangle) = |\psi_1\rangle\,|\psi_1\rangle \text{ (would be).}$$

$$|\psi_2\rangle\,|\emptyset\rangle \xrightarrow{\ \mathsf{U}\ } \mathsf{U}(|\psi_2\rangle\,|\emptyset\rangle) = |\psi_2\rangle\,|\psi_2\rangle \text{ (would be).}$$



Linear superposition $|\psi\rangle = \alpha_1\,|\psi_1\rangle + \alpha_2\,|\psi_2\rangle$

$$|\psi\rangle\,|\emptyset\rangle \xrightarrow{\ \mathsf{U}\ } \mathsf{U}(|\psi\rangle\,|\emptyset\rangle) = \mathsf{U}\big(\alpha_1\,|\psi_1\rangle\,|\emptyset\rangle + \alpha_2\,|\psi_2\rangle\,|\emptyset\rangle\big)$$
$$= \alpha_1\,|\psi_1\rangle\,|\psi_1\rangle + \alpha_2\,|\psi_2\rangle\,|\psi_2\rangle \qquad \text{since U linear.}$$

But $|\psi\rangle\,|\psi\rangle = |\psi\rangle \otimes |\psi\rangle = \big(\alpha_1\,|\psi_1\rangle + \alpha_2\,|\psi_2\rangle\big)\big(\alpha_1\,|\psi_1\rangle + \alpha_2\,|\psi_2\rangle\big)$

$$= \alpha_1^2\,|\psi_1\rangle\,|\psi_1\rangle + \alpha_1\alpha_2\,|\psi_1\rangle\,|\psi_2\rangle + \alpha_1\alpha_2\,|\psi_2\rangle\,|\psi_1\rangle + \alpha_2^2\,|\psi_2\rangle\,|\psi_2\rangle$$

$\neq \mathsf{U}(|\psi\rangle\,|\emptyset\rangle)$ in general. $\Longrightarrow$ No cloning U possible.

Quantum parallelism

For a system of L qubits,
a quantum gate or circuit is any unitary operator U from $\mathcal{H}_2^{\otimes L}$ onto $\mathcal{H}_2^{\otimes L}$.

The quantum gate U is completely defined
by its action on the 2^L basis states of $\mathcal{H}_2^{\otimes L}$: $\big\{|\vec{x}\rangle, \vec{x} \in \{0,1\}^L\big\}$,
just like a classical gate.

Yet, the quantum gate U can be operated
on any linear superposition of the basis states $\big\{|\vec{x}\rangle, \vec{x} \in \{0,1\}^L\big\}$.

This is quantum parallelism, with no classical analogue.

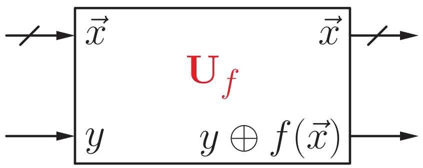
$\log_2(10) \approx 3.32 \Longrightarrow \log_2\big(10^{15}\big) \approx 49.83 \Longleftrightarrow 10^{15} \approx 2^{50}$
So 1000 Tbits can be stored in a register of 50 qubits !

Parallel evaluation of a function (1/4)

A classical Boolean function $f(\cdot)$ from L bits to 1 bit

$$\vec{x} \in \{0,1\}^L \longrightarrow f(\vec{x}) \in \{0,1\}.$$

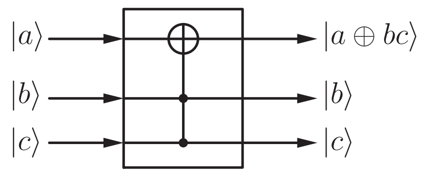
Used to construct a unitary operator U_f as an invertible f-controlled gate :



with binary output $y \oplus f(\vec{x}) = f(\vec{x})$ when $y = 0$, or $= \overline{f(\vec{x})}$ when $y = 1$,
(invertible as $[y \oplus f(\vec{x})] \oplus f(\vec{x}) = y \oplus f(\vec{x}) \oplus f(\vec{x}) = y \oplus 0 = y$).

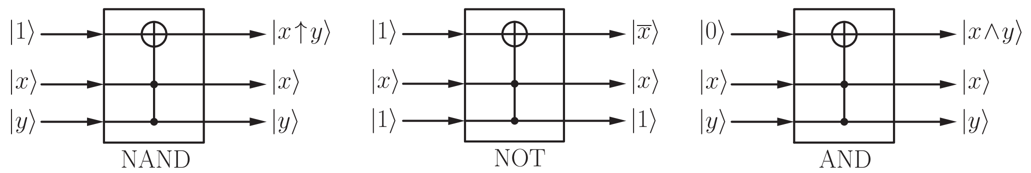
Parallel evaluation of a function (2/4)

Toffoli gate or Controlled-Controlled-Not gate or CC-Not quantum gate :

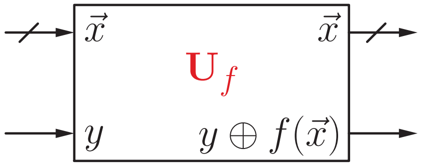


$(\text{CC-Not})^2 = \mathrm{I}_8 \Longleftrightarrow (\text{CC-Not})^{-1} = \text{CC-Not} = (\text{CC-Not})^\dagger$ Hermitian unitary.

Any classical Boolean function $f(\vec{x})$ (invertible or non) on L bits
can always be implemented (simulated) by means of 3-qubit Toffoli gates.



Parallel evaluation of a function (3/4)



For every basis state $|\vec{x}\rangle$, with $\vec{x} \in \{0,1\}^L$:

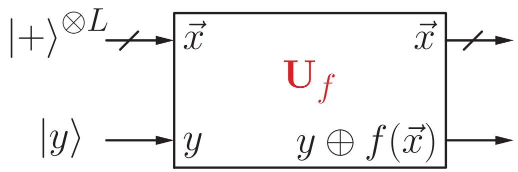
$$|\vec{x}\rangle\,|y=0\rangle \xrightarrow{\ \mathsf{U}_f\ } |\vec{x}\rangle\,|f(\vec{x})\rangle$$

$$|\vec{x}\rangle\,|y=1\rangle \longrightarrow |\vec{x}\rangle\,|\overline{f(\vec{x})}\rangle$$

$$|\vec{x}\rangle\,|+\rangle \longrightarrow |\vec{x}\rangle\,\frac{1}{\sqrt{2}}\Big[|f(\vec{x})\rangle + |\overline{f(\vec{x})}\rangle\Big] = |\vec{x}\rangle\,|+\rangle$$

$$|\vec{x}\rangle\,|-\rangle \longrightarrow |\vec{x}\rangle\,\frac{1}{\sqrt{2}}\Big[|f(\vec{x})\rangle - |\overline{f(\vec{x})}\rangle\Big] = |\vec{x}\rangle\,|-\rangle\,(-1)^{f(\vec{x})}$$

Parallel evaluation of a function (4/4)



$$|+\rangle^{\otimes L} = \left(\frac{1}{\sqrt{2}}\right)^L \sum_{\vec{x}\in\{0,1\}^L} |\vec{x}\rangle$$ superposition of all basis states,

$$|+\rangle^{\otimes L} \otimes |0\rangle \xrightarrow{\ \mathsf{U}_f\ } \left(\frac{1}{\sqrt{2}}\right)^L \sum_{\vec{x}\in\{0,1\}^L} |\vec{x}\rangle\,|f(\vec{x})\rangle$$ superposition of all values $f(\vec{x})$.

$$|+\rangle^{\otimes L} \otimes |-\rangle \xrightarrow{\ \mathsf{U}_f\ } \left(\frac{1}{\sqrt{2}}\right)^L \sum_{\vec{x}\in\{0,1\}^L} |\vec{x}\rangle\,|-\rangle\,(-1)^{f(\vec{x})}$$

¿ How to extract, to measure, useful informations from superpositions ?

Deutsch-Jozsa algorithm (1992) : Parallel test of a function (1/5)

A classical Boolean function $f(\cdot)\left|\begin{array}{ccc} \{0,1\}^L & \longrightarrow & \{0,1\} \\ 2^L \text{ values} & \longrightarrow & 2 \text{ values,} \end{array}\right.$

can be *constant* (all inputs into 0 or 1) or *balanced* (equal numbers of 0, 1 in output).

Classically : Between 2 and $\dfrac{2^L}{2}+1$ evaluations of $f(\cdot)$ to decide.

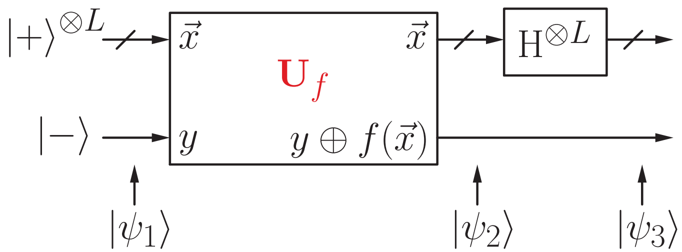
Quantumly : One evaluation of $f(\cdot)$ is enough (on a suitable superposition).

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

$$\Longrightarrow \mathsf{H}^{\otimes L}\,|\vec{x}\rangle = \mathsf{H}\,|x_1\rangle \otimes \cdots \otimes \mathsf{H}\,|x_L\rangle = \left(\frac{1}{\sqrt{2}}\right)^L \sum_{\vec{z}\in\{0,1\}^L} (-1)^{\vec{x}\vec{z}}\,|\vec{z}\rangle\,, \quad \forall\, \vec{x} \in \{0,1\}^L,$$

with scalar product $\vec{x}\vec{z} = x_1 z_1 + \cdots + x_L z_L$ modulo 2. (quantum Hadamard transfo.)

Deutsch-Jozsa algorithm (2/5)



Input state $|\psi_1\rangle = |+\rangle^{\otimes L}\,|-\rangle = \left(\dfrac{1}{\sqrt{2}}\right)^L \sum_{\vec{x}\in\{0,1\}^L} |\vec{x}\rangle\,|-\rangle$

Internal state $|\psi_2\rangle = \left(\dfrac{1}{\sqrt{2}}\right)^L \sum_{\vec{x}\in\{0,1\}^L} |\vec{x}\rangle\,|-\rangle\,(-1)^{f(\vec{x})}$

Deutsch-Jozsa algorithm (3/5)

Output state $|\psi_3\rangle = \left(\mathsf{H}^{\otimes L} \otimes \mathrm{I}_2\right) |\psi_2\rangle$

$$= \left(\frac{1}{\sqrt{2}}\right)^L \sum_{\vec{x}\in\{0,1\}^L} \mathsf{H}^{\otimes L} |\vec{x}\rangle |-\rangle (-1)^{f(\vec{x})}$$

$$= \left(\frac{1}{2}\right)^L \sum_{\vec{x}\in\{0,1\}^L} \sum_{\vec{z}\in\{0,1\}^L} (-1)^{\vec{x}\vec{z}} |\vec{z}\rangle |-\rangle (-1)^{f(\vec{x})} \quad \text{by Lemma 1,}$$

or $|\psi_3\rangle = |\psi\rangle |-\rangle$, with $|\psi\rangle = \left(\frac{1}{2}\right)^L \sum_{\vec{z}\in\{0,1\}^L} w(\vec{z}) |\vec{z}\rangle$

and the scalar weight $w(\vec{z}) = \sum_{\vec{x}\in\{0,1\}^L} (-1)^{f(\vec{x})\oplus\vec{x}\vec{z}}$

Deutsch-Jozsa algorithm (4/5)

So $|\psi\rangle = \frac{1}{2^L} \sum_{\vec{z}\in\{0,1\}^L} w(\vec{z}) |\vec{z}\rangle$ with $w(\vec{z}) = \sum_{\vec{x}\in\{0,1\}^L} (-1)^{f(\vec{x})\oplus\vec{x}\vec{z}}$.

For $|\vec{z}\rangle = |\vec{0}\rangle = |0\rangle^{\otimes L}$ then $w(\vec{z}=\vec{0}) = \sum_{\vec{x}\in\{0,1\}^L} (-1)^{f(\vec{x})}$.

• When $f(\cdot)$ constant : $w(\vec{z}=\vec{0}) = 2^L(-1)^{f(\vec{0})} = \pm 2^L \Longrightarrow$ in $|\psi\rangle$ the amplitude of $|\vec{0}\rangle$ is ±1, and since $|\psi\rangle$ is with unit norm $\Longrightarrow |\psi\rangle = \pm|\vec{0}\rangle$, and all other $w(\vec{z}\neq\vec{0})=0$.
$\Longrightarrow$ When $|\psi\rangle$ is measured, L states $|0\rangle$ are found.

• When $f(\cdot)$ balanced : $w(\vec{z}=\vec{0}) = 0 \Longrightarrow |\psi\rangle$ is not or does not contain state $|\vec{0}\rangle$.
$\Longrightarrow$ When $|\psi\rangle$ is measured, at least one state $|1\rangle$ is found.

$\longrightarrow$ Illustrates quantum ressources of parallelism, coherent superposition, interference.
(When $f(\cdot)$ is neither constant nor balanced, $|\psi\rangle$ contains a little bit of $|\vec{0}\rangle$.)

Deutsch-Jozsa algorithm (5/5)

[1] D. Deutsch; "Quantum theory, the Church-Turing principle and the universal quantum computer"; *Proceedings of the Royal Society of London A* 400 (1985) 97–117.
The case $L = 2$ qubits.

[2] D. Deutsch, R. Jozsa; "Rapid solution of problems by quantum computation"; *Proceedings of the Royal Society of London A* 439 (1992) 553–558.
Extension to arbitrary $L \geq 2$ qubits.

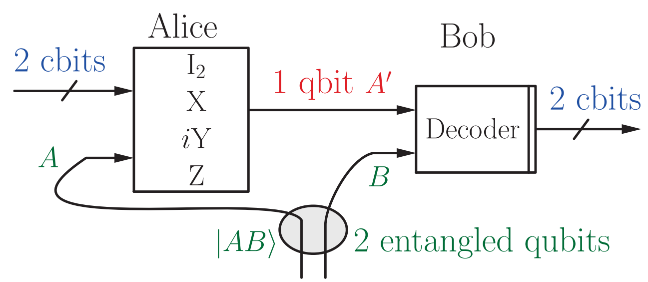
[3] E. Bernstein, U. Vazirani; "Quantum complexity theory"; *SIAM Journal on Computing* 26 (1997) 1411–1473.
Extension to $f(\vec{x}) = \vec{a}\vec{x}$ or $f(\vec{x}) = \vec{a}\vec{x}\oplus b$, to find binary L-word $\vec{a} \longrightarrow$ by producing output $|\psi\rangle = |\vec{a}\rangle$.

[4] R. Cleve, A. Ekert, C. Macchiavello, M. Mosca; "Quantum algorithms revisited"; *Proceedings of the Royal Society of London A* 454 (1998) 339–354.

Superdense coding (Bennett 1992) : exploiting entanglement

Alice and Bob share a qubit pair in entangled state $|AB\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = |\beta_{00}\rangle$.

Alice chooses two classical bits, used to encode by applying to her qubit A one of $\{\mathrm{I}_2, \mathsf{X}, i\mathsf{Y}, \mathsf{Z}\}$, delivering the qubit A' sent to Bob.



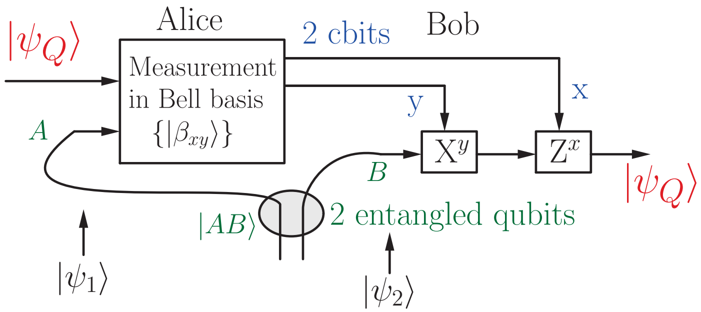
$\mathrm{I}_2 \otimes \mathrm{I}_2 |AB\rangle = |\beta_{00}\rangle$
$\mathsf{X} \otimes \mathrm{I}_2 |AB\rangle = |\beta_{01}\rangle$
$\mathsf{Z} \otimes \mathrm{I}_2 |AB\rangle = |\beta_{10}\rangle$
$i\mathsf{Y} \otimes \mathrm{I}_2 |AB\rangle = |\beta_{11}\rangle$

Bob receives this qubit A'. For decoding, Bob measures $|A'B\rangle$ in the Bell basis $\left\{|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle\right\}$, from which he recovers the two classical bits.

Teleportation (Bennett 1993) : of an arbitrary qubit state (1/3)

Qubit Q in an arbitrary state $|\psi_Q\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$.

Alice and Bob share a qubit pair in entangled state $|AB\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) = |\beta_{00}\rangle$.



Alice measures the pair of qubits QA in the Bell basis (so $|\psi_Q\rangle$ is locally destroyed), and the two resulting cbits x, y are sent to Bob.

Bob on his qubit B applies the gates X^y and Z^x which reconstructs $|\psi_Q\rangle$.

Teleportation (2/3)

$$|\psi_1\rangle = |\psi_Q\rangle\,|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\Big[\alpha_0 |0\rangle \big(|00\rangle + |11\rangle\big) + \alpha_1 |1\rangle \big(|00\rangle + |11\rangle\big)\Big]$$
$$= \frac{1}{\sqrt{2}}\Big[\alpha_0 |000\rangle + \alpha_0 |011\rangle + \alpha_1 |100\rangle + \alpha_1 |111\rangle\Big],$$

factorizable as
$$|\psi_1\rangle = \frac{1}{2}\Big[\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)\big(\alpha_0 |0\rangle + \alpha_1 |1\rangle\big) + \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big)\big(\alpha_0 |1\rangle + \alpha_1 |0\rangle\big) + \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big)\big(\alpha_0 |0\rangle - \alpha_1 |1\rangle\big) + \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big)\big(\alpha_0 |1\rangle - \alpha_1 |0\rangle\big)\Big],$$

Teleportation (3/3)

$$|\psi_1\rangle = \frac{1}{2}\Big[|\beta_{00}\rangle\big(\alpha_0 |0\rangle + \alpha_1 |1\rangle\big) + |\beta_{01}\rangle\big(\alpha_0 |1\rangle + \alpha_1 |0\rangle\big) + |\beta_{10}\rangle\big(\alpha_0 |0\rangle - \alpha_1 |1\rangle\big) + |\beta_{11}\rangle\big(\alpha_0 |1\rangle - \alpha_1 |0\rangle\big)\Big].$$

The first two qubits QA measured in Bell basis $\{|\beta_{xy}\rangle\}$ yield the two cbits xy, used to transform the third qubit B by X^y then Z^x, which reconstructs $|\psi_Q\rangle$.

When QA is measured in $|\beta_{00}\rangle$ then B is in $\alpha_0 |0\rangle + \alpha_1 |1\rangle \xrightarrow{I_2} \cdot \xrightarrow{I_2} |\psi_Q\rangle$

When QA is measured in $|\beta_{01}\rangle$ then B is in $\alpha_0 |1\rangle + \alpha_1 |0\rangle \xrightarrow{\mathsf{X}} \cdot \xrightarrow{I_2} |\psi_Q\rangle$

When QA is measured in $|\beta_{10}\rangle$ then B is in $\alpha_0 |0\rangle - \alpha_1 |1\rangle \xrightarrow{I_2} \cdot \xrightarrow{\mathsf{Z}} |\psi_Q\rangle$

When QA is measured in $|\beta_{11}\rangle$ then B is in $\alpha_0 |1\rangle - \alpha_1 |0\rangle \xrightarrow{\mathsf{X}} \cdot \xrightarrow{\mathsf{Z}} |\psi_Q\rangle$.

Princeps references on superdense coding . . .

[1] C. H. Bennett, S. J. Wiesner; "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states"; *Physical Review Letters* 69 (1992) 2881–2884.

[2] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger; "Dense coding in experimental quantum communication"; *Physical Review Letters* 76 (1996) 4656–4659.

. . . and teleportation

[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters; "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels"; *Physical Review Letters* 70 (1993) 1895–1899.

[4] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger; "Experimental quantum teleportation"; *Nature* 390 (1997) 575–579.

Grover quantum search algorithm (1/4) *Phys. Rev. Let.* 79 (1997) 325.

- Iterative algorithm that finds an item out of N in an unsorted dataset, with $O(\sqrt{N})$ queries instead of $O(N)$ classically.

- A dataset contains N items numbered as $n \in \{1, 2, \cdots N\}$.

One wants to find one (only one here, but extensible) item $n = n_0$ satisfying some criterion or property, indicated by the test function or **oracle** $f(\cdot)$ responding as $f(n) = \delta_{nn_0}$.

With an unsorted dataset, finding n_0 requires **classically** $O(N)$ interrogations of the oracle or evaluations of $f(\cdot)$, while $O(\sqrt{N})$ are enough **quantumly**.

Grover quantum search algorithm (2/4)

- **Quantumly**, an N-dimensional quantum system in $\mathcal{H}_N$ with orthonormal basis $\{|1\rangle, \cdots, |N\rangle\}$, where the N basis states $|n\rangle$, for $n \in \{1, 2, \cdots N\}$, represent the N items of the dataset.

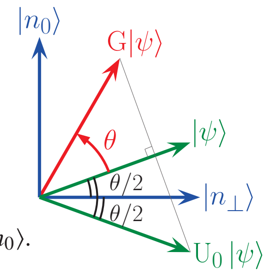
From a quantum implementation of the test function $f(\cdot)$, it is possible to obtain a **quantum oracle** as the unitary operator U_0 realizing $\mathsf{U}_0 |n\rangle = (-1)^{f(n)} |n\rangle$ for any $n \in \{1, 2, \cdots N\}$.
Thus, the quantum oracle returns its response by reversing the sign of $|n\rangle$ when n is the solution n_0, while no change of sign occurs to $|n\rangle$ when n is not the solution.
Equivalently $\mathsf{U}_0 = \mathrm{I}_N - 2|n_0\rangle\langle n_0|$, although $|n_0\rangle$ need not be known, but only $f(\cdot)$ evaluable.

The quantum oracle is able to respond to a superposition of input query states $|n\rangle$ in a single interrogation, for instance to a superposition like $|\psi\rangle = N^{-1/2} \sum_{n=1}^{N} |n\rangle$.

Upon measuring $|\psi\rangle$, any specific item $|n_1\rangle$ would be obtained as measurement outcome with the probability $|\langle n_1|\psi\rangle|^2 = 1/N$, since $\langle n_1|\psi\rangle = 1/\sqrt{N}$ for any $n_1 \in \{1, 2, \cdots N\}$.

Instead, as measurement outcome, we would like to obtain the solution $|n_0\rangle$ with probability 1.

Grover quantum search algorithm (3/4)



- Let $|n_\perp\rangle = \dfrac{1}{\sqrt{N-1}} \sum_{n \neq n_0}^{N} |n\rangle$ normalized state $\perp |n_0\rangle$

$\Longrightarrow |\psi\rangle = N^{-1/2} \sum_{n=1}^{N} |n\rangle$ is in plane $\big(|n_0\rangle, |n_\perp\rangle\big)$.

- With the oracle $\mathsf{U}_0 = \mathrm{I}_N - 2|n_0\rangle\langle n_0| \Longrightarrow \mathsf{U}_0 |n_\perp\rangle = |n_\perp\rangle$ and $\mathsf{U}_0 |n_0\rangle = -|n_0\rangle$.
So in plane $\big(|n_0\rangle, |n_\perp\rangle\big)$, the operator U_0 performs a reflection about $|n_\perp\rangle$.

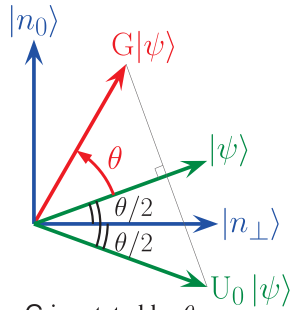
- Let $|\psi_\perp\rangle$ normalized state $\perp |\psi\rangle$ in plane $\big(|n_0\rangle, |n_\perp\rangle\big)$.

- Define the unitary operator $\mathsf{U}_\psi = 2|\psi\rangle\langle\psi| - \mathrm{I}_N \Longrightarrow \mathsf{U}_\psi |\psi\rangle = |\psi\rangle$ and $\mathsf{U}_\psi |\psi_\perp\rangle = -|\psi_\perp\rangle$.
So in plane $\big(|n_0\rangle, |n_\perp\rangle\big)$, the operator U_ψ performs a reflection about $|\psi\rangle$.

- In plane $\big(|n_0\rangle, |n_\perp\rangle\big)$, the composition of two reflections is a rotation $\mathsf{U}_\psi \mathsf{U}_0 = \mathsf{G}$ (Grover amplification operator). It verifies $\mathsf{G}|n_0\rangle = \mathsf{U}_\psi \mathsf{U}_0 |n_0\rangle = -\mathsf{U}_\psi |n_0\rangle = |n_0\rangle - \dfrac{2}{\sqrt{N}} |\psi\rangle$.

The rotation angle θ between $|n_0\rangle$ and $\mathsf{G}|n_0\rangle$, via the scalar product of $|n_0\rangle$ and $\mathsf{G}|n_0\rangle$, verifies
$\cos(\theta) = \langle n_0|\mathsf{G}|n_0\rangle = 1 - \dfrac{2}{N} \approx 1 - \dfrac{\theta^2}{2} \Longrightarrow \theta \approx \dfrac{2}{\sqrt{N}}$ at $N \gg 1$.

Grover quantum search algorithm (4/4)



- In plane $\big(|n_0\rangle, |n_\perp\rangle\big)$, the rotation $\mathsf{G} = \mathsf{U}_\psi \mathsf{U}_0$ is with angle $\theta \approx \dfrac{2}{\sqrt{N}}$.

- $\mathsf{G}|\psi\rangle = \mathsf{U}_\psi \mathsf{U}_0 |\psi\rangle = \mathsf{U}_\psi\Big(|\psi\rangle - \dfrac{2}{\sqrt{N}}|n_0\rangle\Big) = \Big(1 - \dfrac{4}{N}\Big)|\psi\rangle + \dfrac{2}{\sqrt{N}}|n_0\rangle$.
So after rotation by θ the rotated state $\mathsf{G}|\psi\rangle$ is closer to $|n_0\rangle$.

- $\mathsf{G}|\psi\rangle$ remains in plane $\big(|n_0\rangle, |n_\perp\rangle\big)$, and any state in plane $\big(|n_0\rangle, |n_\perp\rangle\big)$ by G is rotated by θ.

So $\mathsf{G}^2|\psi\rangle$ rotates $|\psi\rangle$ by 2θ toward $|n_0\rangle$, and $\mathsf{G}^k|\psi\rangle$ rotates $|\psi\rangle$ by $k\theta$ toward $|n_0\rangle$.

- The angle Θ of $|\psi\rangle$ and $|n_0\rangle$ is such that $\cos(\Theta) = \langle n_0|\psi\rangle = 1/\sqrt{N} \Longrightarrow \Theta = \mathrm{acos}\big(1/\sqrt{N}\big)$.

- So $K = \dfrac{\Theta}{\theta} \approx \dfrac{\sqrt{N}}{2} \mathrm{acos}\big(1/\sqrt{N}\big)$ iterations of G rotate $|\psi\rangle$ onto $|n_0\rangle$.
At most $\Theta = \dfrac{\pi}{2}$ (when $N \gg 1$) $\Longrightarrow$ at most $K \approx \dfrac{\pi}{4}\sqrt{N}$.

- So when the state $\mathsf{G}^K|\psi\rangle \approx |n_0\rangle$ is measured, the probability is almost 1 to obtain $|n_0\rangle$.
$\Longrightarrow$ The searched item $|n_0\rangle$ is found with $O(\sqrt{N})$ interrogations instead of $O(N)$ classically.

Other quantum algorithms

• Shor factoring algorithm (1994) :

Finds the prime factors of an integer with a complexity polynomial in its size, instead of exponential classically.

$15 = 3 \times 5$, with spin-1/2 nuclei (Vandersypen *et al.*, Nature 2001).

$21 = 3 \times 7$, with photons (Martín-López *et al.*, Nature Photonics 2012).

$35 = 5 \times 7$, on IBM Q processor (Amico *et al.*, Phys. Rev. A 2019).

• https://quantumalgorithmzoo.org

"A comprehensive catalog of quantum algorithms . . . "

Quantum cryptography

• The problem of cryptography

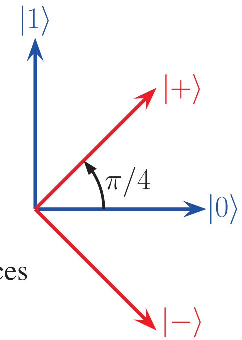
Message X, a string of bits.
Cryptographic key K, a completely random string of bits with proba. $1/2$ and $1/2$.

The cryptogram or encrypted message $C(X, K) = X \oplus K$ (encrypted string of bits).
This is Vernam cipher or one-time pad,
with provably perfect security, since mutual information $I(C; X) = H(X) - H(X|C) = 0$.

Problem : establishing a secret (private) key
between emitter (Alice) and receiver (Bob).

With quantum signals,
any measurement by an eavesdropper (Eve) disturbs the system,
and hence reveals the eavesdropping, and also certifies perfect security conditions.

• BB84 protocol (Bennett & Brassard 1984)



♦ Alice has a string of $4N$ random bits. She encodes with a qubit in a basis state either from $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ randomly chosen for each bit.

♦ Then Bob chooses to measure each received qubit either in basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ so as to decode each transmitted bit.

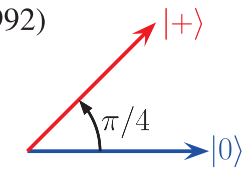
♦ When the whole string of $4N$ bits has been transmitted, Alice and Bob publicly disclose the sequence of their basis choices to identify where they coincide.

♦ Alice and Bob keep only the positions where their basis choices coincide, and they obtain a shared secret key of length approximately $2N$.

♦ If Eve intercepts Alice's qubit, she cannot make a copy (no-cloning theorem). She has to measure (and destroy) it, and forward to Bob a qubit in her known measured state. Roughly half of the time Eve forwards an incorrect state. From this Bob half of the time decodes an incorrect bit value.

♦ From their $2N$ coinciding bits, Alice and Bob classically exchange N bits at random. In case of eavesdropping, around $N/4$ of these N test bits will differ. If all N test bits coincide, then the remaining N bits form the shared secret key.

• B92 protocol with two nonorthogonal states (Bennett 1992)



♦ To encode the bit a Alice uses a qubit in state $|0\rangle$ if $a = 0$ and in state $|+\rangle = \big(|0\rangle + |1\rangle\big)/\sqrt{2}$ if $a = 1$.

♦ Bob, depending on a random bit a' he generates, measures each received qubit either in basis $\{|0\rangle, |1\rangle\}$ if $a' = 0$ or in $\{|+\rangle, |-\rangle\}$ if $a' = 1$. From his measurement, Bob obtains the result $b = 0$ or 1.

♦ Then Bob publishes his series of b, and agrees with Alice to keep only those pairs $\{a, a'\}$ for which $b = 1$,
this providing the final secret key a for Alice and $1 - a' = a$ for Bob.
This is granted because $a = a' \Longrightarrow b = 0$ and hence $b = 1 \Longrightarrow a \neq a' = 1 - a$.

♦ A fraction of this secret key can be publicly exchanged between Alice and Bob to verify they exactly coincide, since in case of eavesdropping by interception and resend by Eve, mismatch ensues with probability $1/4$.

N. Gisin, *et al.*; "Quantum cryptography"; *Reviews of Modern Physics* 74 (2002) 145–195.

• Protocol by broadcast of an entangled qubit pair

♦ With an entangled pair, Alice and Bob do not need a quantum channel between them two, and can exchange only classical information to establish their private secret key. Each one of Alice an Bob just needs a quantum channel from a common server dispatching entangled qubit pairs prepared in one stereotyped quantum state.

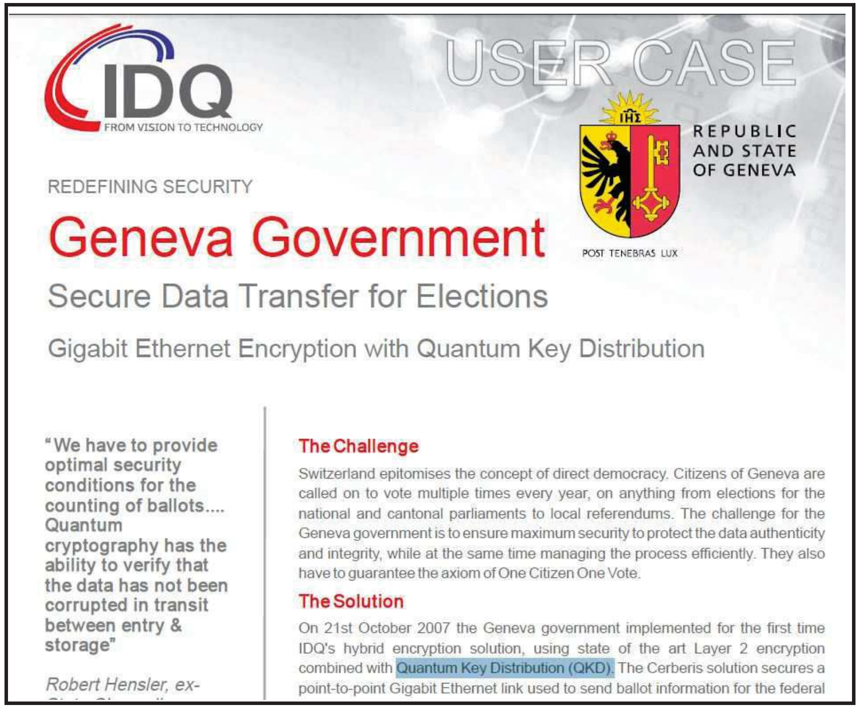
♦ Alice and Bob share a sequence of entangled qubit pairs all prepared in the same entangled (Bell) state $|AB\rangle = \big(|00\rangle + |11\rangle\big)/\sqrt{2}$.

♦ Alice and Bob measure their respective qubit of the pair in the basis $\{|0\rangle, |1\rangle\}$, and they always obtain the same result, either 0 or 1 at random with equal probabilities $1/2$.

♦ To prevent eavesdropping, Alice and Bob can switch independently at random to measuring in the basis $\{|+\rangle, |-\rangle\}$, where one also has $|AB\rangle = \big(|{+}{+}\rangle + |{-}{-}\rangle\big)/\sqrt{2}$.
So when Alice and Bob measure in the same basis, they always obtain the same results, either 0 or 1.

♦ Then Alice and Bob publicly disclose the sequence of their basis choices.
The positions where the choices coincide provide the shared secret key.

♦ A fraction of this secret key is extracted to check exact coincidence, since in case of eavesdropping by interception and resend, mismatch ensues with probability $1/4$.


IDQ
FROM VISION TO TECHNOLOGY

USER CASE

REPUBLIC AND STATE OF GENEVA

POST TENEBRAS LUX

REDEFINING SECURITY

Geneva Government

Secure Data Transfer for Elections

Gigabit Ethernet Encryption with Quantum Key Distribution

"We have to provide optimal security conditions for the counting of ballots.... Quantum cryptography has the ability to verify that the data has not been corrupted in transit between entry & storage"

Robert Hensler, ex-

The Challenge

Switzerland epitomises the concept of direct democracy. Citizens of Geneva are called on to vote multiple times every year, on anything from elections for the national and cantonal parliaments to local referendums. The challenge for the Geneva government is to ensure maximum security to protect the data authenticity and integrity, while at the same time managing the process efficiently. They also have to guarantee the axiom of One Citizen One Vote.

The Solution

On 21st October 2007 the Geneva government implemented for the first time IDQ's hybrid encryption solution, using state of the art Layer 2 encryption combined with Quantum Key Distribution (QKD). The Cerberis solution secures a point-to-point Gigabit Ethernet link used to send ballot information for the federal

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

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

université angers

LARIS

"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.

Summary of "Cours 2/5"

- **No cloning** possible of an arbitrary unknown quantum state $|\psi\rangle$ into $|\psi\rangle\,|\psi\rangle$.
- **Parallel computation :** Any (classical) Boolean function from N_{in} bits into N_{out} bits can always be implemented by a quantum circuit (from the Toffoli gate), and executed in parallel on superposed quantum states.
- **Deutsch-Jozsa algorithm (1992) :** classifies Boolean functions from a single parallel evaluation.
- **Superdense coding (1992) & teleportation (1993) :** exploit a shared stereotyped entanglement for enhanced communication.
- **Grover quantum search algorithm (1997) :** searches an unsorted database of N items with $O(\sqrt{N})$ queries instead of $O(N)$ classically.
- **Shor factoring algorithm (1994) :** Finds the prime factors of an integer with a complexity polynomial in its size, instead of exponential classically.
- **Quantum cryptography :** No-cloning theorem and destructive quantum measurement to guarantee secret key distribution (BB84 protocol, or distributed entanglement).

Quantum correlations by entanglement

Quantum correlations by entanglement (1/5)

For any four random binary variables A_1, A_2, B_1, B_2 with values ± 1,
$\Gamma = (A_1 - A_2)B_1 - (A_1 + A_2)B_2 = A_1B_1 - A_2B_1 - A_1B_2 - A_2B_2 = \pm 2$,
because since $A_1, A_2 = \pm 1$, either $(A_1 - A_2)B_1 = 0$ or $(A_1 + A_2)B_2 = 0$,
and in each case the remaining term is ± 2.

So for any probability distribution on (A_1, A_2, B_1, B_2), the average
$\langle\Gamma\rangle = \big\langle A_1B_1 - A_2B_1 - A_1B_2 - A_2B_2\big\rangle = \langle A_1B_1\rangle - \langle A_2B_1\rangle - \langle A_1B_2\rangle - \langle A_2B_2\rangle$
necessarily verifies $-2 \le \langle\Gamma\rangle \le 2$. Bell inequalities (1964).

The binary variables at ± 1 will be obtained (by Alice and Bob) from the results when measuring an entangled qubit pair.

[1] A. Einstein, B. Podolsky, N. Rosen ; "Can quantum-mechanical description of physical reality be considered complete ?"; *Physical Review* 47, 777–780 (1935).

[2] J. S. Bell ; "On the Einstein–Podolsky–Rosen paradox"; *Physics* 1, 195–200 (1964).

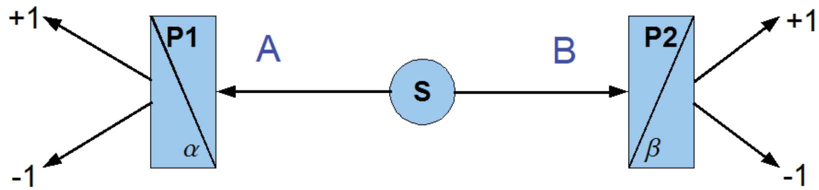
[3] **J. F. Clauser**, M. A. Horne, A. Shimony, R. A. Holt ; "Proposed experiment to test local hidden-variable theories"; *Physical Review Letters* 23, 880–884 (1969).

Quantum correlations by entanglement (2/5)

Alice or Bob gets results ± 1 by measuring qubit observable $\Omega(\theta) = \sin(\theta)\mathsf{X} + \cos(\theta)\mathsf{Z}$,
having eigenvalues ± 1, equivalent to a qubit measurement in the eigenbasis
$\Big\{\, |\lambda_+(\theta)\rangle = [\cos(\theta/2),\ \sin(\theta/2)]^\top, \quad |\lambda_-(\theta)\rangle = [-\sin(\theta/2),\ \cos(\theta/2)]^\top \,\Big\}$.

Alice measures at $\theta = \alpha$ to obtain $A = \pm 1$, and Bob measures at $\theta = \beta$ to obtain $B = \pm 1$,
with the joint probabilities $P(A = \pm 1, B = \pm 1) = \big|\big\langle \lambda_\pm(\alpha) \otimes \lambda_\pm(\beta)\,|\,\psi_{AB}\big\rangle\big|^2$.

Alice and Bob share a qubit pair AB in the entangled state $|\psi_{AB}\rangle = \dfrac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big)$.



Quantum correlations by entanglement (3/5)

$\Longrightarrow$ Joint probabilities

$$P(A=+1, B=+1) = P(A=-1, B=-1) = \frac{1}{4}\big[1-\cos(\alpha-\beta)\big]\,,$$

$$P(A=+1, B=-1) = P(A=-1, B=+1) = \frac{1}{4}\big[1+\cos(\alpha-\beta)\big]\,,$$

and by summation the marginal probabilities

$$P(A=+1) = P(A=-1) = P(B=+1) = P(B=-1) = \frac{1}{2}\,,$$

and the correlation $\langle AB\rangle = -\cos(\alpha-\beta)$,

or alternatively (from p. 15) : $\langle AB\rangle = \langle\psi_{AB}|\Omega(\alpha)\otimes\Omega(\beta)|\psi_{AB}\rangle = -\cos(\alpha-\beta)$.

Quantum correlations by entanglement (4/5)

To obtain four binary variables ± 1 ,
Alice randomly switches between measuring A_1 when $\theta=\alpha_1$ or A_2 when $\theta=\alpha_2$,
Bob randomly switches between measuring B_1 when $\theta=\beta_1$ or B_2 when $\theta=\beta_2$.

For $\langle\Gamma\rangle = \langle A_1B_1\rangle - \langle A_2B_1\rangle - \langle A_1B_2\rangle - \langle A_2B_2\rangle$ one obtains

$$\langle\Gamma\rangle = -\cos(\alpha_1-\beta_1)+\cos(\alpha_2-\beta_1)+\cos(\alpha_1-\beta_2)+\cos(\alpha_2-\beta_2).$$

The choice $\alpha_1=0$, $\alpha_2=\pi/2$ and $\beta_1=3\pi/4$, $\beta_2=\pi/4$ leads to

$$\langle\Gamma\rangle = -\cos(3\pi/4)+\cos(\pi/4)+\cos(\pi/4)+\cos(\pi/4) = 2\sqrt{2} > 2\,.$$

Bell inequalities are violated by quantum correlations !!

Experimentally verified (Aspect *et al.*, Phys. Rev. Let. 1981, 1982.) Nobel 2022

[4] **A. Aspect**, P. Grangier, G. Roger ; "Experimental test of realistic theories via Bell's theorem"; *Physical Review Letters* 47, 460–463 (1981).

Quantum correlations by entanglement (5/5)

- Einstein-Podolsky-Rosen : Quantum mechanics might be incomplete (1935).

[1] A. Einstein, B. Podolsky, N. Rosen ; "Can quantum-mechanical description of physical reality be considered complete ?"; *Physical Review* 47, 777–780 (1935).

- If hidden variables exist $\Longrightarrow$ Bell inequalities are satisfied (1964).
- A. Aspect experiments : Bell inequalities are violated by Reality (1982).

$\Longrightarrow$ No possibility of hidden-variables theories underneath quantum mechanics.

- Quantities that cannot be simultaneously measured (incompatible) have no simultaneous physical existence or reality.
- Correlations between variables obtained from measurements of incompatible quantum quantities on entangled systems, may escape classical constraints.
  $\Longrightarrow$ a resource for information processing.

Physica A 414 (2014) 204–215

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Tsallis entropy for assessing quantum correlation with Bell-type inequalities in EPR experiment

François Chapeau-Blondeau *

Laboratoire Angevin de Recherche en Ingénierie des Systèmes (LARIS), Université d'Angers, 62 avenue Notre Dame du Lac, 49000 Angers, France

HIGHLIGHTS

- A new Bell-type inequality for nonlocal correlation in quantum systems is derived.
- The Tsallis entropy is used as a generalized metric of statistical dependence.
- It is applied to classical outcomes of quantum measurements, as in the EPR setting.
- Superiority and complementarity of the generalized Bell inequality is demonstrated.
- It is able to detect nonlocal quantum correlation from a larger set of observables.

ARTICLE INFO

Article history:
Received 14 April 2014
Received in revised form 13 July 2014
Available online 23 July 2014

Keywords:
Tsallis entropy
Quantum correlation
Bell inequalities
EPR experiment
Quantum information

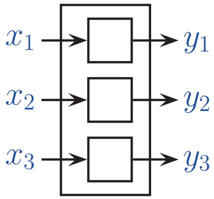
ABSTRACT

A new Bell-type inequality is derived through the use of the Tsallis entropy to quantify the dependence between the classical outcomes of measurements performed on a bipartite quantum system, as typical of an EPR experiment. This new inequality is confronted with standard correlation-based Bell inequalities, and with other known Bell-type inequalities based on the Shannon entropy for which it constitutes a generalization. For an optimal range of the Tsallis order, the new inequality is able to detect nonlocal quantum correlation with measurements from a larger set of quantum observables. In this respect it is more powerful and also complementary compared to the previously known Bell-type inequalities.

GHZ states (1/5) (1989, Greenberger, Horne, Zeilinger) Nobel 2022

3-qubit entangled states.

Three players, each receiving a binary input $x_j = 0/1$, for $j = 1, 2, 3$, with four possible input configurations $x_1x_2x_3 \in \{000, 011, 101, 110\}$.



Each player j responds by a binary output $y_j(x_j) = 0/1$, function only of its own input x_j, for $j = 1, 2, 3$.

Game is won if the players collectively respond according to the input–output matches :

$x_1x_2x_3 = 000 \longrightarrow y_1y_2y_3$ such that $y_1 \oplus y_2 \oplus y_3 = 0$ (conserve parity),

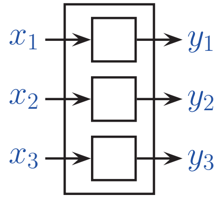
$x_1x_2x_3 \in \{011, 101, 110\} \longrightarrow y_1y_2y_3$ such that $y_1 \oplus y_2 \oplus y_3 = 1$ (reverse parity).

To select their responses $y_j(x_j)$, the players can agree on a collective strategy before, but not after, they have received their inputs x_j.

GHZ states (2/5)

A strategy winning on all four input configurations would consist in three binary functions $y_j(x_j)$ meeting the four constraints :

$$y_1(0) \oplus y_2(0) \oplus y_3(0) = 0$$
$$y_1(0) \oplus y_2(1) \oplus y_3(1) = 1$$
$$y_1(1) \oplus y_2(0) \oplus y_3(1) = 1$$
$$y_1(1) \oplus y_2(1) \oplus y_3(0) = 1$$



$0 \oplus 0 \oplus 0 = 1$, by summation of the four constraints,

$\Longrightarrow$ $0 = 1$, so the four constraints are incompatible.

So no (classical) strategy exists that would win on all four input configurations.
Any (classical) strategy is bound to fail on some input configuration(s).

We show a strategy using quantum resources winning on all four input configurations, (by escaping local realism, $y_j(0) = 0/1$ and $y_j(1) = 0/1$ not existing simultaneously).

GHZ states (3/5)

Before the game starts, each player receives one qubit from a qubit triplet prepared in the entangled state (GHZ state)

$$|\psi\rangle = |\psi_{123}\rangle = \frac{1}{2}\Big(|000\rangle - |011\rangle - |101\rangle - |110\rangle\Big).$$

And the players agree on the common (prior) strategy :
if $x_j = 0$, player j obtains y_j as the outcome of measuring its qubit in basis $\{|0\rangle, |1\rangle\}$,
if $x_j = 1$, player j obtains y_j as the outcome of measuring its qubit in basis $\{|+\rangle, |-\rangle\}$.

We prove this is a winning strategy on all four input configurations :

1) When $x_1x_2x_3 = 000$, the three players measure in $\{|0\rangle, |1\rangle\}$
$\Longrightarrow y_1 \oplus y_2 \oplus y_3 = 0$ is matched.

GHZ states (4/5)

2) When $x_1x_2x_3 = 011$, only player 1 measures in $\{|0\rangle, |1\rangle\}$.

$$|\psi\rangle = \frac{1}{2}\Big(|000\rangle - |011\rangle - |101\rangle - |110\rangle\Big) = \frac{1}{2}\Big[|0\rangle\big(|00\rangle - |11\rangle\big) - |1\rangle\big(|01\rangle + |10\rangle\big)\Big].$$

Since $|0\rangle = \frac{1}{\sqrt{2}}\big(|+\rangle + |-\rangle\big)$, $|1\rangle = \frac{1}{\sqrt{2}}\big(|+\rangle - |-\rangle\big) \Longrightarrow$

$$|00\rangle - |11\rangle = \frac{1}{2}\Big[\big(|+\rangle + |-\rangle\big)\big(|+\rangle + |-\rangle\big) - \big(|+\rangle - |-\rangle\big)\big(|+\rangle - |-\rangle\big)\Big]$$
$$= \frac{1}{2}\Big[\big(|++\rangle + |+-\rangle + |-+\rangle + |--\rangle\big) - \big(|++\rangle - |+-\rangle - |-+\rangle + |--\rangle\big)\Big]$$
$$= |+-\rangle + |-+\rangle ;$$

$$|01\rangle + |10\rangle = \frac{1}{2}\Big[\big(|+\rangle + |-\rangle\big)\big(|+\rangle - |-\rangle\big) + \big(|+\rangle - |-\rangle\big)\big(|+\rangle + |-\rangle\big)\Big] = |++\rangle - |--\rangle ;$$

$$\Longrightarrow |\psi\rangle = \frac{1}{2}\Big(|0+-\rangle + |0-+\rangle - |1++\rangle + |1--\rangle\Big) \Longrightarrow y_1 \oplus y_2 \oplus y_3 = 1 \text{ matched.}$$

GHZ states (5/5)

3) When $x_1x_2x_3 = 101$, only player 2 measures in $\{|0\rangle, |1\rangle\}$.

$$|\psi\rangle = \frac{1}{2}\Big(|000\rangle - |011\rangle - |101\rangle - |110\rangle\Big) = \frac{1}{2}\Big[|{\cdot}0{\cdot}\rangle\Big(|0\cdot 0\rangle - |1\cdot 1\rangle\Big) - |{\cdot}1{\cdot}\rangle\Big(|0\cdot 1\rangle + |1\cdot 0\rangle\Big)\Big]$$

$$= \frac{1}{2}\Big[|{\cdot}0{\cdot}\rangle\Big(|+\cdot -\rangle + |-\cdot +\rangle\Big) - |{\cdot}1{\cdot}\rangle\Big(|+\cdot +\rangle - |-\cdot -\rangle\Big)\Big]$$

$$= \frac{1}{2}\Big(|{+}0{-}\rangle + |{-}0{+}\rangle - |{+}1{+}\rangle + |{-}1{-}\rangle\Big) \Longrightarrow y_1 \oplus y_2 \oplus y_3 = 1 \text{ matched.}$$

4) When $x_1x_2x_3 = 110$, only player 3 measures in $\{|0\rangle, |1\rangle\}$.

$$|\psi\rangle = \frac{1}{2}\Big(|000\rangle - |011\rangle - |101\rangle - |110\rangle\Big) = \frac{1}{2}\Big[\Big(|00\rangle - |11\rangle\Big)|0\rangle - \Big(|01\rangle + |10\rangle\Big)|1\rangle\Big]$$

$$= \frac{1}{2}\Big[\Big(|{+}{-}\rangle + |{-}{+}\rangle\Big)|0\rangle - \Big(|{+}{+}\rangle - |{-}{-}\rangle\Big)|1\rangle\Big]$$

$$= \frac{1}{2}\Big(|+-0\rangle + |-+0\rangle - |++1\rangle + |--1\rangle\Big) \Longrightarrow y_1 \oplus y_2 \oplus y_3 = 1 \text{ matched.}$$

So far,
well defined state vectors (**pure** state),
unitarily evolved,
to represent **closed** or isolated quantum systems.

Next to come,
open quantum systems,
interacting with an uncontrolled environment,
inducing uncertainty to the quantum state (**mixed** state),
and evolving **non-unitarily**,
under **decoherence**.

Density operator (1/3)

Quantum system in (pure) state $|\psi_j\rangle \in \mathcal{H}_N$, measured in an orthonormal basis $\{|n\rangle\}_{n=1}^N$:

$\Longrightarrow$ probability $\Pr\{|n\rangle \big| |\psi_j\rangle\} = |\langle n|\psi_j\rangle|^2 = \langle n|\psi_j\rangle\langle\psi_j|n\rangle$. (nonlinear in the state $|\psi_j\rangle$)

J possible states $|\psi_j\rangle$ with probabilities p_j, $\Big($ with $\sum_{j=1}^{J} p_j = 1\Big)$:

$$\Longrightarrow \Pr\{|n\rangle\} = \sum_{j=1}^{J} p_j \Pr\{|n\rangle \big| |\psi_j\rangle\} = \langle n|\Big(\sum_{j=1}^{J} p_j |\psi_j\rangle\langle\psi_j|\Big)|n\rangle = \langle n|\rho|n\rangle ,$$

with density operator $\rho = \sum_{j=1}^{J} p_j |\psi_j\rangle\langle\psi_j| \in \mathcal{L}(\mathcal{H}_N)$.

and $\Pr\{|n\rangle\} = \langle n|\rho|n\rangle = \mathrm{tr}(\rho|n\rangle\langle n|) = \mathrm{tr}(\rho\,\Pi_n)$. (linear in the state ρ)

The quantum system is in a **mixed** state, corresponding to the statistical ensemble $\big\{\big(p_j, |\psi_j\rangle\big)\big\}$, described by the density operator ρ.

Lemma : For any operator A with trace $\mathrm{tr}(\mathsf{A}) = \sum_n \langle n|\mathsf{A}|n\rangle$, one has
$\mathrm{tr}(\mathsf{A}|\psi\rangle\langle\phi|) = \sum_n \langle n|\mathsf{A}|\psi\rangle\langle\phi|n\rangle = \sum_n \langle\phi|n\rangle\langle n|\mathsf{A}|\psi\rangle = \langle\phi|\big(\sum_n |n\rangle\langle n|\big)\mathsf{A}|\psi\rangle = \langle\phi|\mathsf{A}|\psi\rangle$.

Density operator (2/3)

The statistical ensemble of states $\big\{\big(p_j, |\psi_j\rangle\big)\big\}$ has density operator $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$

$\Longrightarrow \rho = \rho^\dagger$ Hermitian ;

$\forall |\psi\rangle, \langle\psi|\rho|\psi\rangle = \sum_j p_j |\langle\psi|\psi_j\rangle|^2 \geq 0 \Longrightarrow \rho \geq 0$ positive ;

trace $\mathrm{tr}(\rho) = \sum_j p_j \,\mathrm{tr}(|\psi_j\rangle\langle\psi_j|) = \sum_j p_j = 1$.

On $\mathcal{H}_N$, eigen decomposition $\rho = \sum_{n=1}^{N} \lambda_n |\lambda_n\rangle\langle\lambda_n|$, with

eigenvalues $\{\lambda_n\}$ a probability distribution,

eigenstates $\{|\lambda_n\rangle\}$ an orthonormal basis of $\mathcal{H}_N$.

Purity $\mathrm{tr}(\rho^2) = \sum_{n=1}^{N} \lambda_n^2 = 1$ for a pure state, and $\mathrm{tr}(\rho^2) < 1$ for a mixed state.

> A valid density operator on $\mathcal{H}_N \equiv$ any positive operator ρ with unit trace,
> provides a general representation for the state of a quantum system in $\mathcal{H}_N$.

State evolution $|\psi_j\rangle \to \mathsf{U}|\psi_j\rangle \Longrightarrow \big\{\big(p_j, |\psi_j\rangle\big)\big\} \to \big\{\big(p_j, \mathsf{U}|\psi_j\rangle\big)\big\} \Longrightarrow \rho \to \mathsf{U}\rho\mathsf{U}^\dagger$.

Density operator (3/3 another motivation)

A bipartite system AB in a pure (entangled) state $|AB\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$.
Only A is accessible for measurement, with the set of projectors $\{\Pi_m \otimes \mathrm{I}^B\}$.
Probability of outcome m :
$P(m) = \langle AB | \Pi_m \otimes \mathrm{I}^B | AB\rangle = \mathrm{tr}_{AB}\big(\Pi_m \otimes \mathrm{I}^B |AB\rangle\langle AB|\big) = \mathrm{tr}_A\, \mathrm{tr}_B\big(\Pi_m \otimes \mathrm{I}^B |AB\rangle\langle AB|\big)$.

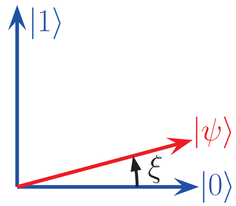
Mathematically $\mathrm{tr}_B\big(\Pi_m \otimes \mathrm{I}^B |AB\rangle\langle AB|\big) = \Pi_m\, \mathrm{tr}_B\big(|AB\rangle\langle AB|\big) = \Pi_m \rho_A$,
with $\rho_A = \mathrm{tr}_B\big(|AB\rangle\langle AB|\big)$ a density operator (positive unit-trace) on $\mathcal{H}^A$,
which alone determines the measurement probabilities $P(m) = \mathrm{tr}_A\big(\Pi_m \rho_A\big)$.

$\Longrightarrow$ A density operator ρ_A arises to describe a system A entangled to an unobserved (unaccessed) environment B.

System A entangled to its environment B has no definite pure state of its own, but an uncertain or mixed state describable by ρ_A.

Classical analog : Joint (A, B) with hidden B described by marginal distribution $P(A) = \sum_B P(A, B)$.

Noisy preparation

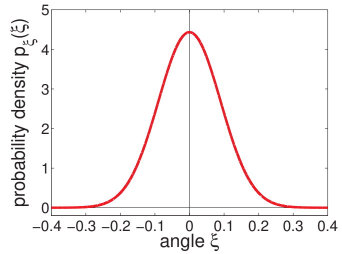


Noise-free preparation of a qubit $|\psi\rangle = |0\rangle$.

Noisy preparation $|\psi\rangle = \cos(\xi)\,|0\rangle + \sin(\xi)\,|1\rangle$
with probability density $p_\xi(\xi)$ (assumed even).

Density operator $\rho = \displaystyle\int_\xi p_\xi(\xi)\, |\psi\rangle\langle\psi|\, d\xi$

$\Longrightarrow \rho = \big\langle \cos^2(\xi) \big\rangle\, |0\rangle\langle 0| + \big\langle \sin^2(\xi)\big\rangle\, |1\rangle\langle 1|$.



Measurement : $\Pr\{|0\rangle \,|\, \rho\} = \langle 0|\rho|0\rangle = \big\langle \cos^2(\xi)\big\rangle$,
$\Pr\{|1\rangle \,|\, \rho\} = \langle 1|\rho|1\rangle = \big\langle \sin^2(\xi)\big\rangle$.

Similar to the statistical ensemble $\Big\{\big(\langle\cos^2(\xi)\rangle, |0\rangle\big), \big(\langle\sin^2(\xi)\rangle, |1\rangle\big)\Big\}$.

Average of an observable

A quantum system in $\mathcal{H}_N$ has observable $\Omega \in \mathcal{L}(\mathcal{H}_N)$ vector space of operators on $\mathcal{H}_N$.

- In pure state $|\psi_j\rangle$: from p. 15 :
  average $\langle\Omega\rangle_j = \langle\psi_j|\Omega|\psi_j\rangle = \mathrm{tr}\big(\Omega\, |\psi_j\rangle\langle\psi_j|\big)$ nonlinear in $|\psi_j\rangle$, but linear in $|\psi_j\rangle\langle\psi_j|$.

- In statistical ensemble $\big\{\big(p_j, |\psi_j\rangle\big)\big\}$ of density operator $\rho = \sum_j p_j\, |\psi_j\rangle\langle\psi_j|$:
  average $\langle\Omega\rangle = \sum_j p_j \langle\Omega\rangle_j = \sum_j p_j\, \mathrm{tr}\big(\Omega\, |\psi_j\rangle\langle\psi_j|\big) = \mathrm{tr}\Big(\Omega \sum_j p_j\, |\psi_j\rangle\langle\psi_j|\Big) = \mathrm{tr}(\Omega\rho)$.

Density operator for the qubit

$\{\sigma_0 = \mathrm{I}_2, \sigma_x, \sigma_y, \sigma_z\}$ a basis of $\mathcal{L}(\mathcal{H}_2)$ (with Pauli operators from p. 19),
orthogonal for the Hilbert-Schmidt inner product $\mathrm{tr}(\mathsf{A}^\dagger \mathsf{B})$.

Any $\rho = \dfrac{1}{2}\big(\mathrm{I}_2 + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z\big) = \dfrac{1}{2}\big(\mathrm{I}_2 + \vec{r}\cdot\vec{\sigma}\big)$.

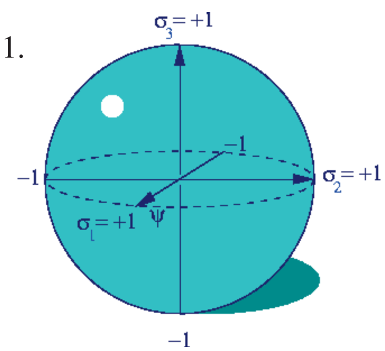
$\Longrightarrow \mathrm{tr}(\rho) = 1$.

$\rho = \rho^\dagger \Longrightarrow r_x = r_x^*,\ \ r_y = r_y^*,\ \ r_z = r_z^* \Longrightarrow r_x, r_y, r_z$ real.

Eigenvalues $\lambda_\pm = \dfrac{1}{2}\big(1 \pm \|\vec{r}\|\big) \geq 0 \Longrightarrow \|\vec{r}\| \leq 1$.

$\|\vec{r}\| = 1$ for pure states,
$\|\vec{r}\| < 1$ for mixed states.

$\vec{r} = [r_x, r_y, r_z]^\top$ Bloch vector for ρ,
in Bloch ball of $\mathbb{R}^3$.



Observables of the qubit

Any operator on $\mathcal{H}_2$ has general form $\mathsf{A} = a_0 \mathrm{I}_2 + \vec{a} \cdot \vec{\sigma}$,
with determinant $\det(\mathsf{A}) = a_0^2 - \vec{a}^2$, two eigenvalues $a_0 \pm \sqrt{\vec{a}^2}$,
and two projectors on the two eigenstates $|\pm\vec{a}\rangle\langle\pm\vec{a}| = \frac{1}{2}\big(\mathrm{I}_2 \pm \vec{a} \cdot \vec{\sigma} / \sqrt{\vec{a}^2}\big)$.

For $\mathsf{A} \equiv \Omega$ an observable, Ω Hermitian requires $a_0 \in \mathbb{R}$ and $\vec{a} = [a_x, a_y, a_z]^\top \in \mathbb{R}^3$.

Probabilities $\Pr\big\{|\pm\vec{a}\rangle\big\} = \langle \pm\vec{a}|\rho|\pm\vec{a}\rangle = \mathrm{tr}\big(|\pm\vec{a}\rangle\langle\pm\vec{a}|\rho\big) = \frac{1}{2}\left(1 \pm \vec{r}\,\frac{\vec{a}}{\|\vec{a}\|}\right)$

when measuring a qubit in state $\rho = \frac{1}{2}\big(\mathrm{I}_2 + \vec{r} \cdot \vec{\sigma}\big)$. ($\Longrightarrow a_0$ has no effect on $\Pr\{|\pm\vec{a}\rangle\}$).

An important observable measurable on the qubit is $\Omega = \vec{a} \cdot \vec{\sigma}$ with $\|\vec{a}\| = 1$,
known as a spin measurement in the direction $\vec{a}$ of $\mathbb{R}^3$,
yielding as possible outcomes the two eigenvalues $\pm\|\vec{a}\| = \pm 1$, with $\Pr\{\pm 1\} = \frac{1}{2}\big(1 \pm \vec{r}\vec{a}\big)$.

Lemma : For any $\vec{r}$ and $\vec{a}$ in $\mathbb{R}^3$, one has : $(\vec{r} \cdot \vec{\sigma})(\vec{a} \cdot \vec{\sigma}) = (\vec{r}\vec{a})\,\mathrm{I}_2 + i\,(\vec{r} \times \vec{a}) \cdot \vec{\sigma}$.

A consequence : $\mathsf{A}' = a_0' \mathrm{I}_2 + \vec{a}' \cdot \vec{\sigma} \Longrightarrow \mathsf{A}\mathsf{A}' = (a_0 a_0' + \vec{a}\,\vec{a}')\mathrm{I}_2 + (a_0'\vec{a} + a_0\vec{a}' + i\,\vec{a} \times \vec{a}') \cdot \vec{\sigma}$.

Generalized measurement of a state $|\psi\rangle \in \mathcal{H}_N$

• **Standard von Neumann projective measurement :** Defined by
a set of N orthogonal projectors $\Pi_n = |n\rangle\langle n| \in \mathcal{L}(\mathcal{H}_N)$, satisfying $\sum_{n=1}^N \Pi_n^\dagger \Pi_n = \mathrm{I}_N$,
with N outcomes of probability $P(n) = \big\|\Pi_n|\psi\rangle\big\|^2 = \langle\psi|\Pi_n^\dagger\Pi_n|\psi\rangle = \mathrm{tr}\big(|\psi\rangle\langle\psi|\,\Pi_n^\dagger\Pi_n\big)$,
and post-measurement state $|\phi_n^{\mathrm{post}}\rangle = \dfrac{\Pi_n|\psi\rangle}{\big\|\Pi_n|\psi\rangle\big\|} = \dfrac{\Pi_n|\psi\rangle}{\sqrt{P(n)}} = |n\rangle$.

Moreover $\sum_{n=1}^N P(n) = 1\,, \forall\,|\psi\rangle \Longleftrightarrow \sum_{n=1}^N \Pi_n^\dagger\Pi_n = \mathrm{I}_N$.

For a mixed state $\rho \in \mathcal{L}(\mathcal{H}_N)$: probability $P(n) = \mathrm{tr}\big(\rho\Pi_n^\dagger\Pi_n\big)$ and $\rho_n^{\mathrm{post}} = \dfrac{\Pi_n\rho\Pi_n^\dagger}{P(n)} = |n\rangle\langle n|$.

• **Generalized measurement :** Defined by
a set of M measurement operators $\mathsf{M}_m \in \mathcal{L}(\mathcal{H}_N)$ satisfying $\sum_{m=1}^M \mathsf{M}_m^\dagger\mathsf{M}_m = \mathrm{I}_N$,
with M outcomes of probability $P(m) = \big\|\mathsf{M}_m|\psi\rangle\big\|^2 = \langle\psi|\mathsf{M}_m^\dagger\mathsf{M}_m|\psi\rangle = \mathrm{tr}\big(|\psi\rangle\langle\psi|\,\mathsf{M}_m^\dagger\mathsf{M}_m\big)$,
and post-measurement state $|\phi_m^{\mathrm{post}}\rangle = \dfrac{\mathsf{M}_m|\psi\rangle}{\big\|\mathsf{M}_m|\psi\rangle\big\|} = \dfrac{\mathsf{M}_m|\psi\rangle}{\sqrt{P(m)}}$.

Moreover $\sum_{m=1}^M P(m) = 1\,, \forall\,|\psi\rangle \Longleftrightarrow \sum_{m=1}^M \mathsf{M}_m^\dagger\mathsf{M}_m = \mathrm{I}_N$.

For a mixed state $\rho \in \mathcal{L}(\mathcal{H}_N)$: probability $P(m) = \mathrm{tr}\big(\rho\mathsf{M}_m^\dagger\mathsf{M}_m\big)$ and $\rho_m^{\mathrm{post}} = \dfrac{\mathsf{M}_m\rho\mathsf{M}_m^\dagger}{P(m)}$.

Justification for the generalized measurement

State $|\psi\rangle \in \mathcal{H}_N$ coupled to an auxiliary M-dimensional space $\mathcal{H}_M$ by

$$|\psi\rangle \otimes |e_0\rangle \xrightarrow{\ \mathsf{U}\ } \mathsf{U}|\psi\rangle \otimes |e_0\rangle = \sum_{m=1}^M \mathsf{M}_m|\psi\rangle \otimes |m\rangle \ ,$$

with arbitrary state $|e_0\rangle \in \mathcal{H}_M$ and $\{|m\rangle\}_{m=1}^M$ an orthonormal basis of $\mathcal{H}_M$.
Operator U from $\mathcal{H}_N \otimes \mathcal{H}_M$ onto $\mathcal{H}_N \otimes \mathcal{H}_M$ is a valid unitary, as it conserves inner product :

$$\big(\mathsf{U}|\psi_1\rangle \otimes |e_0\rangle, \mathsf{U}|\psi_2\rangle \otimes |e_0\rangle\big) = \sum_{m=1}^M \sum_{m'=1}^M \langle\psi_1|\mathsf{M}_m^\dagger\mathsf{M}_{m'}|\psi_2\rangle\langle m|m'\rangle = \langle\psi_1|\sum_{m=1}^M \mathsf{M}_m^\dagger\mathsf{M}_m|\psi_2\rangle = \langle\psi_1|\psi_2\rangle \ .$$

Nothing is done in $\mathcal{H}_N$, while in $\mathcal{H}_M$ a standard VN projective measurement
by M projectors $\mathrm{I}_N \otimes |m\rangle\langle m|$ on the pre-measurement state $\mathsf{U}|\psi\rangle \otimes |e_0\rangle$,
yields $\mathsf{M}_m|\psi\rangle \otimes |m\rangle$ of squared norm $\big\|\mathsf{M}_m|\psi\rangle \otimes |m\rangle\big\|^2 = \langle\psi|\mathsf{M}_m^\dagger\mathsf{M}_m|\psi\rangle = P(m)$,
and post-measurement state $\dfrac{\mathsf{M}_m|\psi\rangle}{\sqrt{P(m)}} \otimes |m\rangle$ separable between $\mathcal{H}_N$ and $\mathcal{H}_M$.

The standard VN projective measurement in $\mathcal{H}_M$ with M outcomes, realizes the generalized measurement in $\mathcal{H}_N$ (thanks to the entanglement by U).

Information quantique, calcul quantique :

Une introduction pour le traitement du signal.

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

université angers

LARIS

"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.

ÉLYSÉE

31 décembre 2024

VŒUX DU PRÉSIDENT DE LA RÉPUBLIQUE AUX FRANÇAIS.

Mes chers compatriotes,

. . .

Pour que nos enfants vivent mieux que nous, il faut aussi que s'inventent en France et en Europe les technologies et les entreprises qui façonneront le monde de demain, notre avenir, notre croissance : l'intelligence artificielle, les révolutions du quantique, de l'énergie, de la biologie pour ne citer que quelques-uns de ces chantiers.

. . .

Très belle, très heureuse année 2025 à vous et à vos proches.
Vive la République.
Vive la France.

Summary of "Cours 3/5"

- **EPR & GHZ experiments :** Correlations between variables obtained from measurements of incompatible quantum quantities on entangled systems, may escape classical constraints. $\Longrightarrow$ a resource for information processing.

- **Density operator :** positive unit-trace $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$ or $\rho_A = \mathrm{tr}_B\big(|AB\rangle\langle AB|\big)$.
For qubit $\rho = \big(\mathrm{I}_2 + \vec{r}\cdot\vec{\sigma}\big)/2$ with in $\mathbb{R}^3$: $\|\vec{r}\| = 1$ pure states, $\|\vec{r}\| < 1$ mixed states.

- **Generalized measurement :** Defined by
a set of M measurement operators $\mathsf{M}_m \in \mathcal{L}(\mathcal{H}_N)$ satisfying $\sum_{m=1}^{M} \mathsf{M}_m^\dagger \mathsf{M}_m = \mathrm{I}_N$,
with M outcomes of probability $P(m) = \big\|\mathsf{M}_m|\psi\rangle\big\|^2 = \langle\psi|\mathsf{M}_m^\dagger\mathsf{M}_m|\psi\rangle = \mathrm{tr}\big(|\psi\rangle\langle\psi|\mathsf{M}_m^\dagger\mathsf{M}_m\big)$,
and post-measurement state $|\phi_m^{\text{post}}\rangle = \dfrac{\mathsf{M}_m|\psi\rangle}{\big\|\mathsf{M}_m|\psi\rangle\big\|} = \dfrac{\mathsf{M}_m|\psi\rangle}{\sqrt{P(m)}}$.

For a mixed state $\rho \in \mathcal{L}(\mathcal{H}_N)$: probability $P(m) = \mathrm{tr}\big(\rho\mathsf{M}_m^\dagger\mathsf{M}_m\big)$ and $\rho_m^{\text{post}} = \dfrac{\mathsf{M}_m\rho\mathsf{M}_m^\dagger}{P(m)}$.

Standard von Neumann projective measurement :
N orthogonal projectors $\mathsf{M}_n = \Pi_n = |n\rangle\langle n|$ acting in $\mathcal{H}_N$.

Purification of a mixed state

A quantum system A of N-dimensional space $\mathcal{H}^A \equiv \mathcal{H}_N$ prepared in the statistical ensemble $\big\{\big(p_j, |\psi_j\rangle\big)\big\}_{j=1}^{J}$ is represented by the density operator $\rho_A = \sum_{j=1}^{J} p_j |\psi_j\rangle\langle\psi_j|$.

Auxiliary system B of J-dimensional space $\mathcal{H}^B \equiv \mathcal{H}_J$ and orthonormal basis $\big\{|j\rangle\big\}_{j=1}^{J}$.

The bipartite system AB prepared in the pure entangled state $|AB\rangle = \sum_{j=1}^{J} \sqrt{p_j}\,|\psi_j\rangle \otimes |j\rangle$
realizes a purification of ρ_A since $\mathrm{tr}_B\big(|AB\rangle\langle AB|\big) = \rho_A$.

Classical analog : Joint (A, B) with hidden B described by marginal distribution $P(A) = \sum_B P(A, B)$.

$\Longrightarrow$ Statistical ensemble and reduction by partial tracing are two alternative representations always available for a given density operator.

Uncertainty on A, with a pure turned into a mixed state, by its entanglement with unaccessed environment B $\equiv$ quantum **decoherence** or quantum noise.

Positive operator-valued measure (POVM)

For the generalized measurement $\{\mathsf{M}_m\}_{m=1}^{M}$ acting in $\mathcal{H}_N$,

when the post-measurement states $\rho_m^{\text{post}} = \mathsf{M}_m \rho \mathsf{M}_m^\dagger / P(m)$ are not needed,

the probabilities $P(m) = \mathrm{tr}\big(\rho \mathsf{M}_m^\dagger \mathsf{M}_m\big) = \mathrm{tr}\big(\rho \mathsf{E}_m\big)$, are determined by the M

positive operators $\mathsf{E}_m = \mathsf{M}_m^\dagger \mathsf{M}_m$ of $\mathcal{L}(\mathcal{H}_N)$, satisfying $\sum_{m=1}^{M} \mathsf{E}_m = \mathrm{I}_N$.

The set $\{\mathsf{E}_m\}_{m=1}^{M}$ defines a POVM, with M elements E_m.

When a POVM $\{\mathsf{E}_m\}_{m=1}^{M}$ is fixed, the set of M measurement operators $\mathsf{M}_m = \sqrt{\mathsf{E}_m}$ verifies $\mathsf{M}_m^\dagger \mathsf{M}_m = \mathsf{E}_m$ and offers one possibility for a physical implementation of the measurement.

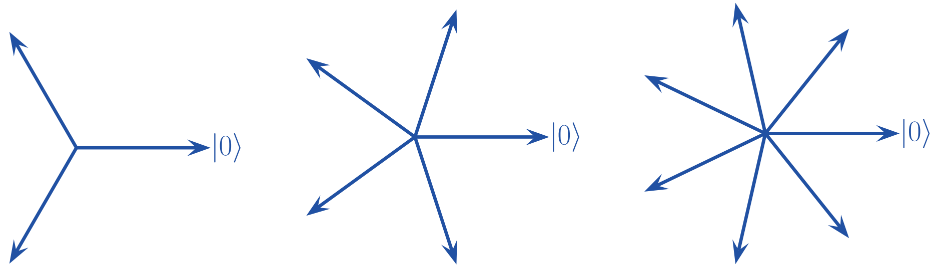
Often, the optimization of statistical performance criteria from the measurement results, fixes or imposes or constrains, the POVM only.

A generalized measurement and POVM for the qubit

Operators of $\mathcal{L}(\mathcal{H}_2)$: $\left\{\mathsf{M}_m = \sqrt{\frac{2}{M}}\, |e_m\rangle\langle e_m|\right\}$ and POVM $\left\{\mathsf{E}_m = \frac{2}{M} |e_m\rangle\langle e_m|\right\}$,

for $m = 0, 1, \ldots M-1$, and $M > 2$,

with $|e_m\rangle = \cos\left(2\pi\frac{m}{M}\right)|0\rangle + \sin\left(2\pi\frac{m}{M}\right)|1\rangle$:



$M = 3$ $\quad M = 5$ $\quad M = 7$

Open quantum systems and quantum noise (1/3)

A quantum system Q interacting (so as to entangle) with its environment E represents an open quantum system.

When the environment E is uncontrolled and unobserved, its entanglement to Q induces uncertainty on the state of Q, or decoherence, acting also as a quantum noise.
As a result, Q undergoes a nonunitary evolution.

At the onset of the interaction, Q is in state $\rho \in \mathcal{L}(\mathcal{H}_N)$ and E in state $|e_0\rangle$.
The compound QE can be considered as a closed or isolated system,
starting in the joint state $\rho \otimes |e_0\rangle\langle e_0|$,
and undergoing a unitary evolution by U_{QE} as $\rho \otimes |e_0\rangle\langle e_0| \longmapsto \mathsf{U}_{QE}\big(\rho \otimes |e_0\rangle\langle e_0|\big)\mathsf{U}_{QE}^\dagger$.

At the end of the interaction, a density operator can be obtained for Q
by the partial trace over the environment E as $\mathcal{N}(\rho) = \mathrm{tr}_E\big(\mathsf{U}_{QE}(\rho \otimes |e_0\rangle\langle e_0|)\mathsf{U}_{QE}^\dagger\big)$.

Open quantum systems and quantum noise (2/3)

To compute $\mathrm{tr}_E(\cdot)$ let $\{|e_k\rangle\}_{k=1}^{K}$ an orthonormal basis for the environment E, giving

$$\mathcal{L}(\mathcal{H}_N) \ni \rho \longmapsto \mathcal{N}(\rho) = \sum_{k=1}^{K} \left\langle e_k \middle| \mathsf{U}_{QE}\big(\rho \otimes |e_0\rangle\langle e_0|\big)\mathsf{U}_{QE}^\dagger \middle| e_k \right\rangle \in \mathcal{L}(\mathcal{H}_N) .$$

Define K operators Λ_k from $\mathcal{H}_N$ onto $\mathcal{H}_N$ as the partial inner product
$\Lambda_k = \langle e_k|\, \mathsf{U}_{QE}\, |e_0\rangle \in \mathcal{L}(\mathcal{H}_N)$.

This is equivalent to $\Lambda_k |Q\rangle = \langle e_k|\, \mathsf{U}_{QE}\, |Q\rangle \otimes |e_0\rangle$ for any $|Q\rangle \in \mathcal{H}_N$,
or $\langle Q'|\Lambda_k|Q\rangle = \langle e_k| \otimes \langle Q'|\, \mathsf{U}_{QE}\, |Q\rangle \otimes |e_0\rangle$, and $\Lambda_k \rho \Lambda_k^\dagger = \left\langle e_k \middle| \mathsf{U}_{QE}\big(\rho \otimes |e_0\rangle\langle e_0|\big)\mathsf{U}_{QE}^\dagger \middle| e_k \right\rangle$,

yielding $\mathcal{N}(\rho) = \sum_{k=1}^{K} \Lambda_k \rho \Lambda_k^\dagger$. (operator-sum representation of the evolution of ρ)

The Λ_k are the Kraus operators.
Since $\mathrm{tr}_Q\big(\mathcal{N}(\rho)\big) = \mathrm{tr}_Q\big(\mathrm{tr}_E(\cdots)\big) = 1, \forall \rho \Longrightarrow \sum_{k=1}^{K} \Lambda_k^\dagger \Lambda_k = \mathrm{I}_N$ and $\mathcal{N}(\cdot)$ is trace-preserving.

They come with an isometric freedom. They need not be more than N^2 for any quantum evolution $\rho \mapsto \mathcal{N}(\rho)$ from $\mathcal{L}(\mathcal{H}_N)$ into $\mathcal{L}(\mathcal{H}_N)$, whatever the size of the envrionment E.

Open quantum systems and quantum noise (3/3)

General evolution $\rho \in \mathcal{L}(\mathcal{H}_N) \longmapsto \mathcal{N}(\rho) \in \mathcal{L}(\mathcal{H}_N)$ of an open quantum system Q by quantum operation $\rho \longmapsto \mathcal{N}(\rho) = \sum_k \Lambda_k \rho \Lambda_k^\dagger$ (superoperator), with $\sum_k \Lambda_k^\dagger \Lambda_k = \mathrm{I}_N$, representing a (nonunitary) completely positive trace-preserving linear map, requiring no more than N^2 Kraus operators Λ_k of $\mathcal{L}(\mathcal{H}_N)$.

When Q is closed: Only one $\Lambda_k \equiv \mathsf{U}$ for unitary evolution $\rho \longmapsto \mathsf{U}^\dagger \rho \mathsf{U}$.

Probabilistic interpretation : the action of the quantum operation is equivalent to randomly replacing the state ρ by the state $\Lambda_k \rho \Lambda_k^\dagger / \mathrm{tr}\left(\Lambda_k \rho \Lambda_k^\dagger\right) = \rho_k$ with probability $\mathrm{tr}\left(\Lambda_k \rho \Lambda_k^\dagger\right) = p_k$, i.e. to replace ρ by the statistical ensemble $\left\{(p_k, \rho_k)\right\}$ having density operator $\sum_k p_k \rho_k = \sum_k \Lambda_k \rho \Lambda_k^\dagger = \mathcal{N}(\rho)$.

The Kraus operators Λ_k can be guessed or postulated empirically, according to the type of environment and its effect envisaged on the quantum system of interest Q.

Quantum noise on the qubit (1/6)

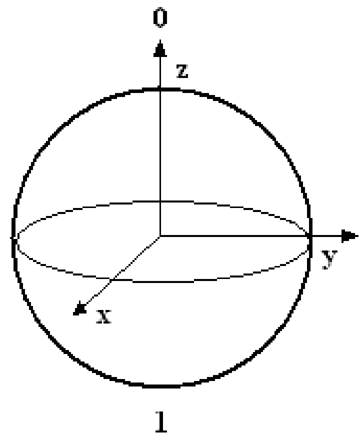
For an arbitrary qubit state defined by $\rho = \frac{1}{2}\left(\mathrm{I}_2 + \vec{r} \cdot \vec{\sigma}\right)$ with $\|\vec{r}\| \leq 1$,

the evolution $\rho \longmapsto \mathcal{N}(\rho) = \sum_k \Lambda_k \rho \Lambda_k^\dagger$,

since every $\Lambda_k = b_k \mathrm{I}_2 + \vec{a}_k \cdot \vec{\sigma}$,

is equivalent to the affine map $\vec{r} \longmapsto A\vec{r} + \vec{c}$,

with A a 3×3 real matrix and $\vec{c}$ a real vector in $\mathbb{R}^3$, mapping the Bloch ball onto itself.



No more than $N^2 = 4$ Kraus operators Λ_k of $\mathcal{L}(\mathcal{H}_2)$ are required.

Quantum noise on the qubit (2/6)

Important quantum noises on a qubit in state ρ can be represented by random applications of some of the 4 Pauli operators $\{\mathrm{I}_2, \sigma_x, \sigma_y, \sigma_z\}$ on the qubit, e.g.

Bit-flip noise : flips the qubit state with probability p by applying σ_x, or leaves the qubit unchanged with probability $1-p$:

Kraus $\Lambda_1 = \sqrt{1-p}\,\mathrm{I}_2$ and $\Lambda_2 = \sqrt{p}\,\sigma_x$,

$$\rho \longmapsto \mathcal{N}(\rho) = (1-p)\rho + p\sigma_x \rho \sigma_x^\dagger, \qquad \vec{r} \longmapsto A\vec{r} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1-2p & 0 \\ 0 & 0 & 1-2p \end{bmatrix} \vec{r}.$$

Examples : • Electronic spin in the earth magnetic field incurring random flips.

• Noisy preparation of the qubit (page 74) :

$|0\rangle \longmapsto |0\rangle$ with probability $\left\langle \cos^2(\xi) \right\rangle = 1-p$,

$|0\rangle \longmapsto |1\rangle = \sigma_x |0\rangle$ with probability $\left\langle \sin^2(\xi) \right\rangle = p$,

representable as a bit-flip noise with probability $p = \left\langle \sin^2(\xi) \right\rangle$.

Quantum noise on the qubit (3/6)

Phase-flip noise : flips the qubit phase with probability p by applying σ_z, or leaves the qubit unchanged with probability $1-p$:

Kraus $\Lambda_1 = \sqrt{1-p}\,\mathrm{I}_2$ and $\Lambda_2 = \sqrt{p}\,\sigma_z$,

$$\rho \longmapsto \mathcal{N}(\rho) = (1-p)\rho + p\sigma_z \rho \sigma_z^\dagger, \qquad \vec{r} \longmapsto A\vec{r} = \begin{bmatrix} 1-2p & 0 & 0 \\ 0 & 1-2p & 0 \\ 0 & 0 & 1 \end{bmatrix} \vec{r}.$$

Example :

Noisy photonic interferometer (page 21) : with a fluctuating phase shift ξ

≡ noise-free interferometer around an average phase shift $\overline{\xi}$,

supplemented by a phase-flip noise with probability $p = \left\langle \sin^2[(\xi - \overline{\xi})/2] \right\rangle$.

Bit-phase-flip noise : $\Lambda_1 = \sqrt{1-p}\,\mathrm{I}_2$ and $\Lambda_2 = \sqrt{p}\,\sigma_y$.

Also Pauli operator $\sigma_y = i\sigma_x\sigma_z = -i\sigma_z\sigma_x$.

Quantum noise on the qubit (4/6)

Depolarizing noise : leaves the qubit unchanged with probability $1-p$, or apply any of σ_x, σ_y or σ_z with equal probability $p/3$:

Kraus $\Lambda_1 = \sqrt{1-p}\,\mathrm{I}_2$, $\Lambda_2 = \sqrt{p/3}\,\sigma_x$, $\Lambda_3 = \sqrt{p/3}\,\sigma_y$ and $\Lambda_4 = \sqrt{p/3}\,\sigma_z$,

$$\rho \longmapsto \mathcal{N}(\rho) = (1-p)\rho + \frac{p}{3}\Big(\sigma_x\rho\sigma_x^\dagger + \sigma_y\rho\sigma_y^\dagger + \sigma_z\rho\sigma_z^\dagger\Big),$$

$$\vec{r} \longmapsto A\vec{r} = \begin{bmatrix} 1-\frac{4}{3}p & 0 & 0 \\ 0 & 1-\frac{4}{3}p & 0 \\ 0 & 0 & 1-\frac{4}{3}p \end{bmatrix}\vec{r}.$$

Can be seen as an equiprobable combination of random bit-flip by σ_x, or phase-flip by σ_z, or bit-phase flip by $\sigma_y = i\sigma_x\sigma_z$.

Quantum noise on the qubit (5/6)

Amplitude damping noise : relaxes the excited state $|1\rangle$ to the ground state $|0\rangle$ with probability γ (for instance by losing a photon) :

$$\rho \longmapsto \mathcal{N}(\rho) = \Lambda_1\rho\Lambda_1^\dagger + \Lambda_2\rho\Lambda_2^\dagger,$$

with $\Lambda_2 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix} = \sqrt{\gamma}\,|0\rangle\langle 1|$ taking $|1\rangle$ to $|0\rangle$ with probability γ,

and $\Lambda_1 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} = |0\rangle\langle 0| + \sqrt{1-\gamma}\,|1\rangle\langle 1|$ which leaves $|0\rangle$ unchanged and reduces the probability amplitude of resting in state $|1\rangle$.

$$\Longrightarrow\ \vec{r} \longmapsto A\vec{r} + \vec{c} = \begin{bmatrix} \sqrt{1-\gamma} & 0 & 0 \\ 0 & \sqrt{1-\gamma} & 0 \\ 0 & 0 & 1-\gamma \end{bmatrix}\vec{r} + \begin{bmatrix} 0 \\ 0 \\ \gamma \end{bmatrix}.$$

Quantum noise on the qubit (6/6)

Generalized amplitude damping noise : interaction of the qubit with a thermal bath at temperature T :

$$\rho \longmapsto \mathcal{N}(\rho) = \Lambda_1\rho\Lambda_1^\dagger + \Lambda_2\rho\Lambda_2^\dagger + \Lambda_3\rho\Lambda_3^\dagger + \Lambda_4\rho\Lambda_4^\dagger,$$

with $\Lambda_1 = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}$, $\Lambda_2 = \sqrt{p}\begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}$, $p, \gamma \in [0, 1]$,

$\Lambda_3 = \sqrt{1-p}\begin{bmatrix} \sqrt{1-\gamma} & 0 \\ 0 & 1 \end{bmatrix}$, $\Lambda_4 = \sqrt{1-p}\begin{bmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{bmatrix}$,

$$\Longrightarrow\ \vec{r} \longmapsto A\vec{r} + \vec{c} = \begin{bmatrix} \sqrt{1-\gamma} & 0 & 0 \\ 0 & \sqrt{1-\gamma} & 0 \\ 0 & 0 & 1-\gamma \end{bmatrix}\vec{r} + \begin{bmatrix} 0 \\ 0 \\ (2p-1)\gamma \end{bmatrix}.$$

Damping $[0, 1] \ni \gamma = 1 - e^{-t/\tau} \to 1$ as the interaction time $t \to \infty$ with the bath of the qubit relaxing to equilibrium $\rho_\infty = p\,|0\rangle\langle 0| + (1-p)\,|1\rangle\langle 1|$, with equilibrium probabilities $p = \exp[-E_0/(k_BT)]/Z$ and $1-p = \exp[-E_1/(k_BT)]/Z$ with $Z = \exp[-E_0/(k_BT)] + \exp[-E_1/(k_BT)]$ governed by the Boltzmann distribution between the two energy levels E_0 of $|0\rangle$ and $E_1 > E_0$ of $|1\rangle$.

$T = 0 \Rightarrow p = 1 \Rightarrow \rho_\infty = |0\rangle\langle 0|$. $T \to \infty \Rightarrow p = 1/2 \Rightarrow \rho_\infty \to (|0\rangle\langle 0| + |1\rangle\langle 1|)/2 = \mathrm{I}_2/2$.

Noise on multiple qubits

On qubit pair AB the noise can often be assumed to act independently on each qubit A, B.

For qubit A, on $\rho_A \in \mathcal{L}(\mathcal{H}_2)$ noise $\mathcal{N}_A(\cdot)$ with K Kraus operators $\Lambda_k \in \mathcal{L}(\mathcal{H}_2)$.

For qubit B, on $\rho_B \in \mathcal{L}(\mathcal{H}_2)$ noise $\mathcal{N}_B(\cdot)$ with K' Kraus operators $\Lambda'_{k'} \in \mathcal{L}(\mathcal{H}_2)$.

For pair AB, on $\rho_{AB} \in \mathcal{L}\big(\mathcal{H}_2^{\otimes 2}\big)$ noise $\mathcal{N}_{AB}(\cdot)$ with KK' Kraus operators $\Lambda_k \otimes \Lambda'_{k'}$ acting as

$$\rho'_{AB} = \mathcal{N}_{AB}(\rho_{AB}) = \mathcal{N}_A \otimes \mathcal{N}_B(\rho_{AB}) = \sum_{k=1}^{K}\sum_{k'=1}^{K'}\big(\Lambda_k \otimes \Lambda'_{k'}\big)\rho_{AB}\big(\Lambda_k^\dagger \otimes \Lambda'^\dagger_{k'}\big).$$

For separable $\rho_{AB} = \rho_A \otimes \rho_B$ then $\rho'_{AB} = \mathcal{N}_{AB}(\rho_{AB}) = \mathcal{N}_A(\rho_A) \otimes \mathcal{N}_B(\rho_B)$.

For entangled ρ_{AB}, decomposition of $\mathcal{N}_{AB}(\rho_{AB})$ in standard basis of $\mathcal{L}\big(\mathcal{H}_2^{\otimes 2}\big)$ via
$\mathcal{N}_{AB}\big(|00\rangle\langle 01|\big) = \mathcal{N}_{AB}\big(|0\rangle\langle 0| \otimes |0\rangle\langle 1|\big) = \mathcal{N}_A\big(|0\rangle\langle 0|\big) \otimes \mathcal{N}_B\big(|0\rangle\langle 1|\big)$,
and similarly for the 16 (separable) basis operators of $\mathcal{L}\big(\mathcal{H}_2^{\otimes 2}\big)$.

Otherwise, correlated noise on AB requires a joint noise model $\mathcal{N}_{AB}(\cdot)$
with Kraus operators acting jointly in $\mathcal{H}_2^{\otimes 2}$, and
not factorizable as tensor products of Kraus operators acting separately in $\mathcal{H}_2$.

More on quantum noise, noisy qubits :

4500 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 61, NO. 8, AUGUST 2015

IEEE TRANSACTIONS ON INFORMATION THEORY

Optimization of Quantum States for Signaling Across an Arbitrary Qubit Noise Channel With Minimum-Error Detection

François Chapeau-Blondeau

Abstract—**For discrimination between two signaling states of a qubit, the optimal detector minimizing the probability of error is applied to the situation where detection has to be performed from a noisy qubit affected by an arbitrary quantum noise separately** inevitable error; and such a general situation is frequent since quantum noise and decoherence are prone to break the orthogonality of two initial quantum states. A meaningful general approach then is to seek the optimal quantum measurement

PHYSICAL REVIEW A **91**, 052310 (2015)

Optimized probing states for qubit phase estimation with general quantum noise

François Chapeau-Blondeau

Laboratoire Angevin de Recherche en Ingénierie des Systèmes (LARIS), Université d'Angers, 62 avenue Notre Dame du Lac, 49000 Angers, France

(Received 27 March 2015; published 12 May 2015)

We exploit the theory of quantum estimation to investigate quantum state estimation in the presence of noise. The quantum Fisher information is used to assess the estimation performance. For the qubit in Bloch representation, general expressions are derived for the quantum score and then for the quantum Fisher information. From this latter expression, it is proved that the Fisher information always increases with the purity of the measured qubit state. An arbitrary quantum noise affecting the qubit is taken into account for its impact on

Quantum state detection or discrimination

for quantum signaling, quantum communication, quantum storage

A quantum system can be in one of two alternative states ρ_0 or ρ_1 with prior probabilities P_0 and $P_1 = 1 - P_0$.

Question : What is the best measuring POVM $\{\mathsf{E}_0, \mathsf{E}_1\}$ to decide with a maximal probability of success P_{suc} ?

Answer : One has $P_{\text{suc}} = P_0 \,\text{tr}(\rho_0 \mathsf{E}_0) + P_1 \,\text{tr}(\rho_1 \mathsf{E}_1) = P_0 + \text{tr}(\mathsf{T}\mathsf{E}_1)$, with the test operator $\mathsf{T} = P_1\rho_1 - P_0\rho_0 = \sum_{n=1}^{N} \lambda_n |\lambda_n\rangle\langle\lambda_n|$.

Then P_{suc} is maximized by $\mathsf{E}_1^{\text{opt}} = \sum_{\lambda_n > 0} |\lambda_n\rangle\langle\lambda_n|$,

the projector on the eigensubspace of T with positive eigenvalues λ_n.

The optimal measurement $\left\{\mathsf{E}_1^{\text{opt}},\ \mathsf{E}_0^{\text{opt}} = \mathrm{I}_N - \mathsf{E}_1^{\text{opt}}\right\}$

achieves the maximum $P_{\text{suc}}^{\max} = \dfrac{1}{2}\left(1 + \sum_{n=1}^{N} |\lambda_n|\right)$. (Helstrom 1976)

Discrimination from noisy qubits

Quantum noise on a qubit in state ρ implements the transformation $\rho \longmapsto \mathcal{N}(\rho)$.

With a noisy qubit, discrimination from $\mathcal{N}(\rho_0)$ and $\mathcal{N}(\rho_1)$.

$\longrightarrow$ Impact • of the preparation $\{\rho_0, \rho_1\}$ (the signaling states),
• and of the quantum noise $\mathcal{N}(\cdot)$ (its type and level),

on the performance $P_{\text{suc}}^{\max}$ of the optimal detector,

F. Chapeau-Blondeau, "Détection quantique optimale sur un qubit bruité", *25ème Colloque GRETSI sur le Traitement du Signal et des Images*, Lyon, France, 8–11 sept. 2015.

in relation to stochastic resonance and enhancement by noise.

F. Chapeau-Blondeau ; "Quantum state discrimination and enhancement by noise" ; *Physics Letters A* 378 (2014) 2128–2136.

N. Gillard, E. Belin, F. Chapeau-Blondeau ; "Qubit state detection and enhancement by quantum thermal noise" ; *Electronics Letters* 54 (2018) 38–39.

Physics Letters A 378 (2014) 2128–2136

Contents lists available at ScienceDirect

ELSEVIER

Physics Letters A

www.elsevier.com/locate/pla

Quantum state discrimination and enhancement by noise

CrossMark

François Chapeau-Blondeau

Laboratoire Angevin de Recherche en Ingénierie des Systèmes (LARIS), Université d'Angers, 62 avenue Notre Dame du Lac, 49000 Angers, France

ARTICLE INFO

Article history:
Received 12 February 2014
Received in revised form 15 May 2014
Accepted 17 May 2014
Available online 27 May 2014
Communicated by C.R. Doering

Keywords:
Quantum state discrimination
Quantum noise
Quantum detection
Signal detection
Enhancement by noise
Stochastic resonance

ABSTRACT

Discrimination between two quantum states is addressed as a quantum detection process where a measurement with two outcomes is performed and a conclusive binary decision results about the state. The performance is assessed by the overall probability of decision error. Based on the theory of quantum detection, the optimal measurement and its performance are exhibited in general conditions. An application is realized on the qubit, for which generic models of quantum noise can be investigated for their impact on state discrimination from a noisy qubit. The quantum noise acts through random application of Pauli operators on the qubit prior to its measurement. For discrimination from a noisy qubit, various situations are exhibited where reinforcement of the action of the quantum noise can be associated with enhanced performance. Such implications of the quantum noise are analyzed and interpreted in relation to stochastic resonance and enhancement by noise in information processing.

Discrimination between $J > 2$ quantum states

A quantum system can be in one of J alternative states ρ_j, for $j = 1$ to J, with prior probabilities P_j with $\sum_{j=1}^{J} P_j = 1$.

Problem : What is the best measuring POVM $\{\mathsf{E}_m\}_{m=1}^{J}$ with J outcomes to decide with a maximal probability of success P_{suc} ?

$$\Longrightarrow \text{Maximize } P_{\text{suc}} = \sum_{j=1}^{J} P_j \operatorname{tr}(\rho_j \mathsf{E}_j) \text{ according to the } J \text{ operators } \mathsf{E}_j\,,$$

$$\text{subject to } \; 0 \le \mathsf{E}_j \le \mathrm{I}_N \quad \text{and} \quad \sum_{j=1}^{J} \mathsf{E}_j = \mathrm{I}_N.$$

For $J > 2$ this problem is only partially solved, in some special cases.
(S. M. Barnett, S. Croke, *Adv. Optics & Photonics*, vol. 1, pp. 238–278, 2009).

Error-free discrimination between $J = 2$ states

Two alternative states ρ_0 or ρ_1 of $\mathcal{H}_N$, with priors P_0 and $P_1 = 1 - P_0$, are not full-rank in $\mathcal{H}_N$, e.g. $\operatorname{supp}(\rho_j) \subset \mathcal{H}_N \iff [\operatorname{supp}(\rho_j)]^{\perp} \equiv \ker(\rho_j) \supset \{\vec{0}\}$.

If $\mathcal{S}_0 = \operatorname{supp}(\rho_0) \cap \equiv \ker(\rho_1) \neq \{\vec{0}\}$, error-free discrimination of ρ_0 is possible.
If $\mathcal{S}_1 = \operatorname{supp}(\rho_1) \cap \equiv \ker(\rho_0) \neq \{\vec{0}\}$, error-free discrimination of ρ_1 is possible.

Necessity to find a three-outcome measurement $\{\mathsf{E}_0, \mathsf{E}_1, \mathsf{E}_{\text{unc}}\}$ ensuring that when E_j is measured, the preparation is certainly ρ_j, for $j = 0, 1$:

Find $0 \le \mathsf{E}_0 \le \mathrm{I}_N$ s.t. $\mathsf{E}_0 = \vec{a}_0 \Pi_1$ "proportional" to Π_1 projector on $\ker(\rho_1) \Rightarrow \operatorname{tr}(\rho_1 \mathsf{E}_0) = 0$,
and $0 \le \mathsf{E}_1 \le \mathrm{I}_N$ s.t. $\mathsf{E}_1 = \vec{a}_1 \Pi_0$ "proportional" to Π_0 projector on $\ker(\rho_0) \Rightarrow \operatorname{tr}(\rho_0 \mathsf{E}_1) = 0$,
and $\mathsf{E}_0 + \mathsf{E}_1 \le \mathrm{I}_N \iff \big[\mathsf{E}_0 + \mathsf{E}_1 + \mathsf{E}_{\text{unc}} = \mathrm{I}_N$ with $0 \le \mathsf{E}_{\text{unc}} \le \mathrm{I}_N\big]$,
maximizing $P_{\text{suc}} = P_0 \operatorname{tr}(\mathsf{E}_0 \rho_0) + P_1 \operatorname{tr}(\mathsf{E}_1 \rho_1)$ $\quad$ ($\equiv \min P_{\text{unc}} = 1 - P_{\text{suc}}$)

This problem is only partially solved, in some special cases,
(Kleinmann *et al.*, J. Mathematical Physics, vol. 51, pp. 032201,1–25, 2010).

Error-free discrimination between $J \ge 2$ states

J alternative states ρ_j of $\mathcal{H}_N$, with prior probabilities P_j, for $j = 1, \cdots, J$;
typically every ρ_j is with defective rank $< N$ (except at most one full rank).

For all $j = 1$ to J, define $\mathcal{S}_j = \operatorname{supp}(\rho_j) \cap \overbrace{\Big\{\bigcap_{\ell \neq j} \ker(\rho_\ell)\Big\}}^{\mathcal{K}_j}$.

For each nontrivial $\mathcal{S}_j \neq \{\vec{0}\}$, then ρ_j can be measured where none other ρ_ℓ can be.
$\Longrightarrow$ Error-free discrimination of ρ_j is possible,
by E_j such that $0 \le \mathsf{E}_j \le \mathrm{I}_N$ and E_j "proportional" to the projector on $\mathcal{K}_j$,
so that when E_j is measured the preparation is certainly $\rho_j \Longrightarrow \operatorname{tr}(\rho_\ell \mathsf{E}_j) = 0$, $\forall \ell \neq j$.

To parametrize E_j, find an orthonormal basis $\{|u_k^j\rangle\}_{k=1}^{\dim(\mathcal{K}_j)}$ of $\mathcal{K}_j$,
then $\mathsf{E}_j = \sum_{k=1}^{\dim(\mathcal{K}_j)} a_k^j |u_k^j\rangle\langle u_k^j| = \vec{a}^{\,j}\, \Pi_j$, with Π_j projector on $\mathcal{K}_j$.

Find the E_j (the $\vec{a}^{\,j}$) with $\sum_j \mathsf{E}_j \le \mathrm{I}_N$ maximizing $P_{\text{suc}} = \sum_j P_j \operatorname{tr}(\mathsf{E}_j \rho_j)$.

This problem is only partially solved, in some special cases, (Kleinmann, *J. Math. Phys.* 2010).

More on quantum detection or discrimination :

Neyman-Pearson detection, minimax detection, minimal Bayesian cost detection, have been considered in the quantum domain,

but all relevant aspects are not yet completely solved.

General considerations and overviews can be found in :

• C. W. Helstrom, "Quantum Detection and Estimation Theory", Academic Press, 1976.

• Y. C. Eldar, A. Megretski, G. C. Verghese, "Designing optimal quantum detectors via semidefinite programming", *IEEE Transactions on Information Theory*, vol. 49, pp. 1007–1012, 2003.

• J. A. Bergou, "Discrimination of quantum states", *Journal of Modern Optics*, vol. 57, pp. 160–180, 2010.

• J. Bae, L.-C. Kwek, "Quantum state discrimination and its applications", *Journal of Physics A*, vol. 48, pp. 083001,1–35, 2015.

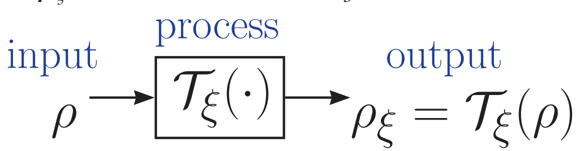
Quantum estimation

for high-sensitivity high-precision quantum sensing & metrology (magnetometry, gravitometry, accelerometers, atomic clocks, frequency standards, etc)

A quantum system has its state $\rho_\xi \in \mathcal{L}(\mathcal{H}_N)$ dependent on an unknown parameter ξ.

A generalized measurement by a POVM with M elements E_m for $m = 1, 2, \dots M$, can be used to measure ρ_ξ in order to estimate ξ.

Often :



An input excitation signal ρ,
to probe a ξ-dependent quantum process $\mathcal{T}_\xi(\cdot)$,
producing the ξ-dependent output signal ρ_ξ to be processed to estimate ξ.

[1] M. G. A. Paris (Ed.); "Quantum State Estimation"; *Lecture Notes in Physics*, vol. 649, Springer (2004).
[2] V. Giovannetti, *et al.*; "Advances in quantum metrology"; *Nature Photonics* 5, 222–229 (2011).
[3] C. L. Degen, *et al.*; "Quantum sensing"; *Reviews of Modern Physics* 89, 035002,1–39 (2017).

• Classically, from some measured data $\vec{x}$ with probability distribution $P(\vec{x};\xi)$, any estimator $\widehat{\xi}(\vec{x})$ for ξ has a mean-squared error $\langle(\widehat{\xi}-\xi)^2\rangle$ lower bounded via the classical Fisher information $F_c(\xi) = \left\langle \left[\partial_\xi \ln P(\vec{x};\xi)\right]^2 \right\rangle$,
ensuring $\langle(\widehat{\xi}-\xi)^2\rangle \geq$ Cramér-Rao bound $\sim \dfrac{1}{F_c(\xi)}$,
with the maximum likelihood estimator saturating the CR bound, at long $\vec{x}$.

• Quantumly, when measuring ρ_ξ,
from the resulting data m with probability distribution $P(m;\xi) = \mathrm{tr}(\rho_\xi \mathsf{E}_m)$,
one has $F_c(\xi)$ upper bounded by the quantum Fisher information $F_q(\xi) = \left\langle \left[\mathcal{D}_\xi \rho_\xi\right]^2 \right\rangle$,
(with $\mathcal{D}_\xi$ symmetric logarithmic derivative) ensuring $F_c(\xi) \leq F_q(\xi)$,

and $$F_q(\xi) = 2\sum_{\ell,n} \frac{|\langle\lambda_\ell|\partial_\xi\rho_\xi|\lambda_n\rangle|^2}{\lambda_\ell+\lambda_n} = \sum_\ell \frac{(\partial_\xi\lambda_\ell)^2}{\lambda_\ell} + 2\sum_{\ell,n}\frac{(\lambda_\ell-\lambda_n)^2}{\lambda_\ell+\lambda_n}|\langle\partial_\xi\lambda_\ell|\lambda_n\rangle|^2,$$
via eigendecomposition $\{\lambda_n, |\lambda_n\rangle\}$ of ρ_ξ.

[4] O. E. Barndorff-Nielsen, R. D. Gill; "Fisher information in quantum statistics"; *Journal of Physics A* 33, 4481–4490 (2000).

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.

Wrap-up at the onset of "Cours 5/5"

3 fundamental principles :

• **State :** unit-norm vector $|\psi\rangle = \sum_n \alpha_n |n\rangle \in \mathcal{H}_N$,
or positive unit-trace operator $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j| = \mathrm{tr}_E\big(|QE\rangle\langle QE|\big) \in \mathcal{L}(\mathcal{H}_N)$.

• **Process :** Closed evolution : $|\psi\rangle \longmapsto \mathsf{U}|\psi\rangle$ linear unitary, from $\mathsf{U}(t_2,t_1) = \exp\left(-\frac{i}{\hbar}\int_{t_1}^{t_2} \mathsf{H}dt\right)$
or open evolution : $\rho \longmapsto \mathcal{N}(\rho) = \mathrm{tr}_E\big(\mathsf{U}_{QE}(\rho\otimes|e_0\rangle\langle e_0|)\mathsf{U}_{QE}^\dagger\big) = \sum_k \Lambda_k\rho\Lambda_k^\dagger$.

• **Measurement :** a set of M operators $\mathsf{M}_m \in \mathcal{L}(\mathcal{H}_N)$ satisfying $\sum_{m=1}^M \mathsf{M}_m^\dagger\mathsf{M}_m = \mathrm{I}_N$,
$\Longrightarrow$ on $\rho \in \mathcal{L}(\mathcal{H}_N)$: probability $P(m) = \mathrm{tr}\big(\rho\mathsf{M}_m^\dagger\mathsf{M}_m\big)$ and post $\rho_m^{\mathrm{post}} = \dfrac{\mathsf{M}_m\rho\mathsf{M}_m^\dagger}{P(m)}$.

• **Computation :** Deutsch-Jozsa parallelism, superdense coding, teleportation, Grover search, Shor factoring, cryptography, non-classical correlation, ···

• **Information processing :**
– Detection, discrimation, of quantum signals in noise ;
– Estimation, identification, of parameter, state, process ;
– Communication, source and channel codings ;
...

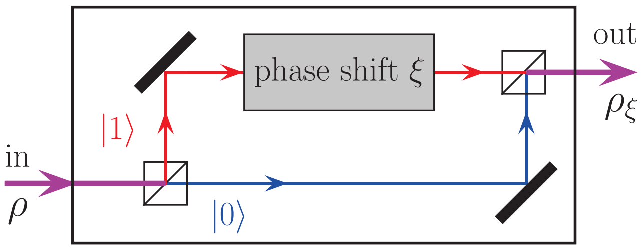
Qubit phase estimation

A photon (qubit) in an interferometer undergoing the unitary transformation

$$\mathsf{U}_\xi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\xi} \end{bmatrix}$$ (see p. 21)

$$\equiv \exp\!\left(-i\,\frac{\xi}{2}\vec{n}\cdot\vec{\sigma}\right) \text{ at } \vec{n} = \vec{e}_z .$$

$$\Longrightarrow \mathcal{T}_\xi(\rho) = \mathsf{U}_\xi\,\rho\,\mathsf{U}_\xi^\dagger .$$



Input $\rho = \frac{1}{2}\left(\mathrm{I}_2 + \vec{r}\cdot\vec{\sigma}\right) \longmapsto$ output $\rho_\xi = \frac{1}{2}\left(\mathrm{I}_2 + \vec{r}_\xi\cdot\vec{\sigma}\right)$, $\vec{r}_\xi$ is $\vec{r}$ rotated by ξ // $\vec{n}$.

Fisher $F_q(\xi\,;\rho) = (\vec{n}\times\vec{r})^2$ maximized at $F_q^{\max} = 1$ by a pure state ρ of $\vec{r}\perp\vec{n}$.

$\Longrightarrow$ optimal input $|\psi\rangle = |+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \Longrightarrow \rho = \rho_{\mathrm{opt}} = |\psi\rangle\langle\psi| = |+\rangle\langle+|$.

[5] F. Chapeau-Blondeau; "Optimizing qubit phase estimation"; *Physical Review A* 94, 022334,1–14 (2016).

Optimal quantum measurement :

Spin observable $\Omega = \vec{\omega}\cdot\vec{\sigma}$, with in $\mathbb{R}^3$ the measurement vector $\|\vec{\omega}\| = 1$,

$\Longrightarrow$ measurement probabilities $\Pr\{\pm 1\} = \frac{1}{2}\big(1 \pm \vec{\omega}\,\vec{r}_\xi\big) = P_\pm$

to reach the classical Fisher $F_c(\xi) = \dfrac{(\partial_\xi P_+)^2}{P_+} + \dfrac{(\partial_\xi P_-)^2}{P_-} = \dfrac{\big[\vec{\omega}\,(\vec{n}\times\vec{r}_\xi)\big]^2}{1-(\vec{\omega}\,\vec{r}_\xi)^2}$.

When $\rho = \rho_{\mathrm{opt}} = |+\rangle\langle+|$ of $\vec{r}\perp\vec{n} \Longrightarrow \vec{r}_\xi \perp \vec{n}$, then $F_c(\xi)$ is maximized at $F_c(\xi) = F_q^{\max} = 1$ by any $\vec{\omega}\perp\vec{n}$.

$\Longrightarrow$ optimal measurement : von Neumann in basis $\big\{|+\rangle, |-\rangle\big\}$,

to yield $\Pr\big\{|\pm\rangle\big\} = \big|\langle\pm|\mathsf{U}_\xi|\psi\rangle\big|^2 = \dfrac{1\pm\cos(\xi)}{2} = P_\pm$.

Optimal classical estimator from the measurement results :

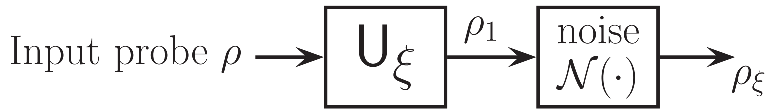
- L successive experiments deliver a sequence of L_+ outcomes $|+\rangle$ and $L_- = L - L_+$ outcomes $|-\rangle$.

- From the measured data (L_+, L_-), the value of ξ is estimated by an estimator $\widehat{\xi} = \widehat{\xi}(L_+, L_-)$.

Maximum likelihood estimator $\widehat{\xi}(L_+, L_-) = \arg\max_\xi \Pr(L_+, L_-\,;\,\xi)$

$$\Longrightarrow \widehat{P}_+ = \frac{L_+}{L} \Longrightarrow \widehat{\xi} = \arccos\big(2\widehat{P}_+ - 1\big) = \arccos\left(\frac{2L_+ - 1}{L}\right).$$

Qubit phase estimation with quantum noise



ξ-dependent unitary U_ξ delivers $\rho_1(\xi) = \mathsf{U}_\xi\,\rho\,\mathsf{U}_\xi^\dagger$

leading to the noisy output $\rho_\xi = \mathcal{N}\big(\rho_1(\xi)\big) = \mathcal{N}\big(\mathsf{U}_\xi\,\rho\,\mathsf{U}_\xi^\dagger\big) = \mathcal{T}_\xi(\rho)$.

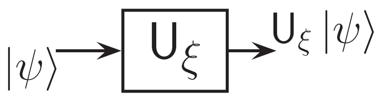
With $\mathcal{N}(\cdot)$ bit-flip, or phase-flip, or depolarizing noise,

the input exitation $|\psi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$ remains optimal, (but not with thermal noise)

but the output measurement in $\big\{|+\rangle, |-\rangle\big\}$ is no longer optimal.

[6] F. Chapeau-Blondeau; "Optimized probing states for qubit phase estimation with general quantum noise"; *Physical Review A* 91, 052310,1–13 (2015).

Entanglement-assisted quantum estimation



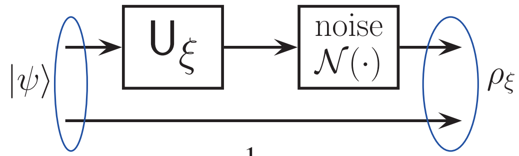
Optimal input $|\psi\rangle = |+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle+|1\rangle\big)$ maximizes quantum Fisher at $F_q(\xi) = F_q^{\max} = 1$.

Two consecutive independent inputs as $|\psi\rangle = |+\rangle\otimes|+\rangle$ reach quantum Fisher information at $F_q(\xi) = 2F_q^{\max} = 2$, by additivity of the Fisher information for independent inputs.
From L independent inputs : shot-noise scaling of $F_q(\xi) \sim L$.

Two optimally entangled inputs as $|\psi\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle+|11\rangle\big)$ reach quantum Fisher at $F_q(\xi) = 4F_q^{\max} = 4$ by superadditivity of quantum Fisher for entangled inputs.
From L optimally entangled inputs : Heisenberg scaling of $F_q(\xi) \sim L^2$.

[7] F. Chapeau-Blondeau; "Entanglement-assisted quantum parameter estimation from a noisy qubit pair: A Fisher information analysis"; *Physics Letters A* 381 (2017) 1369–1378.

Entanglement-assisted quantum estimation



The entangled input $|\psi\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle+|11\rangle\big)$ with one active qubit and one passive qubit, can improve over the configuration with only one active probing qubit.

[8] N. Gillard *et al.*, "Estimation quantique en présence de bruit améliorée par l'intrication", GRETSI 2017.

In the presence of noise, for quantum estimation, optimal entangled probing signals and their processing, are not (yet) fully characterized in all configurations.

• Multiple-parameter estimation, via quantum Fisher information matrix $F_q(\vec{\xi}) = \big[F_{jk}(\vec{\xi})\big]$. • Linear in the multiple parameters is tomography (estimation) of a complete quantum state, or a quantum process. • Bayesian quantum estimation is feasible.

[9] M. G. Paris; "Quantum estimation for quantum technology"; *Int. J. Quantum Information* 7 (2009) 125–137.

Estimation of multiple quantum parameters

A quantum system with state $\rho_{\vec{\xi}} \in \mathcal{L}(\mathcal{H}_N)$ dependent on an unknown vector parameter $\vec{\xi} = [\xi_1, \xi_2, \cdots]^\top$ has a quantum Fisher information matrix $F_q(\vec{\xi}) = \big[F_{jk}^{(q)}(\vec{\xi})\big]$ with

matrix elements $F_{jk}^{(q)}(\vec{\xi}) = 2\sum_{\ell,n} \frac{\langle\lambda_\ell|\partial_j\rho_{\vec{\xi}}|\lambda_n\rangle\langle\lambda_n|\partial_k\rho_{\vec{\xi}}|\lambda_\ell\rangle}{\lambda_\ell+\lambda_n}$.

Measuring $\rho_{\vec{\xi}}$ by means of an arbitrary POVM $\{\mathsf{E}_m\}_{m=1}^M$ leads to the probability distribution $P(m;\vec{\xi}) = \mathrm{tr}(\mathsf{E}_m\rho_{\vec{\xi}})$ having classical Fisher information matrix

$F_c(\vec{\xi}) = \big[F_{jk}^{(c)}(\vec{\xi})\big]$ with matrix elements $F_{jk}^{(c)}(\vec{\xi}) = \sum_m \frac{\partial_j P(m;\vec{\xi})\,\partial_k P(m;\vec{\xi})}{P(m;\vec{\xi})}$,

upper bounded via the matrix inequality $F_c(\vec{\xi}) \le F_q(\vec{\xi})$.

Exploit any flexibility on $\rho_{\vec{\xi}}$ to maximize (not univocal) quantum Fisher $F_q(\vec{\xi})$.
Select the POVM $\{\mathsf{E}_m\}_{m=1}^M$ to maximize classical Fisher $F_c(\vec{\xi})$.

From (classical) measurement results : ML estimator $\widehat{\vec{\xi}}_{\mathrm{ML}} = \arg\max_{\vec{\xi}} P\big(\{m_\ell\};\vec{\xi}\big)$.

Quantum tomography, of state ρ, or of process $\mathcal{T}(\cdot)$

A multiparametric estimation task, usually linear in the parameters, consisting in estimating the coordinates of a density operator ρ, or of a process superoperator $\mathcal{T}(\cdot)$, in some useful basis.

• Example : A qubit **state** $\rho = \frac{1}{2}\big(\mathrm{I}_2 + \vec{r}\cdot\vec{\sigma}\big) = \frac{1}{2}\big(\mathrm{I}_2 + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z\big)$.

$\{\sigma_x, \sigma_y, \sigma_z\}$ three mutually $\perp$ qubit observables $\Longrightarrow r_x = \langle\sigma_x\rangle = \mathrm{tr}(\rho\sigma_x)$, $r_y = \langle\sigma_y\rangle$, $r_z = \langle\sigma_z\rangle$ separately estimable in three independent single-parameter estimations.

Or globally, by measuring a POVM $\{\mathsf{E}_m\}_{m=1}^M$ on L independent repetitions to yield L_m outcomes m and the ML estimator $\widehat{\rho}_{\mathrm{ML}}\big(\{L_m\}\big) = \arg\max_\rho \sum_{m=1}^M L_m \log\big(\mathrm{tr}(\mathsf{E}_m\rho)\big)$.

• A quantum **process** $\rho \longmapsto \mathcal{T}(\rho) = \rho'$ from $\mathcal{L}(\mathcal{H})$ onto $\mathcal{L}(\mathcal{H}')$ can be completely characterized by specifying how $\mathcal{T}(\cdot)$ transforms a basis of $\mathcal{L}(\mathcal{H})$, for example by successively estimating each $\mathcal{T}\big(|j\rangle\langle k|\big)$, each via quantum **state** tomography.

• Many variants % basis, measurement. • This remains a rather considerable effort.

Information of a quantum system

How much information can be stored in a quantum system ?

A pure quantum state $|\psi\rangle = \sum_{n=1}^{N} \alpha_n |n\rangle \in \mathcal{H}_N$ with continuously-valued coordinates α_n, can store an arbitrary number J of discrete values $\{x_j\}_{j=1}^{J}$.

As soon as a qubit state $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle \in \mathcal{H}_2$, via J configurations $|\psi_j\rangle$ with $\theta = \theta_j = (j-1)\pi/J$ for $j = 1$ to J, and φ fixed.

With a probability distribution $\{p_j\}_{j=1}^{J}$ over the set $\{x_j\}_{j=1}^{J}$,

$\Longrightarrow$ information content by Shannon entropy $H(X) = -\sum_{j=1}^{J} p_j \log(p_j) \leq \log(J)$.

With a uniform distribution $\{p_j = 1/J\}_{j=1}^{J}$, the entropy $H(X) = \log(J) \xrightarrow[J \to +\infty]{} +\infty$

$\Longrightarrow$ An arbitrary large information can be stored in a quantum system of dimension N, as soon as $N = 2$ with a qubit.

But how much information can be retrieved out ?

How much information can be retrieved out of a quantum system ?

For a quantum system of dimension N in $\mathcal{H}_N$, with a state ρ (pure or mixed),

a generalized measurement by the POVM with K elements E_k, for $k = 1, 2, \dots K$.

Measurement outcome Y with K possible values $y_k \equiv k$, for $k = 1, 2, \dots K$, of probabilities $\Pr\{Y = y_k\} = \mathrm{tr}(\rho \mathsf{E}_k)$.

$$\text{Shannon output entropy } H(Y) = -\sum_{k=1}^{K} \Pr\{Y = y_k\} \log\Big(\Pr\{Y = y_k\}\Big) .$$
$$= -\sum_{k=1}^{K} \mathrm{tr}(\rho \mathsf{E}_k) \log\Big(\mathrm{tr}(\rho \mathsf{E}_k)\Big) .$$

For any given state ρ (pure or mixed), K-element POVMs can always be found achieving the limit $H(Y) \sim \log(K)$ at large K. (ex. : $\rho = \mathrm{I}_2/2$ and $\mathsf{E}_k = (2/K)|e_k\rangle\langle e_k|$)

In this respect, when $K \longrightarrow \infty$ with $H(Y) \longrightarrow \infty$, an arbitrary large information can be drawn out of a quantum system of dimension N, as soon as $N = 2$ with a qubit.

But how much of the input information can be retrieved out ?

With a quantum system of dimension N in $\mathcal{H}_N$, each classical state x_j is coded by a quantum state $|\psi_j\rangle \in \mathcal{H}_N$ or $\rho_j \in \mathcal{L}(\mathcal{H}_N)$, for $j = 1, 2, \dots J$.

A generalized measurement by the POVM with K elements E_k, for $k = 1, 2, \dots K$.

Measurement outcome Y with K possible values $y_k \equiv k$, for $k = 1, 2, \dots K$, of conditional probabilities $\Pr\{Y = y_k | X = x_j\} = \mathrm{tr}(\rho_j \mathsf{E}_k)$,

and total probabilities $\Pr\{Y = y_k\} = \sum_{j=1}^{J} \Pr\{Y = y_k | X = x_j\} p_j = \mathrm{tr}(\rho \mathsf{E}_k)$,

with $\rho = \sum_{j=1}^{J} p_j \rho_j$ the average state.

The input–output mutual information $I(X;Y) = H(Y) - H(Y|X) \leq \mathcal{X}(\rho)$,

with the Holevo information $\mathcal{X}(\rho) = S(\rho) - \sum_{j=1}^{J} p_j S(\rho_j) \leq \log(N)$,

and von Neumann entropy $S(\rho) = -\mathrm{tr}\big[\rho \log(\rho)\big] \leq \log(N)$.

The von Neumann entropy

For a quantum system of dimension N with density operator ρ on $\mathcal{H}_N$:

$$S(\rho) = -\mathrm{tr}\Big[\rho \log(\rho)\Big] .$$

ρ unit-trace positive has diagonal form $\rho = \sum_{n=1}^{N} \lambda_n |\lambda_n\rangle\langle\lambda_n|$,

whence $S(\rho) = -\sum_{n=1}^{N} \lambda_n \log(\lambda_n) \in [0, \log(N)]$.

- $S(\rho) = 0$ for a pure state $\rho = |\psi\rangle\langle\psi|$,
- $S(\rho) = \log(N)$ at equiprobability when $\lambda_n = 1/N$ and $\rho = \mathrm{I}_N/N$.

Holevo information : $\mathcal{X}(\rho) \equiv \mathcal{X}\Big(\{(p_j, \rho_j)\}\Big) = S(\rho) - \sum_{j=1}^{J} p_j S(\rho_j) \in [0, \log(N)]$.

- $\mathcal{X}(\rho) = 0$ for one $p_j = 1$ of a pure state $\rho_j = |\psi_j\rangle\langle\psi_j|$,
- $\mathcal{X}(\rho) = \log(N)$ for N equiprobable $p_j = 1/N$ orthogonal pure states $|\psi_j\rangle = |j\rangle$.

The accessible information

For a given input ensemble $\{(p_j, \rho_j)\}$:
the accessible information $I_{\rm acc}(X;Y) = \max\limits_{\rm POVM} I(X;Y)$.

For states ρ_j in $\mathcal{L}(\mathcal{H}_N)$, there always exists such an optimal POVM under the form $\{\mathsf{E}_k = \alpha_k |\phi_k\rangle\langle\phi_k|\}$, with $\alpha_k \in [0,1]$, for $k = 1$ to K, and $N \le K \le N^2$,
this by Theorem 3 of E. B. Davies; "Information and quantum measurement"; *IEEE Transactions on Information Theory* 24 (1978) 596–599.

But, there is no general characterization of optimal POVM. [Sasaki, PRA 59 (1999) 3325]
There are hardly some known expressions for some special ensembles $\{(p_j, \rho_j)\}$.
SOMIM (Search for Optimal Measurements by an Iterative Method) for numerical maximization by steepest-ascent that follows the gradient in the POVM space, and also uses conjugate gradients for speed-up. [arXiv:0805.2847]

But an upper bound $I_{\rm acc}(X;Y) \le \chi\big(\{(p_j, \rho_j)\}\big)$.

Compression of a quantum information source (1/2)

A quantum source emits symbols $\rho_j \in \mathcal{L}(\mathcal{H}_N)$ with probabilities p_j, for $j = 1$ to J.

With $\rho = \sum_{j=1}^{J} p_j \rho_j$ of N-ary quantum entropy $S_N(\rho) = -\operatorname{tr}\big[\rho \log_N(\rho)\big] \le \log_N(N) = 1$,
and Holevo information $\chi_N\big(\{(p_j, \rho_j)\}\big) = S_N(\rho) - \sum_{j=1}^{J} p_j S_N(\rho_j) \le \log_N(N) = 1$.

For lossless coding of the source, the average number of N-dimensional quantum systems required per source symbol is lower bounded by $\chi_N\big(\{(p_j, \rho_j)\}\big)$.

For pure states $\rho_j = |\psi_j\rangle\langle\psi_j|$, the lower bound $\chi_N(p_j, \rho_j) = S_N(\rho)$ is achievable, with consecutive blocks of L quantum systems from $\mathcal{H}_N$ encodable by $L S_N(\rho) \le L$ quantum systems from $\mathcal{H}_N$ with asymptotically vanishing loss at $L \to \infty$.

B. Schumacher; "Quantum coding"; *Physical Review A* 51 (1995) 2738–2747.

R. Jozsa, B. Schumacher; "A new proof of the quantum noiseless coding theorem"; *Journal of Modern Optics* 41 (1994) 2343–2349.

Compression of a quantum information source (2/2)

For mixed states ρ_j, the compression rate is lower bounded by $\chi_N\big(\{(p_j, \rho_j)\}\big) \le S_N(\rho)$
but this lower bound $\chi_N\big(\{(p_j, \rho_j)\}\big)$ is not known to be generally achievable.

The compression rate $S_N(\rho)$ is however always achievable (by purification of the ρ_j and optimal compression of these purified states).

Depending on the mixed ρ_j's, and the criterion of faithfulness, there may exist an achievable lower bound between $\chi_N\big(\{(p_j, \rho_j)\}\big)$ and $S_N(\rho)$. (Wilde 2021, §18.4)

The problem of general characterization of an achievable lower bound for the compression rate of mixed states still remains open. (Wilde 2021, §18.5)

M. Horodecki; "Limits for compression of quantum information carried by ensembles of mixed states"; *Physical Review A* 57 (1998) 3364–3369.

H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, B. Schumacher; "On quantum coding for ensembles of mixed states"; *Journal of Physics A* 34 (2001) 6767–6785.

M. Koashi, N. Imoto; "Compressibility of quantum mixed-state signals"; *Physical Review Letters* 87 (2001) 017902,1–4.

Classical information over a quantum channel (1/3)

$$(X = x_j, p_j) \longrightarrow \rho_j \longrightarrow \boxed{\mathcal{N}} \longrightarrow \mathcal{N}(\rho_j) = \rho'_j \longrightarrow \boxed{K\text{-element POVM}} \longrightarrow Y = y_k$$

Mutual info. $I(X;Y) \le \chi\big(\{(p_j, \rho'_j)\}\big) = S(\rho') - \sum_{j=1}^{J} p_j S(\rho'_j)$ with $\rho' = \sum_{j=1}^{J} p_j \rho'_j$.

Yet, $\chi\big(\{(p_j, \rho'_j)\}\big)$ is a maximum <u>achievable</u> rate, for error-free communication, by coding <u>independent</u> consecutive input symbols in blocks of length $L_{\rm cod} \to \infty$, and measuring the output with a <u>collective</u> POVM on $L_{\rm cod}$-long blocks
(and the suboptimal square-root measurement POVM is enough).

$\chi\big(\{(p_j, \rho'_j)\}\big)$ characterizes the best achievable rate without the need to refer to any specific POVM and any $L_{\rm cod}$-long blocks.

B. Schumacher, M. D. Westmoreland; "Sending classical information via noisy quantum channels"; *Physical Review A* 56 (1997) 131–138.

A. S. Holevo; "The capacity of the quantum channel with general signal states"; *IEEE Transactions on Information Theory* 44 (1998) 269–273.

Classical information over a quantum channel (2/3)

For given $\mathcal{N}(\cdot)$ therefore $\chi_{\max} = \max_{\{p_j,\rho_j\}} \chi\Big(\big\{\big(\mathcal{N}(\rho_j), p_j\big)\big\}\Big)$

is the overall maximum and achievable rate for error-free communication of classical information over a noisy quantum channel,
or the Holevo information capacity of the quantum channel,
for product states or successive independent uses of the channel,
and collective decoding over L_{cod}-long blocks, at $L_{\mathrm{cod}} \to \infty$.

The maximum rate $\chi_{\max}$ can be achieved by $J \in [N, N^2]$ *pure* input states $\rho_j = |\psi_j\rangle\langle\psi_j|$ with $|\psi_j\rangle \in \mathcal{H}_N$ (not necessarily easy to characterize).
Shor, *J. Math. Phys.* 43 (2002) 4334. Shor, *Com. Math. Phys.* 246 (2004) 453.

Classical information over a quantum channel (3/3)

For product states or consecutive independent uses of a channel,
the Holevo capacity is additive $\chi_{\max}(\mathcal{N}_1 \otimes \mathcal{N}_2) = \chi_{\max}(\mathcal{N}_1) + \chi_{\max}(\mathcal{N}_2)$.

For non-product states or consecutive non-independent but entangled uses of the channel, due to a convexity property, the Holevo capacity is always superadditive
$\chi_{\max}(\mathcal{N}_1 \otimes \mathcal{N}_2) \geq \chi_{\max}(\mathcal{N}_1) + \chi_{\max}(\mathcal{N}_2)$. [Wilde 2016, Eq. (20.126)]

For many channels it is found additive, $\chi_{\max}(\mathcal{N}_1 \otimes \mathcal{N}_2) = \chi_{\max}(\mathcal{N}_1) + \chi_{\max}(\mathcal{N}_2)$
so that entanglement does not improve over the product-state capacity.

Yet for some channels it has been found strictly superadditive,
$\chi_{\max}(\mathcal{N}_1 \otimes \mathcal{N}_2) > \chi_{\max}(\mathcal{N}_1) + \chi_{\max}(\mathcal{N}_2)$ meaning that entanglement does improve over the product-state capacity.
M. B. Hastings; "Superadditivity of communication capacity using entangled inputs"; *Nature Physics* 5 (2009) 255–257.

$\Longrightarrow$ The classical capacity $C(\mathcal{N})$ of a channel $\mathcal{N}$ is generally the "regularized" Holevo capacity $C(\mathcal{N}) = \lim_{L\to\infty} \dfrac{1}{L}\chi_{\max}\big(\mathcal{N}^{\otimes L}\big)$. (HSW theorem)

Quantum information over a quantum channel (1/2)

Reliable transmission of the quantum states is targeted
(no classical coding / decoding (measurement) ; needs quantum distortion criteria).

- Primal channel, from Q to Q : $\rho_Q \longmapsto \rho'_Q =$

$$\mathcal{N}(\rho_Q) = \mathrm{tr}_E\Big(\mathsf{U}_{QE}(\rho_Q \otimes |e_0\rangle\langle e_0|)\mathsf{U}_{QE}^\dagger\Big) = \mathrm{tr}_E\left(\sum_{k=1}^K\sum_{k'=1}^K \Lambda_k\rho_Q\Lambda_{k'}^\dagger \otimes |e_k\rangle\langle e_{k'}|\right) = \sum_{k=1}^K \Lambda_k\rho_Q\Lambda_k^\dagger \ .$$

- Dual channel, from Q into environment E : $\rho_Q \longmapsto \rho'_E =$

$$\widetilde{\mathcal{N}}(\rho_Q) = \mathrm{tr}_Q\Big(\mathsf{U}_{QE}(\rho_Q \otimes |e_0\rangle\langle e_0|)\mathsf{U}_{QE}^\dagger\Big) = \sum_{k=1}^K\sum_{k'=1}^K \mathrm{tr}\Big(\Lambda_k\rho_Q\Lambda_{k'}^\dagger\Big)|e_k\rangle\langle e_{k'}| \ .$$

Entropy exchange or final quantum entropy of the environment : $S_{\mathrm{ex}}(\rho_Q, \mathcal{N}) = S(\rho'_E)$.

Coherent information : $I_{\mathrm{co}}(\rho_Q, \mathcal{N}) = S(\rho'_Q) - S(\rho'_E) = S\big(\mathcal{N}(\rho_Q)\big) - S_{\mathrm{ex}}(\rho_Q, \mathcal{N})$.

(Intrinsic) channel coherent information : $I_{\mathrm{co}}(\mathcal{N}) = \max_{\rho_Q} I_{\mathrm{co}}(\rho_Q, \mathcal{N})$.

Generally $I_{\mathrm{co}}(\rho_Q, \mathcal{N})$ non-concave ($\not\cap$), maximized at $I_{\mathrm{co}}(\mathcal{N}) \geq 0$ by a mixed state ρ_Q .

Quantum information over a quantum channel (2/2)

Superadditivity in two channel uses : $I_{\mathrm{co}}(\mathcal{N}_1 \otimes \mathcal{N}_2) \geq I_{\mathrm{co}}(\mathcal{N}_1) + I_{\mathrm{co}}(\mathcal{N}_2)$.

For two separable product states : $I_{\mathrm{co}}(\mathcal{N}_1 \otimes \mathcal{N}_2) = I_{\mathrm{co}}(\mathcal{N}_1) + I_{\mathrm{co}}(\mathcal{N}_2)$,
but for two entangled states $I_{\mathrm{co}}(\mathcal{N}_1 \otimes \mathcal{N}_2) > I_{\mathrm{co}}(\mathcal{N}_1) + I_{\mathrm{co}}(\mathcal{N}_2)$ is possible.

$\Longrightarrow$ Quantum capacity $Q(\mathcal{N}) = \lim_{L\to\infty} \dfrac{1}{L} I_{\mathrm{co}}\big(\mathcal{N}^{\otimes L}\big)$. (LSD theorem)

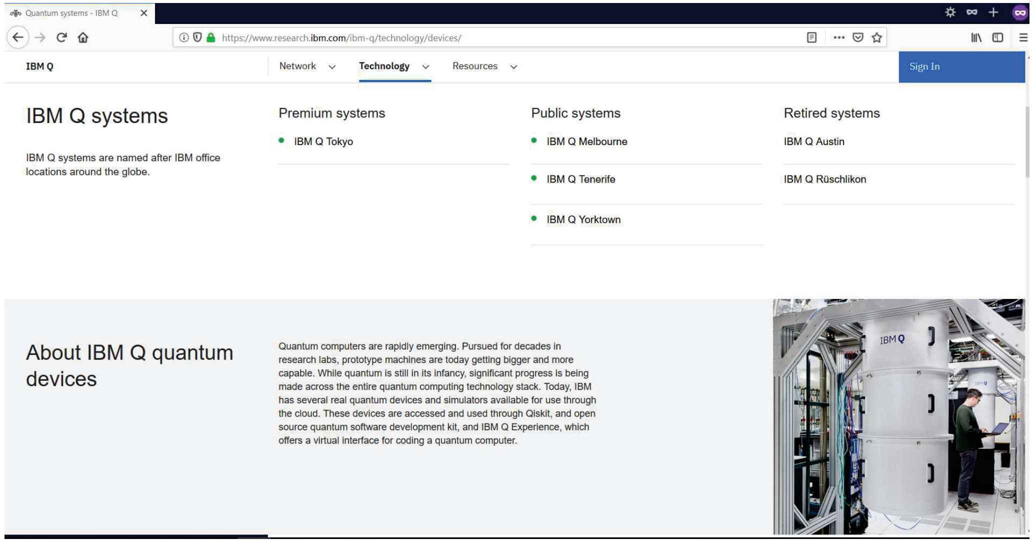
$Q_N(\mathcal{N}) \leq \log_N(N) = 1$ is the maximum rate R at which L input qudits with dimension N, can be encoded into $L/R \geq L$ qudits with same dimension N,
so that from the L/R corrupted qudits at the output,
the L input qudits can be recovered with perfect fidelity, when $L \longrightarrow \infty$.

S. Lloyd; "Capacity of the noisy quantum channel"; *Physical Review A* 55 (1997) 1613–1622.

P. W. Shor; "The quantum channel capacity and coherent information"; *Lecture Notes MSRI Workshop on Quantum Computation*, San Francisco (2002) 1–18.

I. Devetak, "The private classical capacity and quantum capacity of a quantum channel"; *IEEE Transactions on Information Theory* 51 (2005) 44–55.

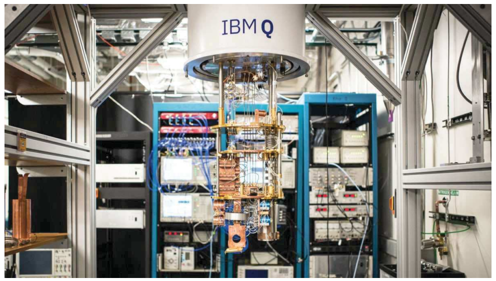
Today remain unknown many $Q(\mathcal{N})$, $C(\mathcal{N})$, the capacity-achieving codings $\cdots$

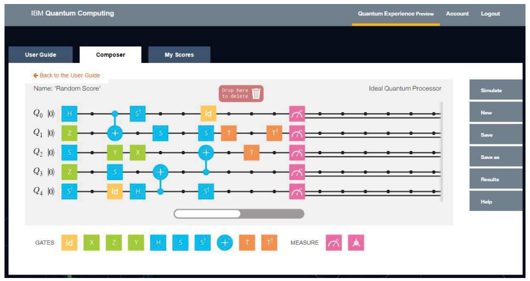


IBM quantum processors online https://research.ibm.com/quantum-computing 2019
5 qubits on IBM Q Tenerife and on IBM Q Yorktown,
14 qubits on IBM Q Melbourne.

Online IBM quantum processors

`https://quantum.ibm.com`





• F. Chapeau-Blondeau; "Modeling and simulation of a quantum thermal noise on the qubit"; *Fluctuation and Noise Letters* 21, 2250060,1–17 (2022).

• N. Delanoue, F. Chapeau-Blondeau ; "Identification sur un système quantique bruité : Théorie et démonstration expérimentale sur un processeur quantique." ; Actes des 6èmes Journées Démonstrateurs en Automatique du Club EEA (Électronique Électrotechnique Automatique), Angers, France, 21–22 juin 2022.

• F. Chapeau-Blondeau, N. Delanoue ; "Détection quantique en présence de bruit : analyse théorique et étude expérimentale sur un processeur quantique." ; Actes du 29ème Colloque GRETSI sur le Traitement du Signal et des Images, Grenoble, France, 28 août – 1 sept. 2023.

Merci de votre attention.

Merci aux organisateurs,
et à la Maison de la Bretagne, à Paris 15ème, pour son accueil.

Si vous avez compris …
c'est que je me suis mal exprimé !

"Nobody really understands quantum mechanics."
R. P. Feynman