Mai 2018 : cours École Doctorale MathSTIC

Quantum information, quantum computation : An introduction.

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

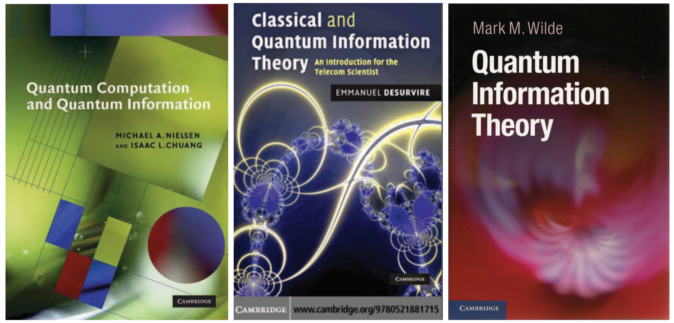
for information and computation :

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

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

3) New field of research, rich of large potentialities.

Some recent textbooks



M. Nielsen & I. Chuang, 2000, 676 pages — E. Desurvire, 2009, 691 pages — M. Wilde, 2013, 655 pages

arXiv:1106.1445v5 [quant-ph] M. Wilde, "From classical to quantum Shannon theory", 670 pages.

Quantum system

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 $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = \langle\psi|\psi\rangle = \|\psi\|^2 = 1$.

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

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

Measurement of the qubit

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

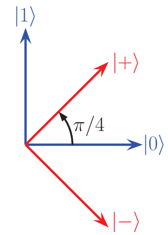
$\Longrightarrow$ only 2 possible outcomes (Born rule) :
state $|0\rangle$ with probability $|\alpha|^2 = |\langle 0|\psi\rangle|^2 = \langle 0|\psi\rangle\langle\psi|0\rangle = \langle 0|\Pi_\psi|0\rangle$, or
state $|1\rangle$ with probability $|\beta|^2 = |\langle 1|\psi\rangle|^2 = \langle 1|\psi\rangle\langle\psi|1\rangle = \langle 1|\Pi_\psi|1\rangle$.

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 $\mathcal{H}_2$

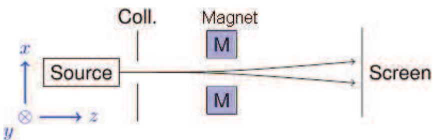
$$\left\{ |+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \; ; \quad |-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) \right\}.$$



$\Longleftrightarrow$ Computational orthonormal basis

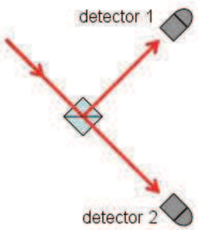
$$\left\{ |0\rangle = \frac{1}{\sqrt{2}}\big(|+\rangle + |-\rangle\big) \; ; \quad |1\rangle = \frac{1}{\sqrt{2}}\big(|+\rangle - |-\rangle\big) \right\}.$$

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, ...)

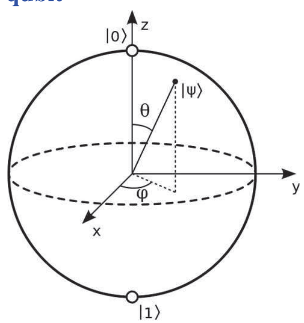


Bloch sphere representation of the qubit

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 infinitely many accessible values
in its two continuous degrees of freedom (θ, φ),
yet when it is measured it can only be found in one of two states
(just like a classical bit).

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

State $|\psi\rangle = \sum_{n=1}^{N} \alpha_n |n\rangle$, in some orthonormal basis $\big\{|1\rangle, |2\rangle, \dots |N\rangle\big\}$ 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 $\big\{|n\rangle\big\}$.

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

Multiple qubits

A system (a word) of N qubits has a state in $\mathcal{H}_2^{\otimes N}$,

a tensor-product vector space with dimension 2^N,

and orthonormal basis $\{|x_1 x_2 \cdots x_N\rangle\}_{\vec{x} \in \{0,1\}^N}$.

Example $N = 2$:

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

Or, as a special separable state ($2N$ 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 : what is done on one part may influence the other part, 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.

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

with
$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big)$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big)$$
$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big).$$

Observables

For a quantum system in $\mathcal{H}_N$ with dimension N,

a projective measurement is defined by an orthonormal basis $\{|1\rangle, \ldots |N\rangle\}$ 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 $\{|\omega_1\rangle, \ldots |\omega_N\rangle\}$ 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 : $\widetilde{\mathsf{A}} = \mathsf{A} - \langle\mathsf{A}\rangle\,\mathrm{I}$,

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

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

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

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

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

Computation on a qubit

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

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

$\equiv$ quantum gate (always reversible)

$$\overset{\text{input}}{|\psi\rangle} \longrightarrow \boxed{\;\mathrm{U}\;} \longrightarrow \overset{\text{output}}{\mathrm{U}|\psi\rangle}$$

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.

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

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

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

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

is the square-root of Not, a typically quantum gate (no classical analog).

In general, the gates U and $e^{i\phi}\mathsf{U}$ give 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

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

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

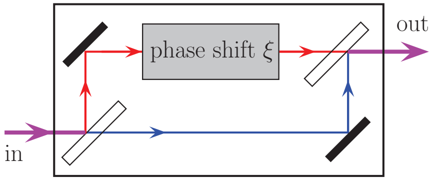
a rotation of the qubit state of an angle ξ around the axis $\vec{n}$ in $\mathbb{R}^3$ $\in \mathrm{SO}(3)$.

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

An optical implementation

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

optically implemented by a Mach-Zehnder interferometer



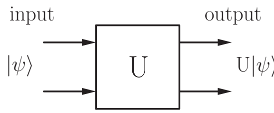
acting on individual photons with two states of polarization $|0\rangle$ and $|1\rangle$
which are selectively shifted in phase,
to operate as well on any superposition $\alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|0\rangle + \beta e^{i\xi}|1\rangle$.

Computation on a pair of qubits

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

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

≡ quantum gate
(always reversible)



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

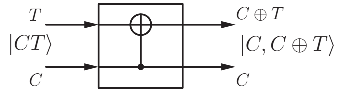
But works equally on any linear superposition of quantum states
$\Longrightarrow$ quantum parallelism.

• 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 N qubits

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

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

≡ quantum gate : N input qubits $\xrightarrow{\mathsf{U}}$ N output qubits.

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

Any N-qubit quantum gate or circuit may always be composed from two-qubit C-Not gates and single-qubit gates (universality).
And in principle this ensures experimental realizability.

This forms the grounding of quantum computation.

No cloning theorem (1982)

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

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

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

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

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

But $|\psi\rangle|\psi\rangle = |\psi\rangle\otimes|\psi\rangle = \big(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle\big)\big(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle\big)$
$= \alpha_1^2|\psi_1\rangle|\psi_1\rangle + \alpha_1\alpha_2|\psi_1\rangle|\psi_2\rangle + \alpha_1\alpha_2|\psi_2\rangle|\psi_1\rangle + \alpha_2^2|\psi_2\rangle|\psi_2\rangle$
$\neq \mathsf{U}(|\psi\rangle|s\rangle)$ in general. $\Longrightarrow$ No cloning U possible.

Quantum parallelism

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

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

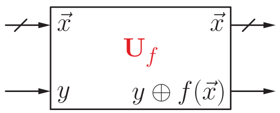
Yet, the quantum gate U can be operated
on any linear superposition of the basis states $\{|\vec{x}\rangle, \vec{x}\in\{0,1\}^N\}$.

This is quantum parallelism, with no classical analog.

Parallel evaluation of a function (1/4)

A classical Boolean function $f(\cdot)$ from N bits to 1 bit
$\vec{x}\in\{0,1\}^N \longrightarrow f(\vec{x})\in\{0,1\}$.

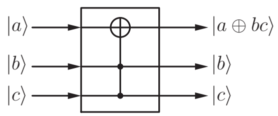
Used to construct a unitary operator U_f as an invertible f-controlled gate :



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

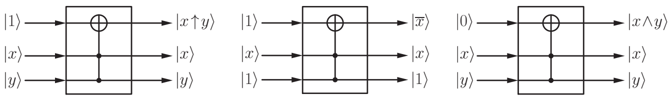
Parallel evaluation of a function (2/4)

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



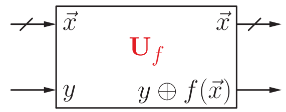
$(\text{CC-Not})^2 = \mathrm{I}_8 \Longleftrightarrow (\text{CC-Not})^{-1} = \text{CC-Not} = (\text{CC-Not})^\dagger$ Hermitian unitary.

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



NAND NOT AND

Parallel evaluation of a function (3/4)



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

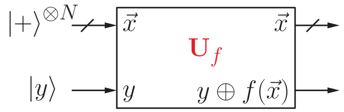
$|\vec{x}\rangle|y=0\rangle \xrightarrow{\mathsf{U}_f} |\vec{x}\rangle|f(\vec{x})\rangle$

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

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

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

Parallel evaluation of a function (4/4)



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

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

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

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

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

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

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

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

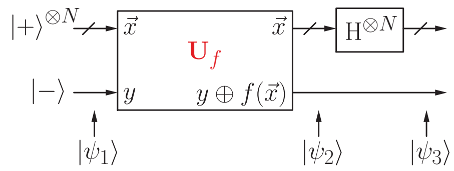
Quantumly : One evaluation of $f(\cdot)$ is enough (on a suitable superposition).

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

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

with scalar product $\vec{x}\vec{z} = x_1 z_1 + \cdots + x_N z_N$ modulo 2. (quant. Hadamard transfo.)

Deutsch-Jozsa algorithm (2/5)



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

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

Deutsch-Jozsa algorithm (3/5)

Output state $|\psi_3\rangle = \Big(\mathsf{H}^{\otimes N} \otimes \mathrm{I}_2\Big)\,|\psi_2\rangle$

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

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

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

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

Deutsch-Jozsa algorithm (4/5)

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

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

- When $f(\cdot)$ constant : $w(\vec{z} = \vec{0}\,) = 2^N (-1)^{f(\vec{0})} = \pm 2^N \Longrightarrow$ 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, N 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 $N = 2$.

[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 $N \geq 2$.

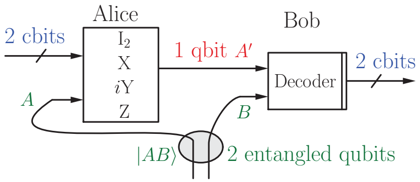
[3] E. Bernstein, U. Vazirani; "Quantum complexity theory"; *SIAM Journal on Computing* 26 (1997) 1411–1473.
Extension to $f(\vec{x}) = \vec{a}\vec{x}$ or $f(\vec{x}) = \vec{a}\vec{x} \oplus b$, to find binary N-word $\vec{a} \longrightarrow$ by producing output $|\psi\rangle = |\vec{a}\,\rangle$.

[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 $|AB\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) = |\beta_{00}\rangle$.

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.



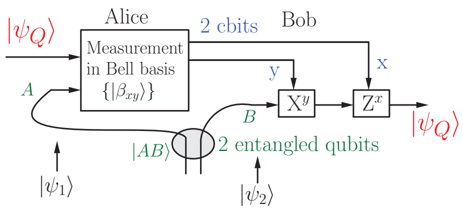
$\mathrm{I}_2 \otimes \mathrm{I}_2\,|AB\rangle = |\beta_{00}\rangle$
$\mathsf{X} \otimes \mathrm{I}_2\,|AB\rangle = |\beta_{01}\rangle$
$\mathsf{Z} \otimes \mathrm{I}_2\,|AB\rangle = |\beta_{10}\rangle$
$i\mathsf{Y} \otimes \mathrm{I}_2\,|AB\rangle = |\beta_{11}\rangle$

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

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

Qubit Q in unknown 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 $\alpha_0|0\rangle + \alpha_1|1\rangle \xrightarrow{\mathrm{I}_2} \cdot \xrightarrow{\mathrm{I}_2} |\psi_Q\rangle$

When QA is measured in $|\beta_{01}\rangle$ then B is in $\alpha_0|1\rangle + \alpha_1|0\rangle \xrightarrow{\mathsf{X}} \cdot \xrightarrow{\mathrm{I}_2} |\psi_Q\rangle$

When QA is measured in $|\beta_{10}\rangle$ then B is in $\alpha_0|0\rangle - \alpha_1|1\rangle \xrightarrow{\mathrm{I}_2} \cdot \xrightarrow{\mathsf{Z}} |\psi_Q\rangle$

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.

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

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

- A dataset contains N possible items or states indexed by $n \in \{1, 2, \cdots N\}$. One wants to find one (only one here, but extensible) state $n = n_0$ satisfying some criterion or property. For the search of the solution n_0, one can test whether any state n is solution or not, by interrogating a **classical oracle**, which amounts to evaluate a classical function $f(\cdot)$ responding as $f(n) = \delta_{nn_0}$.

For this, we note that the oracle does not need to know or to establish the solution n_0, but it needs to be able to evaluate (efficiently at low computing cost) at each n the function $f(n)$ so as to tell whether the proposed n is solution or not.
For instance, for the RSA factoring problem, the oracle does not need to know the two prime factors of the large integer key ; the oracle only needs to be able to tell efficiently whether a query integer n is a factor or not, i.e. whether the query integer n divides the key or not. The oracle can do this efficiently by computing the integer division to implement $f(\cdot)$.

Classically, for such search based on interrogating the oracle, it requires $O(N)$ **interrogations of the classical oracle** in order to find the solution n_0.

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.

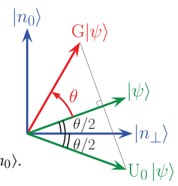
From a quantum implementation of the function $f(\cdot)$, it is possible to obtain the **quantum oracle** as the unitary operator U_0 realizing $\mathsf{U}_0|n\rangle = (-1)^{f(n)}|n\rangle$ for any $n \in \{1, 2, \cdots N\}$.
Thus, the quantum oracle returns its response by reversing the sign of $|n\rangle$ 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 $|n_0\rangle$ may 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 $|n_\perp\rangle = \dfrac{1}{\sqrt{N-1}}\displaystyle\sum_{n\neq n_0}^{N}|n\rangle$ normalized state $\perp |n_0\rangle$

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

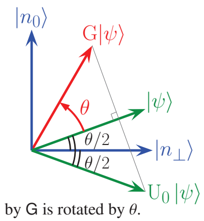
- With the oracle $\mathsf{U}_0 = \mathrm{I}_N - 2|n_0\rangle\langle n_0| \Longrightarrow \mathsf{U}_0|n_\perp\rangle = |n_\perp\rangle$ and $\mathsf{U}_0|n_0\rangle = -|n_0\rangle$.
So in plane $\big(|n_0\rangle, |n_\perp\rangle\big)$, the operator U_0 performs a reflection about $|n_\perp\rangle$.

- 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 in $O(\sqrt{N})$ operations instead of $O(N)$ classically.

Other quantum algorithms

- Shor factoring algorithm (1997) :

Factors any integer in polynomial complexity
(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).

- http://math.nist.gov/quantum/zoo/

"A comprehensive catalog of quantum algorithms ..."

Quantum cryptography

- The problem of cryptography

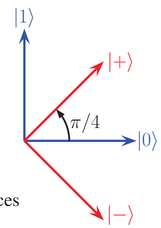
Message X, a string of bits.
Cryptographic key K, a completely random string of bits with proba. 1/2 and 1/2.

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) perturbs the system,
and hence reveals the eavesdropping, and also identifies 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.

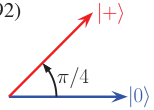
♦ When the whole string of $4N$ bits has been transmitted, Alice and Bob publicly disclose the sequence of their basis choices to identify where they coincide.

♦ 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 and measures Alice's qubit and forward her measured state to Bob, roughly half of the time Eve forwards an incorrect state, and 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 $1/4$.


T +41 22 301 83 71 | E info

IDQ

ID Quantique

Redefining the fields of Random Numbers,
Quantum-Safe Crypto & Photon Counting

ID Quantique

QUANTUM-SAFE CRYPTO – PHOTON COUNTING – RANDOMNESS

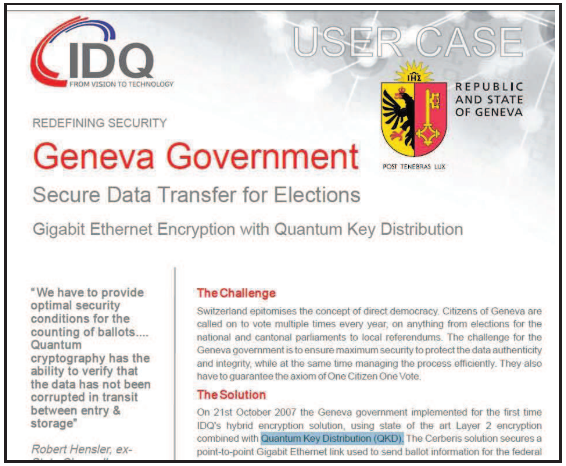
ID Quantique (IDQ) is the world leader in quantum-safe crypto solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions and services to the financial industry, enterprises and

Cerberis QKD Server

Cerberis from IDQ is a standalone rack-mountable QKD server; providing secure quantum keys based on the BB84 and SARG protocols. Integrated with IDQ's Centauris Ethernet and Fiber Channel encryptors, Cerberis has been deployed by governments, enterprises and financial institutions since 2007.

Clavis² QKD Platform

Open QKD platform for R&D, based on BB84 and SARG protocols with auto-compensating interferometric set-up. Widely deployed in the academic community for quantum cryptography research , quantum hacking and certification, and technology evaluations.


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

Quantum correlations (1/2)

For any four random binary variables A_1, A_2, B_1, B_2 with values ± 1,
$\Gamma = (A_1 + A_2)B_1 - (A_1 - A_2)B_2 = A_1B_1 + A_2B_1 + A_2B_2 - A_1B_2 = \pm 2$,
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), necessarily
$\langle\Gamma\rangle = \langle A_1B_1 + A_2B_1 + A_2B_2 - A_1B_2\rangle = \langle A_1B_1\rangle + \langle A_2B_1\rangle + \langle A_2B_2\rangle - \langle A_1B_2\rangle$
verifies $-2 \leq \langle\Gamma\rangle \leq 2$. Bell inequalities (1964).

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

Alice or Bob on its qubit can measure observables of the form $\Omega(\theta) = \sin(\theta)\mathsf{X} + \cos(\theta)\mathsf{Z}$, having eigenvalues ± 1.

Alice measures $\Omega(\alpha)$ to obtain $A = \pm 1$, and Bob measures $\Omega(\beta)$ to obtain $B = \pm 1$,
then we have the average $\langle AB\rangle = \langle\psi_{AB}|\Omega(\alpha) \otimes \Omega(\beta)|\psi_{AB}\rangle = -\cos(\alpha - \beta)$.

Quantum correlations (2/2)

A long series of experiments repeated on identical copies of $|\psi_{AB}\rangle$:
EPR experiment (Einstein, Podolsky, Rosen, 1935).

Alice chooses to randomly switch between measuring $\mathsf{A}_1 \equiv \Omega(\alpha_1)$ or $\mathsf{A}_2 \equiv \Omega(\alpha_2)$,
and Bob chooses to randomly switch between measuring $\mathsf{B}_1 \equiv \Omega(\beta_1)$ or $\mathsf{B}_2 \equiv \Omega(\beta_2)$.

For $\langle\Gamma\rangle = \langle A_1B_1\rangle + \langle A_2B_1\rangle + \langle A_2B_2\rangle - \langle A_1B_2\rangle$ one obtains
$\langle\Gamma\rangle = -\cos(\alpha_1 - \beta_1) - \cos(\alpha_2 - \beta_1) - \cos(\alpha_2 - \beta_2) + \cos(\alpha_1 - \beta_2)$.

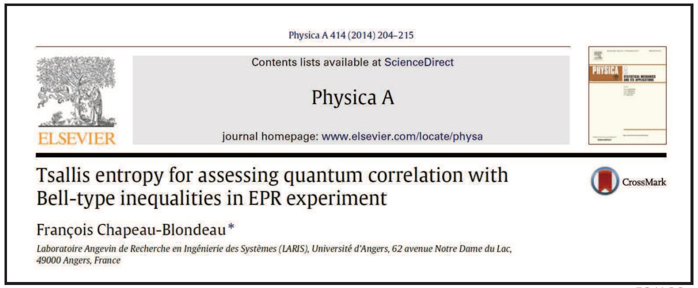
The choice $\alpha_1 = 0$, $\alpha_2 = \pi/2$ and $\beta_1 = \pi/4$, $\beta_2 = 3\pi/4$ leads to
$\langle\Gamma\rangle = -\cos(\pi/4) - \cos(\pi/4) - \cos(\pi/4) + \cos(3\pi/4) = -2\sqrt{2} < -2$.

Bell inequalities are violated by quantum measurements.

Experimentally verified (Aspect *et al.*, Phys. Rev. Lett. 1981, 1982).

Local realism and separability (classical) replaced by
a nonlocal nonseparable reality (quantum).

EPR paradox (Einstein-Podolski-Rosen) :
A. Einstein, B. Podolsky, N. Rosen ; "Can quantum-mechanical description of physical reality be considered complete ?"; *Physical Review*, 47 (1935) 777–780.
Bell inequalities :
J. S. Bell ; "On the Einstein–Podolsky–Rosen paradox"; *Physics*, 1 (1964) 195–200.
Aspect experiments :
A. Aspect, P. Grangier, G. Roger ; "Experimental test of realistic theories via Bell's theorem"; *Physical Review Letters*, 47 (1981) 460–463.



Physica A 414 (2014) 204–215

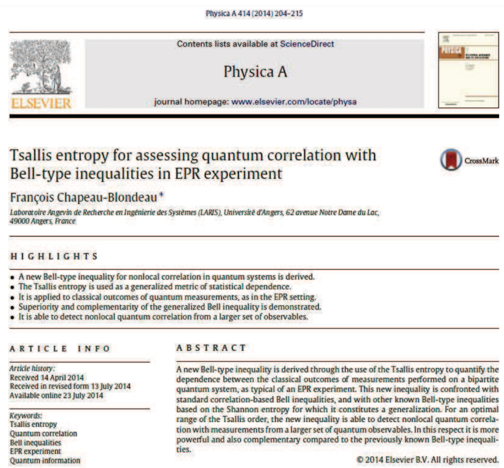
Contents lists available at ScienceDirect

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



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

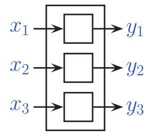
ABSTRACT

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)

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),

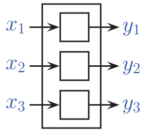
$x_1x_2x_3 \in \{011, 101, 110\} \longrightarrow y_1y_2y_3$ such that $y_1 \oplus y_2 \oplus y_3 = 1$ (reverse parity).

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 :

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



$0 \quad \oplus \quad 0 \quad \oplus \quad 0 \quad = 1\,,$ by summation of the four constraints,
$\Longrightarrow \qquad 0 = 1\,,$ 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 $|0\rangle = \frac{1}{\sqrt{2}}\big(|+\rangle + |-\rangle\big), \quad |1\rangle = \frac{1}{\sqrt{2}}\big(|+\rangle - |-\rangle\big) \Longrightarrow$

$$|00\rangle - |11\rangle = \frac{1}{2}\Big[\big(|+\rangle + |-\rangle\big)\big(|+\rangle + |-\rangle\big) - \big(|+\rangle - |-\rangle\big)\big(|+\rangle - |-\rangle\big)\Big]$$
$$= \frac{1}{2}\Big[\big(|++\rangle + |+-\rangle + |-+\rangle + |--\rangle\big) - \big(|++\rangle - |+-\rangle - |-+\rangle + |--\rangle\big)\Big]$$
$$= |+-\rangle + |-+\rangle\,;$$
$$|01\rangle + |10\rangle = \frac{1}{2}\Big[\big(|+\rangle + |-\rangle\big)\big(|+\rangle - |-\rangle\big) + \big(|+\rangle - |-\rangle\big)\big(|+\rangle + |-\rangle\big)\Big] = |++\rangle - |--\rangle\,;$$

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

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 $\{|0\rangle\,, |1\rangle\}$.

$$|\psi\rangle = \frac{1}{2}\Big(|000\rangle - |011\rangle - |101\rangle - |110\rangle\Big) = \frac{1}{2}\Big[\big(|00\rangle - |11\rangle\big)|0\rangle - \big(|01\rangle + |10\rangle\big)|1\rangle\Big]$$
$$= \frac{1}{2}\Big[\big(|+-\rangle + |-+\rangle\big)|0\rangle - \big(|++\rangle - |--\rangle\big)|1\rangle\Big]$$
$$= \frac{1}{2}\Big(|+-0\rangle + |-+0\rangle - |++1\rangle + |--1\rangle\Big) \Longrightarrow y_1 \oplus y_2 \oplus y_3 = 1 \ \text{ matched.}$$

Density operator (1/2)

Quantum system in (pure) state $|\psi_j\rangle$, measured in an orthonormal basis $\{|n\rangle\}$:

$\Longrightarrow$ probability $\Pr\{|n\rangle \big| |\psi_j\rangle\} = |\langle n|\psi_j\rangle|^2 = \langle n|\psi_j\rangle\langle\psi_j|n\rangle$.

Several possible states $|\psi_j\rangle$ with probabilities p_j (with $\sum_j p_j = 1$) :

$\Longrightarrow \Pr\{|n\rangle\} = \sum_j p_j \Pr\{|n\rangle \big| |\psi_j\rangle\} = \langle n|\Big(\sum_j p_j |\psi_j\rangle\langle\psi_j|\Big)|n\rangle = \langle n|\rho\,|n\rangle$,

with density operator $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$.

and $\Pr\{|n\rangle\} = \langle n|\rho\,|n\rangle = \mathrm{tr}(\rho\,|n\rangle\langle n|) = \mathrm{tr}(\rho\,\Pi_n)$.

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 (2/2)

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.

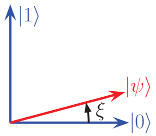
> A valid density operator on $\mathcal{H}_N \equiv$ any positive operator ρ with unit trace,
> provides a general representation for the state of a quantum system in $\mathcal{H}_N$.

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

Noisy preparation

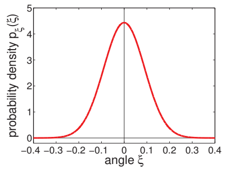
Noise-free preparation of a qubit $|\psi\rangle = |0\rangle$.

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

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 Ω of diagonal form $\Omega = \sum_{n=1}^{N} \omega_n |\omega_n\rangle\langle\omega_n|$.

When the quantum system is in state ρ, measuring Ω amounts to performing
a projective measurement on ρ in the orthonormal eigenbasis $\{|\omega_1\rangle, \dots |\omega_N\rangle\}$ of $\mathcal{H}_N$,
with the N orthogonal projectors $|\omega_n\rangle\langle\omega_n|$, for $n = 1$ to N.

The outcome yields the eigenvalue $\omega_n \in \mathbb{R}$ with probability
$\Pr\{\omega_n\} = \langle\omega_n|\rho\,|\omega_n\rangle = \mathrm{tr}(\rho\,|\omega_n\rangle\langle\omega_n|)$.

Over repeated measurements of Ω on the system prepared in the same state ρ,
the average value of Ω is

$$\langle\Omega\rangle = \sum_{n=1}^{N} \omega_n \Pr\{\omega_n\} = \sum_{n=1}^{N} \omega_n\, \mathrm{tr}(\rho\,|\omega_n\rangle\langle\omega_n|) = \mathrm{tr}\Big(\rho\sum_{n=1}^{N} \omega_n |\omega_n\rangle\langle\omega_n|\Big)$$
$$= \mathrm{tr}(\rho\Omega).$$

Density operator for the qubit

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

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

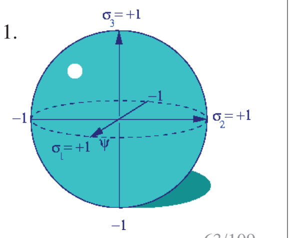
$\Longrightarrow \mathrm{tr}(\rho) = 1$.

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

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

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

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



Observables on the qubit

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

For an observable, Ω Hermitian requires $a_0 \in \mathbb{R}$ and $\vec{a} = [a_x, a_y, a_z]^\top \in \mathbb{R}^3$.
Probabilites $\Pr\{|\pm\vec{a}\rangle\} = \frac{1}{2}\left(1 \pm \vec{r}\frac{\vec{a}}{\|\vec{a}\|}\right)$ when measuring a qubit in state $\rho = \frac{1}{2}\left(\mathrm{I}_2 + \vec{r}\vec{\sigma}\right)$.
($\Longrightarrow a_0$ has no effect on $\Pr\{|\pm\vec{a}\rangle\}$).

An important observable measurable on the qubit is $\Omega = \vec{a}\vec{\sigma}$ 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 $\Pr\{\pm 1\} = \frac{1}{2}\left(1 \pm \vec{r}\vec{a}\right)$.

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

Generalized measurement

In a Hilbert space $\mathcal{H}_N$ with dimension N, the state of a quantum system is specified by a Hermitian positive unit-trace density operator ρ.

- **Projective measurement :**

Defined by a set of N orthogonal projectors $|n\rangle\langle n| = \Pi_n$,
verifying $\sum_n |n\rangle\langle n| = \sum_n \Pi_n = \mathrm{I}_N$,
and $\Pr\{|n\rangle\} = \mathrm{tr}(\rho\Pi_n)$. Moreover $\sum_n \Pr\{|n\rangle\} = 1, \forall\rho \Longleftrightarrow \sum_n \Pi_n = \mathrm{I}_N$.

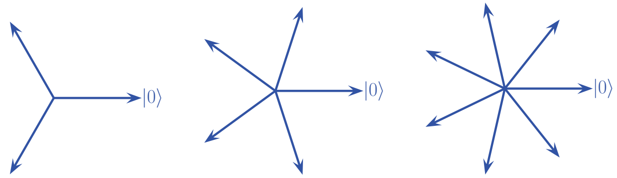
- **Generalized measurement (POVM) :** (positive operator valued measure)

Equivalent to a projective measurement in a larger Hilbert space (Naimark th.).
Defined by a set of an arbitrary number of positive operators M_m,
verifying $\sum_m \mathsf{M}_m = \mathrm{I}_N$,
and $\Pr\{\mathsf{M}_m\} = \mathrm{tr}(\rho\mathsf{M}_m)$. Moreover $\sum_m \Pr\{\mathsf{M}_m\} = 1, \forall\rho \Longleftrightarrow \sum_m \mathsf{M}_m = \mathrm{I}_N$.

A generalized measurement (POVM) for the qubit

POVM $\left\{\mathsf{M}_k = \frac{2}{K}|e_k\rangle\langle e_k|\right\}$, for $k = 0, 1, \dots K-1$, and $K > 2$,

with $|e_k\rangle = \cos\left(\frac{2\pi k}{K}\right)|0\rangle + \sin\left(\frac{2\pi k}{K}\right)|1\rangle$.



$K = 3$ $K = 5$ $K = 7$

Information in a quantum system

How much information can be stored in a quantum system ?

A classical source of information : a random variable X, with J possible states x_j, for $j = 1, 2, \dots J$, with probabilities $\Pr\{X = x_j\} = p_j$.

Information content by Shannon entropy : $H(X) = -\sum_{j=1}^{J} p_j \log(p_j) \le \log(J)$.

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 $j = 1, 2, \dots J$.

Since there is a continuous infinity of quantum states in $\mathcal{H}_N$,
an infinite quantity of information can be stored in a quantum system of dim. N
(an infinite number J), as soon as $N = 2$ with a qubit.

But how much information can be retrieved out ?

Entropy from a quantum system

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

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

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

Shannon output entropy
$$H(Y) = -\sum_{k=1}^{K} \Pr\{Y = y_k\}\log\big(\Pr\{Y = y_k\}\big)$$
$$= -\sum_{k=1}^{K} \mathrm{tr}(\rho\Lambda_k)\log\big(\mathrm{tr}(\rho\Lambda_k)\big).$$

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.

In this respect, with $H(Y) \longrightarrow \infty$ when $K \longrightarrow \infty$,
an infinite quantity of information can be drawn from a quantum system of dim. 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 dim. 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 Λ_k, for $k = 1, 2, \dots K$.

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

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

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

The input–output mutual information $I(X;Y) = H(Y) - H(Y|X) \le \chi(\rho) \le H(X)$,

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

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

The von Neumann entropy

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

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

ρ unit-trace Hermitian 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 $\rho = \mathrm{I}_N/N$.

The accessible information

For a given input ensemble $\{(p_j, \rho_j)\}$:
the accessible information $I_{\mathrm{acc}}(X;Y) = \max_{\mathrm{POVM}} I(X;Y) \le \chi(p_j, \rho_j)$,
is the maximum amount of information about X
which can be retrieved out from Y,
by using the maximally efficient generalized measurement or POVM.

For states ρ_j in $\mathcal{L}(\mathcal{H}_N)$, there always exists such an optimal POVM under the form $\{\Lambda_k = \alpha_k|\phi_k\rangle\langle\phi_k|\}$, 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]

Compression of a quantum source (1/2)

A quantum source emits states or symbols ρ_j with probabilities p_j, for $j = 1$ to J.

With $\rho = \sum_{j=1}^{J} p_j\rho_j$, the D-ary quantum entropy is $S_D(\rho) = -\mathrm{tr}\big[\rho\log_D(\rho)\big]$,
and the Holevo information is $\chi_D(p_j, \rho_j) = S_D(\rho) - \sum_{j=1}^{J} p_j S_D(\rho_j)$.

For lossless coding of the source, the average number of D-dimensional quantum systems required per source symbol is lower bounded by $\chi_D(p_j, \rho_j)$.

For pure states $\rho_j = |\psi_j\rangle\langle\psi_j|$, the lower bound $\chi_D(p_j, \rho_j) = S_D(\rho)$ is achievable
(by coding successive symbols in blocks of length $L \to \infty$).

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 source (2/2)

For mixed states ρ_j, the compressed rate is lower bounded by $\chi_D(p_j, \rho_j) \le S_D(\rho)$ but this lower bound $\chi_D(p_j, \rho_j)$ is not known to be generally achievable.

The compressed rate $S_D(\rho)$ 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 index of faithfulness, there may exist an achievable lower bound between $\chi_D(p_j, \rho_j)$ and $S_D(\rho)$. (Wilde 2016, §18.4)

The problem of general characterization of an achievable lower bound for the compressed rate of mixed states still remains open. (Wilde 2016, §18.5)

M. Horodecki; "Limits for compression of quantum information carried by ensembles of mixed states"; *Physical Review A* 57 (1997) 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.

Quantum noise (1/2)

A quantum system of $\mathcal{H}_N$ in state ρ interacting with its environment represents an open quantum system. The state ρ usually undergoes a nonunitary evolution.

With ρ_{env} the state of the environment at the onset of the interaction, the joint state $\rho \otimes \rho_{\text{env}}$ can be considered as that of an isolated system, undergoing a unitary evolution by U as $\rho \otimes \rho_{\text{env}} \longrightarrow \mathsf{U}(\rho \otimes \rho_{\text{env}})\mathsf{U}^\dagger$.

At the end of the interaction, the state of the quantum system of interest is obtained by the partial trace over the environment : $\rho \longrightarrow \mathcal{N}(\rho) = \mathrm{tr}_{\text{env}}\big[\mathsf{U}(\rho \otimes \rho_{\text{env}})\mathsf{U}^\dagger\big]$. (1)

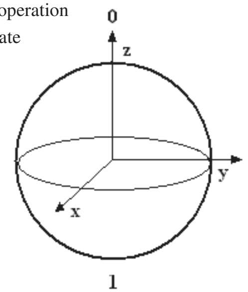
Very often, the environment incorporates a huge number of degrees of freedom, and is largely uncontrolled ; it can be understood as quantum noise inducing decoherence.

A very nice feature is that, independently of the complexity of the environment, Eq. (1) can always be put in the form $\rho \longrightarrow \mathcal{N}(\rho) = \sum_\ell \Lambda_\ell \rho \Lambda_\ell^\dagger$ operator-sum or Kraus representation, with the Kraus operators Λ_ℓ, which need not be more than N^2, satisfying $\sum_\ell \Lambda_\ell^\dagger \Lambda_\ell = \mathrm{I}_N$.

Quantum noise (2/2)

A general transformation of a quantum state ρ can be expressed by the quantum operation $\rho \longrightarrow \mathcal{N}(\rho) = \sum_\ell \Lambda_\ell \rho \Lambda_\ell^\dagger$, with $\sum_\ell \Lambda_\ell^\dagger \Lambda_\ell = \mathrm{I}_N$, representing a linear completely positive trace-preserving map, mapping a density operator on $\mathcal{H}_N$ into a density operator on $\mathcal{H}_N$.

Probabilistic interpretation : the action of the quantum operation is equivalent to randomly replacing the state ρ by the state $\Lambda_\ell \rho \Lambda_\ell^\dagger / \mathrm{tr}\big(\Lambda_\ell \rho \Lambda_\ell^\dagger\big)$ with probability $\mathrm{tr}\big(\Lambda_\ell \rho \Lambda_\ell^\dagger\big)$.



For an arbitrary qubit state defined by $\rho = \dfrac{1}{2}\big(\mathrm{I}_2 + \vec{r}\,\vec{\sigma}\big)$ with $\|\vec{r}\| \le 1$,

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

with A a 3×3 real matrix

and $\vec{c}$ a real vector in $\mathbb{R}^3$,

mapping the Bloch ball onto itself.

Quantum noise on the qubit (1/4)

Quantum noise 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 $1-p$:

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

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

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

Quantum noise on the qubit (2/4)

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

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

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

Quantum noise on the qubit (3/4)

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

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

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 $|1\rangle$.

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

Quantum noise on the qubit (4/4)

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

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

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

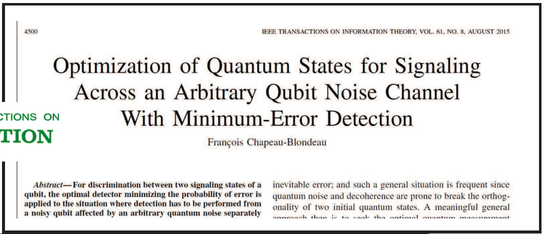
$$\Lambda_3 = \sqrt{1-p}\begin{bmatrix} \sqrt{1-\gamma} & 0 \\ 0 & 1 \end{bmatrix}, \quad \Lambda_4 = \sqrt{1-p}\begin{bmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{bmatrix},$$

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

Damping $[0,1] \ni \gamma = 1 - e^{-t/T_1} \to 1$ 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 $|1\rangle$.

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

More on quantum noise, noisy qubits :

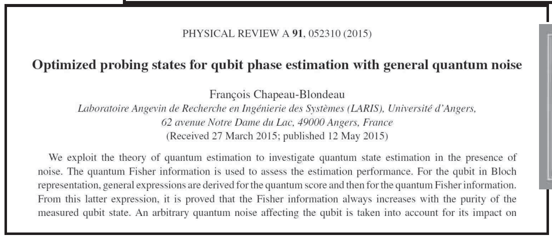


4500 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 61, NO. 8, AUGUST 2015

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



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 discrimination

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 measurement $\{\mathsf{M}_0, \mathsf{M}_1\}$ to decide with a maximal probability of success P_{suc} ?

Answer : One has $P_{\text{suc}} = P_0\,\mathrm{tr}(\rho_0\mathsf{M}_0) + P_1\,\mathrm{tr}(\rho_1\mathsf{M}_1) = P_0 + \mathrm{tr}(\mathsf{T}\mathsf{M}_1)$, with the test operator $\mathsf{T} = P_1\rho_1 - P_0\rho_0$.

Then P_{suc} is maximized by $\mathsf{M}_1^{\text{opt}} = \sum_{\lambda_n > 0} |\lambda_n\rangle\langle\lambda_n|$, the projector on the eigensubspace of T with positive eigenvalues λ_n.

The optimal measurement $\Big\{\mathsf{M}_1^{\text{opt}},\ \mathsf{M}_0^{\text{opt}} = \mathrm{I}_N - \mathsf{M}_1^{\text{opt}}\Big\}$

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

Discrimination from noisy qubits

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

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

$\longrightarrow$ Impact of the preparation and level of quantum noise,

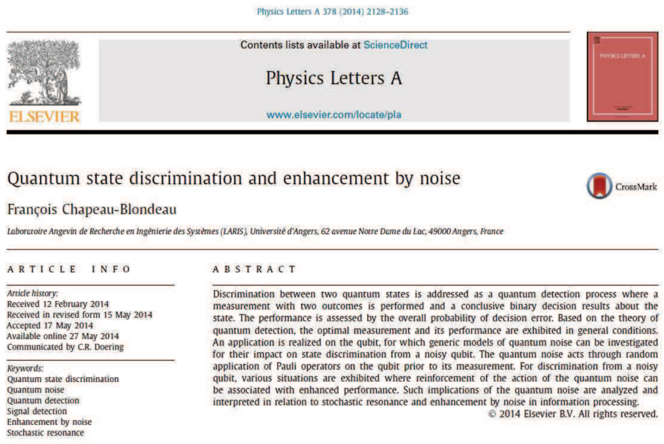
on the performance $P_{\rm suc}^{\max}$ of the optimal detector,

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

Physics Letters A

www.elsevier.com/locate/pla

Quantum state discrimination and enhancement by 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

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 among $M > 2$ quantum states

A quantum system can be in one of M alternative states ρ_m, for $m = 1$ to M, with prior probabilities P_m with $\sum_{m=1}^{M} P_m = 1$.

Problem : What is the best measurement $\{\mathsf{M}_m\}$ with M outcomes to decide with a maximal probability of success $P_{\rm suc}$?

$\Longrightarrow$ Maximize $P_{\rm suc} = \sum_{m=1}^{M} P_m \,{\rm tr}(\rho_m \mathsf{M}_m)$ according to the M operators M_m,

subject to $0 \le \mathsf{M}_m \le \mathrm{I}_N$ and $\sum_{m=1}^{M} \mathsf{M}_m = \mathrm{I}_N$.

For $M > 2$ this problem is only partially solved, in some special cases. (Barnett *et al.*, Adv. Opt. Photon. 2009).

Error-free discrimination between $M = 2$ 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. ${\rm supp}(\rho_0) \subset \mathcal{H}_N \Longleftrightarrow [{\rm supp}(\rho_0)]^\perp \supset \{\vec{0}\}$.

If $\mathcal{S}_0 = {\rm supp}(\rho_0) \cap [{\rm supp}(\rho_1)]^\perp \ne \{\vec{0}\}$, error-free discrimination of ρ_0 is possible.
If $\mathcal{S}_1 = {\rm supp}(\rho_1) \cap [{\rm supp}(\rho_0)]^\perp \ne \{\vec{0}\}$, error-free discrimination of ρ_1 is possible.

Necessity to find a three-outcome measurement $\{\mathsf{M}_0, \mathsf{M}_1, \mathsf{M}_{\rm unc}\}$:

Find $0 \le \mathsf{M}_0 \le \mathrm{I}_N$ s.t. $\mathsf{M}_0 = \vec{a}_0 \Pi_1$ "proportional" to Π_1 projector on $[{\rm supp}(\rho_1)]^\perp$,
and $0 \le \mathsf{M}_1 \le \mathrm{I}_N$ s.t. $\mathsf{M}_1 = \vec{a}_1 \Pi_0$ "proportional" to Π_0 projector on $[{\rm supp}(\rho_0)]^\perp$,
and $\mathsf{M}_0 + \mathsf{M}_1 \le \mathrm{I}_N \Longleftrightarrow \big[\mathsf{M}_0 + \mathsf{M}_1 + \mathsf{M}_{\rm unc} = \mathrm{I}_N$ with $0 \le \mathsf{M}_{\rm unc} \le \mathrm{I}_N\big]$,
maximizing $P_{\rm suc} = P_0\,{\rm tr}(\mathsf{M}_0\rho_0) + P_1\,{\rm tr}(\mathsf{M}_1\rho_1)$ ($\equiv$ min $P_{\rm unc} = 1 - P_{\rm suc}$)

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

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

M alternative states ρ_m of $\mathcal{H}_N$, with prior P_m, for $m = 1, \dots M$;
every ρ_m must be with defective rank $< N$.

For all $m = 1$ to M, define $\mathcal{S}_m = {\rm supp}(\rho_m) \cap \overbrace{\Big\{\bigcap_{\ell \ne m} [{\rm supp}(\rho_\ell)]^\perp\Big\}}^{\mathcal{K}_m}$.

For each nontrivial $\mathcal{S}_m \ne \{\vec{0}\}$, then ρ_m can go where none other ρ_ℓ can go.
$\Longrightarrow$ Error-free discrimination of ρ_m is possible,

by M_m such that $0 \le \mathsf{M}_m \le \mathrm{I}_N$ and M_m "proportional" to the projector on $\mathcal{K}_m$.

To parametrize M_m, find an orthonormal basis $\{|u_j^m\rangle\}_{j=1}^{\dim(\mathcal{K}_m)}$ of $\mathcal{K}_m$,
then $\mathsf{M}_m = \sum_{j=1}^{\dim(\mathcal{K}_m)} a_j^m |u_j^m\rangle\langle u_j^m| = \vec{a}^m\,\Pi_m$, with Π_m projector on $\mathcal{K}_m$.

Find the M_m (the $\vec{a}^m$) with $\sum_m \mathsf{M}_m \le \mathrm{I}_N$ maximizing $P_{\rm suc} = \sum_m P_m\,{\rm tr}(\mathsf{M}_m\rho_m)$.

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

Communication over a noisy quantum channel (1/3)

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

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

$\forall\{(p_j, \rho_j)\}$ and $\mathcal{N}(\cdot)$ given, there always exists a POVM to achieve $I(X;Y) = \mathcal{X}(\rho'_j, p_j)$,
i.e. $\mathcal{X}(\rho'_j, p_j)$ is an achievable maximum rate for error-free communication, by coding successive classical input symbols X in blocks of length $L \to \infty$.

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.

Communication over a noisy quantum channel (2/3)

For given $\mathcal{N}(\cdot)$ therefore $\mathcal{X}_{\max} = \max_{\{p_j, \rho_j\}} \mathcal{X}\big(\mathcal{N}(\rho_j), p_j\big)$

is the overall maximum and achievable rate for error-free communication of classical information over a noisy quantum channel,
or the classical information capacity of the quantum channel,
for product states or successive independent uses of the channel.

NB : The maximum $\mathcal{X}_{\max}$ can be achieved by no more than N^2 *pure* input states $\rho_j = |\psi_j\rangle\langle\psi_j|$ with $|\psi_j\rangle \in \mathcal{H}_N$.
[Shor, *J. Math. Phys.* 43 (2002) 4334. Shor, *Com. Math. Phys.* 246 (2004) 453].

Communication over a noisy quantum channel (3/3)

For non-product states or successive non-independent but entangled uses of the channel, due to a convexity property, the Holevo information is always superadditive $\mathcal{X}_{\max}(\mathcal{N}_1 \otimes \mathcal{N}_2) \ge \mathcal{X}_{\max}(\mathcal{N}_1) + \mathcal{X}_{\max}(\mathcal{N}_2)$. (Wilde 2016 Eq. (20.126))

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

Yet for some channels it has been found strictly superadditive,
$\mathcal{X}_{\max}(\mathcal{N}_1 \otimes \mathcal{N}_2) > \mathcal{X}_{\max}(\mathcal{N}_1) + \mathcal{X}_{\max}(\mathcal{N}_2)$ 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.

Then, which channels ? which entanglements ? which improvement ? which capacity ? . . . (largely, these are open issues).

Continuous infinite dimensional states (1/5)

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),
$\int_{-\infty}^{\infty} |x\rangle\langle x|\,dx = \mathrm{I}$ (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 position operator (observable) $\mathsf{X} = \int_{-\infty}^{\infty} x\,|x\rangle\langle x|\,dx$ (diagonal form).

Continuous infinite dimensional states (2/5)

A particle moving in three dimensions has a state $|\psi\rangle = \displaystyle\int \psi(\vec r)\,|\vec r\rangle\,d\vec r$ in an orthonormal basis $\{|\vec r\rangle\}$ of a continuous infinite-dimensional Hilbert space $\mathcal{H}$.

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

$$\int |\vec r\rangle\langle\vec r|\,d\vec r = \mathrm{I} \quad \text{(completeness).}$$

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

$$1 = \int |\psi(\vec r)|^2 d\vec r = \int \psi^*(\vec r)\,\psi(\vec r)\,d\vec r = \int \langle\psi|\vec r\rangle\langle\vec r|\psi\rangle\,d\vec r = \langle\psi|\psi\rangle\,,$$

with $|\psi(\vec r)|^2$ the probability density for finding the particle at position $\vec r$ when measuring the position observable $\vec{\mathsf{R}} = \int \vec r\,|\vec r\rangle\langle\vec r|\,d\vec r$ (diagonal form), vector operator with components the 3 commuting position operators $\mathsf{X} = \mathsf{R}_x$, $\mathsf{Y} = \mathsf{R}_y$, $\mathsf{Z} = \mathsf{R}_z$, and orthonormal basis of eigenstates $\{|\vec r\rangle\}$ i.e. $\vec{\mathsf{R}}\,|\vec r\rangle = \vec r\,|\vec r\rangle$.

Continuous infinite dimensional states (3/5)

Another orthonormal basis of $\mathcal{H}$ is formed by $\{|\vec p\rangle\}$ the eigenstates of the momentum observable $\vec{\mathsf{P}}$ or velocity $\vec{\mathsf{V}} = \vec{\mathsf{P}}/m$, also satisfying $\langle\vec p|\vec p\,'\rangle = \delta(\vec p - \vec p\,')$ (orthonormality), $\int |\vec p\rangle\langle\vec p|\,d\vec p = \mathrm{I}$ (completeness), and $\vec{\mathsf{P}}\,|\vec p\rangle = \vec p\,|\vec p\rangle$ (eigen invariance).

After De Broglie, by empirical postulation, a particle with a well defined momentum $\vec p$ is endowed with a wave vector $\vec k = \vec p/\hbar$ and a wave function

$$\phi(\vec r) = \frac{1}{(2\pi\hbar)^{3/2}}\exp\!\big(i\vec k\,\vec r\big) = \frac{1}{(2\pi\hbar)^{3/2}}\exp\!\left(i\frac{\vec p\,\vec r}{\hbar}\right) \quad \text{in position representation,}$$

defining the state $|\vec p\rangle = \displaystyle\int \phi(\vec r)\,|\vec r\rangle\,d\vec r = \frac{1}{(2\pi\hbar)^{3/2}}\int \exp\!\left(i\frac{\vec p\,\vec r}{\hbar}\right)|\vec r\rangle\,d\vec r\,,$

with $\langle\vec r|\vec p\rangle = \phi(\vec r)$.

Continuous infinite dimensional states (4/5)

Particle with arbitrary state $\mathcal{H} \ni |\psi\rangle = \displaystyle\int \underbrace{\psi(\vec r)}_{\langle\vec r|\psi\rangle}\,|\vec r\rangle\,d\vec r = \int \underbrace{\Psi(\vec p)}_{\langle\vec p|\psi\rangle}\,|\vec p\rangle\,d\vec p\,,$

with $\Psi(\vec p) = \langle\vec p|\psi\rangle = \displaystyle\int \psi(\vec r)\,\langle\vec p|\vec r\rangle\,d\vec r = \frac{1}{(2\pi\hbar)^{3/2}}\int \psi(\vec r)\exp\!\left(-i\frac{\vec p\,\vec r}{\hbar}\right)d\vec r\,,$

i.e. the wave function $\Psi(\vec p)$ in momentum representation is the Fourier transform of the wave function $\psi(\vec r)$ in position representation.

Position operator $\vec{\mathsf{R}} = \int \vec r\,|\vec r\rangle\langle\vec r|\,d\vec r$ acting on state $|\psi\rangle$ with wave function $\psi(\vec r)$ in $\vec r$-representation $\Longrightarrow \vec{\mathsf{R}}\,|\psi\rangle$ has wave function $\vec r\,\psi(\vec r)$ in $\vec r$-representation,

since $\vec{\mathsf{R}}\,|\psi\rangle = \displaystyle\int \vec r\,|\vec r\rangle\langle\vec r|\,d\vec r\,|\psi\rangle = \int \vec r\,|\vec r\rangle\underbrace{\langle\vec r|\psi\rangle}_{\psi(\vec r)}\,d\vec r = \int \underbrace{\vec r\,\psi(\vec r)}_{\text{wf of }\vec{\mathsf{R}}|\psi\rangle}\,|\vec r\rangle\,d\vec r\,.$

Continuous infinite dimensional states (5/5)

Momentum operator $\vec{\mathsf{P}} = \int \vec p\,|\vec p\rangle\langle\vec p|\,d\vec p$ (its diagonal form) acting on state $|\psi\rangle$ with wave function $\Psi(\vec p)$ in $\vec p$-representation $\Longrightarrow \vec{\mathsf{P}}\,|\psi\rangle$ has wave function $\vec p\,\Psi(\vec p)$ in $\vec p$-representation,

since $\vec{\mathsf{P}}\,|\psi\rangle = \displaystyle\int \vec p\,|\vec p\rangle\langle\vec p|\,d\vec p\,|\psi\rangle = \int \vec p\,|\vec p\rangle\underbrace{\langle\vec p|\psi\rangle}_{\Psi(\vec p)}\,d\vec p = \int \underbrace{\vec p\,\Psi(\vec p)}_{\text{wf of }\vec{\mathsf{P}}|\psi\rangle}\,|\vec p\rangle\,d\vec p\,.$

$\mathrm{FT}^{-1}\big[\vec p\,\Psi(\vec p)\big] = -i\hbar\,\vec\nabla\psi(\vec r)$ gives wave function(s) of $\vec{\mathsf{P}}\,|\psi\rangle$ in $\vec r$-representation.

Canonical commutation relations $[\mathsf{R}_k, \mathsf{P}_\ell] = i\hbar\,\delta_{k\ell}\,\mathrm{I}$, for $k, \ell = x, y, z$,

then $\Delta r_k\,\Delta p_\ell \geq \dfrac{\hbar}{2}\,\delta_{k\ell}$ Heisenberg uncertainty relations.

Continuous-time evolution of a quantum system

By empirical postulation Schrödinger equation (for isolated systems) :

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

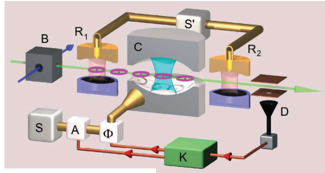
Hermitian operator Hamiltonian H, or energy operator.

A particle of mass m in potential $V(\vec r, t)$ has Hamiltonian $\mathsf{H} = \dfrac{1}{2m}\vec{\mathsf{P}}^2 + V(\vec{\mathsf{R}}, t)$,

giving rise to the Schrödinger equation for the wave function $\psi(\vec r, t) = \langle\vec r|\psi\rangle$

in $\vec r$-representation $\quad i\hbar\dfrac{\partial}{\partial t}\psi(\vec r, t) = -\dfrac{\hbar^2}{2m}\Delta\psi(\vec r, t) + V(\vec r, t)\,\psi(\vec r, t)$.

Quantum feedback control



PHYSICAL REVIEW A **80**, 013805 (2009)

Quantum feedback by discrete quantum nondemolition measurements: Towards on-demand generation of photon-number states

I. Dotsenko,[1,2,*] M. Mirrahimi,[3] M. Brune,[1] S. Haroche,[1,2] J.-M. Raimond,[1] and P. Rouchon[4]
[1]*Laboratoire Kastler Brossel, Ecole Normale Supérieure, CNRS, Université P. et M. Curie, 24 rue Lhomond, F-75231 Paris Cedex 5, France*
[2]*Collège de France, 11 Place Marcelin Berthelot, F-75231 Paris Cedex 5, France*
[3]*INRIA Rocquencourt, Domaine de Voucea*u*, BP 105, 78153 Le Chesnay Cedex, France*
[4]*Centre Automatique et Systèmes, Mathématiques et Systèmes, Mines ParisTech, 60 Boulevard Saint-Michel, 75272 Paris Cedex 6, France*
(Received 1 May 2009; published 9 July 2009)

We propose a quantum feedback scheme for the preparation and protection of photon-number states of light trapped in a high-Q microwave cavity. A quantum nondemolition measurement of the cavity field provides information on the photon-number distribution. The feedback loop is closed by injecting into the cavity a coherent pulse adjusted to increase the probability of the target photon number. The efficiency and reliability of the closed-loop state stabilization is assessed by quantum Monte Carlo simulations. We show that, in realistic experimental conditions, the Fock states are efficiently produced and protected against decoherence.

DOI: 10.1103/PhysRevA.80.013805 PACS number(s): 42.50.Dv, 02.30.Yy, 42.50.Pq

System dynamics :

• Schrödinger equation (for isolated systems)

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

Hermitian operator Hamiltonian $\mathsf{H} = \mathsf{H}_0 + \mathsf{H}_u$ (control part H_u).

$$\frac{d}{dt}\rho = -\frac{i}{\hbar}[\mathsf{H},\rho] \quad \text{(Liouville – von Neumann equa.)} \Longrightarrow \rho(t_2) = \mathsf{U}(t_1,t_2)\,\rho(t_1)\,\mathsf{U}^\dagger(t_1,t_2).$$

• Lindblad equation (for open systems)

$$\frac{d}{dt}\rho = -\frac{i}{\hbar}[\mathsf{H},\rho] + \sum_j\Big(2\mathsf{L}_j\rho\mathsf{L}_j^\dagger - \{\mathsf{L}_j^\dagger\mathsf{L}_j,\rho\}\Big), \quad \text{Lindblad op. } \mathsf{L}_j \text{ for interaction with environment.}$$

Measurement : Arbitrary operators $\{\mathsf{E}_m\}$ such that $\sum_m \mathsf{E}_m^\dagger\mathsf{E}_m = \mathrm{I}_N$,

$\Pr\{m\} = \mathrm{tr}(\mathsf{E}_m\rho\mathsf{E}_m^\dagger) = \mathrm{tr}(\rho\mathsf{E}_m^\dagger\mathsf{E}_m) = \mathrm{tr}(\rho\mathsf{M}_m)$ with $\mathsf{M}_m = \mathsf{E}_m^\dagger\mathsf{E}_m$ positive,

Post-measurement state $\rho_m = \dfrac{\mathsf{E}_m\rho\mathsf{E}_m^\dagger}{\mathrm{tr}(\mathsf{E}_m\rho\mathsf{E}_m^\dagger)}$.

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 the Fisher information. The task is then specified to estimating the phase of a qubit in a rotation around an arbitrary axis, equivalent to estimating the phase of an arbitrary single-qubit quantum gate. The analysis enables determination of the optimal probing states best resistant to the noise, and proves that they always are pure states but need to be specifically matched to the noise. This optimization is worked out for several noise models important to the qubit. An adaptive scheme and a Bayesian approach are presented to handle phase-dependent solutions.

DOI: 10.1103/PhysRevA.91.052310 PACS number(s): 03.67.−a, 42.50.Lc, 05.40.−a

PHYSICAL REVIEW A **94**, 022334 (2016)

Optimizing qubit phase estimation

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 5 June 2016; revised manuscript received 2 August 2016; published 24 August 2016)

The theory of quantum state estimation is exploited here to investigate the most efficient strategies for this task, especially targeting a complete picture identifying optimal conditions in terms of Fisher information, quantum measurement, and associated estimator. The approach is specified to estimation of the phase of a qubit in a rotation around an arbitrary given axis, equivalent to estimating the phase of an arbitrary single-qubit quantum gate, both in noise-free and then in noisy conditions. In noise-free conditions, we establish the possibility of defining an optimal quantum probe, optimal quantum measurement, and optimal estimator together capable of achieving the ultimate best performance uniformly for any unknown phase. With arbitrary quantum noise, we show that in general the optimal solutions are phase dependent and require adaptive techniques for practical implementation. However, for the important case of the depolarizing noise, we again establish the possibility of a quantum probe, quantum measurement, and estimator uniformly optimal for any unknown phase. In this way, for qubit phase estimation, without and then with quantum noise, we characterize the phase-independent optimal solutions when they generally exist, and also identify the complementary conditions where the optimal solutions are phase dependent and only adaptively implementable.

DOI: 10.1103/PhysRevA.94.022334

Quantum Information Processing
July 2016, Volume 15, Issue 7, pp 2685–2700

Quantum image coding with a reference-frame-independent scheme

Authors | Authors and affiliations

François Chapeau-Blondeau, Etienne Belin

Article
First Online: 23 April 2016
DOI: 10.1007/s11128-016-1318-8

Cite this article as:
Chapeau-Blondeau, F. & Belin, E.
Quantum Inf Process (2016) 15: 2685.
doi:10.1007/s11128-016-1318-8

107 Downloads

Abstract

For binary images, or bit planes of non-binary images, we investigate the possibility of a quantum coding decodable by a receiver in the absence of reference frames shared with the emitter. Direct image coding with one qubit per pixel and non-aligned frames leads to decoding errors equivalent to a quantum bit-flip noise increasing with the misalignment. We show the feasibility of frame-invariant coding by using for each pixel a qubit pair prepared in one of two controlled entangled states. With just one common axis shared between the emitter and receiver, exact decoding for each pixel can be obtained by means of two two-outcome projective measurements operating separately on each qubit of the pair. With strictly no alignment information between the emitter and receiver, exact decoding can be obtained by means of a two-outcome projective measurement operating jointly on the qubit pair. In addition, the frame-invariant coding is shown much more resistant to quantum bit-flip noise compared to the direct non-invariant coding. For a cost per pixel of two (entangled) qubits instead of one, complete frame-invariant image coding and enhanced noise resistance are thus obtained.

Dimensionality explosion in quantum theory

• The most elementary and nontrivial object of quantum information is the qubit, representable with a state vector $|\psi_1\rangle$ in the 2-dimensional complex Hilbert space $\mathcal{H}_2$.
Such a pure state $|\psi_1\rangle$ of a qubit is thus a 2-dimensional object (a 2×1 vector).

On such a pure state $|\psi_1\rangle$, any unitary evolution is described by a unitary operator belonging to the 4-dimensional space $\mathcal{L}(\mathcal{H}_2)$, the space of linear applications or operators on $\mathcal{H}_2$.
A unitary evolution of a pure state $|\psi_1\rangle$ of a qubit is thus a 4-dimensional object (a 2×2 matrix).

• Accounting for the essential property of decoherence on a qubit, requires it be represented with the extended notion of a density operator ρ_1, existing in the 4-dimensional space $\mathcal{L}(\mathcal{H}_2)$.
Such a mixed state ρ_1 of a qubit is thus a 4-dimensional object (a 2×2 matrix).

On such a mixed state ρ_1 of a qubit, any nonunitary evolution such as decoherence, should be described by an operator belonging to the 16-dimensional space $\mathcal{L}\big(\mathcal{L}(\mathcal{H}_2)\big)$.
A nonunitary evolution of a mixed state ρ_1 of a qubit is thus a 16-dimensional object (a 4×4 matrix).

• The essential property of intrication starts to arise with a qubit pair. A qubit pair in a pure state $|\psi_2\rangle$ exists in the 4-dimensional Hilbert space $\mathcal{H}_2 \otimes \mathcal{H}_2$, while a qubit pair in a mixed state is represented by a density operator ρ_2 existing in the 16-dimensional Hilbert space $\mathcal{L}(\mathcal{H}_2 \otimes \mathcal{H}_2)$.
A mixed state ρ_2 of a qubit pair is thus a 16-dimensional object (a 4×4 matrix).

On such a mixed state ρ_2 of a qubit pair, any nonunitary evolution such as decoherence, should be described by an operator belonging to the 256-dimensional space $\mathcal{L}\big(\mathcal{L}(\mathcal{H}_2 \otimes \mathcal{H}_2)\big)$.
A nonunitary evolution of a mixed state ρ_2 of a qubit pair is thus a 256-dimensional object (a 16×16 matrix).

Technologies for quantum computer

♦ Quantum-circuit decomposition approach :

• Photons : with mirrors, beam splitters, phase shifters, polarizers.

• Trapped ions : confined by electric fields, qubits stored in stable electronic states, manipulated with lasers. Interact via phonons.

• Light & atoms in cavity : Cavity quantum electrodynamics (Jaynes-Cummings model).

2012 Nobel Prize of D. Wineland (USA) and S. Haroche (France).

• Nuclear spin : manipulated with radiofrequency electromagnetic waves.

• Superconducting Josephson junctions : in electric circuits and control by electric signals.

(Quantronics Group, CEA Saclay, France.)

• Electron spins : in quantum dots or single-electron transistor, and control by electric signals.

M. Veldhorst *et al.*; "A two-qubit logic gate in silicon"; *Nature* 526 (2015) 410–414.

♦ Quantum annealing, adiabatic quantum computation :

For finding the global minimum of a given objective function, coded as the ground state of an objective Hamiltonian.

Computation decomposed into a slow continuous transformation of an initial Hamiltonian into a final Hamiltonian, whose ground states contain the solution.

Starts from a superposition of all candidate states, as stationary states of a simple controllable initial Hamiltonian.

Probability amplitudes of all candidate states are evolved in parallel, with the time-dependent Schrödinger equation from the Hamiltonian progressively deformed toward the (complicated) objective Hamiltonian to solve.

Quantum tunneling out of local minima helps the system converge to the ground state solution.

A class of universal Hamiltonians is the lattice of qubits (with Pauli operators X, Z) :

$$\mathrm{H} = \sum_j h_j \mathrm{Z}_j + \sum_k g_k \mathrm{X}_k + \sum_{j,k} J_{jk}(\mathrm{Z}_j\mathrm{Z}_k + \mathrm{X}_j\mathrm{X}_k) + \sum_{j,k} K_{jk}\mathrm{X}_j\mathrm{Z}_k \,.$$

J. D. Biamonte, P. J. Love; "Realizable Hamiltonians for universal adiabatic quantum computers"; *Physical Review A* 78 (2008) 012352,1–7.

A commercial quantum computer : Canadian D-Wave :

Since 2011 : a 128-qubit processor, with superconducting circuit implementation.

Based on quantum annealing, to solve optimization problems.

May 2013 : D-Wave 2, with 512 qubits. $15-million joint purchase by NASA & Google.

Aug. 2015 : D-Wave 2X with 1000 qubits. Jan. 2017 : D-Wave 2000Q with 2000 qubits.

M. W. Johnson, *et al.*; "Quantum annealing with manufactured spins"; *Nature* 473 (2011) 194–198.
T. Lanting, *et al.*; "Entanglement in a quantum annealing processor"; *Phys. Rev. X* 4 (2014) 021041.

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information

Article | Talk | Read | Edit | View history | Search Wikipedia

Quantum Experiments at Space Scale

From Wikipedia, the free encyclopedia

Quantum Experiments at Space Scale (**QUESS**; Chinese: 量子科学实验卫星; pinyin: *Liàngzǐ kēxué shíyàn wèixīng*; literally: "Quantum Science Experiment Satellite"), is an international research project in the field of quantum physics. A satellite, nicknamed **Micius** or **Mozi** (Chinese: 墨子) after the ancient Chinese philosopher and scientist, is operated by the Chinese Academy of Sciences, as well as ground stations in China. The University of Vienna and the Austrian Academy of Sciences are running the satellite's European receiving stations.[4][5] QUESS is a proof-of-concept mission designed to facilitate quantum optics experiments over long distances to allow the development of quantum encryption and quantum teleportation technology.[5] Quantum encryption uses the principle of entanglement to facilitate communication that is totally safe against eavesdropping, let alone decryption, by a third party. By producing pairs of entangled photons, QUESS will allow ground stations separated by many thousands of kilometres to establish secure quantum channels.[3] QUESS itself has limited communication capabilities: it needs line-of-sight, and can only operate when not in sunlight.[6] If QUESS is successful, further Micius satellites will follow, allowing a European–Asian quantum-encrypted network by 2020, and a global network by 2030.[6][7]

The mission will cost around US$100 million in total.[2]

Quantum Experiments at Space Scale	
Names	Quantum Space Satellite Micius / Mozi
Mission type	Technology demonstrator
Operator	Chinese Academy of Science
COSPAR ID	2016-051A[1]
Mission duration	2 years (planned)
Spacecraft properties	
Manufacturer	Chinese Academy of Science
BOL mass	631 kg (1,391 lb)
Start of mission	
Launch date	17:40 UTC, 16 August 2016[2]
Rocket	Long March 2D
Launch site	Jiuquan LA-4
Contractor	Shanghai Academy of Spaceflight Technology

QUATRE GÉANTS ET UN PIONNIER POUR FABRIQUER LE PROCESSEUR DE DEMAIN

Google — POUR LA SUPRÉMATIE QUANTIQUE
De ses échanges initiaux avec D-Wave, Google a gardé une démarche hybride qui mêle l'approche souple et dédiée à une gamme de problèmes de D-Wave et la correction d'erreurs à la IBM. Le géant de Mountain View travaillerait sur un prototype de 20 qubits et espère « démontrer la suprématie quantique dans le courant de 2018 » avec une machine de 49 qubits.

IBM — PAS À PAS VERS L'UNIVERSEL
Lancée en 2016, l'IBM Q Experience se traduit aujourd'hui par un ordinateur de 16 qubits accessible dans le cloud. Utilisant des qubits supraconducteurs implantés sur du silicium et s'attachant à maîtriser les erreurs liées à la décohérence, IBM dispose aussi d'une machine de 17 qubits sur laquelle il travaille pour développer un ordinateur universel d'ici à 2026.

intel — LE SILICIUM ROI
Intel veut mettre le silicium au cœur de l'ordinateur quantique. Avec l'avantage de pouvoir utiliser le savoir-faire et les process traditionnels. L'américain travaille sur un qubit matérialisé par un électron piégé dans un transistor modifié. Mais Intel suit aussi la piste supraconductrice, comme en témoigne la puce de 17 qubits supraconducteurs présentée mi-octobre.

Microsoft — LE PARI TOPOLOGIQUE
La firme de Redmond suit une voie originale en pariant pour ses qubits sur des tresses de quasi-particules, appelées fermions de Majorana, générées dans des gaz d'électrons 2D. L'intérêt de cette approche dite topologique est d'avoir une protection intrinsèque contre la décohérence et donc de limiter la redondance en qubits utilisée pour corriger les erreurs. Une première machine est attendue « pour bientôt ».

D:Wave — LE PIONNIER CONTESTÉ
Ce spécialiste américain né en 1999 est le seul à avoir déjà vendu des machines (à la Nasa, à Lockheed Martin...) et a présenté en 2017 son nouveau modèle à 2 000 qubits supraconducteurs. Mais ces qubits connaissent beaucoup d'erreurs et le caractère quantique des calculs est contesté. Une chose est sûre, la machine de D-Wave est cantonnée à des calculs spécifiques (mais très utiles) d'optimisation.

L'Usine Nouvelle, N°3536 du 2 nov. 2017.

« NOUS INTÉGRERONS DES ACCÉLÉRATEURS QUANTIQUES »

Philippe Vannier est conseiller d'Atos pour la technologie. Il affirme que l'ordinateur quantique est un impératif pour surmonter la fin de la loi de Moore.

La communauté française du chiffrement se mobilise. Elle a lancé en début d'année l'initiative Risq (Regroupement de l'industrie française pour la sécurité post-quantique). Une quinzaine d'acteurs se sont regroupés, à la fois des laboratoires académiques (CEA, Inria, Irisa, UPMC...), des grands groupes et des PME (Airbus, Gemalto, Orange, Thales, CS, Secure-IC...). L'initiative a bénéficié d'un financement du programme des investissements d'avenir à hauteur d'environ 7,5 millions d'euros sur trois ans dans le cadre de l'appel à projets liés aux grands défis du numérique. Vu la sensibilité du sujet, l'État soutient et suit de près cette initiative, fournissant des renforts de l'Agence nationale pour la sécurité des systèmes d'information (Anssi) et de la Direction générale de l'armement (DGA). « Le projet Risq définit une feuille de route pour la commercialisation de produits de sécurité post-quantique », précise Adrien Facon, le porte-parole de cette initiative. Des démonstrateurs sont prévus pour répondre aux différents cas

« Le projet Risq définit une feuille de route pour la commercialisation de produits de sécurité post-quantique. »

Adrien Facon, porte-parole du Regroupement de l'industrie française pour la sécurité post-quantique (Risq)

L'USINE NOUVELLE I N° 3536 I 2 NOVEMBRE 2017

INDUSTRIELS La puissance de l'ordinateur quantique séduit déjà. Après Lockheed Martin, Volkswagen et Biogen travaillent avec le pionnier D-Wave et Airbus a monté une équipe dédiée.

FROM RESEARCH TO INDUSTRY cea

From research to industry
English Portal

CONTACT | PARTNERS / SUPPLIERS | FRENCH PORTAL

ABOUT CEA | RESEARCH AREAS | NEWS | RESOURCES | EUROPEAN PROJECTS' NEWSLETTER

You are here : Home > News >

▸ ALL THE NEWS
▸ PRESS CONTACTS
▸ EUROPEAN PROJECTS' NEWSLETTER

Press release | **International** | **Partnerships** | **European & international partnerships** | New technologies | Micro-nanotechnologies | Computing | Quantum Physics

Australian Prime Minister and French President announce plans for new quantum computing collaboration

© Fotolia.com / MG

The Prime Minister of Australia, Malcolm Turnbull, and the President of France, Emmanuel Macron, today announced plans for a new French-Australian collaboration between Australia's first quantum computing company, Silicon Quantum Computing Pty Ltd (SQC), and the world leading French research and development organisation, the Commissariat à l'Energie Atomique et aux Energies Alternatives (the CEA).

Published on 2 May 2018

http://www.cea.fr/english/Pages/News/Australian-Prime-Minister-and-French-President-announce-plans-for-new-quantum-computing-collaboration.aspx