Quantum information, quantum computation : An introduction.

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

École Doctorale Sciences et Technologies de l'Information et Mathématiques

Une définition (large)

Exploiter les propriétés et phénomènes quantiques pour le traitement de l'information et le calcul.

Motivations pour le quantique

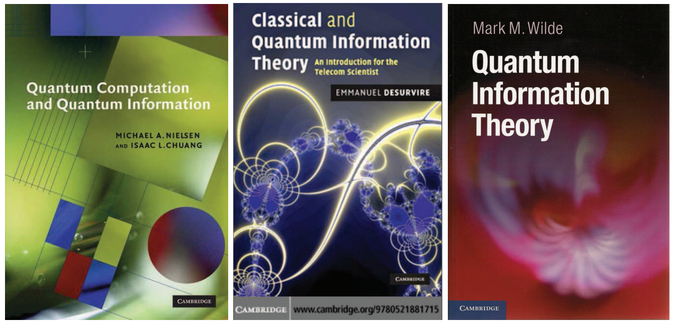
pour le traitement de l'information :

1) Quand on utilise des systèmes élémentaires (photons, électrons, atomes, nanodevices, ...).

2) Pour bénéficier d'effets purement quantiques (parallèlisme, intrication, ...).

3) Domaine de recherche récent, riche et largement ouvert.

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

$|\psi\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix}$, $|\psi\rangle^\dagger = \langle\psi| = [\alpha^*, \beta^*]$ $\Longrightarrow \langle\psi|\psi\rangle = \|\psi\|^2 = |\alpha|^2 + |\beta|^2$ 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 $\{|0\rangle, |1\rangle\}$,

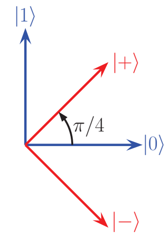
$\Longrightarrow$ only 2 possible outcomes (Born rule) :
state $|0\rangle$ with probability $|\alpha|^2 = |\langle 0|\psi\rangle|^2 = \langle 0|\psi\rangle\langle\psi|0\rangle = \langle 0|\Pi_\psi|0\rangle$, or
state $|1\rangle$ with probability $|\beta|^2 = |\langle 1|\psi\rangle|^2 = \langle 1|\psi\rangle\langle\psi|1\rangle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

Measurement :
- a probabilistic process,
- as a 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 $\mathcal{H}_2$

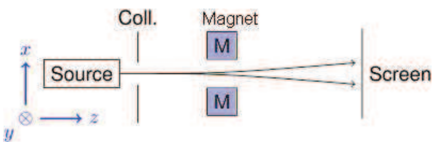
$$\left\{ |+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)\ ; \quad |-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) \right\}.$$



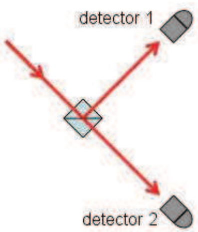
$\Longleftrightarrow$ Computational orthonormal basis

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

Experiments



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



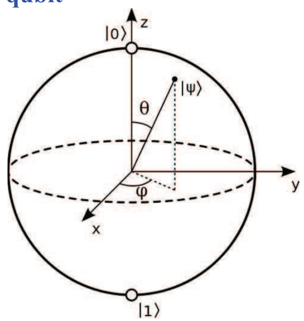
Two states of polarization of a photon :
(Nicol prism, Glan-Thompson, polarizing beam splitter, ...)

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



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.

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

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

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.

Entangled states

- Example of a separable state of two qubits AB :

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

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 $\{|1\rangle, \dots |N\rangle\}$ of $\mathcal{H}_N$,
and the N orthogonal projectors $|n\rangle\langle n|$, for $n = 1$ to N.

Also, any Hermitian (i.e. $\Omega = \Omega^\dagger$) operator Ω on $\mathcal{H}_N$,
has its eigenstates forming an orthonormal basis $\{|\omega_1\rangle, \dots |\omega_N\rangle\}$ of $\mathcal{H}_N$.
Therefore, any Hermitian operator Ω on $\mathcal{H}_N$ defines a valid measurement,

and has a spectral decomposition $\Omega = \sum_{n=1}^{N} \omega_n\,|\omega_n\rangle\langle\omega_n|$, with the real eigenvalues ω_n.

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

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

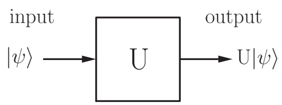
The average is $\langle\Omega\rangle = \sum_n \omega_n \Pr\{\omega_n\} = \langle\psi|\Omega|\psi\rangle$.

Computation on a qubit

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

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

$\equiv$ quantum gate



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

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

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

$\Longrightarrow$ in a compact notation $\mathrm{H}\,|x\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + (-1)^x\,|1\rangle\Big)$, $\forall\, x \in \{0, 1\}$.

Pauli gates

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

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

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

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

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

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

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

In general, the gates U and $e^{i\phi}\mathrm{U}$ 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 $e^{i\phi}\mathrm{U}_\xi$ with

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

where $\vec{n} = [n_x, n_y, n_z]^\top$ is a real unit vector of $\mathbb{R}^3$,

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

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

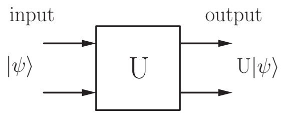
For example : $\mathrm{W} = \sqrt{\sigma_x} = e^{i\pi/4}\big[\cos(\pi/4)\,\mathrm{I}_2 - i\sin(\pi/4)\,\sigma_x\big]$.

Computation on a pair of qubits

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

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

$\equiv$ quantum gate
(always reversible)



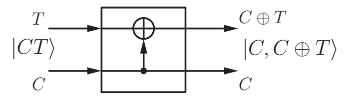
Completely defined for instance by the transformation of the four state vectors of the computational basis $\big\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\big\}$.

- 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)

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



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

$(\text{C-Not})^2 = \mathrm{I}_2 \Longleftrightarrow (\text{C-Not})^{-1} = \text{C-Not} = (\text{C-Not})^\dagger$ 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 $|\psi\rangle \in \mathcal{H}_2^{\otimes N} \longrightarrow \mathrm{U}\,|\psi\rangle$ normalized vector $\in \mathcal{H}_2^{\otimes N}$.

$\equiv$ quantum gate : N input qubits $\xrightarrow{\mathrm{U}}$ N output qubits.

Completely defined for instance by the transformation of the 2^N state vectors of the computational basis.

Any N-qubit quantum gate or circuit may always be composed from two-qubit C-Not gates and single-qubit gates (universality).

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 $|\psi\rangle\,|\psi\rangle$?

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

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

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

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

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

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 $\mathcal{H}_2^{\otimes N}$: $\big\{|\vec{x}\rangle\,, \vec{x} \in \{0,1\}^N\big\}$,
just like a classical gate.

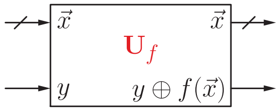
Yet, the quantum gate U can be operated
on any linear superposition of the basis states $\big\{|\vec{x}\rangle\,, \vec{x} \in \{0,1\}^N\big\}$.

This is quantum parallelism, with no classical analog.

Parallel evaluation of a function (1/3)

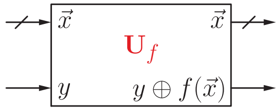
A classical function $f(\cdot)$ from N bits to 1 bit
$$\vec{x} \in \{0,1\}^N \longrightarrow f(\vec{x}) \in \{0,1\}.$$

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 $y = 1$.

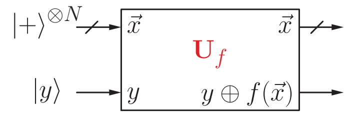
Parallel evaluation of a function (2/3)



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

$$|\vec{x}\rangle\,|y=0\rangle \xrightarrow{\mathrm{U}_f} |\vec{x}\rangle\,|f(\vec{x})\rangle$$
$$|\vec{x}\rangle\,|y=1\rangle \longrightarrow |\vec{x}\rangle\,\big|\overline{f(\vec{x})}\big\rangle$$
$$|\vec{x}\rangle\,|+\rangle \longrightarrow |\vec{x}\rangle\,\frac{1}{\sqrt{2}}\Big[|f(\vec{x})\rangle + \big|\overline{f(\vec{x})}\big\rangle\Big] = |\vec{x}\rangle\,|+\rangle$$
$$|\vec{x}\rangle\,|-\rangle \longrightarrow |\vec{x}\rangle\,\frac{1}{\sqrt{2}}\Big[|f(\vec{x})\rangle - \big|\overline{f(\vec{x})}\big\rangle\Big] = |\vec{x}\rangle\,|-\rangle\,(-1)^{f(\vec{x})}$$

Parallel evaluation of a function (3/3)



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

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

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

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

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

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

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

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

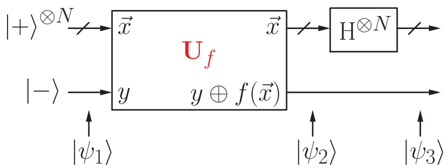
Quantumly : One evaluation of $f(\cdot)$ is enough (on a suitable superposition).

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

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

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

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

Deutsch-Jozsa algorithm (3/5)

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

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

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

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

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

Deutsch-Jozsa algorithm (4/5)

So $|\psi\rangle = \dfrac{1}{2^N} \displaystyle\sum_{\vec z \in \{0,1\}^N} u(\vec z)\,|\vec z\rangle$ with $u(\vec z) = \displaystyle\sum_{\vec x \in \{0,1\}^N} (-1)^{f(\vec x)+\vec x\vec z}$.

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

• When $f(\cdot)$ constant : $u(\vec z = \vec 0) = 2^N(-1)^{f(\vec 0)} = \pm 2^N \Longrightarrow$ 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 $u(\vec z \neq \vec 0) = 0$.
$\Longrightarrow$ When $|\psi\rangle$ is measured, N states $|0\rangle$ are found.

• When $f(\cdot)$ balanced : $u(\vec z = \vec 0) = 0 \Longrightarrow |\psi\rangle$ 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 (1993) 553–558.
Extension to arbitrary $N \geq 2$.

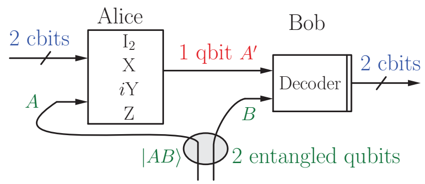
[3] E. Bernstein, U. Vazirani; "Quantum complexity theory"; *SIAM Journal on Computing* 26 (1997) 1411–1473.
Extension to $f(\vec x) = \vec a\vec x$ or $f(\vec x) = \vec a\vec x \oplus \vec b$, to find binary N-word $\vec a \longrightarrow$ by producing output $|\psi\rangle = |\vec a\rangle$.

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

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



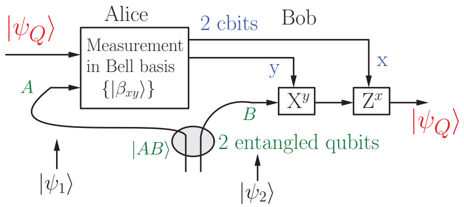
$\mathrm{I}_2 \otimes \mathrm{I}_2\,|AB\rangle = |\beta_{00}\rangle$
$\mathrm{X} \otimes \mathrm{I}_2\,|AB\rangle = |\beta_{01}\rangle$
$\mathrm{Z} \otimes \mathrm{I}_2\,|AB\rangle = |\beta_{10}\rangle$
$i\mathrm{Y} \otimes \mathrm{I}_2\,|AB\rangle = |\beta_{11}\rangle$

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 $|AB\rangle = \dfrac{1}{\sqrt 2}\big(|00\rangle + |11\rangle\big) = |\beta_{00}\rangle$.



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 $\alpha_0|1\rangle + \alpha_1|0\rangle \xrightarrow{\mathrm{X}} \cdot \xrightarrow{\mathrm{I}_2} |\psi_Q\rangle$

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

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

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 (1/3) *Phys. Rev. Lett.* 79 (1997) 325.

• Finds an item out of N in an unsorted database, in $O(\sqrt N)$ complexity instead of $O(N)$ classically.

• An N-dimensional quantum system in $\mathcal{H}_N$ with orthonormal basis $\{|1\rangle, \cdots, |N\rangle\}$, the basis states $|n\rangle$, $n = 1, \ldots N$, representing the N items stored in the database.

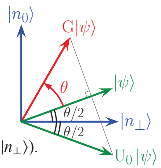
• A set of N real values $\{\omega_1, \cdots, \omega_N\}$ representing the address of each item $|n\rangle$ in the database.

• The unsorted database is in the state $|\psi\rangle = \dfrac{1}{\sqrt N}\displaystyle\sum_{n=1}^{N} |n\rangle$.

• A query of the database, in order to obtain the address ω_n of an item $|n\rangle$, is performed by a measurement of the observable $\Omega = \displaystyle\sum_{n=1}^{N} \omega_n |n\rangle\langle n|$.

• Any specific item $|n_0\rangle$ is obtained as measurement outcome with its eigenvalue (address) ω_{n_0}, with the probability $|\langle n_0|\psi\rangle|^2 = 1/N$ (since $\langle n_0|\psi\rangle = 1/\sqrt N$).

Grover quantum search algorithm (2/3)



• For this specific item $|n_0\rangle$ that we want to retrieve (obtain its address ω_{n_0}), it is possible to amplify this uniform probability $|\langle n_0|\psi\rangle|^2 = 1/N$.

• Let $|n_\perp\rangle = \dfrac{1}{\sqrt{N-1}}\displaystyle\sum_{n\neq n_0}^{N} |n\rangle$ normalized state $\perp |n_0\rangle \Longrightarrow |\psi\rangle$ in plane $(|n_0\rangle, |n_\perp\rangle)$.

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

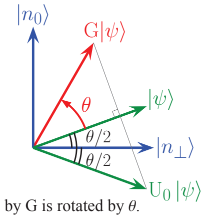
• Let $|\psi_\perp\rangle$ normalized state $\perp |\psi\rangle$ in plane $(|n_0\rangle, |n_\perp\rangle)$.

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

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

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

Grover quantum search algorithm (3/3)



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

- $\mathrm{G}\,|\psi\rangle = \mathrm{U}_\psi \mathrm{U}_0\,|\psi\rangle = \mathrm{U}_\psi\Big(|\psi\rangle - \dfrac{2}{\sqrt{N}}\,|n_0\rangle\Big) = \Big(1 - \dfrac{4}{N}\Big)|\psi\rangle + \dfrac{2}{\sqrt{N}}\,|n_0\rangle$.

So after rotation by θ the rotated state $\mathrm{G}\,|\psi\rangle$ is closer to $|n_0\rangle$.

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

So $\mathrm{G}^2\,|\psi\rangle$ rotates $|\psi\rangle$ by 2θ toward $|n_0\rangle$, and $\mathrm{G}^k\,|\psi\rangle$ 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 $\mathrm{G}^K\,|\psi\rangle \approx |n_0\rangle$ is measured, the probability is almost 1 to obtain $|n_0\rangle$ and its address $\omega_{n_0} \Longrightarrow$ The searched item 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

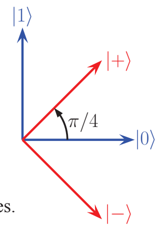
Message X, a string of bits.
Cryptographic key K, a completely random (i.i.d.) string of bits.

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 $4N$ 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.

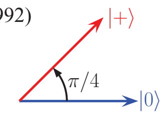
♦ Once the whole string of $4N$ bits from Alice has been received by Bob, Alice publicly discloses the sequence of her basis choices.

♦ Bob keeps only the positions where his choices of basis coincide with those of Alice to obtain a 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 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

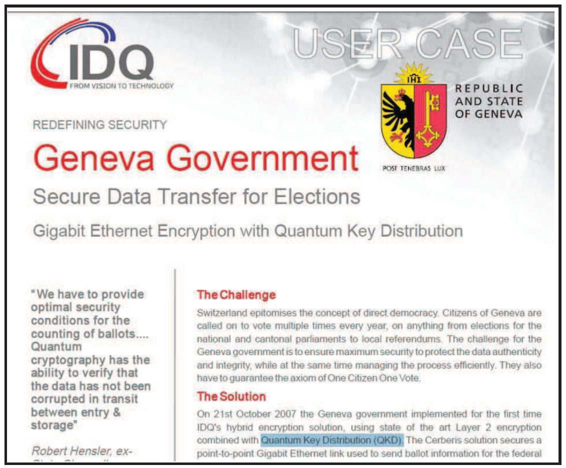
ID Quantique (IDQ) is the world leader in quantum-safe crypto solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions and services to the financial industry, enterprises and

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)

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 $\Omega(\theta) = \sin(\theta)\mathrm{X} + \cos(\theta)\mathrm{Z}$, 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 $\langle AB\rangle = \langle \psi_{AB}\,|\,\Omega(\alpha) \otimes \Omega(\beta)\,|\,\psi_{AB}\rangle = -\cos(\alpha - \beta)$.

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 $-2 \le \langle\Gamma\rangle \le 2$. Bell inequalities (1964).

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 $A_1 \equiv \Omega(\alpha_1)$ or $A_2 \equiv \Omega(\alpha_2)$,
and Bob chooses to randomly switch between measuring $B_1 \equiv \Omega(\beta_1)$ or $B_2 \equiv \Omega(\beta_2)$.

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.

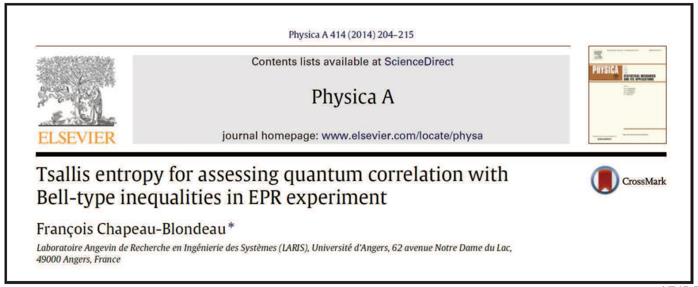
Experimentally verified (Aspect *et al.*, Phys. Rev. Lett. 1981, 1982).

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.

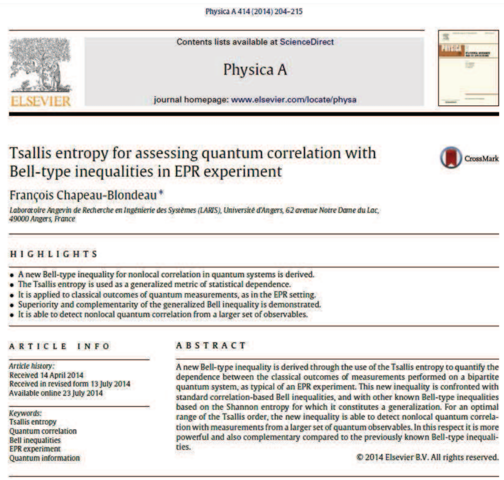
Bell inequalities :
J. S. Bell ; "On the Einstein–Podolsky–Rosen paradox"; *Physics*, 1 (1964) 195–200.

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 :

$$x_1x_2x_3 = 000 \longrightarrow y_1y_2y_3 \ \text{such that}\ y_1 \oplus y_2 \oplus y_3 = 0,$$
$$x_1x_2x_3 \in \{011, 101, 110\} \longrightarrow y_1y_2y_3 \ \text{such that}\ y_1 \oplus y_2 \oplus y_3 = 1.$$

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

GHZ states (2/5)

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

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

$0 \ \oplus\ 0\ \oplus\ 0\ = 1$, by summation of the four constraints,
$\Longrightarrow$ $0 = 1$, so the four constraints are incompatible.

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

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

GHZ states (3/5)

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

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

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

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

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

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

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

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 $\{p_j, |\psi_j\rangle\}$, described by the density operator ρ.

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

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 $|\psi_j\rangle \to \mathrm{U}|\psi_j\rangle \Longrightarrow \rho \to \mathrm{U}\rho\mathrm{U}^\dagger$.

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 $\mathcal{H}_2$, orthogonal for the Hilbert-Schmidt inner product $\mathrm{tr}(\mathrm{A}^\dagger\mathrm{B})$.

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

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

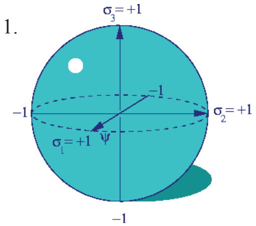
$\rho = \rho^\dagger \Longrightarrow r_x = r_x^*, \;\; r_y = r_y^*, \;\; r_z = r_z^* \Longrightarrow r_x, r_y, r_z$ real.

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

$\|\vec{r}\| < 1$ for 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 eigenvectors $|\pm\vec{a}\rangle\langle\pm\vec{a}| = \dfrac{1}{2}\big(\mathrm{I}_2 \pm \vec{a}\,\vec{\sigma}/\sqrt{\vec{a}^2}\big)$.

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

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 probabilites $\Pr\{\pm 1\} = \dfrac{1}{2}\big(1 \pm \vec{r}\,\vec{a}\big)$ for a qubit in state $\rho = \dfrac{1}{2}\big(\mathrm{I}_2 + \vec{r}\,\vec{\sigma}\big)$,

$\Big($since $\Pr\{\pm 1\} = \mathrm{tr}\big(\rho|\pm\vec{a}\rangle\langle\pm\vec{a}|\big) = \dfrac{1}{2} \pm \dfrac{1}{2}\mathrm{tr}(\rho\,\vec{a}\,\vec{\sigma})$ with $(\vec{r}\,\vec{\sigma})(\vec{a}\,\vec{\sigma}) = (\vec{r}\,\vec{a})\,\mathrm{I}_2 + i(\vec{r} \times \vec{a})\vec{\sigma}\Big)$.

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) :

Defined by a set of an arbitrary number of positive operators M_m,

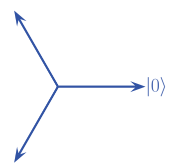
verifying $\sum_m \mathrm{M}_m = \mathrm{I}_N$,

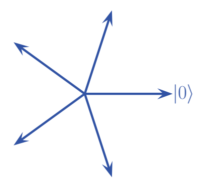
and $\Pr\{\mathrm{M}_m\} = \mathrm{tr}(\rho\mathrm{M}_m)$. Moreover $\sum_m \Pr\{\mathrm{M}_m\} = 1, \forall\rho \Longleftrightarrow \sum_m \mathrm{M}_m = \mathrm{I}_N$.

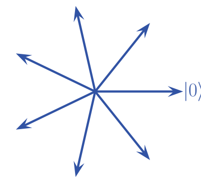
A generalized measurement (POVM) for the qubit

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

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







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

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 : $H(X) = -\sum_{j=1}^{J} p_j \log(p_j)$.

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 $I(X;Y) = H(Y) - H(Y|X) \leq \chi(\rho) \leq H(X)$,

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

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

The von Neumann entropy

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

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

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 $\rho = \mathrm{I}_N/N$.

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 a closed system, undergoing a unitary evolution by U as $\rho \otimes \rho_{\text{env}} \longrightarrow \mathrm{U}(\rho \otimes \rho_{\text{env}})\mathrm{U}^\dagger$.

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

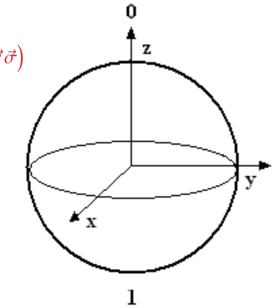
Quantum noise (2/2)

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 $\mathcal{H}_N$.

For an arbitrary qubit state defined by $\rho = \frac{1}{2}\big(\mathrm{I}_2 + \vec{r}\vec{\sigma}\big)$ 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 $\Lambda_1 = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}$, $\Lambda_2 = \sqrt{p}\begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}$, $p, \gamma \in [0,1]$,

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

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

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 :

IEEE TRANSACTIONS ON INFORMATION THEORY

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

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

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

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

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

Discrimination from noisy qubits

Quantum noise on a qubit in state ρ can be represented by random applications of (one of) the 4 Pauli operators $\{\mathrm{I}_2, \sigma_x, \sigma_y, \sigma_z\}$ on the qubit, e.g.

Bit-flip noise : $\rho \longrightarrow \mathcal{N}(\rho) = (1-p)\rho + p\sigma_x\rho\sigma_x^\dagger$,

Depolarizing noise : $\rho \longrightarrow \mathcal{N}(\rho) = (1-p)\rho + \dfrac{p}{3}\Big(\sigma_x\rho\sigma_x^\dagger + \sigma_y\rho\sigma_y^\dagger + \sigma_z\rho\sigma_z^\dagger\Big)$.

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

$\longrightarrow$ Impact of the probability p of action of the quantum noise,
on the performance $P_{\rm suc}^{\max}$ of the optimal detector,
in relation to stochastic resonance and enhancement by noise.
(Chapeau-Blondeau, *Physics Letters A* 378 (2014) 2128-2136.)

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

CrossMark

François Chapeau-Blondeau

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

ARTICLE INFO

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

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

ABSTRACT

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

Discrimination 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 $\{\mathrm{M}_m\}$ with M outcomes to decide with a maximal probability of success $P_{\rm suc}$?

$\Longrightarrow$ Maximize $P_{\rm suc} = \displaystyle\sum_{m=1}^{M} P_m \operatorname{tr}(\rho_m\mathrm{M}_m)$ according to the M operators M_m,
subject to $0 \le \mathrm{M}_m \le \mathrm{I}_N$ and $\sum_{m=1}^M \mathrm{M}_m = \mathrm{I}_N$.

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. $\operatorname{supp}(\rho_0) \subset \mathcal{H}_N \Longleftrightarrow [\operatorname{supp}(\rho_0)]^\perp \supset \{\vec{0}\}$.

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

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

Find $0 \le \mathrm{M}_0 \le \mathrm{I}_N$ s.t. $\mathrm{M}_0 = \vec{a}_0\Pi_1$ "proportional" to Π_1 projector on $[\operatorname{supp}(\rho_1)]^\perp$,
and $0 \le \mathrm{M}_1 \le \mathrm{I}_N$ s.t. $\mathrm{M}_1 = \vec{a}_1\Pi_0$ "proportional" to Π_0 projector on $[\operatorname{supp}(\rho_0)]^\perp$,
and $\mathrm{M}_0 + \mathrm{M}_1 \le \mathrm{I}_N \Longleftrightarrow \Big[\mathrm{M}_0 + \mathrm{M}_1 + \mathrm{M}_{\rm unc} = \mathrm{I}_N$ with $0 \le \mathrm{M}_{\rm unc} \le \mathrm{I}_N\Big]$,
maximizing $P_{\rm suc} = P_0 \operatorname{tr}(\mathrm{M}_0\rho_0) + P_1 \operatorname{tr}(\mathrm{M}_1\rho_1)$ ($\equiv$ 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 $m = 1, \dots M$;
each ρ_m must be with defective rank $< N$.

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

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

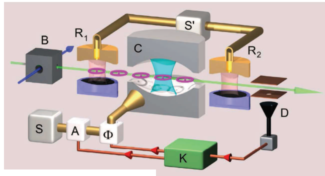
by M_m such that $0 \le \mathrm{M}_m \le \mathrm{I}_N$ and M_m "proportional" to the projector on $\mathcal{K}_m$.

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

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

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

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 Vouceau, 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 closed systems)

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

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

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

• Lindblad equation (for open systems)

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

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

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

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

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

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 maxima 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.

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.

Merci de votre attention.

Si vous avez compris . . .
c’est que je me suis mal exprimé !

“Nobody really understands quantum mechanics.”
R. P. Feynman