

**Information quantique,
calcul quantique :
des rudiments à la recherche (en 45 min !).**

François CHAPEAU-BLONDEAU

LARIS, Université d'Angers, France.



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 (parallélisme, intrication, ...).
- 3) It's fun !

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

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

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

Measurement of the qubit

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

\implies only 2 possible outcomes (Born rule) :

state $|0\rangle$ with probability $|\alpha|^2 = |\langle 0|\psi\rangle|^2$, or
state $|1\rangle$ with probability $|\beta|^2 = |\langle 1|\psi\rangle|^2$.

Measurement :

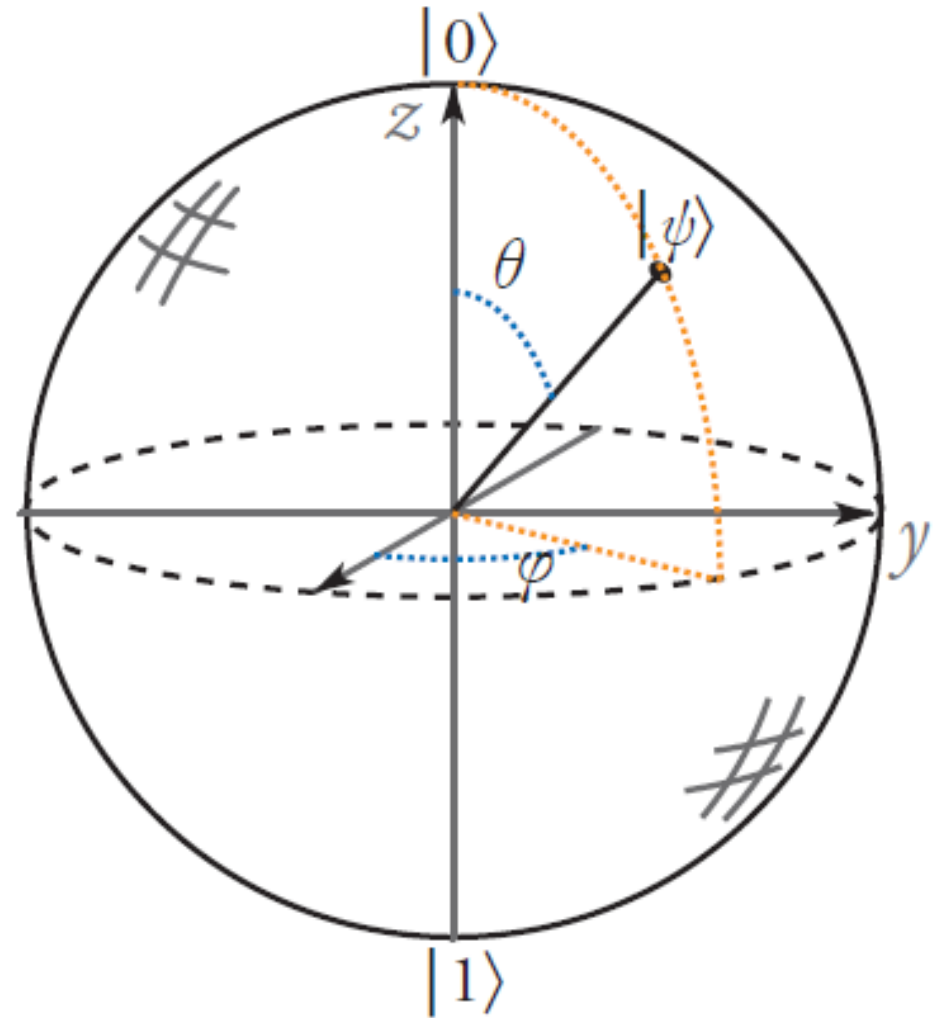
- a probabilistic process,
- as a projection of the state $|\psi\rangle$ in an orthonormal basis,
- with statistics evaluable over repeated experiments with same preparation $|\psi\rangle$.

Bloch sphere representation of the qubit

Qubit in state

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \text{ with } |\alpha|^2 + |\beta|^2 = 1.$$

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



As a quantum object

the qubit has infinitely many 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).

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 $|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$.

Or, as a special separable state

$$\begin{aligned} |\phi\rangle &= \left(\alpha_1 |0\rangle + \beta_1 |1\rangle \right) \otimes \left(\alpha_2 |0\rangle + \beta_2 |1\rangle \right) \\ &= \alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |10\rangle + \beta_1 \beta_2 |11\rangle. \end{aligned}$$

A multipartite state which is not separable is entangled.

Entangled states

- Example of a **separable state** of two qubits AB :

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

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 $1/2$.

- Example of an **entangled state** of two qubits AB :

$$|AB\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right).$$

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 measure).

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 $|1\rangle$,

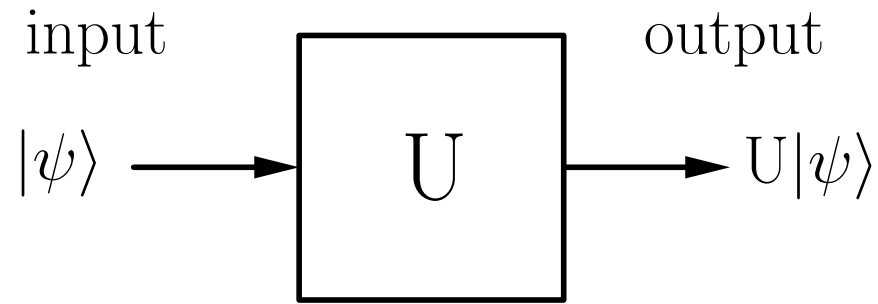
no matter how distant the two qubits are before measurement.

Computation on a qubit

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

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

\equiv quantum gate



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

Identity gate $\mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Pauli gates $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

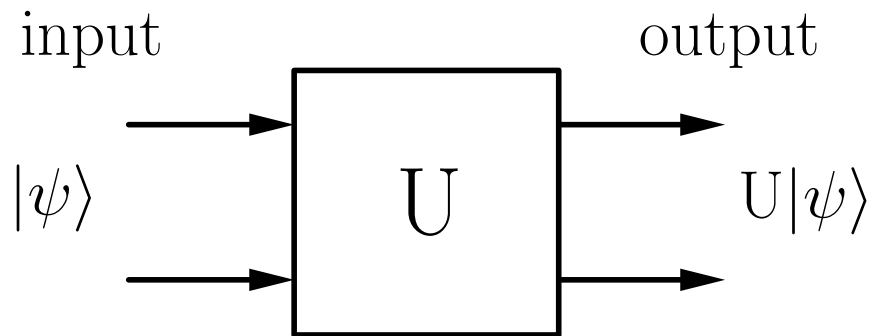
$\{\mathbb{1}, X, Y, Z\}$ a basis for operators on \mathcal{H}_2 .

Computation on a pair of qubits

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

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

\equiv quantum gate
(always reversible)



Controlled-Not gate :

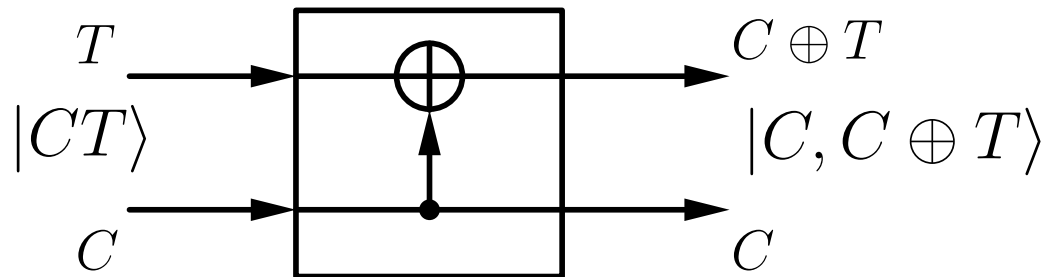
$|CT\rangle \longrightarrow |C, C \oplus T\rangle$

$|00\rangle \longrightarrow |00\rangle$

$|01\rangle \longrightarrow |01\rangle$

$|10\rangle \longrightarrow |11\rangle$

$|11\rangle \longrightarrow |10\rangle$



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

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

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

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

This forms the grounding of quantum computation.

Deutsch-Jozsa algo. (1992) : Parallel evaluation of a function

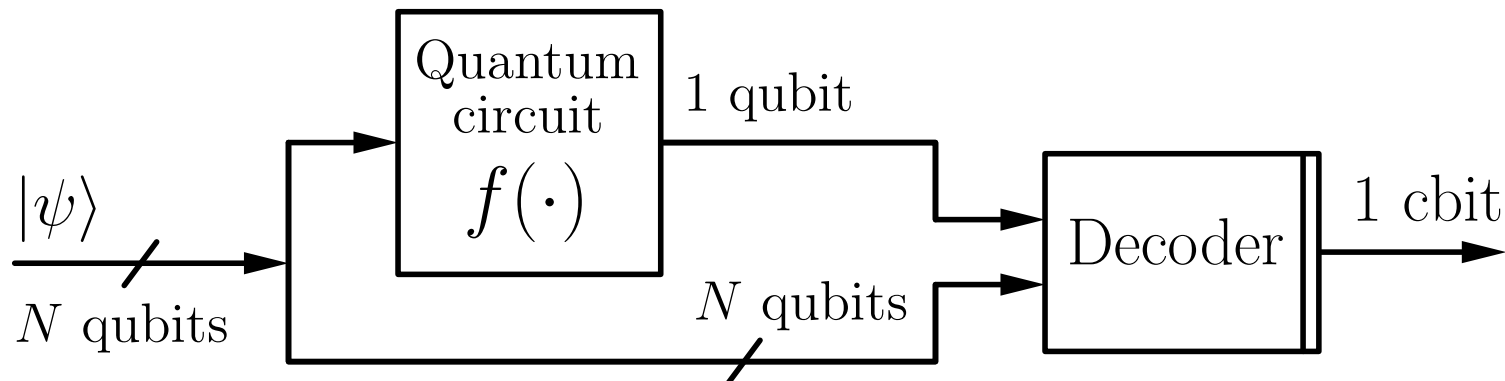
A classical function $f(\cdot)$ $\left| \begin{array}{l} \{0, 1\}^N \longrightarrow \{0, 1\} \\ 2^N \text{ values} \longrightarrow 2 \text{ values,} \end{array} \right.$

can be constant 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.

$$|\psi\rangle = \left(\frac{1}{2^N}\right)^{1/2} (|0\rangle + |1\rangle)^{\otimes N} = \left(\frac{1}{2^N}\right)^{1/2} \sum_{\vec{x} \in \{0,1\}^N} |x_1 x_2 \cdots x_N\rangle$$



Deutsch-Jozsa algorithm

(Desurvire 2009,

Cambridge Univ. Press)

we obtain¹

$$\begin{aligned}
 |\psi_2\rangle &= H^{\otimes n} H_2 |\psi_1\rangle \\
 &= H^{\otimes n} |0\rangle^{\otimes n} \otimes H|1\rangle \\
 &= |+\rangle^{\otimes n} |-\rangle \\
 &= \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle)^{\otimes n} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
 &= \frac{1}{\sqrt{2^n}} \left[\sum_{x_i \in \{0,1\}} |x_1 x_2 \dots x_n\rangle \right] \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
 &= \frac{1}{\sqrt{2^n}} \left[\sum_{x=0}^{2^n-1} |x\rangle \right] \frac{|0\rangle - |1\rangle}{\sqrt{2}}.
 \end{aligned} \tag{19.7}$$

We call $|x\rangle$ the *query register*, similarly to the “register” in the classical von Neumann architecture (Chapter 15) the difference being that it is made of *qubits*. At ③, we obtain²

$$\begin{aligned}
 |\psi_3\rangle &= U_f |\psi_2\rangle \\
 &= \sum_x \frac{|x\rangle}{\sqrt{2^n}} \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \\
 &\equiv \sum_x \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} |-\rangle.
 \end{aligned} \tag{19.8}$$

And at ④, after passing the top n -qubit through the parallel gate $H^{\otimes n}$, we obtain:

$$\begin{aligned}
 |\psi_4\rangle &= H^{\otimes n} |\psi_3\rangle \\
 &= \frac{1}{\sqrt{2^n}} \left[\sum_x (-1)^{f(x)} H^{\otimes n} |x\rangle \right] |-\rangle.
 \end{aligned} \tag{19.9}$$

To develop the right-hand side in Eq. (19.9), we must calculate $H^{\otimes n} |x\rangle = H^{\otimes n} |x_1 x_2 \dots x_n\rangle$. It is an easy exercise to establish that:

$$H^{\otimes n} |x\rangle = \sum_z (-1)^{x \cdot z} |z\rangle, \tag{19.10}$$

where $x \cdot z = x_1 z_1 + x_2 z_2 + \dots + x_n z_n$ is a scalar product modulo 2. Combining Eqs. (19.9) and (19.10), we then obtain:

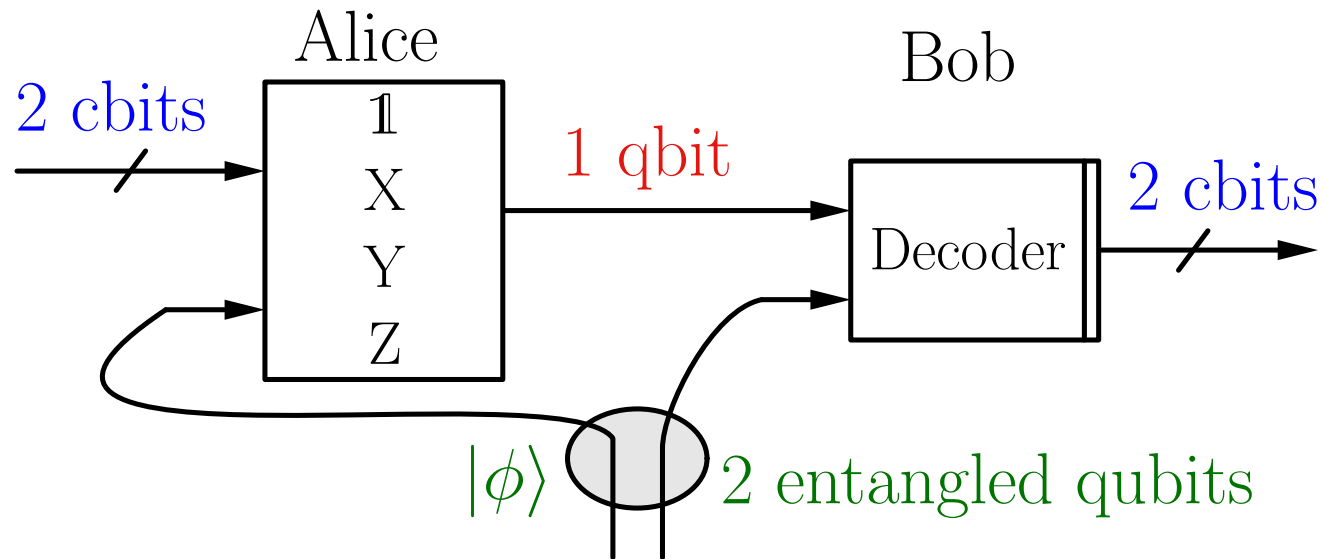
$$\begin{aligned}
 |\psi_4\rangle &= \frac{1}{2^n} \left[\sum_z \sum_x (-1)^{f(x)+x \cdot z} |z\rangle \right] |-\rangle \\
 &\equiv |\Psi\rangle |-\rangle,
 \end{aligned} \tag{19.11}$$

Superdense coding (Bennett 1992) : exploiting entanglement

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

Alice chooses two classical bits, pack them into a single qubit.

Bob receives this qubit, from which he recovers the two classical bits.



Teleportation (1993) is the opposite : a shared pair of entangled qubits and two classical bits transmitted from Alice to Bob

enable the transfer of an arbitrary quantum state $|\psi\rangle$ of a qubit.

Other quantum algorithms

- Grover quantum search algorithm (1996) :

Quantum search in an unsorted database.

Finds one item among N in $O(\sqrt{N})$ steps (instead of $O(N)$ classically).

- 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).

Density operator

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

$$\implies \text{probability } \Pr\{|k\rangle|\psi_j\rangle\} = |\langle k|\psi_j\rangle|^2 = \langle k|\psi_j\rangle \langle\psi_j|k\rangle .$$

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

$$\implies \Pr\{|k\rangle\} = \sum_j p_j \Pr\{|k\rangle|\psi_j\rangle\} = \langle k| \left(\sum_j p_j |\psi_j\rangle \langle\psi_j| \right) |k\rangle = \langle k| \rho |k\rangle ,$$

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

and $\Pr\{|k\rangle\} = \langle k| \rho |k\rangle = \text{tr}(\rho |k\rangle \langle k|) = \text{tr}(\rho \Pi_k)$.

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 $\text{tr}(A) = \sum_k \langle k| A |k\rangle$, one has

$$\text{tr}(A |\psi\rangle \langle\psi|) = \sum_k \langle k| A |\psi\rangle \langle\psi|k\rangle = \sum_k \langle\psi|k\rangle \langle k| A |\psi\rangle = \langle\psi| \left(\sum_k |k\rangle \langle k| \right) A |\psi\rangle = \langle\psi| A |\psi\rangle$$

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 $|k\rangle\langle k| = \Pi_k$,

verifying $\sum_k |k\rangle\langle k| = \sum_k \Pi_k = \mathbb{1}$,

and $\Pr\{|k\rangle\} = \text{tr}(\rho\Pi_k)$. Moreover $\sum_k \Pr\{|k\rangle\} = 1, \forall\rho \iff \sum_k \Pi_k = \mathbb{1}$.

- **Generalized measurement :**

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

verifying $\sum_m M_m = \mathbb{1}$,

and $\Pr\{M_m\} = \text{tr}(\rho M_m)$. Moreover $\sum_m \Pr\{M_m\} = 1, \forall\rho \iff \sum_m M_m = \mathbb{1}$.

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 $\{M_0, M_1\}$ to decide with a maximal probability of success P_{suc} ?

Answer : One has $P_{\text{suc}} = P_0 \text{tr}(\rho_0 M_0) + P_1 \text{tr}(\rho_1 M_1) = P_0 + \text{tr}(T M_1)$, with the test operator $T = P_1 \rho_1 - P_0 \rho_0$.

Then P_{suc} is maximized by $M_1^{\text{opt}} = \sum_{\lambda_n > 0} |\lambda_n\rangle \langle \lambda_n|$,

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

The optimal measurement $\{M_1^{\text{opt}}, M_0^{\text{opt}} = \mathbb{1} - M_1^{\text{opt}}\}$

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

Discrimination from noisy qubits

Quantum noise on a qubit in state ρ can be represented by random applications of (one of) the 4 Pauli operators $\{\mathbb{1}, X, Y, Z\}$ on the qubit, e.g.

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

Depolarizing noise : $\rho \longrightarrow \mathcal{N}(\rho) = (1 - p)\rho + \frac{p}{3} \left(X\rho X^\dagger + Y\rho Y^\dagger + Z\rho Z^\dagger \right)$.

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

→ Impact of the probability p of action of the quantum noise, on the performance $P_{\text{suc}}^{\text{max}}$ of the optimal detector, in relation to stochastic resonance and enhancement by noise.

(Chapeau-Blondeau, *Physics Letters A* 2014)



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.

© 2014 Elsevier B.V. All rights reserved.

Discrimination among $M > 2$ quantum states

A quantum system can be in one of M 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 $\{M_m\}$ with M outcomes to decide with a maximal probability of success P_{suc} ?

$$\begin{aligned} \implies \text{Maximize } P_{\text{suc}} &= \sum_{m=1}^M P_m \text{tr}(\rho_m M_m) \text{ according to the } M \text{ operators } M_m, \\ &\text{subject to } 0 \leq M_m \leq \mathbb{1} \quad \text{and} \quad \sum_{m=1}^M M_m = \mathbb{1}. \end{aligned}$$

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

Try interval analysis, etc ? ...

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

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

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

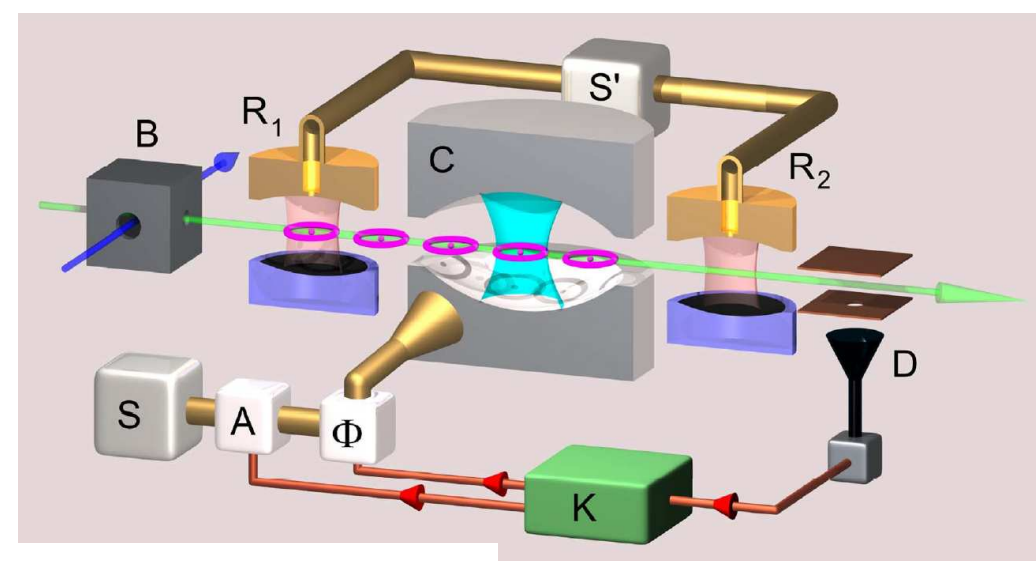
Necessity to find a three-outcome measurement $\{M_0, M_1, M_{\text{unc}}\}$:

\implies Find M_0 such that $0 \leq M_0 \leq \mathbb{1}$ and $\{\vec{0}\} \subseteq \text{supp}(M_0) \subseteq \mathcal{S}_0$,
and M_1 such that $0 \leq M_1 \leq \mathbb{1}$ and $\{\vec{0}\} \subseteq \text{supp}(M_1) \subseteq \mathcal{S}_1$,
and $M_0 + M_1 \leq \mathbb{1} \iff \left[M_0 + M_1 + M_{\text{unc}} = \mathbb{1} \text{ with } 0 \leq M_{\text{unc}} \leq \mathbb{1} \right]$,
maximizing $P_{\text{suc}} = P_0 \text{tr}(M_0 \rho_0) + P_1 \text{tr}(M_1 \rho_1)$ ($\equiv \min P_{\text{unc}} = 1 - P_{\text{suc}}$)

This problem is only partially solved, in some special cases, even more so for extension at $M > 2$.

(Kleinmann *et al.*, 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. Rouchon⁴

¹Laboratoire Kastler Brossel, Ecole Normale Supérieure, CNRS, Université P. et M. Curie,
24 rue Lhomond, F-75231 Paris Cedex 5, France

²Collège de France, 11 Place Marcelin Berthelot, F-75231 Paris Cedex 5, France

³INRIA Rocquencourt, Domaine de Vouiseau, BP 105, 78153 Le Chesnay Cedex, France

⁴Centre 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.

System dynamics :

- Schrödinger equation (for closed systems)

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

Hermitian operator Hamiltonian $H = H_0 + H_u$ (control part H_u).

$$\frac{d}{dt} \rho = -\frac{i}{\hbar} [H, \rho] \implies \rho(t_2) = U(t_1, t_2) \rho(t_1) U^\dagger(t_1, t_2).$$

- Lindblad equation (for open systems)

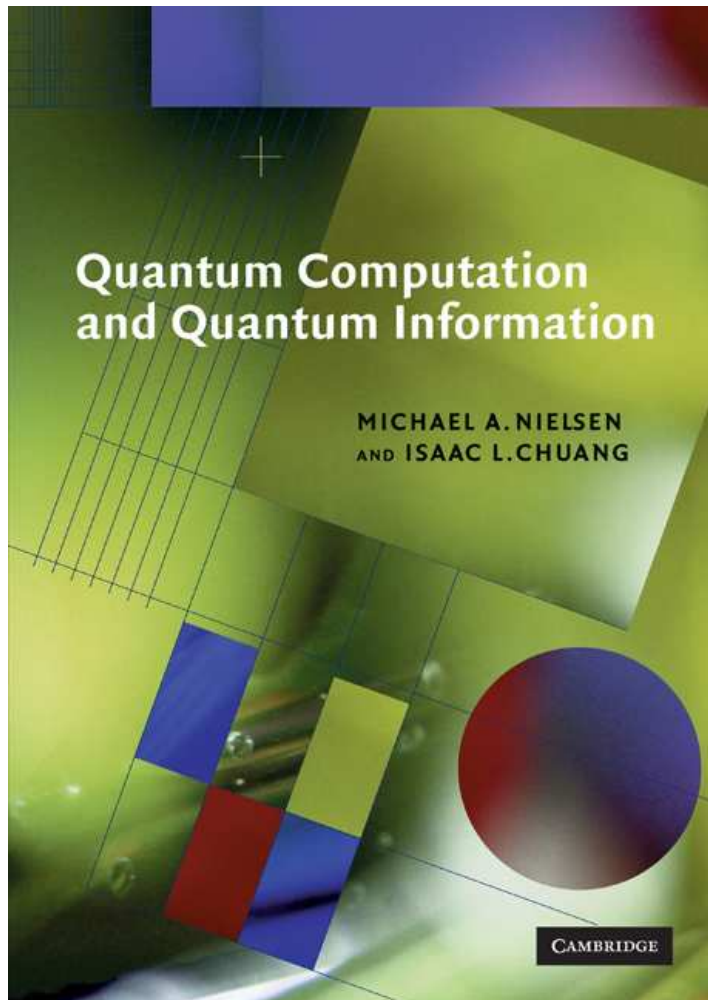
$$\frac{d}{dt} \rho = -\frac{i}{\hbar} [H, \rho] + \sum_j \left(2L_j \rho L_j^\dagger - \{L_j^\dagger L_j, \rho\} \right), \quad \text{Lindblad op. } L_j \text{ for interact. with environent.}$$

Measurement : Arbitrary operators $\{E_m\}$ such that $\sum_m E_m^\dagger E_m = \mathbb{1}$,

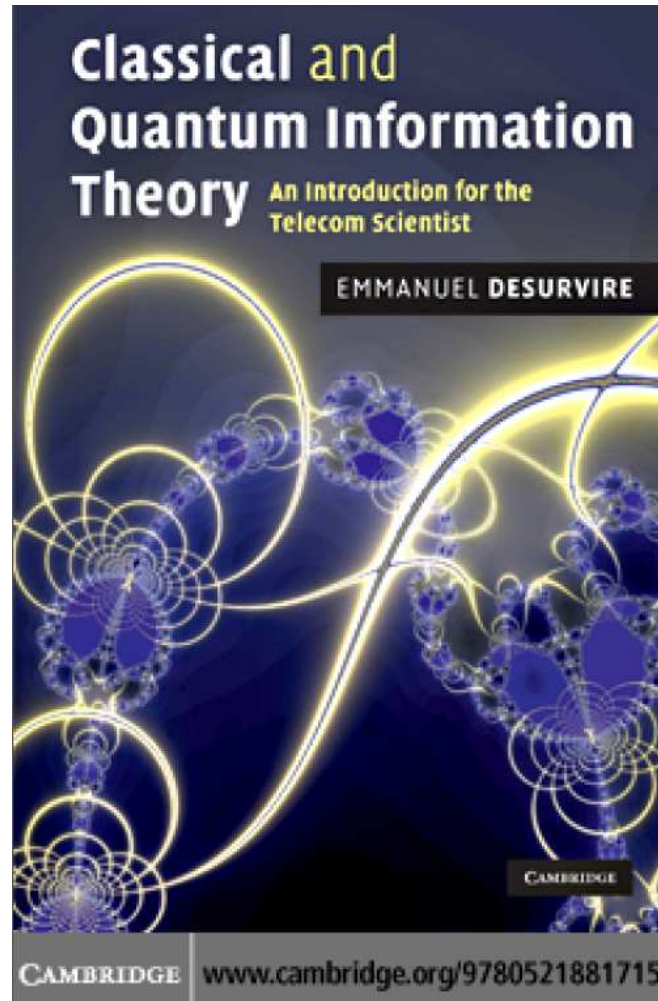
$\Pr\{m\} = \text{tr}(E_m \rho E_m^\dagger) = \text{tr}(\rho E_m^\dagger E_m) = \text{tr}(\rho M_m)$ with $M_m = E_m^\dagger E_m$ positive,

Post-measurement state $\rho_m = \frac{E_m \rho E_m^\dagger}{\text{tr}(E_m \rho E_m^\dagger)}$.

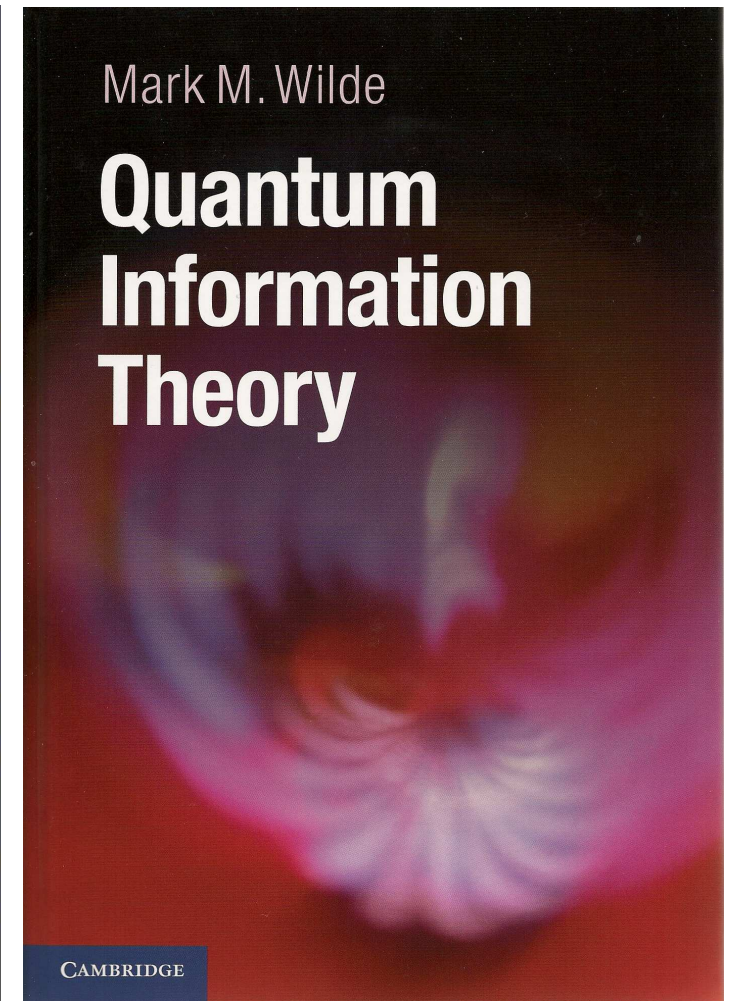
Pour aller plus loin



M. Nielsen & I. Chuang
2000, 676 pages



E. Desurvire
2009, 691 pages



M. Wilde
2013, 655 pages

Merci de votre attention.

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

“Nobody really understands quantum mechanics.”

R. P. Feynman