

# Information quantique, calcul quantique :

## Une introduction pour le traitement du signal.

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



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

1/79

## A definition (at large)

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

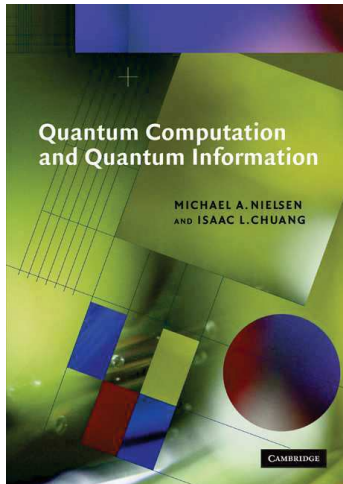
## Motivations for the quantic

for information and computation :

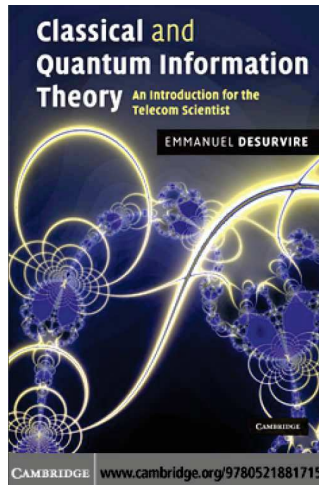
- 1) When using elementary systems (photons, electrons, atoms, ions, nanodevices, ...).
- 2) To benefit from purely quantum effects (parallelism, entanglement, ...).
- 3) Recent field of research, rich of large potentialities (science & technology).

2/79

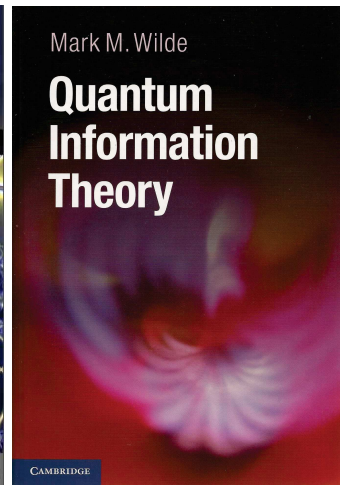
## Some basic textbooks



M. Nielsen & I. Chuang  
2000, 676 pages



E. Desurvire  
2009, 691 pages



M. Wilde  
2017, 757 pages

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

3/79

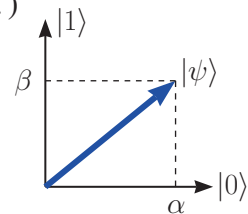
## Quantum system

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

**(1) State**

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

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



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

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

4/79

## Measurement of the qubit

### (2) Measurement

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

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

state  $|0\rangle$  with probability  $|\alpha|^2 = |\langle 0|\psi\rangle|^2 = \langle \psi|0\rangle\langle 0|\psi\rangle = \langle \psi|\Pi_0|\psi\rangle$ , or  
state  $|1\rangle$  with probability  $|\beta|^2 = |\langle 1|\psi\rangle|^2 = \langle \psi|1\rangle\langle 1|\psi\rangle = \langle \psi|\Pi_1|\psi\rangle$ .

**Quantum measurement** : usually :

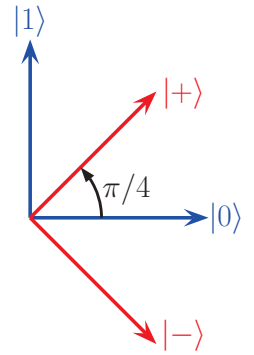
- a probabilistic process,
- as a destructive projection of the state  $|\psi\rangle$  in an orthonormal basis,
- with statistics evaluable over repeated experiments with same preparation  $|\psi\rangle$ .

5/79

## Hadamard basis

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

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

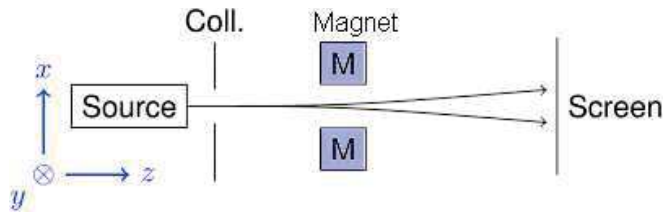


$\Leftrightarrow$  Computational orthonormal basis

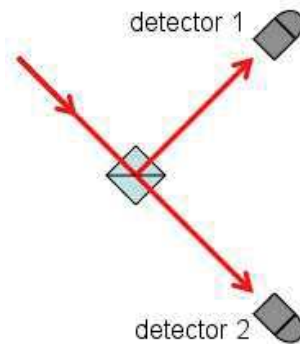
$$\left\{ |0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle); \quad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \right\}.$$

6/79

## 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, ...)

7/79

## Bloch sphere representation of the qubit

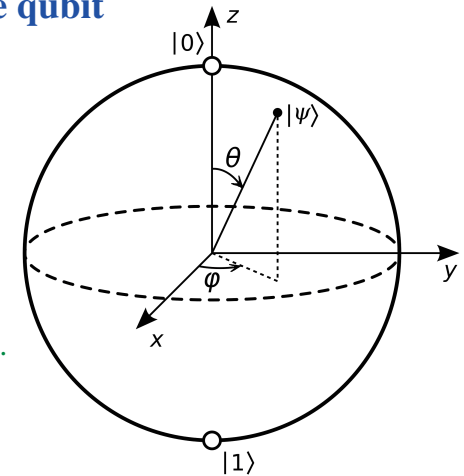
Qubit in state

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

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

with  $\theta \in [0, \pi]$ ,

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



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

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

8/79

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

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

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

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

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

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

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

9/79

## Continuous infinite dimensional states

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

The basis states  $\{|x\rangle\}$  in  $\mathcal{H}$  satisfy  $\langle x|x'\rangle = \delta(x-x')$  (orthonormality),  
 $\int_{-\infty}^{\infty} |x\rangle\langle x| dx = \text{Id}$  (completeness).

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

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

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

10/79

## Multiple qubits

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

### Example $L = 2$ :

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

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

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

**A multipartite state which is not separable is entangled.**

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

11/79

## Entangled states

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

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

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  $AB$  :

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

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.

12/79

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

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

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

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



13/79

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

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

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

14/79

## Observables

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

Also, any Hermitian (i.e.  $\Omega = \Omega^\dagger$ ) operator  $\Omega$  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  $\Omega$  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  $\omega_n$ .

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

When system in state  $|\psi\rangle$ , measuring observable  $\Omega$  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  $\omega_n$  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  $\langle \Omega \rangle = \sum_n \omega_n \Pr\{\omega_n\} = \langle \psi | \Omega | \psi \rangle$ .

15/79

## Heisenberg uncertainty relation (1/2)

For two operators  $A$  and  $B$ : **commutator**  $[A, B] = AB - BA$ ,

**anticommutator**  $\{A, B\} = AB + BA$ ,

so that  $AB = \frac{1}{2}[A, B] + \frac{1}{2}\{A, B\}$ .

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

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

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

$$|\langle \psi | AB | \psi \rangle|^2 \leq \langle \psi | A^2 | \psi \rangle \langle \psi | B^2 | \psi \rangle,$$

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

16/79

## Heisenberg uncertainty relation (2/2)

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

$$\implies \langle \tilde{A}^2 \rangle = \langle A^2 \rangle - \langle A \rangle^2 \text{ scalar variance,}$$

$$\text{also } [\tilde{A}, \tilde{B}] = [A, B] .$$

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

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

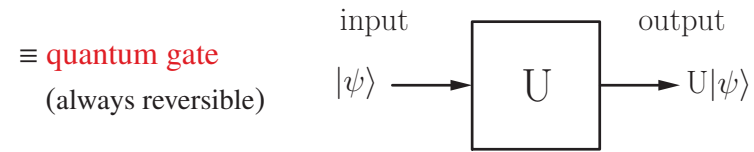
then  $\Delta A \Delta B \geq \frac{1}{2} |\langle [A, B] \rangle|$  **Heisenberg uncertainty relation.**

17/79

## Computation on a qubit

### (3) Evolution

Through a unitary (linear) operator  $U$  on  $\mathcal{H}_2$  (a  $2 \times 2$  matrix) : (i.e.  $U^{-1} = U^\dagger$ )  
 normalized vector  $|\psi\rangle \in \mathcal{H}_2 \longrightarrow U|\psi\rangle$  normalized vector  $\in \mathcal{H}_2$  .



$$\text{Hadamard gate } H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} . \quad \text{Identity gate } I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} .$$

$$H^2 = I_2 \iff H^{-1} = H = H^\dagger \text{ Hermitian unitary.}$$

$$H|0\rangle = |+\rangle \quad \text{and} \quad H|1\rangle = |-\rangle$$

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

18/79

## Pauli gates

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

$$X^2 = Y^2 = Z^2 = I_2 . \quad \text{Hermitian unitary.} \quad XY = -YX = iZ, \quad ZX = iY, \text{ etc.}$$

$\{I_2, X, Y, Z\}$  a basis for operators on  $\mathcal{H}_2$ .

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

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

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

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

19/79

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

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

$$U_\xi = \exp\left(-i \frac{\xi}{2} \vec{n} \cdot \vec{\sigma}\right) = \cos\left(\frac{\xi}{2}\right) I_2 - i \sin\left(\frac{\xi}{2}\right) \vec{n} \cdot \vec{\sigma} \in \text{SU}(2) ,$$

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

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

implementing in the Bloch sphere representation

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

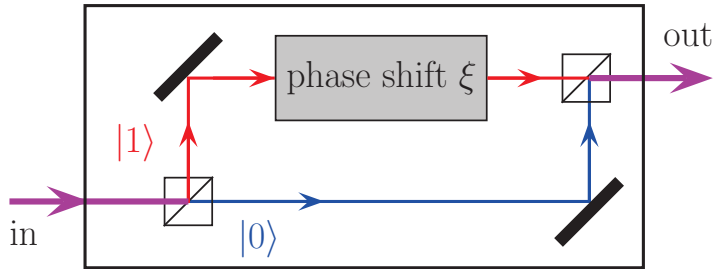
$$\text{Example : } W = \sqrt{\sigma_x} = e^{i\pi/4} \left[ \cos(\pi/4) I_2 - i \sin(\pi/4) \sigma_x \right], \quad (\xi = \pi/2, \vec{n} = \vec{e}_x) .$$

20/79

## An optical implementation

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

optically implemented by a Mach-Zehnder interferometer



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

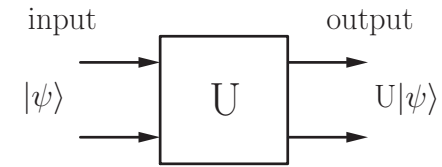
21/79

## Computation on a pair of qubits

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

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

$\equiv$  quantum gate  
(always reversible)



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

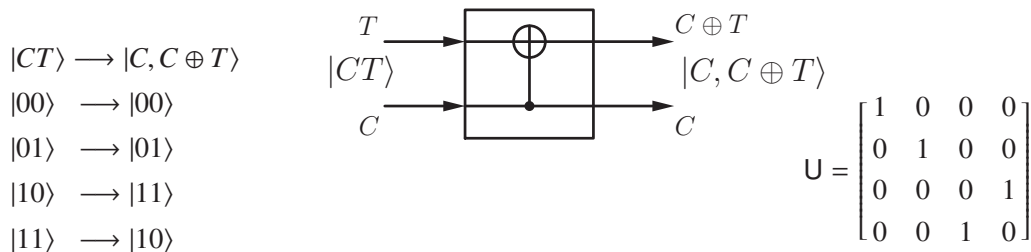
But works equally on any linear superposition of quantum states  $\Rightarrow$  quantum parallelism.

22/79

### • Example : Controlled-Not gate

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

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



$(\text{C-Not})^2 = I_4 \iff (\text{C-Not})^{-1} = \text{C-Not} = (\text{C-Not})^\dagger$  Hermitian unitary.

23/79

## Computation on a system of $L$ qubits

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

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

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

Completely defined for instance by the transformation of the  $2^L$  state vectors of the computational basis ;

but works equally on any linear superposition of them (parallelism).

### Universal set of gates :

Any  $L$ -qubit quantum gate or circuit  $U$  can always be obtained from two-qubit C-Not gates and single-qubit gates.

And in principle this ensures experimental realizability of any unitary  $U$ .

This provides a foundation for quantum computation.

24/79

By empirical postulation **Schrödinger equation** (for isolated systems) :

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

Hermitian operator **Hamiltonian H**, or energy operator.

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

## Information quantique, calcul quantique :

### Une introduction pour le traitement du signal.

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



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

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

• **State** : Unit-norm vector  $|\psi\rangle = \sum_{n=1}^N \alpha_n |n\rangle \in \mathcal{H}_N$  complex Hilbert space.

Realizable with  $L$  two-dimensional qubits, with  $2^L \geq N$ .

Multipartite states in tensor-product space  $\implies$  quantum entanglement.

• **Measurement** : Random and destructive, in  $\mathcal{H}_N$  via a set of  $M$  orthogonal projectors  $\Pi_m = \Pi_m^\dagger \Pi_m$ , satisfying  $\sum_{m=1}^M \Pi_m = \mathbf{I}_N$ ,

with  $M$  outcomes of probability  $P(m) = \|\Pi_m |\psi\rangle\|^2 = \langle \psi | \Pi_m | \psi \rangle$ ,

and post-measurement state  $|\psi_{\text{post}}\rangle = \frac{\Pi_m |\psi\rangle}{\|\Pi_m |\psi\rangle\|}$ .

• **Evolution** : Linear unitary :  $|\psi\rangle \xrightarrow{\mathbf{U}} \mathbf{U} |\psi\rangle$

Realizable from one-qubit gates and the two-qubit C-Not gate.

**In particular :**

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

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

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

$$\text{or with } \begin{cases} \Pi'_1 = |0\rangle\langle 0| \otimes \mathbf{I}_2 \\ \Pi'_2 = |1\rangle\langle 1| \otimes \mathbf{I}_2 \end{cases} \implies \sum_{m=1}^2 \Pi'_m = \mathbf{I}_2 \otimes \mathbf{I}_2 = \mathbf{I}_4.$$

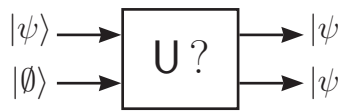
• **Evolution** :  $|\psi\rangle \xrightarrow{\mathbf{U}} \mathbf{U} |\psi\rangle \iff \frac{d}{dt} |\psi\rangle = -\frac{i}{\hbar} \mathbf{H} |\psi\rangle \implies |\psi(t_2)\rangle = \mathbf{U}(t_2, t_1) |\psi(t_1)\rangle$ , (p. 25)

with  $\mathbf{U}(t_2, t_1) = \exp\left(-\frac{i}{\hbar} \int_{t_1}^{t_2} \mathbf{H} dt\right)$ . Trivial  $\mathbf{H} = H_0 \mathbf{Id} \implies |\psi(t_2)\rangle = \exp\left(-i \frac{H_0}{\hbar} (t_2 - t_1)\right) |\psi(t_1)\rangle$ .

## No cloning theorem (1982)

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

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

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


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

$$|\psi\rangle|\emptyset\rangle \xrightarrow{U} U(|\psi\rangle|\emptyset\rangle) = U(\alpha_1 |\psi_1\rangle|\emptyset\rangle + \alpha_2 |\psi_2\rangle|\emptyset\rangle)$$

$$= \alpha_1 |\psi_1\rangle|\psi_1\rangle + \alpha_2 |\psi_2\rangle|\psi_2\rangle \quad \text{since } U \text{ linear.}$$

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

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

$$\neq U(|\psi\rangle|\emptyset\rangle) \quad \text{in general.} \implies \text{No cloning } U \text{ possible.}$$

29/79

## Quantum parallelism

For a system of  $L$  qubits,

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

The quantum gate  $U$  is completely defined

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

Yet, the quantum gate  $U$  can be operated

on any linear superposition of the basis states  $\{|\vec{x}\rangle, \vec{x} \in \{0, 1\}^L\}$ .

This is **quantum parallelism**, with no classical analogue.

$$\log_2(10) \approx 3.32 \implies \log_2(10^{15}) \approx 49.83 \iff 10^{15} \approx 2^{50}$$

Donc 1000 Tbits sont stockables dans un registre de 50 qubits !



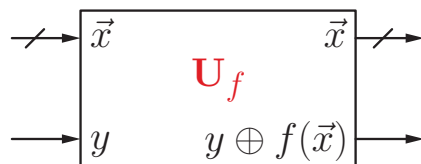
30/79

## Parallel evaluation of a function (1/4)

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

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

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

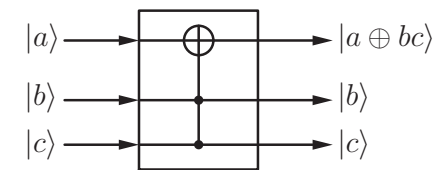


with binary output  $y \oplus f(\vec{x}) = f(\vec{x})$  when  $y = 0$ , or  $\overline{f(\vec{x})}$  when  $y = 1$ , (invertible as  $[y \oplus f(\vec{x})] \oplus f(\vec{x}) = y \oplus f(\vec{x}) \oplus f(\vec{x}) = y \oplus 0 = y$ ).

31/79

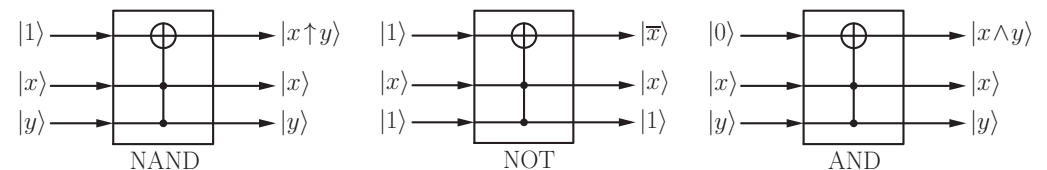
## Parallel evaluation of a function (2/4)

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



$$(\text{CC-Not})^2 = I_8 \iff (\text{CC-Not})^{-1} = \text{CC-Not} = (\text{CC-Not})^\dagger \quad \text{Hermitian unitary.}$$

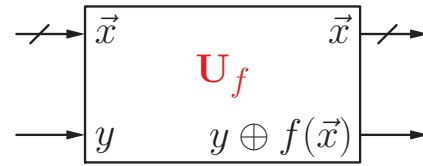
Any classical Boolean function  $f(\vec{x})$  (invertible or non) on  $L$  bits can always be implemented (simulated) by means of 3-qubit Toffoli gates.



32/79



## Parallel evaluation of a function (3/4)



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

$$|\vec{x}\rangle |y = 0\rangle \xrightarrow{U_f} |\vec{x}\rangle |f(\vec{x})\rangle$$

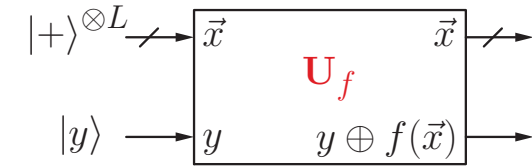
$$|\vec{x}\rangle |y = 1\rangle \xrightarrow{U_f} |\vec{x}\rangle |\overline{f(\vec{x})}\rangle$$

$$|\vec{x}\rangle |+\rangle \xrightarrow{U_f} |\vec{x}\rangle \frac{1}{\sqrt{2}} \left[ |f(\vec{x})\rangle + |\overline{f(\vec{x})}\rangle \right] = |\vec{x}\rangle |+\rangle$$

$$|\vec{x}\rangle |-\rangle \xrightarrow{U_f} |\vec{x}\rangle \frac{1}{\sqrt{2}} \left[ |f(\vec{x})\rangle - |\overline{f(\vec{x})}\rangle \right] = |\vec{x}\rangle |-\rangle (-1)^{f(\vec{x})}$$

33/79

## Parallel evaluation of a function (4/4)



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

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

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

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

34/79

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

A classical Boolean function  $f(\cdot) : \{0, 1\}^L \rightarrow \{0, 1\}$   
 $2^L$  values  $\rightarrow$  2 values,

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

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

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

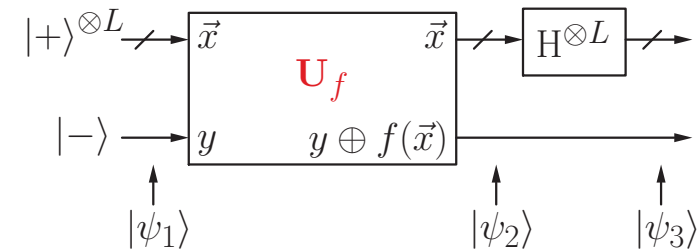
$$\text{Lemma 1 : } H|x\rangle = \frac{1}{\sqrt{2}} (|0\rangle + (-1)^x |1\rangle) = \frac{1}{\sqrt{2}} \sum_{z \in \{0,1\}} (-1)^{xz} |z\rangle, \quad \forall x \in \{0, 1\}$$

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

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

35/79

## Deutsch-Jozsa algorithm (2/5)



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

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

36/79

## Deutsch-Jozsa algorithm (3/5)

Output state  $|\psi_3\rangle = (H^{\otimes L} \otimes I_2)|\psi_2\rangle$

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

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

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

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

37/79

## Deutsch-Jozsa algorithm (4/5)

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

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

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

$\implies$  When  $|\psi\rangle$  is measured,  $L$  states  $|0\rangle$  are found.

- When  $f(\cdot)$  **balanced**:  $w(\vec{z} = \vec{0}) = 0 \implies |\psi\rangle$  is not or does not contain state  $|\vec{0}\rangle$ .

$\implies$  When  $|\psi\rangle$  is measured, at least one state  $|1\rangle$  is found.

$\rightarrow$  Illustrates quantum resources of parallelism, coherent superposition, interference.

(When  $f(\cdot)$  is neither constant nor balanced,  $|\psi\rangle$  contains a little bit of  $|\vec{0}\rangle$ .)

38/79

## Deutsch-Jozsa algorithm (5/5)

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

The case  $L = 2$  qubits.

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

Extension to arbitrary  $L \geq 2$  qubits.

[3] E. Bernstein, U. Vazirani; "Quantum complexity theory"; *SIAM Journal on Computing* 26 (1997) 1411–1473.

Extension to  $f(\vec{x}) = \vec{a}\vec{x}$  or  $f(\vec{x}) = \vec{a}\vec{x} \oplus b$ , to find binary  $L$ -word  $\vec{a} \rightarrow$  by producing output  $|\psi\rangle = |\vec{a}\rangle$ .

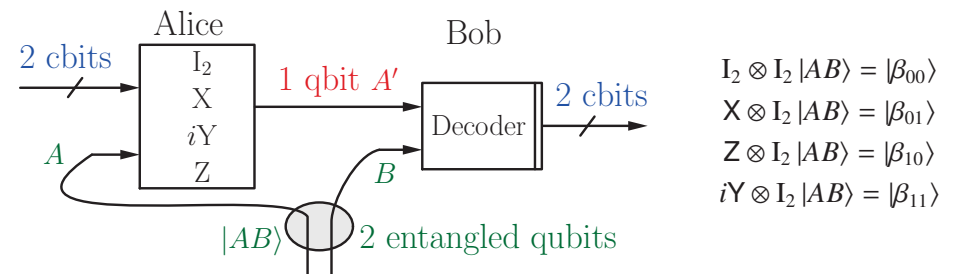
[4] R. Cleve, A. Ekert, C. Macchiavello, M. Mosca; "Quantum algorithms revisited"; *Proceedings of the Royal Society of London A* 454 (1998) 339–354.

39/79

## Superdense coding (Bennett 1992) : exploiting entanglement

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

Alice chooses two classical bits, used to encode by applying to her qubit  $A$  one of  $\{I_2, X, iY, Z\}$ , delivering the qubit  $A'$  sent to Bob.



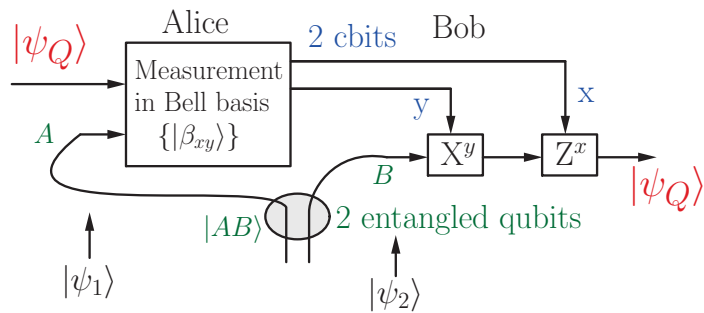
Bob receives this qubit  $A'$ . For decoding, Bob measures  $|A'B\rangle$  in the Bell basis  $\{|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle\}$ , from which he recovers the two classical bits.

40/79

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

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

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



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  $|\psi_Q\rangle$ .

41/79

## Teleportation (2/3)

$$\begin{aligned} |\psi_1\rangle &= |\psi_Q\rangle |\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left[ \alpha_0 |0\rangle (|00\rangle + |11\rangle) + \alpha_1 |1\rangle (|00\rangle + |11\rangle) \right] \\ &= \frac{1}{\sqrt{2}} \left[ \alpha_0 |000\rangle + \alpha_0 |011\rangle + \alpha_1 |100\rangle + \alpha_1 |111\rangle \right], \end{aligned}$$

$$\begin{aligned} \text{factorizable as } |\psi_1\rangle &= \frac{1}{2} \left[ \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) (\alpha_0 |0\rangle + \alpha_1 |1\rangle) + \right. \\ &\quad \left. \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) (\alpha_0 |1\rangle + \alpha_1 |0\rangle) + \right. \\ &\quad \left. \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) (\alpha_0 |0\rangle - \alpha_1 |1\rangle) + \right. \\ &\quad \left. \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) (\alpha_0 |1\rangle - \alpha_1 |0\rangle) \right], \end{aligned}$$

42/79

## Teleportation (3/3)

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{2} \left[ |\beta_{00}\rangle (\alpha_0 |0\rangle + \alpha_1 |1\rangle) + |\beta_{01}\rangle (\alpha_0 |1\rangle + \alpha_1 |0\rangle) + \right. \\ &\quad \left. |\beta_{10}\rangle (\alpha_0 |0\rangle - \alpha_1 |1\rangle) + |\beta_{11}\rangle (\alpha_0 |1\rangle - \alpha_1 |0\rangle) \right]. \end{aligned}$$

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

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

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

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

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

43/79

## Principes references on superdense coding ...

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

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

## ... and teleportation

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

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

44/79

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

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

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

One wants to find one (only one here, but extensible) item  $n = n_0$

satisfying some criterion or property,

indicated by the test function or **oracle**  $f(\cdot)$  responding as  $f(n) = \delta_{nn_0}$ .

With an unsorted dataset, finding  $n_0$  requires

**classically**  $O(N)$  interrogations of the oracle or evaluations of  $f(\cdot)$ ,

while  $O(\sqrt{N})$  are enough **quantumly**.

45/79

## Grover quantum search algorithm (2/4)

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

From a quantum implementation of the test function  $f(\cdot)$ , it is possible to obtain a **quantum oracle** as the unitary operator  $U_0$  realizing  $U_0 |n\rangle = (-1)^{f(n)} |n\rangle$  for any  $n \in \{1, 2, \dots, N\}$ .

Thus, the quantum oracle returns its response by reversing the sign of  $|n\rangle$  when  $n$  is the solution  $n_0$ , while no change of sign occurs to  $|n\rangle$  when  $n$  is not the solution.

Equivalently  $U_0 = I_N - 2|n_0\rangle\langle n_0|$ , although  $|n_0\rangle$  need not be known, but only  $f(\cdot)$  evaluable.

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

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

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

46/79

## Grover quantum search algorithm (3/4)

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

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

- With the oracle  $U_0 = I_N - 2|n_0\rangle\langle n_0| \Rightarrow U_0 |n_\perp\rangle = |n_\perp\rangle$  and  $U_0 |n_0\rangle = -|n_0\rangle$ .

So in plane  $(|n_0\rangle, |n_\perp\rangle)$ , the operator  $U_0$  performs a reflection about  $|n_\perp\rangle$ .

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

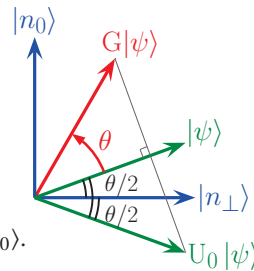
- Define the unitary operator  $U_\psi = 2|\psi\rangle\langle\psi| - I_N \Rightarrow U_\psi |\psi\rangle = |\psi\rangle$  and  $U_\psi |\psi_\perp\rangle = -|\psi_\perp\rangle$ .

So in plane  $(|n_0\rangle, |n_\perp\rangle)$ , the operator  $U_\psi$  performs a reflection about  $|\psi\rangle$ .

- In plane  $(|n_0\rangle, |n_\perp\rangle)$ , the composition of two reflections is a rotation  $U_\psi U_0 = G$  (Grover amplification operator). It verifies  $G |n_0\rangle = U_\psi U_0 |n_0\rangle = -U_\psi |n_0\rangle = |n_0\rangle - \frac{2}{\sqrt{N}} |\psi\rangle$ .

The rotation angle  $\theta$  between  $|n_0\rangle$  and  $G |n_0\rangle$ , via the scalar product of  $|n_0\rangle$  and  $G |n_0\rangle$ , verifies

$$\cos(\theta) = \langle n_0 | G | n_0 \rangle = 1 - \frac{2}{N} \approx 1 - \frac{\theta^2}{2} \Rightarrow \theta \approx \frac{2}{\sqrt{N}} \text{ at } N \gg 1.$$



47/79

## Grover quantum search algorithm (4/4)

- In plane  $(|n_0\rangle, |n_\perp\rangle)$ , the rotation  $G = U_\psi U_0$  is with angle  $\theta \approx \frac{2}{\sqrt{N}}$ .

- $G |\psi\rangle = U_\psi U_0 |\psi\rangle = U_\psi (|\psi\rangle - \frac{2}{\sqrt{N}} |n_0\rangle) = (1 - \frac{4}{N}) |\psi\rangle + \frac{2}{\sqrt{N}} |n_0\rangle$ . So after rotation by  $\theta$  the rotated state  $G |\psi\rangle$  is closer to  $|n_0\rangle$ .

- $G |\psi\rangle$  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  $\theta$ .

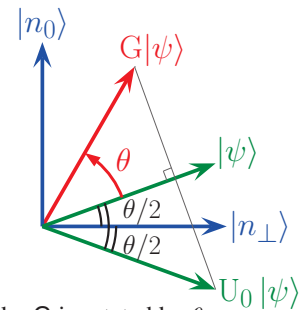
So  $G^2 |\psi\rangle$  rotates  $|\psi\rangle$  by  $2\theta$  toward  $|n_0\rangle$ , and  $G^k |\psi\rangle$  rotates  $|\psi\rangle$  by  $k\theta$  toward  $|n_0\rangle$ .

- The angle  $\Theta$  of  $|\psi\rangle$  and  $|n_0\rangle$  is such that  $\cos(\Theta) = \langle n_0 | \psi \rangle = 1/\sqrt{N} \Rightarrow \Theta = \arccos(1/\sqrt{N})$ .

- So  $K = \frac{\Theta}{\theta} \approx \frac{\sqrt{N}}{2} \arccos(1/\sqrt{N})$  iterations of  $G$  rotate  $|\psi\rangle$  onto  $|n_0\rangle$ .

At most  $\Theta = \frac{\pi}{2}$  (when  $N \gg 1$ )  $\Rightarrow$  at most  $K \approx \frac{\pi}{4} \sqrt{N}$ .

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



48/79

## Other quantum algorithms

- Shor factoring algorithm (1994) :

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

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

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

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

- <https://quantumalgorithmzoo.org>

“A comprehensive catalog of quantum algorithms ...”

49/79

## Quantum cryptography

- The problem of cryptography

Message  $X$ , a string of bits.

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

The cryptogram or encrypted message  $C(X, K) = X \oplus K$  (encrypted string of bits).

This is Vernam cipher or one-time pad,

with provably perfect security, since mutual information  $I(C; X) = H(X) - H(X|C) = 0$ .

**Problem** : establishing a secret (private) key

between emitter (Alice) and receiver (Bob).

With quantum signals,

any measurement by an eavesdropper (Eve) disturbs the system,

and hence reveals the eavesdropping, and also certifies perfect security conditions.

50/79

- BB84 protocol (Bennett & Brassard 1984)

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

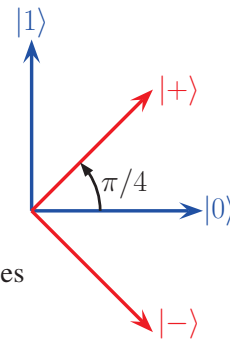
- ◆ Then Bob chooses to measure each received qubit either in basis  $\{|0\rangle, |1\rangle\}$  or  $\{|+\rangle, |-\rangle\}$  so as to decode each transmitted bit.

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

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

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

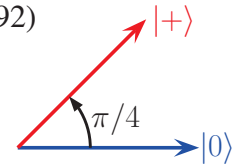
- ◆ From their  $2N$  coinciding bits, Alice and Bob classically exchange  $N$  bits at random. In case of eavesdropping, around  $N/4$  of these  $N$  test bits will differ. If all  $N$  test bits coincide, then the remaining  $N$  bits form the shared secret key.



51/79

- 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  $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$  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  $a = a' \implies b = 0$  and hence  $b = 1 \implies a \neq a' = 1 - a$ .

- ◆ 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.

52/79

• 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 and Bob just needs a quantum channel from a common server dispatching entangled qubit pairs prepared in one stereotyped quantum state.

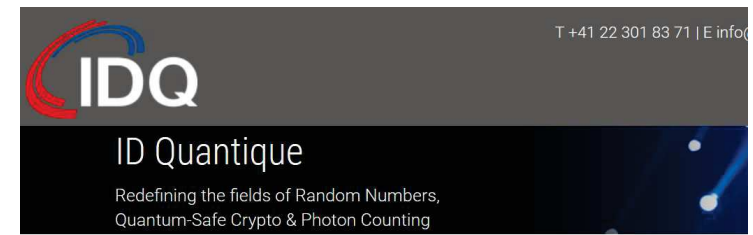
◆ Alice and Bob share a sequence of entangled qubit pairs all prepared in the same entangled (Bell) state  $|AB\rangle = (|00\rangle + |11\rangle) / \sqrt{2}$ .

◆ 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  $|AB\rangle = (|++\rangle + |--\rangle) / \sqrt{2}$ . 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.



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 governments.

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 Centaurus Ethernet and Fiber Channel encryptors, Cerberis has been deployed by governments, enterprises and financial institutions since 2007.

Clavis<sup>2</sup> 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.

**USER CASE**

**IDQ**  
FROM VISION TO TECHNOLOGY

REDEFINING SECURITY

**Geneva Government**

Secure Data Transfer for Elections

Gigabit Ethernet Encryption with Quantum Key Distribution

**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

"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-

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

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



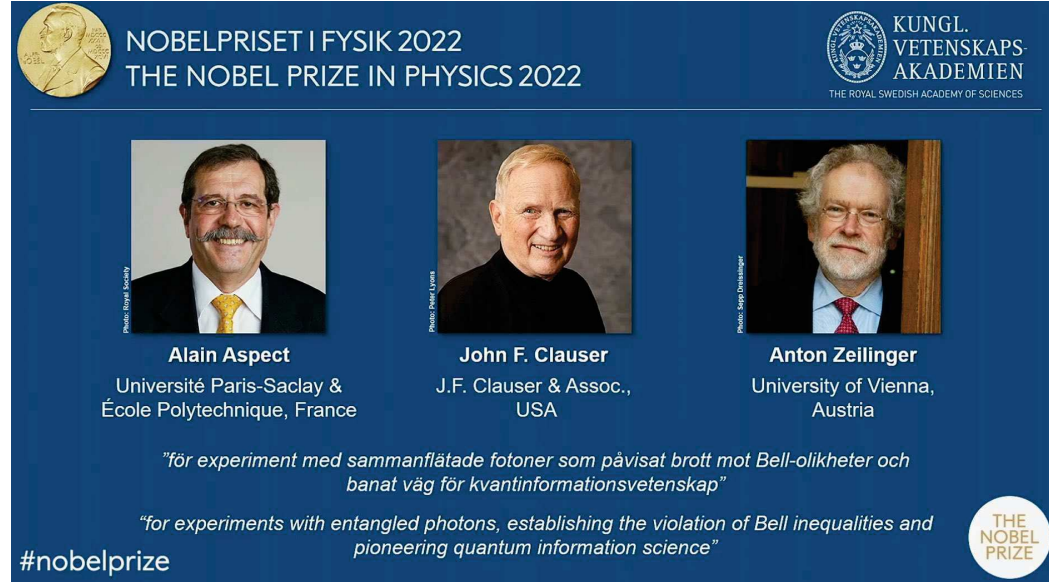
"I believe that science is not simply a matter of exploring new horizons. One must also make the new knowledge readily available, and we have in this work a beautiful example of such a pedagogical effort." Claude Cohen-Tannoudji, in foreword to the book "Introduction to Quantum Optics" by G. Grynberg,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

## Summary of "Cours 2"

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

57/79

## Quantum correlations by entanglement



NOBELPRISET I FYSIK 2022  
THE NOBEL PRIZE IN PHYSICS 2022

KUNGL. VETENSKAPS-AKADEMIEN  
THE ROYAL SWEDISH ACADEMY OF SCIENCES

**Alain Aspect**  
Université Paris-Saclay & École Polytechnique, France

**John F. Clauser**  
J.F. Clauser & Assoc., USA

**Anton Zeilinger**  
University of Vienna, Austria

"för experiment med sammanflätade fotoner som påvisat brott mot Bell-olikheter och banat väg för kvantinformationsvetenskap"

"for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science"

#nobelprize

THE NOBEL PRIZE

58/79

## Quantum correlations by entanglement (1/5)

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

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

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

- [1] A. Einstein, B. Podolsky, N. Rosen; "Can quantum-mechanical description of physical reality be considered complete?"; *Physical Review* 47, 777-780 (1935).
- [2] J. S. Bell; "On the Einstein-Podolsky-Rosen paradox"; *Physics* 1, 195-200 (1964).
- [3] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt; "Proposed experiment to test local hidden-variable theories"; *Physical Review Letters* 23, 880-884 (1969).

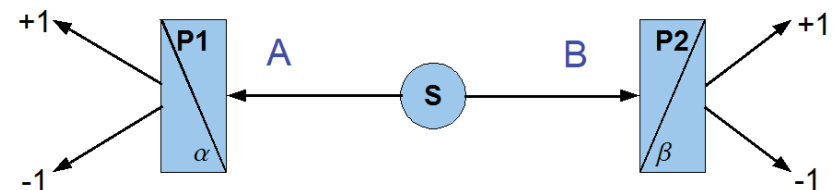
59/79

## Quantum correlations by entanglement (2/5)

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

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

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



60/79

## Quantum correlations by entanglement (3/5)

⇒ Joint probabilities

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

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

and by summation the marginal probabilities

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

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

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

61/79

## Quantum correlations by entanglement (4/5)

To obtain **four** binary variables  $\pm 1$ ,

Alice randomly switches between measuring  $A_1$  when  $\theta = \alpha_1$  or  $A_2$  when  $\theta = \alpha_2$ ,

Bob randomly switches between measuring  $B_1$  when  $\theta = \beta_1$  or  $B_2$  when  $\theta = \beta_2$ .

For  $\langle \Gamma \rangle = \langle A_1 B_1 \rangle - \langle A_2 B_1 \rangle - \langle A_1 B_2 \rangle - \langle A_2 B_2 \rangle$  one obtains

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

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

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

**Bell inequalities are violated** by quantum correlations !!

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

Nobel 2022

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

62/79

## Quantum correlations by entanglement (5/5)

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

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

• If hidden variables exist ⇒ Bell inequalities are satisfied (1964).

• A. Aspect experiments : Bell inequalities are violated by Reality (1982).

⇒ No possibility of hidden-variables theories underneath quantum mechanics.

• Quantities that cannot be simultaneously measured (incompatible) have no simultaneous physical existence or reality.

• Correlations between variables obtained from measurements of incompatible quantum quantities on entangled systems, may escape classical constraints.

⇒ a resource for information processing.

63/79



### 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.

© 2014 Elsevier B.V. All rights reserved.

64/79

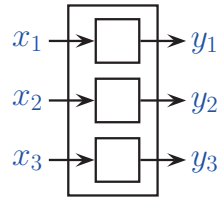


## GHZ states (1/5) (1989, Greenberger, Horne, Zeilinger) Nobel 2022

3-qubit entangled states.

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

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



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

$$\left| \begin{array}{l} x_1x_2x_3 = 000 \longrightarrow y_1y_2y_3 \text{ such that } y_1 \oplus y_2 \oplus y_3 = 0 \quad (\text{conserve parity}), \\ x_1x_2x_3 \in \{011, 101, 110\} \longrightarrow y_1y_2y_3 \text{ such that } y_1 \oplus y_2 \oplus y_3 = 1 \quad (\text{reverse parity}). \end{array} \right.$$

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  $x_j$ .

65/79

## 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 :

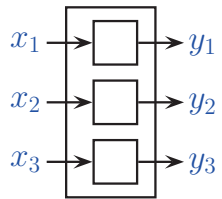
$$\begin{aligned} y_1(0) \oplus y_2(0) \oplus y_3(0) &= 0 \\ y_1(0) \oplus y_2(1) \oplus y_3(1) &= 1 \\ y_1(1) \oplus y_2(0) \oplus y_3(1) &= 1 \\ y_1(1) \oplus y_2(1) \oplus y_3(0) &= 1 \end{aligned}$$

$$\begin{aligned} \implies 0 \oplus 0 \oplus 0 &= 1, \quad \text{by summation of the four constraints,} \\ \implies 0 &= 1, \quad \text{so the four constraints are incompatible.} \end{aligned}$$

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).



66/79

## GHZ states (3/5)

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

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

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

$$\implies y_1 \oplus y_2 \oplus y_3 = 0 \text{ is matched.}$$

67/79

## GHZ states (4/5)

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

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

$$\text{Since } |0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), \quad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \implies$$

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

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

$$= |+-\rangle + |-+\rangle;$$

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

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

68/79

## GHZ states (5/5)

3) When  $x_1 x_2 x_3 = 101$ , only player 2 measures in  $\{|0\rangle, |1\rangle\}$ .

$$\begin{aligned} |\psi\rangle &= \frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle) = \frac{1}{2} \left[ |0\rangle (|0\rangle - |1\rangle) - |1\rangle (|0\rangle + |1\rangle) \right] \\ &= \frac{1}{2} \left[ |0\rangle (|+\rangle - |-\rangle) - |1\rangle (|+\rangle + |-\rangle) \right] \\ &= \frac{1}{2} (|+0\rangle - |-0\rangle - |+1\rangle + |-1\rangle) \implies y_1 \oplus y_2 \oplus y_3 = 1 \text{ matched.} \end{aligned}$$

4) When  $x_1 x_2 x_3 = 110$ , only player 3 measures in  $\{|0\rangle, |1\rangle\}$ .

$$\begin{aligned} |\psi\rangle &= \frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle) = \frac{1}{2} \left[ (|00\rangle - |11\rangle) |0\rangle - (|01\rangle + |10\rangle) |1\rangle \right] \\ &= \frac{1}{2} \left[ (|+-\rangle + |-+\rangle) |0\rangle - (|++\rangle - |--\rangle) |1\rangle \right] \\ &= \frac{1}{2} (|+-0\rangle + |-+0\rangle - |++1\rangle + |--1\rangle) \implies y_1 \oplus y_2 \oplus y_3 = 1 \text{ matched.} \end{aligned}$$

69/79

So far,

well defined state vectors (**pure** state),

**unitarily** evolved,

to represent **closed** or isolated quantum systems.



Next to come,

**open** quantum systems,

interacting with an uncontrolled environment,

inducing uncertainty to the quantum state (**mixed** state),

and evolving **non-unitarily**,

under **decoherence**.

70/79

## Density operator (1/3)

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

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

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

$$\implies \Pr\{|n\rangle\} = \sum_{j=1}^J p_j \Pr\{|n\rangle | |\psi_j\rangle\} = \langle n | \left( \sum_{j=1}^J p_j |\psi_j\rangle \langle \psi_j| \right) | n \rangle = \langle n | \rho | n \rangle,$$

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

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

The quantum system is in a **mixed** state, corresponding to the statistical ensemble

$\{(p_j, |\psi_j\rangle)\}$ , described by the density operator  $\rho$ .

**Lemma**: For any operator  $A$  with trace  $\text{tr}(A) = \sum_n \langle n | A | n \rangle$ , one has

$$\text{tr}(A |\psi\rangle \langle \phi|) = \sum_n \langle n | A |\psi\rangle \langle \phi | n \rangle = \sum_n \langle \phi | n \rangle \langle n | A |\psi\rangle = \langle \phi | \left( \sum_n |n\rangle \langle n| \right) A |\psi\rangle = \langle \phi | A |\psi\rangle.$$

71/79

## Density operator (2/3)

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

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

$$\forall |\psi\rangle, \langle \psi | \rho | \psi \rangle = \sum_j p_j |\langle \psi | \psi_j \rangle|^2 \geq 0 \implies \rho \geq 0 \text{ positive ;}$$

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

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

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

State evolution  $|\psi_j\rangle \rightarrow U |\psi_j\rangle \implies \langle \psi_j | \rightarrow \langle \psi_j | U^\dagger \implies \rho \rightarrow U \rho U^\dagger$ .

72/79

## Density operator (3/3 another motivation)

A bipartite system  $AB$  in a pure (entangled) state  $|AB\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$ .

Only  $A$  is accessible for measurement, with the set of projectors  $\{\Pi_m \otimes \mathbf{I}^B\}$ .

Probability of outcome  $m$  :

$$P(m) = \langle AB | \Pi_m \otimes \mathbf{I}^B | AB \rangle = \text{tr}_{AB}(\Pi_m \otimes \mathbf{I}^B |AB\rangle \langle AB|) = \text{tr}_A \text{tr}_B(\Pi_m \otimes \mathbf{I}^B |AB\rangle \langle AB|).$$

$$\text{Mathematically } \text{tr}_B(\Pi_m \otimes \mathbf{I}^B |AB\rangle \langle AB|) = \Pi_m \text{tr}_B(|AB\rangle \langle AB|) = \Pi_m \rho_A,$$

with  $\rho_A = \text{tr}_B(|AB\rangle \langle AB|)$  a density operator (positive unit-trace) on  $\mathcal{H}^A$ ,

which alone determines the measurement probabilities  $P(m) = \text{tr}_A(\Pi_m \rho_A)$ .

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

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

73/79

## Noisy preparation

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

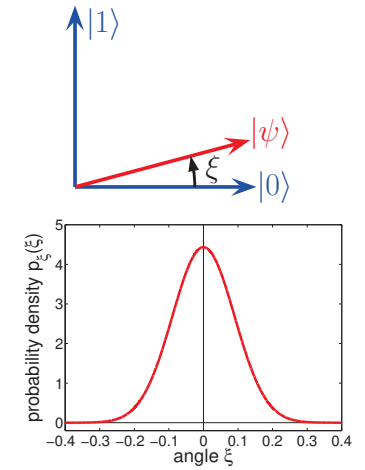
Noisy preparation  $|\psi\rangle = \cos(\xi) |0\rangle + \sin(\xi) |1\rangle$  with probability density  $p_\xi(\xi)$  (assumed even).

$$\text{Density operator } \rho = \int_{\xi} p_\xi(\xi) |\psi\rangle \langle \psi| d\xi$$

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

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

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



74/79

## Average of an observable

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

• In pure state  $|\psi_j\rangle$ : from p. 15 :

$$\text{average } \langle \Omega \rangle_j = \langle \psi_j | \Omega | \psi_j \rangle = \text{tr}(\Omega | \psi_j \rangle \langle \psi_j |) \quad \text{nonlinear in } |\psi_j\rangle, \text{ but linear in } |\psi_j\rangle \langle \psi_j|.$$

• In statistical ensemble  $\{(p_j, |\psi_j\rangle)\}$  of density operator  $\rho = \sum_j p_j |\psi_j\rangle \langle \psi_j|$  :

$$\text{average } \langle \Omega \rangle = \sum_j p_j \langle \Omega \rangle_j = \sum_j p_j \text{tr}(\Omega | \psi_j \rangle \langle \psi_j |) = \text{tr}(\Omega \sum_j p_j | \psi_j \rangle \langle \psi_j |) = \text{tr}(\Omega \rho).$$

75/79

## Density operator for the qubit

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

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

$$\implies \text{tr}(\rho) = 1.$$

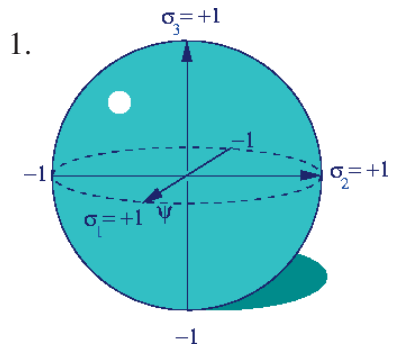
$$\rho = \rho^\dagger \implies r_x = r_x^*, \quad r_y = r_y^*, \quad r_z = r_z^* \implies r_x, r_y, r_z \text{ real.}$$

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

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

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

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



76/79

## Observables of the qubit

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

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

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

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

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

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

A consequence :  $\mathbf{A}' = a'_0 \mathbf{I}_2 + \vec{a}' \cdot \vec{\sigma} \implies \mathbf{A}\mathbf{A}' = (a_0 a'_0 + \vec{a} \cdot \vec{a}') \mathbf{I}_2 + (a'_0 \vec{a} + a_0 \vec{a}' + i \vec{a} \times \vec{a}') \cdot \vec{\sigma}$ .

77/79

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

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

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

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

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

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

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

78/79

## Justification for the generalized measurement

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

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

with arbitrary state  $|e_0\rangle \in \mathcal{H}_M$  and  $\{|m\rangle\}_{m=1}^M$  an orthonormal basis of  $\mathcal{H}_M$ .

Operator  $\mathbf{U}$  from  $\mathcal{H}_N \otimes \mathcal{H}_M$  onto  $\mathcal{H}_N \otimes \mathcal{H}_M$  is a valid unitary, as it conserves inner product :

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

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

and post-measurement state  $\frac{\mathbf{M}_m |\psi\rangle}{\sqrt{P(m)}} \otimes |m\rangle$  separable between  $\mathcal{H}_N$  and  $\mathcal{H}_M$ .

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

79/79