Quantum information, quantum computation:
An introduction.

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

“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. Grynsztag, A. Aspect, C. Fabre; Cambridge University Press 2010

A definition (at large)
To exploit quantum properties and phenomena for information processing and computation.

Motivations for the quantum
for information and computation:
1) When using elementary systems (photons, electrons, atoms, nanodevices, . .).
2) To benefit from purely quantum effects (parallelism, entanglement, . .).
3) New field of research, rich of large potentialities.

Quantum system
Represented by a state vector |ψ⟩
in a complex Hilbert space H,
with unit norm (|ψ⟩⟨ψ|) = |ψ|² = 1.

In dimension 2 : the qubit
(photons, electron, atom, . .)
State |ψ⟩ = α|0⟩ + β|1⟩
in some orthonormal basis {0, 1} of H₂,
with complex α, β ∈ C such that |α|² + |β|² = (ψψ) = |ψ|² = 1.

|ψ⟩ = α|0⟩ + β|1⟩,
ψψ = α*β,
ψψ = α*β = |ψ|² = |α|² + |β|² scalar.

Measurement
a probabilistic process,
as a destructive projection of the state |ψ⟩ in an orthonormal basis,
with statistics evaluable over repeated experiments with same preparation |ψ⟩.

Bloch sphere representation of the qubit
Qubit in state
|ψ⟩ = α|0⟩ + β|1⟩ with |α|² + |β|² = 1.

⇒ |ψ⟩ = cos(θ/2)|0⟩ + e²sin(θ/2)|1⟩
with θ ∈ [0, π],
φ ∈ [0, 2π].

Two states ⊥ in H₂ are antipodal on sphere.

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

Measurement of the qubit
When a qubit in state |ψ⟩ is measured in the orthonormal basis {0, 1},

⇒ only 2 possible outcomes (Born rule):
state 0 with probability |α|² = (0|ψ⟩⟨ψ|0) = 0|I₀|₀, or
state 1 with probability |β|² = (1|ψ⟩⟨ψ|1) = 1|I₁|₁.

State |ψ⟩ = α|0⟩ + β|1⟩,
ψψ = α*β,
ψψ = α*β = |ψ|² = |α|² + |β|² scalar.

Quantum computation:
An introduction.

Quantum information, quantum computation:
An introduction.

Quantum system
Represented by a state vector |ψ⟩
in a complex Hilbert space H,
with unit norm (|ψ⟩⟨ψ|) = |ψ|² = 1.

In dimension 2 : the qubit
(photons, electron, atom, . .)
State |ψ⟩ = α|0⟩ + β|1⟩
in some orthonormal basis {0, 1} of H₂,
with complex α, β ∈ C such that |α|² + |β|² = (ψψ) = |ψ|² = 1.

|ψ⟩ = α|0⟩ + β|1⟩,
ψψ = α*β,
ψψ = α*β = |ψ|² = |α|² + |β|² scalar.

Measurement
a probabilistic process,
as a destructive projection of the state |ψ⟩ in an orthonormal basis,
with statistics evaluable over repeated experiments with same preparation |ψ⟩.

Hadamard basis
Another orthonormal basis of H₂

{ (+) = 1/√2 (|0⟩ + |1⟩) ; -) = 1/√2 (|0⟩ - |1⟩) }.

⇒ Computational orthonormal basis

{ |0⟩ = 1/√2 (|+) - |-) ; |1⟩ = 1/√2 (|+) + |-) }.

In dimension N (finite) (extendible to infinite dimension)
State |ψ⟩ = ∑ αₙ |n⟩ , in some orthonormal basis { |1⟩, |2⟩, . . . |N⟩ } of H_N,
with αₙ ∈ C, and ∑ₙ |αₙ|² = (ψψ) = 1.

Proba. P(|n⟩) = |αₙ|² in a projective measurement of |ψ⟩ in basis { |n⟩ }.

Inner product (k|ψ⟩) = ∑ₙ αₙ (k|n⟩) = αₙ coordinate.

S = ∑ₙ |n⟩ ⟨n| = I_N identity of H_N (closure or completeness relation),
since, Y(ψ) : S |ψ⟩ = ∑ₙ |n⟩ (ψ|n⟩) = ∑ₙ αₙ |n⟩ = |ψ⟩ ⇒ S = I_N.
Multiple qubits
A system (a word) of $N$ qubits has a state in $\mathcal{H}_2^\otimes N$, a tensor-product vector space with dimension $2^N$, and orthonormal basis $\{|x_1,x_2,\ldots,x_N\rangle\}_{x_i\in\{0,1\}^N}$.

Example $N = 2$:
Generally $|\psi\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle$ ($2^N$ coord.).

Or, as a special separable state ($2N$ coord.) $|\phi\rangle = (|00\rangle + |01\rangle) \otimes (|0\rangle + |1\rangle) = |00\rangle |0\rangle + |00\rangle |1\rangle + |01\rangle |0\rangle + |01\rangle |1\rangle$.

A multipartite state which is not separable is entangled.

An entangled state behaves as a nonlocal whole: what is done on one part may influence the other part, no matter how distant they are.

Entangled states
- Example of a separable state of two qubits $AB$:
  $|AB\rangle = |+\rangle |0\rangle + |0\rangle |+\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$.

  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 $1/2$.

  $Pr(A = 0 | B) = Pr(|AB\rangle = |00\rangle + |01\rangle) = 1/4 + 1/4 = 1/2$.

- Example of an entangled state of two qubits $AB$:
  $|AB\rangle = \sqrt{2} (|00\rangle + |11\rangle)$.

  When measured in the basis $\{|0\rangle, |1\rangle\}$, each qubit $A$ and $B$ can be found in state $|0\rangle$ or $|1\rangle$ with probability $1/2$ (randomly, no predetermined 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.

Observables
For a quantum system in $\mathcal{H}_N$ with a dimension $N$, a 
projective measurement is defined by an orthonormal basis $\{|\psi_1\rangle, \ldots, |\psi_N\rangle\}$ of $\mathcal{H}_N$.

A projector $P_i = |\psi_i\rangle \langle \psi_i|$,

and for any $\langle \psi | \rho | \psi \rangle$, the probability of the $i$th outcome $P_i = \langle \psi_i | \rho | \psi_i \rangle$.

Heisenberg uncertainty relation (1/2)
For two operators $A$ and $B$:

For two operators $A$ and $B$:

$[A,B] = AB - BA$,

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

so that $\frac{1}{2} (A^2 + B^2) = A^2 + B^2 - \{A,B\}$.

When $A$ and $B$ Hermitian:

$\{A,B\} = 2 \mathcal{V}(A,B) \mathcal{V}^\dagger$.

and for any $\langle \psi | \rho | \psi \rangle$, the Cauchy-Schwarz inequality is

$\langle \psi | \rho | \psi \rangle \leq \langle \psi | A^2 | \psi \rangle \langle \psi | B^2 | \psi \rangle$.

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

$X^2 = Y^2 = Z^2 = I$.

Hermitian unitary.

$XY = -YX = iZ$, $ZX = -YZ$, etc.

$|1,0,0\rangle$ a basis for operators on $\mathcal{H}_2$.

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

$X = \sigma_x$ the inversion or Not quantum gate.

$X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$.

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

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

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 useful orthonormal basis of $\mathcal{H}_2^\otimes 2$ is the Bell basis

$\{|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$.

with $|\psi_0\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$.

$|\psi_1\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$.

$|\psi_3\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$.

Computation on a qubit
Through a unitary operator $U$ on $\mathcal{H}_2$ ($2 \times 2$ matrix): $U|\psi\rangle$ normalized vector $|\psi\rangle \in \mathcal{H}_2$.

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

quantum gate
input
|ψ⟩
output
U|ψ⟩

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

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

If $H|\psi\rangle$ is say 1, |ψ⟩ H = |ψ⟩.

$H|\psi\rangle = \frac{1}{\sqrt{2}} (|\psi\rangle + \text{conj}(\psi\rangle)$.

$\text{conj}(\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

$H^2 = I = H$.

Pauli gates
$X = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

$Y = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$.

$Z = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

$H^2 = I = H$.

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

$X = \sigma_x$ the inversion or Not quantum gate.

$X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$.

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

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

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

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

$U_\xi = \exp(-i \frac{\xi}{2} \hat{\sigma} \theta) = \cos(\frac{\xi}{2}) I - i \sin(\frac{\xi}{2}) \hat{\sigma} \theta \in SU(2)$,

with a formal “vector” of $2 \times 2$ matrix $\sigma = [\sigma_x, \sigma_y, \sigma_z]$ and $\hat{\sigma}$ a real unit vector of $\mathbb{R}^3 \cong \text{det}(U_\xi) = 1$.

implementing in the Bloch sphere representation a rotation of the qubit state of an angle $\xi$ around the axis $\hat{\sigma}$ in $\mathbb{R}^3 \in \text{SO}(3)$.

Example: $W = \sqrt{\sigma_x} = e^{i\pi/4} \cos(\pi/4) I_2 - i \sin(\pi/4) \sigma_x = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. \xi = \pi/2, \hat{\sigma} = \hat{z}.$
An optical implementation

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

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 $a|0\rangle + b|1\rangle \rightarrow a|0\rangle + be^{i\xi}|1\rangle$.

Computation on a pair of qubits

Through a unitary operator $U$ on $\mathcal{H}_2^0$ (a $4 \times 4$ matrix):

normalized vector $|\psi\rangle \in \mathcal{H}_2^0 \rightarrow U|\psi\rangle$ normalized vector in $\mathcal{H}_2^2$.

≡ quantum gate (always reversible)

Completely defined for instance by the transformation of the four state vectors

of the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

But works equally on any linear superposition of quantum states

$\implies$ quantum parallelism.

Computation on a system of $N$ qubits

Through a unitary operator $U$ on $\mathcal{H}_N^0$ (a $2^N \times 2^N$ matrix):

normalized vector $|\psi\rangle \in \mathcal{H}_N^0 \rightarrow U|\psi\rangle$ normalized vector in $\mathcal{H}_N^N$.

≡ quantum gate: $N$ input qubits $\rightarrow$ $N$ output qubits.

Completely defined for instance by the transformation of the $2^N$ state vectors

of the computational basis; but works equally on any linear superposition of them (parallelism).

Any $N$-qubit quantum gate or circuit may always be composed

two-qubit C-Not gates and single-qubit gates (universality).

And in principle this ensures experimental realizability.

This forms the grounding of quantum computation.

Parallel evaluation of a function

A classical Boolean function $f(x)$ from $N$ bits to 1 bit

$f(x) \in \{0, 1\}^N \rightarrow f(x) \in \{0, 1\}$.

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

with binary output $y \oplus f(x) = f(x)$ when $y = 0$, or $= \bar{f}(x)$ when $y = 1$,

(invertible as $[y \oplus f(x)] \oplus f(x) = y \oplus (f(x) \oplus f(x)) = y \oplus 0 = y$).

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

$(\text{CC-Not})^2 = I_\mathbb{H} \iff (\text{CC-Not})^{-1} = \text{CC-Not} = (\text{CC-Not})^3 \iff$ Hermitian unitary.

Any classical Boolean function $f(x)$ (invertible or non) on $N$ bits

can always be implemented (simulated) by means of 3-qubit Toffoli gates.

Parallel evaluation of a function

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:

$(\text{C-Not})^2 = I_\mathbb{H} \iff (\text{C-Not})^{-1} = \text{C-Not} = (\text{C-Not})^3 \iff$ Hermitian unitary.

Quantum parallelism

For a system of $N$ qubits,

a quantum gate is any unitary operator $U$ from $\mathcal{H}_N^0$ onto $\mathcal{H}_N^N$.

The quantum gate $U$ is completely defined by its action on the $2^N$ basis states of $\mathcal{H}_N^N$: $[|\xi\rangle, \xi \in \{0, 1\}^N]$,

just like a classical gate.

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

This is quantum parallelism, with no classical analog.

Parallel evaluation of a function
Parallel evaluation of a function (4/4)
\[ |+\rangle \otimes |\psi\rangle \rightarrow U_f (|+\rangle \otimes |\psi\rangle) \]

Deutsch-Jozsa algorithm (1992): Parallel test of a function (1/5)
A classical Boolean function \( f(x) : \{0, 1\}^n \rightarrow \{0, 1\} \), can be constant (all inputs into 0 or 1) or balanced (equal numbers of 0, 1 in output).
Classically: Between 2 and \( \sum \frac{N}{2} + 1 \) evaluations of \( f() \) to decide.
Quantumly: One evaluation of \( f() \) is enough (on a suitable superposition).

Lemma 1: \( |H f(x)\rangle = \frac{1}{\sqrt{2^n}} (|0\rangle \oplus |1\rangle) f(x) = \frac{1}{\sqrt{2^n}} \sum_{z \in \{0, 1\}} (-1)^{f(x) z} |z\rangle \) for \( x \in \{0, 1\}^n \).
\( \Rightarrow |H |1\rangle = \frac{1}{\sqrt{2}} (-|0\rangle + |1\rangle) = \sum_{z \in \{0, 1\}} (-1)^z |z\rangle \)
\( \Rightarrow |H |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \sum_{z \in \{0, 1\}} (-1)^\bar{0} z |z\rangle \)

Superdense coding (Bennett 1992): exploiting entanglement
Alice and Bob share a qubit pair in entangled state \( |AB\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \).

Teleportation (Bennett 1993): of an unknown qubit state (1/3)
Qubit \( Q \) in unknown arbitrary state \( |\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \).
Alice and Bob share a qubit pair in entangled state \( |AB\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \).

Teletoration (2/3)
\[ |\psi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \]

Extension to arbitrary N ≥ 2.
Extension to factorizable as a product of entangled states.

Teleportation (3/3)

Princpes references on superdense coding . . .

1 C. H. Bennett, S. J. Wiesner; “Communication via one- and two-particle operators on


2 K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, “Dense coding in experimental


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”,


... and teleportation

Grover quantum search algorithm (2/4)

• Quantumly, an N-dimensional quantum system in \( H_N \) with orthonormal basis \( |1\rangle, \ldots, |N\rangle \), where the N basis states \(|n\rangle\), for \( n \in \{1, 2, \ldots, N\} \), represent the N items of the dataset.

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

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 \( n \neq n_0 \).

Equiv.: \( U_f = I_2 - 2|\psi\rangle\langle\psi| \), although \(|\psi\rangle\) may not be known, but only \( f(.) \) to be evaluated.

The quantum oracle is able to respond to a superposition of input query states \( |\phi\rangle \) in a single interrogation, for instance to a superposition like \( |\phi\rangle = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} |n\rangle \).

Upon measuring \(|\phi\rangle\), every specific item \(|n\rangle\) would be obtained as measurement outcome with the probability \( |\langle n|\phi\rangle|^2 = \frac{1}{N} \), since \( \langle n|\phi\rangle = 1/\sqrt{N} \) for any \( n \in \{1, 2, \ldots, N\} \).

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

Grover quantum search algorithm (3/4)

• Let \(|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} |n\rangle \) normalized state \( |\psi_0\rangle \) in plane \( \{|\phi\rangle \} \) containing \(|\psi_0\rangle\).

\( F = \sum_{n=1}^{N} |n\rangle \langle n| \), the total quantum of \( |\phi\rangle \).

\( |\phi\rangle \) in plane \( \{|\psi_0\rangle \} \), the composition of two reflections is a rotation \( U_0U_0 = G \) (Grover amplification operator). It verifies \( G|\psi_0\rangle = |\psi_0\rangle \), \( |\psi_0\rangle \) via the scalar product of \( |\psi_0\rangle \) and \( G|\psi_0\rangle \), verifies cost(\( \theta \)) = \( n(\theta) = 1 - \frac{1}{N} = 1 - \frac{1}{2} = \theta = \frac{\pi}{N} \).

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.

This is Vernam cipher or one-time pad, with provably perfect security, since mutual information \( I(C; X) = H(X) - H(X|C) = 0 \).

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

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

Grover quantum search algorithm (4/4)

• In plane \( \{|\mu_0\rangle, |\nu_1\rangle\} \), the rotation \( G = U_0U_0 \) is with angle \( \theta = \frac{\pi}{\sqrt{N}} \).

• \( |\alpha\rangle \) or \( |\beta\rangle \) remains in plane \( \{|\mu_0\rangle, |\nu_1\rangle\} \), and any state in plane \( \{|\mu_0\rangle, |\nu_1\rangle\}\) by \( G \) is rotated by \( \theta \).

• So \( G^2 \) rotates \( |\psi_0\rangle \) by \( 2\theta \) toward \( |\nu_1\rangle \), and \( |\psi_0\rangle \) by \( 2\theta \) toward \( |\mu_0\rangle \).

• The angle of \( |\psi_0\rangle \) and \( |\mu_0\rangle \) is such that \( \cos(\theta) = |\langle \mu_0|\psi_0\rangle| = 1/\sqrt{N} \) \( \Rightarrow \theta = \frac{\pi}{\sqrt{N}} \).

• So \( K = \frac{\pi}{\sqrt{N}} \) (when \( N > 1 \)) \( \Rightarrow \theta = \frac{\pi}{\sqrt{N}} \).

• So when the state \( G^2 \) \( = |\psi_0\rangle \) is measured, the probability is almost 1 to obtain \(|\mu_0\rangle \).

• The searched item \(|\mu_0\rangle \) is found in \( O(\sqrt{N}) \) operations instead of \( O(N) \) classically.

Other quantum algorithms

• Shor factoring algorithm (1997):

Factors any integer in polynomial complexity (instead of exponential classically).

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

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

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

“A comprehensive catalog of quantum algorithms . . . “

Quantum cryptography

Alice has a string of 4N random bits. She encodes with a qubit in a basis state either from \( |00\rangle, |11\rangle \) or \( |+, |-\rangle \) randomly chosen for each bit.

Then Bob chooses to measure each received qubit either in basis \( |00\rangle, |11\rangle \) or \( |+, |-\rangle \) 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 \( 2^{N} \).

• If Eve intercepts and measures Alice’s qubit and forward her measured state to Bob roughly half of the time Eve forwards an incorrect state, and from this Bob half of the time decodes an incorrect bit value.

• From their 2N coinciding bits, Alice and Bob classically exchange N bits at random.

In case of eavesdropping, around 4N of these N test bits will differ.

If all N test bits coincide, then the remaining N bits form the shared secret key.
• 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 $b = a'$. This provides the final secret key.

• 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.

Protocol by broadcast of an entangled qubit pair

• With an entangled pair, Alice and Bob do not need a quantum channel between them, and can exchange only classical information to establish their private secret key. Each one of Alice an Bob just needs a quantum channel from a common server dispatching entangled qubit pairs prepared in the same entangled state $|AB\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

• 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.
A strategy winning on all four input configurations would consist in three binary functions \( j_1, j_2, j_3 \) meeting the four constraints:

\[
\begin{align*}
    &y_1(0) \oplus y_2(0) \oplus y_3(0) = 0 \\
    &y_1(0) \oplus y_2(1) \oplus y_3(1) = 1 \\
    &y_1(1) \oplus y_2(0) \oplus y_3(1) = 0 \\
    &y_1(1) \oplus y_2(1) \oplus y_3(0) = 1
\end{align*}
\]

by summation of the four constraints, \( \Rightarrow y_1 \oplus y_2 \oplus y_3 = 0 \), so the four constraints are incompatible.

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

We show a strategy using quantum resources winning on all four input configurations, (by escaping local realism, \( y_1(0) = 0/1 \) and \( y_2(1) = 0/1 \) not existing simultaneously).

**GHZ states (2/5)**

A strategy winning on all four input configurations would consist in three binary functions \( j_1, j_2, j_3 \) meeting the four constraints:

\[
\begin{align*}
    &y_1(0) \oplus y_2(0) \oplus y_3(0) = 0 \\
    &y_1(0) \oplus y_2(1) \oplus y_3(1) = 1 \\
    &y_1(1) \oplus y_2(0) \oplus y_3(1) = 0 \\
    &y_1(1) \oplus y_2(1) \oplus y_3(0) = 1
\end{align*}
\]

**Density operator (1/2)**

Quantum system in (pure) state \( |\psi\rangle \), measured in an orthonormal basis \((|n\rangle)\):

\[\Rightarrow \text{probability } \text{Pr}(\text{|n\rangle}) \equiv (\langle n | \psi \rangle)^2 = (\langle n | \psi \rangle | \psi \rangle) = (\langle n | \psi \rangle | \psi \rangle) \text{ for } n = 1, 2 \]

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

\[\Rightarrow \text{Pr}(\text{|n\rangle}) = \sum_j p_j \text{Pr}(\text{|n\rangle}) = (\sum_j p_j | n \rangle \langle n |) | \psi \rangle = \sum_j p_j | n \rangle \langle n | \psi \rangle \]

with density operator \( \rho = \sum_j p_j | n \rangle \langle n | \psi \rangle \).

The quantum system is in a mixed state, corresponding to the statistical ensemble \( \{p_j, |j\rangle\} \), described by the density operator \( \rho \).

**Noisy preparation**

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

Noise-free preparation \( |\psi\rangle = \cos(\xi)|0\rangle + \sin(\xi)|1\rangle \) with probability density \( \rho(\xi) \) (assumed even).

Density operator \( \rho \equiv \int \rho(\xi) \langle j | \langle j | \mathrm{d}\xi} \)

\[\Rightarrow \rho = \left\{ \cos(\xi) |0\rangle \langle 0| + \sin(\xi) |1\rangle \langle 1| \right\}.

**Average of an observable**

A quantum system in \( \mathcal{H}\) has observable \( \Omega \) of diagonal form \( \Omega = \sum_{n=1}^{N} a_n |a_n\rangle \langle a_n| \).

When the quantum system is in state \( \rho \), measuring \( \Omega \) amounts to performing a projection measurement on \( \rho \) in the orthonormal eigenbasis \( \{|n\rangle\} \) of \( \mathcal{H}\), with the \( N \) orthogonal projectors \( |a_n\rangle \langle a_n| \), for \( n = 1 \) to \( N \).

The outcome yields the eigenvalue \( a_n \in \mathbb{R} \) with probability

\[\text{Pr}(a_n) = |\langle a_n | \rho | a_n \rangle| = \text{tr}(\rho |a_n\rangle \langle a_n|) \]

Over repeated measurements of \( \Omega \) on the system prepared in the same state \( \rho \), the average value of \( \Omega \) is

\[\langle \Omega \rangle = \sum_{n=1}^{N} a_n \text{Pr}(a_n) = \sum_{n=1}^{N} a_n |\langle a_n | \rho | a_n \rangle| = \text{tr}(\rho \sum_{n=1}^{N} |a_n\rangle \langle a_n|) \]

\[= \text{tr}(\rho \Omega) \].

**Density operator (2/2)**

Density operator \( \rho = \sum_j p_j | n \rangle \langle n | \psi \rangle \)

\[\Rightarrow \rho = \rho^\dagger \text{ Hermitian; } \]

\[\forall |\psi\rangle, \langle \psi | \rho | \psi \rangle = \sum_j p_j | \langle j | \psi \rangle|^2 \geq 0 \Rightarrow \rho \geq 0 \text{ positive; } \]

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

On \( \mathcal{H}\), eigen decomposition \( \rho = \sum_{k=1}^{\text{dim} \mathcal{H}} |a_k\rangle \langle a_k| \cdot |a_k\rangle \langle a_k| \), with eigenvalues \( \{a_k\} \) a probability distribution, eigenstates \( |a_k\rangle \) an orthonormal basis of \( \mathcal{H}\).

Purity \( \text{tr}(\rho^2) = \sum_{k=1}^{\text{dim} \mathcal{H}} a_k^2 = 1 \) for a pure state, and \( \text{tr}(\rho^2) < 1 \) for a mixed state.

A valid density operator on \( \mathcal{H}\) is any positive operator \( \rho \) with unit trace, providing a general representation for the state of a quantum system in \( \mathcal{H}\).

State evolution \(|\psi\rangle \rightarrow U |\psi\rangle \Rightarrow \rho \rightarrow U \rho U^\dagger \).
Observables on the qubit

Any operator on $H_2$ has general form $\Omega = a_0 \mathbb{1} + \vec{a} \cdot \vec{x}$, with determinant det$(\Omega) = a_0^2 - \vec{a}^2$; two eigenvalues, $a_\pm = \frac{1}{2}(1 \pm \vec{a} \cdot \vec{x})$.

For an observable, $\Omega$ in $H_2$ requires $a_0 \in \mathbb{R}$ and $\vec{a} = [a_x, a_y, a_z] \in \mathbb{R}^3$.

Probabilities $P(\{a\}) = \frac{1}{2} (1 + \vec{a} \cdot \vec{x})$ when measuring a qubit in state $\rho = \frac{1}{2}(\mathbb{1} + \vec{r} \cdot \vec{x})$.

An important observable measurable on the qubit is $\Omega = a_2 \mathbb{1} + \vec{a} \cdot \vec{x}$, known as a spin measurement of $\vec{a}$.

In a Hilbert space $H_N$, the state of a quantum system is specified by a Hermitian positive unit-trace density operator $\rho$. For a given input ensemble $\{p_j, |\phi_j\rangle\}$:

The accessible information:

For a given input ensemble $\{p_j, |\phi_j\rangle\}$, the accessible information $I_{ac}(X;Y) = \max_{\Omega \in \text{POVM}} I(X;Y) \leq x(p_j, |\phi_j\rangle)$ is the maximum amount of information about $X$ which can be retrieved out from $Y$, by using the maximally efficient generalized measurement or POVM.

For states $|\phi_j\rangle \in L(H_N)$, there always exists such an optimal POVM under the form $\{A_{\pm} = a_\pm |\phi_j\rangle \langle \phi_j|\}$, with $a_\pm \in [0,1], \forall p_j \leq N \leq N^2$, this by Theorem 3 of E. B. Davies; “Information and quantum measurement”; IEEE Transactions on Information Theory 24 (1978) 596–599.

But, there is no general characterization of optimal POVM. [Sasaki, PRA 59 (1999) 3325]

There are hardly some known expressions for some specific ensembles $(p_j, |\phi_j\rangle)$. SOMIM (Search for Optimal Measurements by an Iterative Method) for numerical maximization by steepest-ascent that follows the gradient in the POVM space, and also uses conjugate gradients for speed-up. [arXiv:0805.2847]

Generalized measurement:

In a Hilbert space $H_N$ with dimension $N$, the state of a quantum system is specified by a Hermitian positive unit-trace density operator $\rho$.

- Projective measurement:
  Defined by a set of $N$ orthogonal projectors $|\eta\rangle \langle \eta| = \Pi_k$, verifying $\sum_k |\eta\rangle \langle \eta| = \mathbb{1}$, and $P(\{|\eta\rangle \langle \eta|\}) = \text{tr}(\rho \Pi_k)$.
  Moreover $\sum_k P(\{|\eta\rangle \langle \eta|\}) = 1$, $\forall \rho \Rightarrow \sum_k \Pi_k = \mathbb{1}$.

- Generalized measurement (POVM): (positive operator valued measure)
  Equivalent to a projective measurement in a larger Hilbert space (Naimark th.). Defined by a set of an arbitrary number of positive operators $M_k$, verifying $\sum_k M_k = \mathbb{1}$, and $P(M_k) = \text{tr}(\rho M_k)$. Moreover $\sum_k P(M_k) = 1$, $\forall \rho \Rightarrow \sum_k M_k = \mathbb{1}$.

Entropy from a quantum system:

For a quantum system of dim. $N$ in $H_N$, with a state $\rho$ (pure or mixed), a generalized measurement by the POVM with $K$ elements $\Lambda_k$, for $k = 1,2,\ldots K$.

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

Shannon output entropy $H(Y) = -\sum_{y_k} P(Y = y_k) \log P(Y = y_k)$.

For any given state $\rho$ (pure or mixed), $K$-element POVMs can always be found achieving the limit $H(Y) \to \log(K)$ at large $K$.

In this respect, with $H(Y) \to \infty$ when $K \to \infty$, an infinite quantity of information can be drawn from a quantum system of dim. $N$, as soon as $N = 2$ with a qubit.

Information in a quantum system:

How much information can be stored in a quantum system?

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

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

With a quantum system of dimension $N$ in $H_N$, each classical state $x_j$ is coded by a quantum state $|\phi_j\rangle \in H_N$ or $\rho_j \in L(H_N)$, for $j = 1,2,\ldots J$.

Since there is a continuous infinity of quantum states in $H_N$, an infinite quantity of information can be stored in a quantum system of dim. $N$ (an infinite number $J_0$), as soon as $N = 2$ with a qubit.

But how much information can be retrieved out?

The von Neumann entropy:

For a quantum system of dimension $N$ with state $\rho$ on $H_N$:

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

$\rho$ unit-trace Hermitian has diagonal form $\rho = \sum_{k=1}^N \lambda_k |\lambda_k\rangle \langle \lambda_k|$.

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

- $S(\rho) = 0$ for a pure state $\rho = |\phi\rangle \langle \phi|$.
- $S(\rho) = \log(N)$ at equiprobability when $\lambda_k = 1/N$ and $\rho = \mathbb{1}/N$.

Compression of a quantum source (1/2):

A quantum source emits states or symbols $|\phi_j\rangle$ with probabilities $p_j$, for $j = 1$ to $J$.

With $\rho = \sum_{j=1}^J p_j |\phi_j\rangle \langle \phi_j|$, the $D$-ary quantum entropy is $S_p(\rho) = -\sum_{j=1}^J p_j \log(p_j)$.

and the Holevo information is $\chi_{el}(p_j, |\phi_j\rangle) = S(\rho) - \sum_{j=1}^J p_j S(\rho_j)$.

For lossless coding of the source, the average number of $D$-dimensional quantum systems required per source symbol is lower bounded by $\chi_{el}(p_j, |\phi_j\rangle)$.

For pure states $|\phi_j\rangle = |\psi_j\rangle$, the lower bound $\chi_{el}(p_j, |\phi_j\rangle) = S(\rho_j)$ is achievable (by coding successive symbols in blocks of length $L \to \infty$).


Quantum noise on the qubit (1/4)
Quantum noise on a qubit in state $\rho$, the compressed rate is lower bounded by $H(\rho) \geq 0$ but this lower bound $H(\rho)$ is not known to be generally achievable.

The compressed rate $H(\rho)$ is however always achievable (by purification of the $\rho$ and optimal compression of this purified states).

Depending on the mixed $\rho$, and the index of faithfulness, there may exist an achievable lower bound between $H(\rho)$ and $H(\rho, \rho)$ but $\rho$ depends on $\rho$ (Wilde 2016, [18.4]).

A quantum system in state $\rho$, the compressed rate is lower bounded by $H(\rho) \geq 0$ but this lower bound $H(\rho)$ is not known to be generally achievable.

The compressed rate $H(\rho)$ is however always achievable (by purification of the $\rho$ and optimal compression of this purified states).

A quantum system of $\rho$, the compressed rate is lower bounded by $H(\rho) \geq 0$ but this lower bound $H(\rho)$ is not known to be generally achievable.

The compressed rate $H(\rho)$ is however always achievable (by purification of the $\rho$ and optimal compression of this purified states).

A quantum system of $\rho$, the compressed rate is lower bounded by $H(\rho) \geq 0$ but this lower bound $H(\rho)$ is not known to be generally achievable.

The compressed rate $H(\rho)$ is however always achievable (by purification of the $\rho$ and optimal compression of this purified states).

Quantum noise on the qubit (2/4)
Depolarizing noise : leaves the quantum state unchanged with probability $1 - p$.

$$\rho \rightarrow N(p) = (1 - p)\rho + p\sigma Y \sigma Y,$$

Phase-flip noise : flips the quantum state with probability $p$ by applying $\sigma_y$.

$$\rho \rightarrow N(p) = (1 - p)\rho + p\sigma_y \rho \sigma_y.$$
Discrimination from noisy qubits

Quantum noise on a qubit in state $\rho$ implements the transformation $\rho \xrightarrow{\text{noise}} N(\rho)$. With a noisy qubit, discrimination from $N(\rho_0)$ and $N(\rho_1)$.

---

Impact of the preparation and level of quantum noise, on the performance $P_{\text{max}}$ of the optimal detector,

in relation to stochastic resonance and enhancement by noise.
F. Chapeau-Blondeau: “Quantum state discrimination and enhancement by noise”,

N. Gillard, E. Belin, F. Chapeau-Blondeau; “Qubit state detection and enhancement by quantum thermal noise”,

---

Discrimination among $M$ states

Two alternative states $\rho_0$ or $\rho_1$ of $\mathcal{H}_0$, with priors $P_0$ and $P_1 = 1 - P_0$, are not full-rank in $\mathcal{H}_0$, e.g.
$\text{supp}(\rho_0) \cap \text{supp}(\rho_1) \neq \emptyset$ if $\text{dim}(\mathcal{H}_0) \leq M$.

For $X \equiv \{0,1\}$, $\text{supp}(\rho_0)$ is not full-rank in $\mathcal{H}_0$.

If $X \equiv \{0,1\}$, $\text{supp}(\rho_0)$ is not full-rank in $\mathcal{H}_0$.

For each nontrivial $X = \{1\}$, $\text{supp}(\rho_0)$ is not full-rank in $\mathcal{H}_0$.

---

Communication over a noisy quantum channel (2/3)

For given $N(\cdot)$ therefore $x_{\text{max}} = \max_{(\rho_0,\rho_1)} \{N(\rho_0),\rho_1\}$ is the overall maximum and achievable rate for error-free communication of classical information over a noisy quantum channel, or the classical information capacity of the quantum channel, for product states or successive independent uses of the channel.

NB : The maximum $x_{\text{max}}$ can be achieved by no more than $N^2$ pure input states $\rho_j = |\psi_j\rangle\langle\psi_j|$ with $|\psi_j\rangle \in \mathcal{H}_0$.


---

Communication over a noisy quantum channel (3/3)

For non-product states or successive non-independent but entangled states of the channel, due to a convexity property, the Holevo information is always superadditive $x_{\text{max}}(N_1 \otimes N_2) \geq x_{\text{max}}(N_1) + x_{\text{max}}(N_2)$.

(Wilde 2016 Eq (20.126))

For many channels it is found additive, $x_{\text{max}}(N_1 \otimes N_2) = x_{\text{max}}(N_1) + x_{\text{max}}(N_2)$ so that entanglement does not improve over the product-state capacity.

Yet for some channels it has been found strictly superadditive, $x_{\text{max}}(N_1 \otimes N_2) > x_{\text{max}}(N_1) + x_{\text{max}}(N_2)$ meaning that entanglement does improve over the product-state capacity.

M. B. Hastings; “Superadditivity of communication capacity using entangled inputs”,

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

---

Continuous infinite dimensional states (1/5)

A particle moving in one dimension has a state $|\psi(x)\rangle = \int_{-\infty}^{\infty} \psi(x) |x\rangle \, dx$ 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), $\int_{-\infty}^{\infty} |x\rangle \langle x| dx = 1$ (completeness).

The coordinate $x \equiv \phi(x) = |x\rangle \langle x|$ is the wave function, satisfying
$1 = \int |\psi(x)|^2 \, dx = \int \psi(x) \psi(x) \, dx = \int (\phi(x) |x\rangle \langle x| \phi(x))$, with $|\phi(x)|^2$ the probability density for finding the particle at position $x$ when measuring position operator (observable) $X = \int x |x\rangle \langle x| dx$ (diagonal form).

---

Discrimination among $M > 2$ quantum states

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

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

$\Rightarrow$ Maximize $P_{\text{success}} = \sum_{m=1}^{M} P_m \text{tr}(\rho_m \mathcal{M}_m)$ according to the $M$ operators $\mathcal{M}_m$ subject to $0 \leq \mathcal{M}_m \leq I_N$ and $\sum_{m=1}^{M} \mathcal{M}_m = I_N$.

For $M > 2$ this problem is only partially solved, in some special cases. (Barrett et al., Adv. Opt. Photon. 2009).
Continuous infinite dimensional states (2/5)

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

The basis states \( \{|\vec{r}\rangle\} \) in \( \mathcal{H} \) satisfy \( \langle\vec{r}'|\vec{r}\rangle = 0 \iff \vec{r} \neq \vec{r}' \) (orthonormality),

\[
|\vec{r}'\rangle \langle\vec{r}| = \delta(\vec{r}' - \vec{r}),
\]

the completeness relation:

\[
\int |\vec{r}\rangle \langle\vec{r}| d\vec{r} = \mathbb{1}.
\]

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

\[
1 = \int |\varphi(\vec{r})|^2 d\vec{r} = \int \psi(\vec{r})^{*} \psi(\vec{r}) d\vec{r} = \int |\varphi(\vec{r}')|^2 d\vec{r}' = \langle\psi(\vec{r})|\psi(\vec{r})\rangle,
\]

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

91/109

Continuous infinite dimensional states (3/5)

Another orthonormal basis of \( \mathcal{H} \) is formed by

\[
\{ |\vec{r}\rangle \} \text{ with } |\vec{r}\rangle = \frac{1}{\sqrt{(2\pi \hbar)^3}} \int \psi(\vec{r}) e^{-i\vec{p}\cdot\vec{r}/\hbar} d\vec{p}.
\]

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

\[
\phi(\vec{k}) = \frac{1}{(2\pi \hbar)^3} \exp(i\vec{k}\cdot\vec{r}) = \frac{1}{(2\pi \hbar)^3} \exp\left(\frac{\vec{p} \cdot \vec{r}}{\hbar}\right),
\]

in position representation, defining the state \( |\vec{r}\rangle = \int \phi(\vec{k}) |\vec{k}\rangle d\vec{k} = \int \exp\left(\frac{\vec{p} \cdot \vec{r}}{\hbar}\right) d\vec{p} \).

92/109

Continuous infinite dimensional states (4/5)

Particle with arbitrary state \( \mathcal{H} \ni |\psi(\vec{r})\rangle \) in \( \mathcal{H} \) with wave function \( \psi(\vec{r}) \) in \( \mathcal{H} \) representation

\[
\Rightarrow |H| |\psi(\vec{r})\rangle = \psi(\vec{r}) |\vec{r}\rangle.
\]

Position operator \( \vec{R} \equiv \int |\vec{r}\rangle \langle\vec{r}| d\vec{r}' \) acting on state \( |\psi(\vec{r})\rangle \) with wave function \( \psi(\vec{r}) \) in \( \mathcal{H} \) representation

\[
\Rightarrow |\vec{R}| |\psi(\vec{r})\rangle = \int |\vec{r}\rangle \langle\vec{r}| |\psi(\vec{r})\rangle d\vec{r} = \int \vec{r} |\psi(\vec{r})\rangle d\vec{r}.
\]

93/109

Quantum feedback control

System dynamics:

\[ \dot{\rho} = -\frac{i}{\hbar}[H,\rho] = \sum_{j,k} \left[L_j \rho L_k^{\dagger} - \frac{1}{2}[L_j^{\dagger},L_k^{\dagger}]\rho - [L_j, L_k^{\dagger}]\rho \right], \]

where \( L_j^{\dagger}, L_k \) are the basis operators of the measurement, and \( \rho \) is the density matrix of the system.

Measurement:

\[ \text{Post-measurement state: } \rho_m = \text{tr}_{\text{sys}}(\rho L_j^{\dagger} L_j) = \text{tr}_{\text{sys}}(L_j^{\dagger} \rho L_j), \]

with \( \text{tr}_{\text{sys}} \) denoting the trace over the system.

94/109

Continuous-time evolution of a quantum system

By empirical postulation Schrödinger equation (for isolated systems):

\[ \frac{d}{dt} |\psi(t)\rangle = -\frac{i}{\hbar} H |\psi(t)\rangle, \]

Hamitonian operator.

95/109

Optimized probing states for qubit phase estimation with general quantum noise

François Chapeau-Blondeau
Laboratoire Angélique de Recherche en Ingénierie des Systèmes (LARS), Université d'Angers, 62 avenue Sainte Dîme Du Lac, 49400 Angers, France

(Received 27 March 2015; published 12 May 2015)

We exploit the theory of quantum estimation to investigate quantum state estimation in the presence of noise. The quantum Fisher information is used to assess the estimation performance. For the qubit in Bloch representation, general expressions are derived for the quantum Fisher information and then for the quantum information.

97/109

Optimizing qubit phase estimation

François Chapeau-Blondeau
Laboratoire Angélique de Recherche en Ingénierie des Systèmes (LARS), Université d'Angers, 62 avenue Sainte Dîme Du Lac, 49400 Angers, France

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

We exploit the theory of quantum estimation to optimize qubit phase estimation with general quantum noise. The quantum Fisher information is used to assess the estimation performance. For the qubit in Bloch representation, general expressions are derived for the quantum Fisher information and then for the quantum information.

99/109
Dimensionality explosion in quantum theory

• The most elementary and nontrivial object of quantum information is the qubit, representable with a state vector $|\psi\rangle$ in the 2-dimensional complex Hilbert space $H_2$.

• Such a pure state $|\psi\rangle$ of a qubit is thus a 2-dimensional object (a 2 × 1 vector).

• Accounting for the essential property of decoherence on a qubit, requires it be represented with the extended density operator $\rho_1$ existing in the 4-dimensional space $L(2)_2$.

• A nonunitary evolution of a pure state $|\psi\rangle$ of a qubit is thus a 16-dimensional object (a 4 × 4 matrix).

• A nonunitary evolution of a mixed state $\rho_1$ of a qubit pair is thus a 256-dimensional object (a 16 × 16 matrix).

Technologies for quantum computer

• Quantum-circuit decomposition approach:
  - Quantum states: with mirrors, beam splitters, phase shifters, polarizers.
  - Light & atoms in cavity: Cavity quantum electrodynamics (Jaynes-Cummings model).

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

• Nuclear spin: manipulated with radiofrequency electromagnetic waves.

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

  (Quantionics Group, CEA Saclay, France.)

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


A commercial quantum computer: Canadian D-Wave :

Since 2011: a 128-qubit processor, with superconducting circuit implementation. Based on quantum annealing, to solve optimization problems.

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


Abstract

For binary images, or bit planes of false colour images, we investigate the possibility of a quantum-computer codification by a macroscopic assembly of reference frames shared with the electron. Direct image coding with one qubit per pixel and non-aligned frames leads to decoding errors equivalent to a quantum bit flip noise increasing with the misalignment. We show the feasibility of fast-read-invariant coding by using for each pixel a qubit pair prepared in one of two controlled-not-gates states. With just one control axis shared between the electron and matrices, direct decoding for each qubit can be obtained by means of two extra controllable projection measurements operating separately on each qubit of the pair. With an extended parameterisation of the electron and readout, direct decoding may be obtained by means of a two-controllable projection measurement operating jointly on the qubit pair. In addition, the frame-invariant coding is shown to much more resistant to quantum bit flip noise compared to the direct two-invariant coding. For a not pair of two controllable-qubits instead of two, complete fast-read-invariant image coding and enhanced error tolerance is thus obtained.