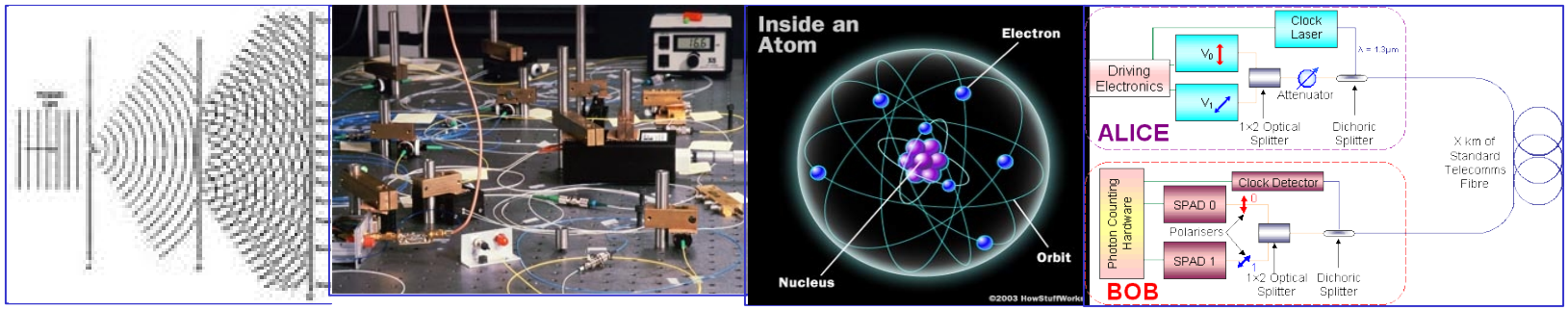
Introduction to Quantum Information Theory and Applications to Classical Computer Science

Iordanis Kerenidis
CNRS – University of Paris

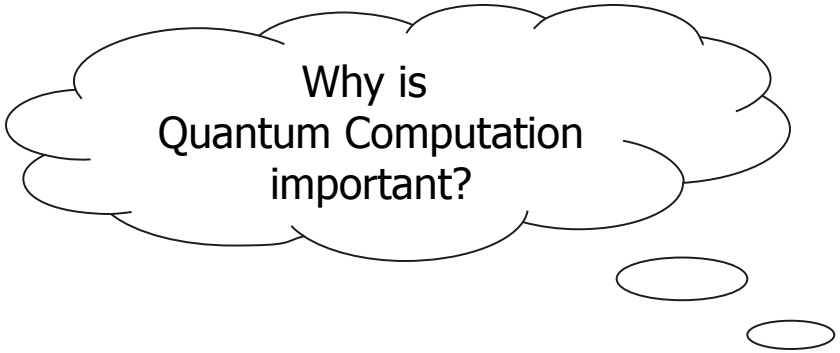
Quantum information and computation

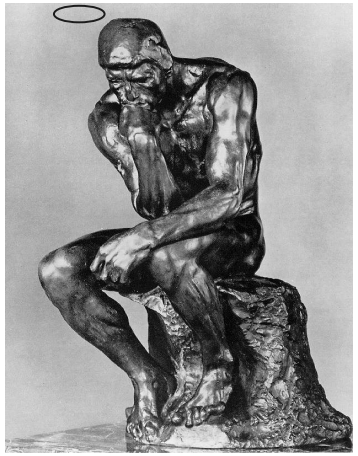
- Quantum information and computation
  - How is information encoded in nature?
  - What is nature's computational power?

- Quantum algorithm for Factoring [Shor 93]
- Unconditionally secure key distribution [Bennett-Brassard 84]
- Quantum computers probably won't solve NP-complete problems [BBBV94]



Why care about Quantum Information?





- Quantum Information and Computation
  - Computational power of nature
  - Advances in Theoretical Physics
  - Rich Mathematical Theory
  - Advances in classical Computer Science
  - Practical Quantum Cryptography
  - Advances in Experimental Physics

Quantum Information

- Quantum bit (qubit): Carrier of quantum information
  - A quantum mechanical system, which can be in a state $|0\rangle$, $|1\rangle$ or any linear combination of them. $\{|0\rangle, |1\rangle\}$ is any orthonormal basis

    $a_0|0\rangle + a_1|1\rangle, \quad a_0, a_1 \in C, \ |a_0|^2 + |a_1|^2 = 1 \qquad (\alpha_0, \alpha_1)$

- Physical Examples:

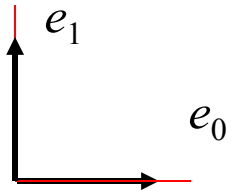
  Spin of an electron, Spin of a nuclear, Photon polarization, Two-level atom, Non-abelian anyon, …

- Here, a qubit is an abstract mathematical object, i.e. a unit vector in a 2D Hilbert space.

Probability Theory – Quantum Information I

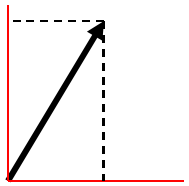
Binary Random Var. X:

$X = 0$ or $X = 1$



Quantum bit: unit vector in a 2D Hilbert space

$a_0|0\rangle + a_1|1\rangle, \quad a_0, a_1 \in \mathcal{C}, \; |a_0|^2 + |a_1|^2 = 1$



Random Variable X:

$X = \mathbf{e_i}, \quad i \in [n]$

Quantum state: on logn qubits

$$|\phi\rangle = \sum_{i=0}^{n-1} a_i|i\rangle, \quad \sum_{i=0}^{n-1} |a_i|^2 = 1$$

Correlations

$X_1 = X_2$,
i.e. $X_1X_2 = 00$ or $X_1X_2 = 11$.

Entanglement (more general than correlations!!!)

$a_0|00\rangle + a_1|11\rangle$

Probability Theory – Quantum Information II

Evolution by Stochastic Matrices

(preserve ℓ_1-norm)

$$S \cdot p = p'$$

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$$

Evolution by Unitary Matrices

(preserve ℓ_2-norm)

$$U \cdot |\phi\rangle = |\phi'\rangle$$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}(a_0 + a_1) \\ \frac{1}{\sqrt{2}}(a_0 - a_1) \end{pmatrix}$$

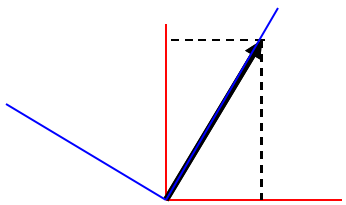
Measurement

$$\Pr[X = b] = p_b, \quad p_b \in [0, 1]$$

Measurement (Projective)

A measurement of $|\phi\rangle$ in an orthonormal basis $\{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}\}$ is a projection onto the basis vectors and

$$\Pr[\text{outcome is } \mathbf{b_i}] = |\langle \phi | b_i \rangle|^2$$

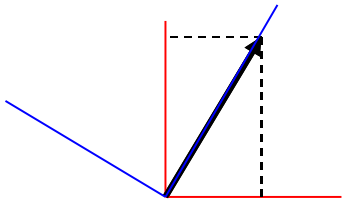


Probability Theory – Quantum Information II

Measurement (Projective)

A measurement of $|\phi\rangle$ in an orthonormal basis $\{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}\}$ is a projection onto the basis vectors and

Pr[outcome is b_i] = $|\langle\phi|b_i\rangle|^2$



Examples

- $|\phi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \qquad B = \{\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\}$

$$Prob[b_1] = \frac{(1+\sqrt{3})^2}{8}, \; Prob[b_2] = \frac{(1-\sqrt{3})^2}{8}$$

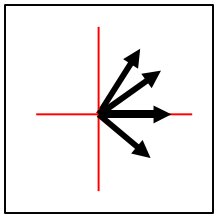
- XOR of two bits $\qquad |\phi\rangle = \frac{(-1)^{x_1}}{\sqrt{2}}|0\rangle + \frac{(-1)^{x_2}}{\sqrt{2}}|1\rangle$

$$Prob[b_1] = \frac{1}{4}((-1)^{x_1} + (-1)^{x_2})^2, \; Prob[b_2] = \frac{1}{4}((-1)^{x_1} - (-1)^{x_2})^2$$

Density matrix

- **Mixed state:** Classical distribution over pure quantum states

$$\rho = \begin{cases} |\phi_1\rangle, & \text{with prob. } p_1 \\ \cdot & \cdot \\ |\phi_k\rangle, & \text{with prob. } p_k \end{cases}$$



- **Density matrix:** $\rho = \sum_{i=1}^{n} p_i |\phi_i\rangle\langle\phi_i|$ (hermitian, trace 1, positive)

1. contains all information about the state.

$$\Pr[\text{outcome is } b_k] = \sum p_i |\langle\phi_i|b_k\rangle|^2 = \sum p_i \langle b_k|\phi_i\rangle\langle\phi_i|b_k\rangle$$
$$= \langle b_k| \left(\sum p_i |\phi_i\rangle\langle\phi_i| \right) |b_k\rangle = \langle b_k|\rho|b_k\rangle$$

5. Different ensembles can have the same ρ

$$\rho = \left\{ \begin{array}{ll} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & w.p.\ 1/2 \\ |0\rangle & w.p.\ 1/2 \end{array} \right\}$$

$$\rho = \begin{cases} \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle), & \text{w.p. } 1/\sqrt{3} \\ |0\rangle, & \text{w.p. } \frac{3}{4}(1 - \frac{1}{\sqrt{3}}) \\ |1\rangle, & \text{w.p. } \frac{1}{4}(1 - \frac{1}{\sqrt{3}}) \end{cases} \qquad \rho = \begin{pmatrix} \frac{3}{4} & -\frac{1}{4} \\ -\frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

Entropy of Quantum states

- **Shannon Entropy:** randomness in the measurement

  Random variable X, distribution P

  $$H(X) = -\sum p_i \log p_i$$

- **Von Neumann Entropy:** randomness in the *best possible* measurement

  Mixed quantum state ρ, Density matrix ρ

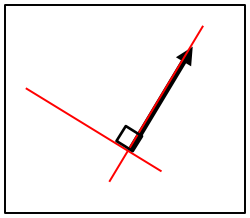
  $\rho = E \Lambda E^*$, where E are the eigenvectors and λ_i the eigenvalues.

  $$S(\rho) = -\sum \lambda_i \log \lambda_i$$

- Von Neumann Entropy shares many properties with the Shannon Entropy.

Properties of von Neumann Entropy

- $S(|\phi\rangle) = 0$



- $0 \leq S(\rho) \leq m$, where ρ contains m qubits.
- Conditional Entropy $S(\rho|\sigma) = S(\rho\sigma) - s(\sigma)$
- Mutual information $S(\rho:\sigma) = S(\rho) + S(\sigma) - S(\rho\sigma)$
- Strong subadditivity $S(\rho_1\rho_2|\sigma) \leq S(\rho_1|\sigma) + S(\rho_2|\sigma)$
- "Quantum" Fano's Inequality $S(\rho|\sigma) \leq H(\frac{1}{2} + \epsilon)$

Probability Theory - Quantum Information

Random Variable X Positive probabilities	Quantum state Complex amplitudes
Correlations	Entanglement (more general than correlations!!!)
Stochastic Matrices	Unitary Matrices
Measurement	Measurements (in different bases)
Probability Distributions	Mixed states (distribution over pure quantum states)
Shannon Entropy	Von Neumann Entropy (similar properties)

Amplitudes vs. Accessible Information

- Exponential number of amplitudes

  We can encode n bits $x \in \{0,1\}^n$ into log(n) qubits $\sum_{i=1}^{n} (-1)^{x_i} |i\rangle$

  e.g. $x = 0011 \;\mapsto\; \frac{1}{2}(|1\rangle + |2\rangle - |3\rangle - |4\rangle)$

- Only indirect access to the information via measurements

  No measurement can give us all the bits of x.

- *Holevo's bound :* n qubits encode at most n bits.

  - X: classical random variable, ρ: quantum encoding, Y: result of a measurment on ρ. Then S(X:Y) ≤ n
  - Bits cannot be compressed into fewer quantum bits.

Random Access Codes

- Random Access Code

  Let C be a probabilistic encoding from $\{0,1\}^n$ to R s.t.

  $$\forall x \forall i \in [n], Pr[A(C(x),i)=x_i] \geq 1/2+\epsilon$$

- Lower bound on length

$$I(x;C(x)) \leq H(C(x)) \leq \log|R|$$

$$H(x,y|z) \leq H(x|z)+H(y|z)$$

$$I(x;C(x)) = H(x) - H(x|C(x)) \geq H(x) - \sum_i H(x_i|C(x)) \geq (1-H(1/2+\epsilon))n$$

$$H(x|y) \leq H(1/2+\epsilon)$$

- Hence, $\log|R| \geq \Omega(n)$

Quantum Random Access Codes

- Quantum Random Access Code

  Let C be a quantum encoding from $\{0,1\}^n$ to R s.t.

  $$\forall i \in [n], Pr[A(C(x),i)=x_i] \geq 1/2+\epsilon$$

- Lower bound on length

Highly nontrivial!!!

$$S(x;C(x)) \leq S(C(x)) \leq \log dim(R)$$

$$S(x,y|z) \leq S(x|z)+S(y|z)$$

$$S(x;C(x)) = S(x) - S(x|C(x)) \geq S(x) - \sum_i S(x_i|C(x)) \geq (1-H(1/2+\epsilon))n$$

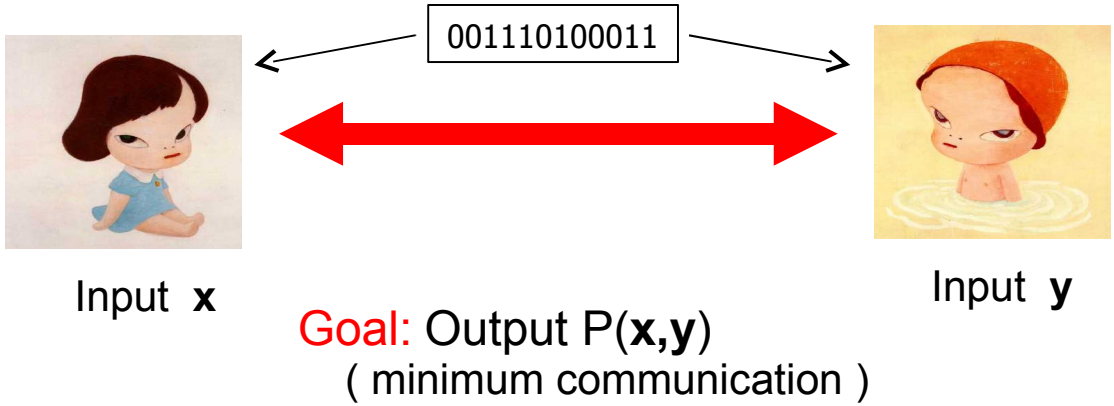
$$S(x|y) \leq H(1/2+\epsilon)$$

Holevo's bound

- Hence, $\log dim(R) \geq \Omega(n)$

Quantum vs. Classical Information

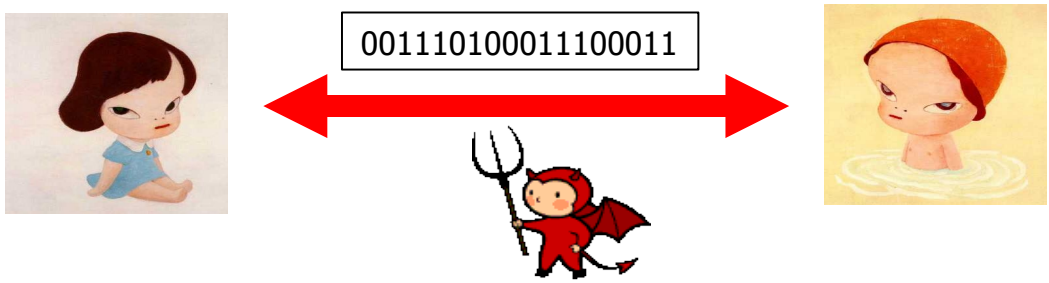
Communication complexity



- Quantum communication can be exponentially smaller than classical communication complexity
  - Two-way communication [Raz99]
  - One-way communication [Bar-Yossef, Jayram, Kerenidis 04], [Gavinsky, Kempe, Kerenidis, Raz, deWolf 06]
  - Simultaneous Messages [BJK 04]

Quantum Information and Cryptography

- Unconditionally Secure Key distribution [Bennett, Brassard 84]



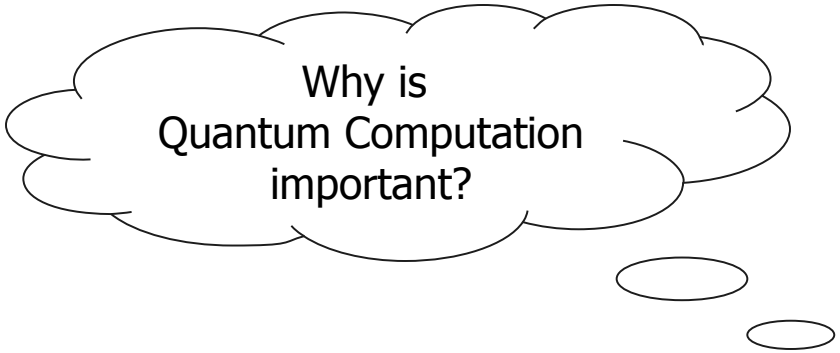
- Random number Generators [id Quantique]
- Private Information Retrieval [Kerenidis, deWolf 03, 04]
- Message Authentication, Signatures [Barnum et al. 02, Gottesman, Chuang 01]
- Quantum One-way functions [Kashefi, Kerenidis 05]

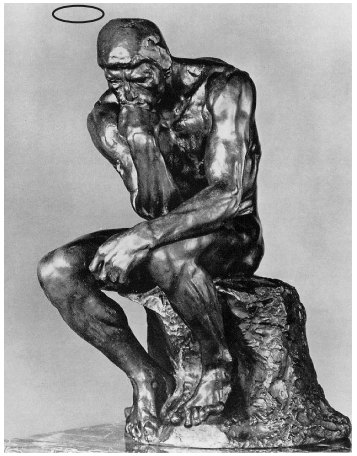
- Quantum cryptography in practice

Quantum Information & Classical Computer Science

- Classical results via quantum arguments
  - Lower bound for Locally Decodable Codes [Kerenidis, deWolf 03]
  - Lattice Problems in NP ∩ coNP [Aharonov, Regev 04]
  - Matrix Rigidity [deWolf 05]
  - Circuit Lower Bounds [Kerenidis 05]
  - Lower bounds for Local Search [Aaronson 03]

Why care about Quantum Information revisited





- Quantum Information and Computation
  - Computational power of nature
  - Advances in Theoretical Physics
  - Rich Mathematical Theory
  - Advances in classical Computer Science
  - Practical Quantum Cryptography
  - Advances in Experimental Physics