QUANTUM COMPUTATION AND INFORMATION SEMINAR

SECURITY AND QUANTUM INFORMATION GROUP

TECHNICAL UNIVERSITY OF LISBON

- 9 October 2009

A mathematical view of quantum computation

JUANJO RUÉ AND SEBASTIAN XAMBÓ

FACULTAT DE MATEMÀTIQUES I ESTADÍSTICA

UNIVERSITAT POLITÈCNICA DE CATALUNYA

08028 BARCELONA (SPAIN)

JOINT WORK WITH JUANJO RUÉ

Quantum Computation:
Foundations and State of the Art

(Master Thesis UPC)

MAIN POINTS

- Introduction
- Quantum computation in mathematical terms
  - *q*-computation and *q*-algorithms
  - *q*-computer and *q*-programs
- Comments about some *q*-algorithms
- Quantum computation in physical terms
  - Main characteristics of quantum phenomena
  - States and observables. Example: *q*-bits (or qubits)
  - Quantum computer.
- Ending remarks

ABSTRACT

A mathematical model of a quantum computer, or *q*-computer, will be presented, together with related concepts such as *q*-gates, *q*-computations and *q*-algorithms/programs.

Emphasis will be given to examples, such as the *q*-Fourier transform and *q*-algorithm of Shor to factor integers in polynomial time. The possible physical realizations of the model will be analyzed using an axiomatic version of quantum mechanics. At the end, a few lines for future work will be mentioned.

INTRODUCTION

	COMPUTACIÓN	
Level	CLASSICAL	QUANTUM
Mathematical	Mathematical logic Turing machine Boole algebra (Shannon) von Neumann machines Algorithmic theory Parallel computing	Linear algebra Vectors Matrices
Physical theory	Mechanics Electromagnetism	Quantum Mechanics (basic axioms)
Technology	Circuits, transistors, …	Ionic traps, …
Economics	Ubiquity of processors computers mobile phones digital cameras, …	Future

QUANTUM COMPUTATION IN MATHEMATICAL TERMS

Notations

- n positive integer (number of *bits* or *q-bits*)
- j positive integer in the range $0 \cdot\cdot 2^n - 1$
- $j_{n-1}j_{n-2}\cdots j_1 j_0$ binary expression of j

  $(j = j_0 + j_1 2 + \cdots + j_{n-1}2^{n-1})$

If $u = \alpha + \beta i \in \mathbb{C}$, we write $\bar{u} = \alpha - \beta i$ (*conjugate* of u)

- $H^{(n)}$ space of q-vectors of order n: $\boldsymbol{a} = \sum_j a_j \boldsymbol{u}_j = \sum_j a_j \, |j\rangle$, $a_j \in \mathbb{C}$

  These are complex vectors of 2^n components:

$$\boldsymbol{a} \equiv \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{2^n-1} \end{bmatrix}; \quad |0\rangle \equiv \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, |2^n - 1\rangle \equiv \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

- If $\boldsymbol{b} = \sum_j b_j \, |j\rangle$ is another q-vector, and $c \in \mathbb{C}$,

$$\boldsymbol{a} + \boldsymbol{b} = \sum_j \left(a_j + b_j\right) |j\rangle \, , \, c\boldsymbol{a} = \sum_j c a_j \, |j\rangle, \langle \boldsymbol{a} | \boldsymbol{b} \rangle = \sum_j \bar{a}_j b_j .$$

$\langle j|k\rangle = \delta_{jk}$ (we say that $|0\rangle$, $|1\rangle$, …, $|2^n - 1\rangle$ is an *orthonormal basis*)

Example $(n = 1)$

$$\boldsymbol{a} = a_0|0\rangle + a_1|1\rangle \equiv \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = a_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + a_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Example $(n = 2)$

$$\begin{aligned} \boldsymbol{a} &= a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + a_3|3\rangle \\ &= a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \\ &\equiv \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix} = a_{00} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + a_{01} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + a_{10} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + a_{11} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \end{aligned}$$

Proposition. $|jk\rangle = |j\rangle \otimes |k\rangle \equiv |j\rangle|k\rangle$, where $\begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \otimes \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{bmatrix}$.

In general,

$$\begin{aligned} |j_{n-1} \cdots j_1 j_0\rangle &= |j_{n-1}\rangle \otimes \cdots \otimes |j_1\rangle \otimes |j_0\rangle \\ &\equiv |j_{n-1}\rangle \cdots |j_1\rangle|j_0\rangle \end{aligned}$$

$$H^{(n)} \simeq H^{(1)} \otimes \cdots \otimes H^{(1)}$$

Proof

$$|0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} = |00\rangle$$

$$|0\rangle \otimes |1\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} = |01\rangle$$

$$|1\rangle \otimes |0\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} = |10\rangle$$

$$|1\rangle \otimes |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix} = |11\rangle$$

q-Computation

If $U = [u_{jk}]$ is a matrix, its *transpose* is $U^T = [u_{kj}]$ and its *adjoint*

$$U^\dagger = [\bar{u}_{kj}] = \overline{U^T}.$$

A *q-computation of order n* is a matrix

$$U = [u_{jk}]_{0 \le j,k < 2^n}, u_{jk} \in \mathbb{C}, \text{ such that } UU^\dagger = I_{2^n - 1}$$

(that is, U is a *unitary matrix* of order $2^n - 1$: $U \in \boldsymbol{U}(2^n) = \boldsymbol{U}^{(n)}$).

- If $U, V \in \boldsymbol{U}^{(n)}$, $VU \in \boldsymbol{U}^{(n)}$ and $U^{-1} = U^\dagger$. In other words,
  Composition. *The composition of two q-computations of order n is a q-computation of order n*; and
  Reversibility. *The inverse of a q-computation of order n is a q-computation of order n.*

A *q-input* for a q-computation U is a vector $\boldsymbol{a} \in H^n$ such that $\langle \boldsymbol{a} | \boldsymbol{a} \rangle = 1$ (unitary vector).

Example: $\boldsymbol{h}^{(n)} = (|0\rangle + |1\rangle + \cdots + |2^n - 1\rangle)/\sqrt{2^n}$

The *q-output* of a q-computation U is the (unitary) vector $\boldsymbol{b} = U\boldsymbol{a}$.

Examples $(n = 1)$**.** A q-computation of order 1 is a matrix $U \in \boldsymbol{U}^{(1)}$, i.e., a matrix of the form

$$U = e^{i\alpha} \begin{bmatrix} u_0 & u_1 \\ -\bar{u}_1 & \bar{u}_0 \end{bmatrix}, \ \alpha \in \mathbb{R}, \ u_0, u_1 \in \mathbb{C}, u_0\bar{u}_0 + u_1\bar{u}_1 = 1.$$

$$U \begin{bmatrix} a_0 \\ b_0 \end{bmatrix} = e^{i\alpha} \begin{bmatrix} u_0 a_0 + u_1 a_1 \\ -\bar{u}_1 a_0 + \bar{u}_0 a_1 \end{bmatrix}$$

Note. It is easy to check that $e^{i\alpha} \begin{bmatrix} u_0 & u_1 \\ -\bar{u}_1 & \bar{u}_0 \end{bmatrix}$ is unitary. The claim is that any unitary matrix of order 2 has this form.

Special cases: a) Pauli matrices

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

$$\Rrightarrow X|0\rangle = |1\rangle,\ X|1\rangle = |0\rangle \qquad \boxed{X = NOT = N}$$

Note. The Pauli matrices are self-adjoint: $X^2 = Y^2 = Z^2 = \mathbf{1}$.

b) Hadamard matrix

$$H_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad \begin{cases} |0\rangle \mapsto (|0\rangle + |1\rangle)/\sqrt{2} \\ |1\rangle \mapsto (|0\rangle - |1\rangle)/\sqrt{2} \end{cases}$$

c) Fase matrices

$$U_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix} = e^{i\alpha/2} \begin{bmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{bmatrix}$$

In particular, $U_{\pi/2} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ and $U_{\pi/4} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

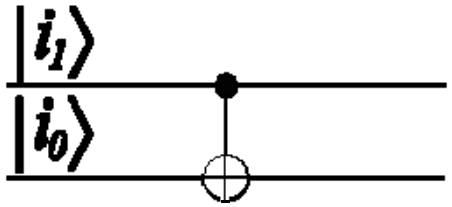
Examples $n = 2$

Let $U \in \boldsymbol{U}^{(1)}$. The we define $C_{01}(U) \in \boldsymbol{U}^{(4)}$ as follows:

$$C_{01}(U)|0a\rangle = |0a\rangle,\ C_{01}(U)|1a\rangle = |1\rangle U|a\rangle.$$

If $U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$, then

$$C_{01}(U) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$



In particular we set $C_{01} = C_{01}(N)$:

$$C_{01}|0a\rangle = |0a\rangle,\ C_{01}|1a\rangle = |1\rangle|1 + a\rangle:$$

$$C_{01} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Leaves the second bit unchanged or negates it according to whether the first bit is 0 or 1. It is a *conditional negation* (CONTROLED-NOT)

$C_{10}(U)$ is defined in an analogous way. For example,

$$C_{10} = C_{10}(N) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$C_{10,\alpha} = C_{10}(U_\alpha) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\alpha} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

q-Computer

A *q-computer of order* n is a system that allows to perform the following operations:

1. $I(\boldsymbol{a})$

   Selects the unitary vector $\boldsymbol{a} \in H^{(n)}$.

   Initialization or Input $\boldsymbol{a}$

2. $R_{j,U}, U \in \boldsymbol{U}^{(1)}$

   $$|\cdots b_j \cdots\rangle = \cdots |b_j\rangle \cdots \mapsto \cdots U|b_j\rangle \cdots$$

   Action U on the j-th bit

3. $C_{j,k}$

   Negationof the k-th bit if the j-th bit is $|1\rangle$
   (see examples $C_{0,1}$ and $C_{1,0}$ above for $n = 2$)

   $$|\cdots 1_j \cdots 0_k \cdots\rangle \mapsto |\cdots 1_j \cdots 1_k \cdots\rangle$$
   $$|\cdots 1_j \cdots 1_k \cdots\rangle \mapsto |\cdots 1_j \cdots 0_k \cdots\rangle$$

4. $O(\boldsymbol{b}), \boldsymbol{b} \in H^{(n)}$ unitary

   Observation of $\boldsymbol{b}$

   Returns $j \in 0 \cdot\cdot (2^n - 1)$ with probability $|b_j|^2$ and resets as $I(|j\rangle)$.

A *q-algorithm* is a sequence $U_1, \dots, U_r \in \boldsymbol{U}^{(n)}$ such that each U_s is either of $R_{j,U}$ or of type $C_{j,k}$, and we say that it performs the q-computation $U = U_r \cdots U_1$ (r is called the *complexity* of the algorithm).

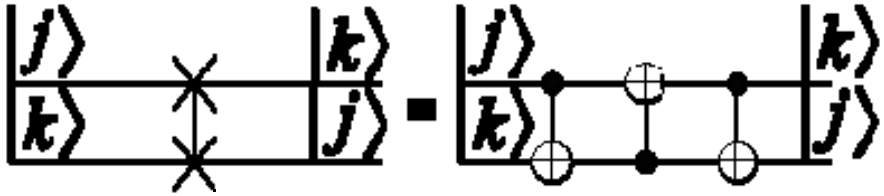
$$\text{SWAP}[0,1] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Example

Swap (trasposition of 2 bits)

SWAP$[j,k]$

$C_{j,k}, C_{k,j}, C_{j,k}$



Indeed,

$$C_{j,k}: |\cdots b_j \cdots b_k \cdots\rangle \mapsto |\cdots b_j \cdots b_j + b_k \cdots\rangle$$

$$C_{k,j}: |\cdots b_j \cdots b_j + b_k \cdots\rangle \mapsto |\cdots b_j + (b_j + b_k) \cdots b_j + b_k \cdots\rangle$$

$$= |\cdots b_k \cdots b_j + b_k \cdots\rangle$$

$$C_{j,k}: |\cdots b_k \cdots b_j + b_k \cdots\rangle \mapsto |\cdots b_k \cdots b_j \cdots\rangle$$

Theorem

Any q-computation can be realized by a q-algorithm.

A *q-algorithm* is said to be *special* or *restricted* if the operations $R_{j,U}$ apperaring in it are such that U is one of the following three matrices:

$$H_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},\ U_{\pi/2} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix},\ U_{\pi/4} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}.$$

Theorem

For any q-computation there exists a special q-algorithm that performs the computation with as much approximation as wanted.

The basic idea of the proof is that any $U \in \boldsymbol{U}^{(1)}$ can be approximated to any wanted degree by products formed with matrices taken from $\{H_1, U_{\pi/2}, U_{\pi/4}\}$.

Example

The *discrete Fourier transform* of $\boldsymbol{H}^{(n)}$ is the linear operator

$$F\colon \boldsymbol{H}^{(n)} \to \boldsymbol{H}^{(n)}\ ,\ F|j\rangle = \frac{1}{\sqrt{2^n}}\sum_k \xi^{jk}|k\rangle\ ,$$

where $\xi = \xi_n = e^{2\pi i/2^n} = e^{\pi i/2^{n-1}}$.

Observe that $F \in \boldsymbol{U}^{(n)}$**:**

$$\langle\, F|j\rangle \mid F|j'\rangle\,\rangle = \frac{1}{2^n}\sum_k \xi^{(j'-j)k} = \begin{cases} 1 & \text{if } j' = j \\ 0 & \text{if } j' \neq j \end{cases}\ ,$$

for, if $l \neq 0$, $\sum_{k=0}^{2^n-1} \xi^{lk} = \left(\left(\xi^l\right)^{2^n} - 1\right)/(\xi^l - 1) = 0.$

Let us give an idea of how to produce a q-algorithm to obtain F.

After some calculations we get that

$$F|j\rangle = \frac{1}{\sqrt{2^n}}\left(|0\rangle + e^{\pi i j}|1\rangle\right)\left(|0\rangle + e^{\pi i j/2}|1\rangle\right)\cdots\left(|0\rangle + e^{\pi i j/2^{n-1}}|1\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}}\left(|0\rangle + e^{\pi i j_0}|1\rangle\right)\left(|0\rangle + e^{\pi i (j_1 + j_0/2)}|1\rangle\right)\cdots$$

$$\left(|0\rangle + e^{\pi i (j_{n-1} + j_{n-2}/2 + \cdots + j_0/2^{n-1}}|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}}(H|j_0\rangle)\frac{1}{\sqrt{2}}(R_1 H|j_1\rangle)\cdots\frac{1}{\sqrt{2}}(R_{n-1}\cdots R_2 R_1 H|j_{n-1}\rangle),$$

where $R_l = R_{n-l-1,l}(U_{\pi/2^l})$.

This shows that F can be computed by a q-algorithm of complexity $n + (n-1) + \cdots + 1 = \binom{n+1}{2} \sim \frac{1}{2}n^2$.

q-Programs

A *[restricted] q-program* has the following structure:

INITILAZATION

$$I(\boldsymbol{a})$$

[RESTRICTED] *Q*-ALGORITHM

$$U_1, \dots, U_r$$

OUTPUT

The vector $\boldsymbol{b} = U_r U_{r-1} \cdots U_1 \boldsymbol{a}$

OBSERVATION [Optional]

$$O(\boldsymbol{b})$$

Complexity. As measure of the *complexity* of a *q*-program we take the number r (the complexity of the algorithm). We say that an algorithm is *polynomial* if its complexity is bounded by a polynomial in n.

Example

Generator of random numbers in the range $0 \cdot\cdot (2^n - 1)$ with uniform distribution:

RANDOM

$I(\boldsymbol{h}^{(n)})$

$O(\boldsymbol{h}^{(n)})$

Note that $\langle j|\boldsymbol{h}^{(n)}\rangle^2 = 1/2^n$.

COMMENTS ABOUT SOME POLYNOMIAL *Q*-ALGORITHMS

- q-Fourier transform.
- Estimate of the phase φ of the eigenvalue $e^{2\pi i\varphi}$ of a unitary operator U given the eigenvector $|u\rangle$ and the operators $C_j(U^{2^k})$.
- Given positive integers a and n, $a < n$, such that $\gcd(a, n) = 1$, to find the least positive integer r such that $a^r = 1 \bmod n$ (Shor)
- Given a positive integer, to find its factorization (Shor)
- (Discrete logarithm): Given positive integers a, b and n $(a, b < n)$ to find the least positive integer s such that $a = b^s \bmod n$, if it exists (Shor).
- (Grover's algorithm). To finding an arbitrary element in a database of order n (complexity $O(\sqrt{n})$).

QUANTUM COMPUTATION IN PHYSICAL TERMS

1. A quantum system Σ is characterized by a *complex vector space* E endowed with a Hermitian scalar product $\langle \boldsymbol{x}|\boldsymbol{y}\rangle$ (i.e., linear in $\boldsymbol{y}$ and linear-conjugate in $\boldsymbol{x}$). For the purposes of quantum computation we may also asume that E has finite dimension.

The non-zero vectores $\boldsymbol{x} \in E$ represent *states* of Σ, and two non-zero vectors $\boldsymbol{x}, \boldsymbol{y} \in E$ represent the same state if and only if there exists $c \in \mathbb{C}$ such that $\boldsymbol{y} = c\boldsymbol{x}$.

In particular, any state can be represented by a unitary vector $\boldsymbol{u}$ (determined up to a *phase factor* $e^{i\alpha}$). Thus the state space of Σ is $\mathbf{P}E$ (the *projective space* associated to E).

Following Dirac, we will write $|\boldsymbol{u}\rangle$ to denote the state corresponding to $\boldsymbol{u}$ (in projective geometry it is denoted $[\boldsymbol{u}]$).

Quantum superposition: $(\alpha + \beta i)|\boldsymbol{u}\rangle + (\alpha' + \beta' i)|\boldsymbol{u}'\rangle$.

2. (Observables) An *observable* of Σ is a linear map $A: E \to E$ such that

$$\langle A\boldsymbol{x}|\boldsymbol{y}\rangle = \langle \boldsymbol{x}|A\boldsymbol{y}\rangle \, .$$

If we express A with respect to an orthonormal basis, it is easy to check that this condition is equivalent to $A = A^{\dagger}$

observable ≡ self-adjoint operator

If $a_1, \ldots, a_r$ are the distinct eigenvalues of A, then $a_1, \ldots, a_r \in \mathbb{R}$ and $A = \sum_j a_j P_{a_j}$, where $P_{a_j}: E \to E_{a_j}$ is the orthogonal projection E onto the space $E_{a_j} = \{\boldsymbol{x} \in E | A\boldsymbol{x} = a_j\boldsymbol{x}\}$ of eigenvectors of A with eigenvalue a_j.

The result of an *observation* or *measure* of A when Σ is in the state $|\boldsymbol{u}\rangle$ is one of the eigenvalues a_j, with probability $p_{a_j} = \left\langle \boldsymbol{u} \middle| P_{a_j}\boldsymbol{u} \right\rangle$, and also that Σ is reset to the state $P_{a_j}\boldsymbol{u}$ (or, more precisely, to $|P_{a_j}\boldsymbol{u}\rangle$).

In particular, if $\boldsymbol{u} \in E_{a_j}$, then the observation yields a_j with certainty and Σ remains in the state $|\boldsymbol{u}\rangle$.

Example (Eventualities). If F is a subspace of E, the orthogonal projection $P_F: E \to F$ is an observable with eigenvalues 1 and 0: $E_1 = F$, $E_0 = F^{\perp}$. The observables of this form are called *eventualities*.

3. (Unitary dynamics) If Σ lies in a non-reactive environment (i.e., the environment is not affected by Σ) in the time interval $[0, t]$, there exists a unitary operator

$$U: E \to E$$

such that

$$\boldsymbol{b} = U\boldsymbol{a}$$

represents the state of Σ at time t if $\boldsymbol{a} \in E$ represents the state of Σ at time 0.

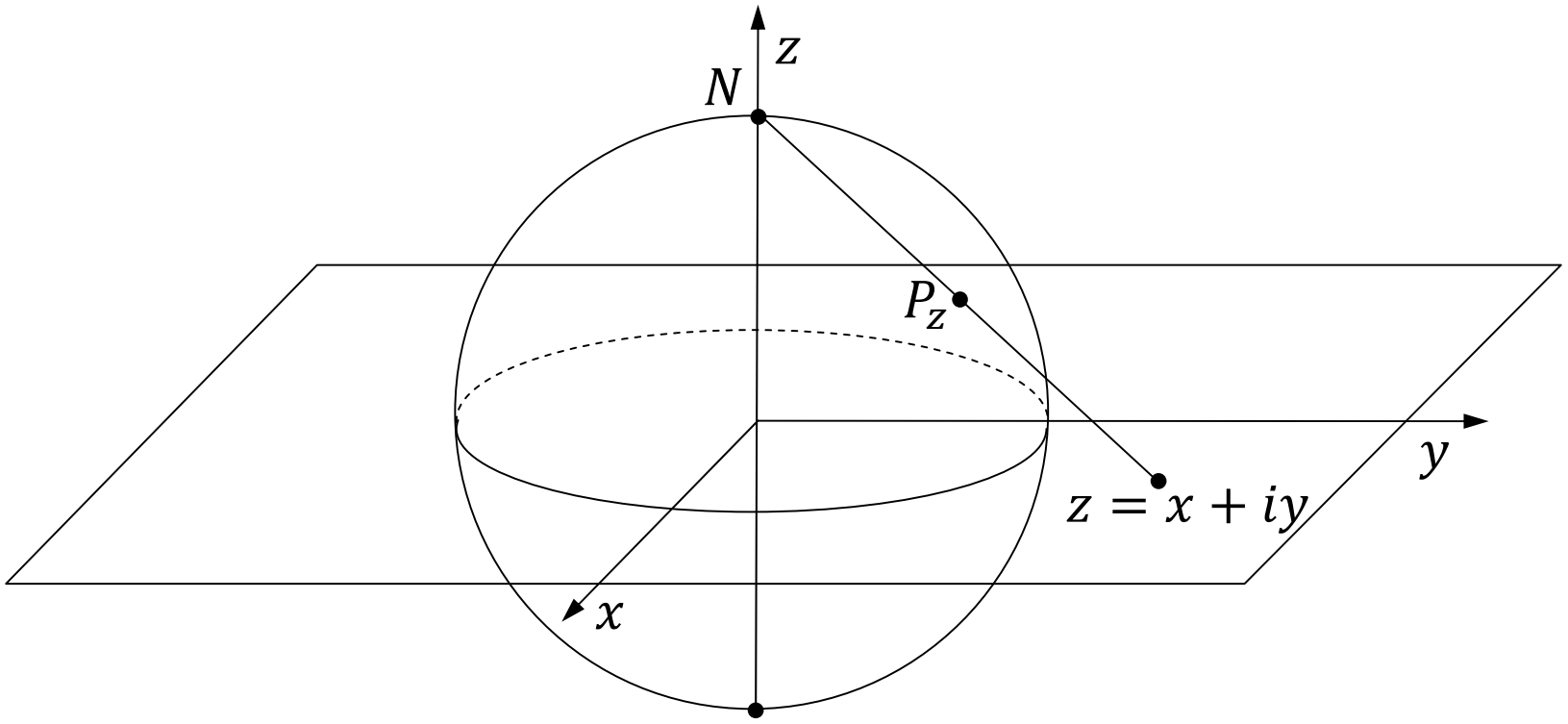
4. (Entanglement) If Σ' is a second quantum system with associated space E', then the associated space of the composite system $\Sigma_1 + \Sigma_2$ is $E \otimes E'$.

q-bits (qubits)

The states of a spin ½ particle (system $\Sigma^{(1)}$) can be thought as points lying on the sphere S^2 of radius 1 (with suitable units).

The complex space associated to this system according to axiom 1 is $\mathbb{C}^2$ (*spinor space*).

This fact can be argued as follows.



- Identify $z = x + iy \in \mathbb{C}$ with the point $(x, y, 0) \in \mathbb{R}^3$ and consider the point $P = P_z$ of

$$S^2 = \{(x, y, z) \in \mathbb{R}^3 | x^2 + y^2 + z^2 = 1\}$$

obtained by stereographic projection from $N = (0,0,1)$:

$$P = \left(\frac{2x}{x^2+y^2+1}, \frac{2y}{x^2+y^2+1}, \frac{x^2+y^2-1}{x^2+y^2+1}\right).$$

Setting $P_\infty = N$, we get a bijection between $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ and S^2. The inverse map is given by

$$(x, y, z) \mapsto \frac{x}{1-z} + i\frac{y}{1-z}.$$

- On the other hand we also have $\hat{\mathbb{C}} \simeq \mathbf{P}\mathbb{C}^2 = \mathbf{P}^1_{\mathbb{C}}$, for any element $[z_1, z_2] \in \mathbb{C}^2$ is proportional to a unique vector of the form $[1, z]$ when $z_1 \neq 0$, and to $[0,1]$ if $z_1 = 0$. Thus we have a map

$$\hat{\mathbb{C}} \to \mathbf{P}^1_{\mathbb{C}}\ ,\ z \mapsto [1, z],\ \infty \mapsto [1,0].$$

The inverse map is given by

$$[z_1, z_2] \mapsto \begin{cases} z_2/z_1 \text{ if } z_1 \neq 0 \\ \infty \text{ if } z_1 = 0 \end{cases}$$

Therefore $S^2 \simeq \hat{\mathbb{C}} \simeq \mathbf{P}^1_{\mathbb{C}}$.

This shows that the space associated to Σ is $\mathbb{C}^2$.

Note. The sphere S^2, with the structure of $\mathbf{P}^1_{\mathbb{C}}$**,** is called the *Riemann sphere.* In quantum computation references, it is called the *Bloch sphere.*

q-Registers

By axiom 4 and the formula $H^{(n)} \simeq H^{(1)} \otimes \cdots \otimes H^{(1)}$, the space $H^{(n)}$ is the associated space of $\Sigma^{(n)} = \Sigma^{(1)} + \cdots + \Sigma^{(1)}$ (n summands), the system composed of n *q*-bits (and which is called a *q-register* of order n).

Then axiom 3 tells us that the time evolution of $\Sigma^{(n)}$ is given by a unitary matrix of order 2^n. In other words, the time evolution of $\Sigma^{(n)}$ is a *q*-computation.

Finally, axiom 2 indicates that the [optional] operation $O(\boldsymbol{b})$ at the end of *q*-programs corresponds to the operation of measuring the (diagonal) observable

$$L = \sum_j j|j\rangle\langle j| \quad \text{(that is, } L|k\rangle \mapsto k|k\rangle\text{)}$$

when $\Sigma^{(n)}$ is in the state $|\boldsymbol{b}\rangle$.

Note that $\left(H^{(n)}\right)_j = \mathbb{C}\,|j\rangle$, hence $P_j\boldsymbol{b} = b_j|j\rangle$ and $p_j = \left|b_j\right|^2$.

Example (EPR states). A possible state of a q-register of order 2 is

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

Such states are called *EPR states* (also called *entangled states*).

Suppose the first q-bit is located at A and the other at B. Then if an observer at A measures the first q-bit and then and observer at B measures the second q-bit, we note that they get the same value:

A	State	B
0	$\|00\rangle$	0
1	$\|11\rangle$	1

Indeed, the EPR state $|\boldsymbol{u}\rangle$ "collapses" to $|00\rangle$ or $|11\rangle$ if A measures 0 or 1, respectively (ie, the projection of $|\boldsymbol{u}\rangle$ to the space $\{|0b\rangle\}$ is $|00\rangle$, and to the space $\{|1b\rangle\}$ is $|11\rangle$).

QUANTUM COMPUTERS

From the preceding observations it follows that it is sufficient, in order to execute q-programs of order n on a physical support, to have a quantum register $\Sigma^{(n)}$ and "implementations" of the operations

$I(\boldsymbol{a})$, $O(\boldsymbol{b})$

$C_j(U)$ [with $U = H_2$, $U_{\pi/2}$, $U_{\pi/4}$ in the restricted case]

$C_{j,k}$

A *quantum computer* (of order n) is a quantum register $\Sigma^{(n)}$ endowed with such implementations.

Its main beauty is that such a computer allows us to perform (or approximate) any q-computation.

ENDING REMARKS

Quantum parallelism

This feature stems from the possibility of initializing the q-computation in states such as $\boldsymbol{h}^{(n)} = (|0\rangle + |1\rangle + \cdots + |2^n - 1\rangle)/\sqrt{2^n}$:

- This state contains (actually is the normalized sum of) all numbers of n bits.
- Hence, any operation of the quantum computer acts on all numbers simultaneously. This "explains" why the quantum computer can be much faster than a classical computer.
- In general, the usefulness of the algorithms (as Shor's factorization, for instance) is based in the fact that after its execution the amplitudes of "useful numbers" are high and the others are small.

The problem of decoherence

This difficulty arises from the fact that interactions with the environment can quickly "perturb" the states of $\Sigma^{(n)}$ (uncontrolled "entanglement" between states of the environment and of $\Sigma^{(n)}$).

Such problems in the road of building quantum computers are of a "physical" nature. Research in many labs around the world is focussed on those questions, with continuous progress and in many direction:

http://en.wikipedia.org/wiki/Timeline_of_quantum_computing

(we see an explosion of activity in the last years, and especially since 2006).

See http://en.wikipedia.org/wiki/Quantum_computer for over a dozen lines of inquiry toward the realization of a quantum computer.

(On 24 February 2009 D-Wave Systems announced a 128 *q*-bits QC)

Teleportation

The techniques of quantum computation allow to transfer the state of q-bit at A to the same state of a q-bit at B (the *state* disappears at A and appears at B). Here is a sketch of the procedure.

- Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be the (unknown) state of a q-bit to be teleported from A to B.
- Let $|\boldsymbol{u}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ be an EPR pair shared by A and B.
- A applies C_{21} to the state

  $|\psi\rangle|\boldsymbol{u}\rangle = \frac{1}{\sqrt{2}}[\,\alpha|0\rangle\,(|00\rangle + |11\rangle)\; + \beta|1\rangle\,(|00\rangle + |11\rangle)]$, to get

  $\frac{1}{\sqrt{2}}[\,\alpha|0\rangle\,(|00\rangle + |11\rangle)\; + \beta|1\rangle\,(|10\rangle + |01\rangle)].$
- Next A applies H to the first bit, to get

  $\frac{1}{2}[\,\alpha(|0\rangle + |1\rangle)\,(|00\rangle + |11\rangle)\; + \;\beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]$

  And collecting with respect to the first two q-bits,

$$\frac{1}{2}\Big[\,|00\rangle\,(\alpha|0\rangle+\beta|1\rangle)+|01\rangle\,(\alpha|1\rangle+\beta|0\rangle)+\;\;|10\rangle\,(\alpha|0\rangle-\beta|1\rangle)\;+|11\rangle\,(\alpha|1\rangle-\beta|0\rangle)\,\Big]$$

- Now A measures the first two q-bits. The values and the corresponding state of the q-bit at B are given in the following table:

Value	00	01	10	11
State B	$\alpha\|0\rangle+\beta\|1\rangle$	$\alpha\|1\rangle+\beta\|0\rangle$	$\alpha\|0\rangle-\beta\|1\rangle$	$\alpha\|1\rangle-\beta\|0\rangle$

- So B can reproduce the state $|\psi\rangle$ in its q-bit if he knows the two classical bits produced by the measures of A by applying the gates

$$I, X, Z, XZ,$$

respectively.

Recently this possibility has been demostrated with Yb atoms at a distance of 1m (Olmschenk et al. 2009).

This opens great potential for quantum networks.

REFERENCES

Mermin, N. David [“known for the clarity and wit of his scientific writings”]
Quantum Somputer Science: an introduction
Cambridge University Press, 2007

Kaye, Phillip - Laflamme, Raymond - Mosca, Michele
An introduction to quantum computing
Oxford University Press, 2007

Jaeger, Gregg
Quantum Information—An overview
Springer, 2007

Parthasarathy, K. R.
Lecture notes on quantum computation, quantum error correcting codes and information theory
Tata Institute of Fundamental Research, Narosa Publishing House, 2006
(distributed by the AMS)

M. A. Nielsen and I. L. Chuang
Quantum computation and quantum information
Cambridge University Press, 2000

Stephen P. Jordan
Quantum Computation Beyond the Circuit Model
Tesis MIT, Sep. 2008

Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484-1509, 2005.

S. Olmschenk, D. N. Matsukevich, P. Maunz, D. Hayes, L.-M. Duan and C. Monroe: *Quantum teleportation between distant matter Qbits.* Science, 323 (23 Jan 2009).

Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6/7):467-488, 1982

¡Muito obrigado!