Mathematical Essentials of Quantum Computing

Juanjo Rué* and Sebastian Xambó-Descamps**
*Instituto de Ciencias Matemáticas-CSIC (juanjo.rue@icmat.es)
**Universitat Politècnica de Catalunya (sebastia.xambo@upc.edu, http://www-ma2.upc.edu/sxd/)

This poster is a pointer to an expository article aimed at presenting the essential notions of quantum computing in purely mathematical terms. It is aimed at mathematicians looking for an accessible approach to the subject in familiar terms, but also to physicists, chemists and engineers wishing a map of the mathematics involved.

Summary

We provide mathematical definitions of notions such as q-computation, q-measurement, q-procedure, q-computer and q-algorithm, and each of them is illustrated with several examples.

In addition to some low level q-algorithms, we discuss a good sample of the most relevant that were discovered in the last years, including q-Fourier transform and q-algorithms of Deutsch, Grover, Kitaev and Shor (for finding the multiplicative order of an integer modulo another integer and for factoring an integer).

The possible physical realizations of the model, and its potential use to obtain gains with respect to classical algorithms (sometimes even exponential gains), are analyzed in terms of a standard axiomatic formulation of (finite dimensional) quantum theory.

Some lines for future work are also indicated.

Introduction

The mathematical side of quantum processing, which we call q-processing, is presented as a suitable rephrasing of mathematical notions, most notably complex linear algebra and basic notions of elementary probability theory.

Our aim is to cover from the most basic concepts up to the expression and analysis of a good sample of the remarkable q-algorithms discovered in the last twenty five years.

Since the link to physics is not addressed until a late section, our approach might be judged as a vacuous game by scientists and technologists, and perhaps even as an inconsequential story by mathematicians. Yet in our experience the approach turns out to be surprisingly powerful and illuminating, and we much hope that this appreciation will be shared by other people as well.

Actually, the phrasing of our scheme is crafted in such a way that the tacit physical meaning will be apparent to physicists and, we expect, a reliable basis for mathematicians to appreciate the key physical ideas with minimal effort.

At the earliest stages, the most visible reason for the robustness of the paradigm, and perhaps also for its esthetical appeal, is its close relation with Boolean algebra, the mathematical side of classical computing. This relation is rooted in the fact that the basic playground of q-processing is the complex space $\boldsymbol{H}^n$ generated by the set $\boldsymbol{B}^n$ of binary vectors of length n, which is the basic arena of classical computation.

Later, when the q of q-processing is interpreted as genuine quantum feature, the scheme delivers its full meaning as a mathematical model of interesting physical phenomena that are being intensively explored in labs around the world and which hold a broad range of scientific and technological possibilities for the years to come.

It may be worth reflecting that if computing with classical bits has brought about the 'digital era', dominated by information theory and computer science, together with all the various enabling technologies, the long term development of the much more comprehensive q-processing is likely to be even mightier and certainly not less interesting.

Main Points

Notations

- n, a positive integer (number of q-*bits*).
- $j, k, \ldots$ positive integers in the range $0, \ldots, 2^n - 1$.
- $\boldsymbol{B} = \{0,1\}$, set of *binary digits*.
- $\boldsymbol{B}^n$: set of *binary vectors* of length n.
- $j = j_1 j_2 \cdots j_n$, binary expression of j:
  $j_1, \ldots, j_n \in \boldsymbol{B}^n$, $j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_{n-1}2 + j_n$.
  This allows the identification $j \leftrightarrow j_1 j_2 \cdots j_n$.
- $\boldsymbol{H}^{(n)} = \mathbb{C}^{2^n}$: $\mathbb{C}$-vector space of *q-vectors of order* n. Its canonical basis
  $\boldsymbol{u}_0 = [1{,}0, \ldots {,}0]$, $\boldsymbol{u}_1 = [0{,}1{,}0, \ldots {,}0], \ldots, \boldsymbol{u}_{2^n-1} = [0, \ldots {,}0{,}1]$,
  is often written in *Dirac's notation*: $\boldsymbol{u}_j = |j\rangle$.
- $\boldsymbol{h}^{(n)} = \rho^n(|0\rangle + |1\rangle + \cdots + |2^n - 1\rangle)$, $\rho = 1/\sqrt{2}$:
  Hadamard q-vector of order n.
- If $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{H}^{(n)}$, its *bracket* (*product*) is $\langle \boldsymbol{a}|\boldsymbol{b}\rangle = \sum_j \bar{a}_j b_j$.
  If $\langle \boldsymbol{a}|\boldsymbol{b}\rangle = 0$, we say $\boldsymbol{a}$ and $\boldsymbol{b}$ are orthogonal.
  Example: $\langle \boldsymbol{u}_j|\boldsymbol{u}_k\rangle = 0$ if $j \neq k$, $= 1$ if $j = k$.
  In Dirac notation: $\langle j|k\rangle = \delta_j^k$ (*orthonormal basis*).
- $\langle \boldsymbol{a}|\boldsymbol{a}\rangle = |\boldsymbol{a}|^2$, $|\boldsymbol{a}|^2 = |a_0|^2 + |a_1|^2 + \cdots + |a_{2^n-1}|^2$
  (the *norm* squared of $\boldsymbol{a}$).

1 Preliminaries

The main point is that there is an isomorphism

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

such that

$$|j\rangle \leftrightarrow |j_1\rangle \otimes \cdots \otimes |j_n\rangle \equiv |j_1\rangle \cdots |j_n\rangle.$$

A q-vector of order n of the form $\boldsymbol{a}_1 \otimes \cdots \otimes \boldsymbol{a}_n$, $\boldsymbol{a}_l \in \boldsymbol{H}^{(1)}$, is said to be *decomposable*. The basis vectors $|j_1 j_2 \cdots j_n\rangle = |j_1\rangle|j_2\rangle \cdots |j_n\rangle$ are examples of decomposable vectors. In general, however, q-vectors are not decomposable, and in this case they are said to be *entangled*. A simple example is the q-vector $|00\rangle + |11\rangle \in \boldsymbol{H}^{(2)}$.

2 q-Computations

They are defined as complex unitary matrices of dimension 2^n (order n), which form a group (denoted $\boldsymbol{U}^{(n)}$). They are usually defined by specifying the images of the base vectors $|j\rangle$, in which case it is necessary to check unitarity). For example, we can view a classical computation $f\colon \boldsymbol{B}^n \to \boldsymbol{B}^n$ as the q-computation given by

$$U_f|j\rangle = |f(j)\rangle.$$

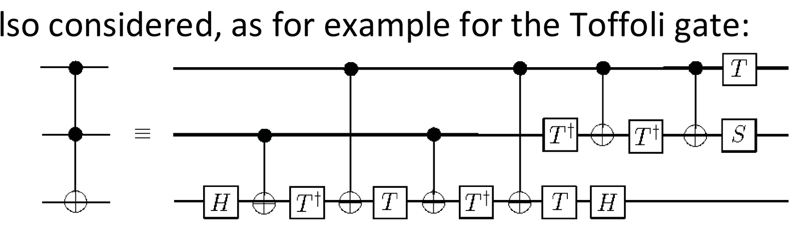
Where there is only one non trivial computation of order 1, namely Not (Not(0)=1, Not(1)=0), q-computations of order 1 depend on 4 independent real parameters.

3 q-Measurements and q-Procedures

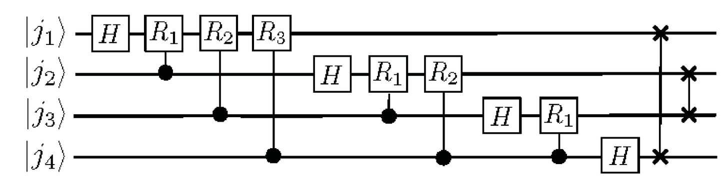
They are defined in purely mathematical terms using elementary linear algebra and probability theory. We write $M_L(\boldsymbol{a})$ to denote the measuring of the q-bits $L = \{l_1, \ldots, l_r\}$ assuming the memory is in the state $\boldsymbol{a}$.

4 q-Computers and q-Algorithms

Basic operations: q-Memory, One q-bit rotations ($R_l(U)$, $U \in \boldsymbol{U}^{(1)}$, $l \in 1..n$), Controlled negations $N_{r,s}$ and Measurements $M_L(\boldsymbol{a})$. The standard use of graphical representations is also considered, as for example for the Toffoli gate:



or the QFT (the q-algorithm for the Fourier Transform):



5 Deutsch's and Grover's q-Algorithms

Analysis of Deutsch q-algorithm that determines if $f\colon \boldsymbol{B}^n \to \boldsymbol{B}$ is balanced or constant (knowing it must be one of the two) and of Grover's search q-algorithm.

6 Phase estimation

Analysis of Kitaev's q-algorithm for approximating the phase φ of an unknown eigenvalue $e^{i\varphi}$ of a known eigenvector $\boldsymbol{u}$ of a q-computation.

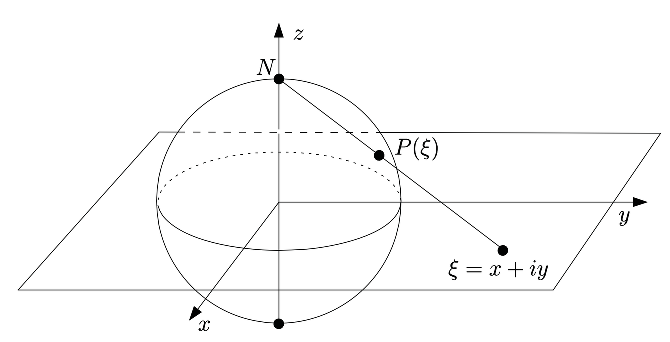
7 Modular Order of an Integer and Shor's Factoring q-Algorithm

The analysis of Shor's the q-algorithm for finding the modular order of an integer is done by means of Kitaev's q-algorithm. Then the Shor's q-algoritm for factoring integers follows from well-known techniques factoring theory.

9 Physical Interpretations

A quick presentation of the basic axioms, in mathematical terms, for (finite dimensional) quantum mechanics, and its relation to basic mathematical notions, such as the projective space $\mathbb{P}(E)$, which is the space of quantum states of a quantum system associated to a Hermitian vector space E. Special emphasis is devoted to the (physical) *qubit*, including the fundamental role played by the Riemann sphere (called Bloch sphere in quantum computing): we view $\xi = x + iy \in \mathbb{C}$ as $(x, y, 0) \in \mathbb{R}^3$, and consider the point $P = P(\xi)$ of

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



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

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

Setting $P(\infty) = N$, we get a bijection between $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ and S^2. This, together with the standard identification

$$\hat{\mathbb{C}} \simeq \mathbb{P}(\boldsymbol{H}^{(1)})$$

allows to see S^2 as the state space of a spin ½ particle.

10 Annex: Remarks and Proofs

In this section we collect the more technical aspects of our approach.

11 Conclusions and future outlook

Summary of the main points and a few ideas for further work.

Selected References

G. Alber and et al. Quantum information. *An introduction to basic theory, concepts and experiments*, volume 173 of Tracts in Math Physics. Springer-Verlag, 2001.

R. Feynman. *The Feynman Lectures on Computation*. Addison-Wesley, 1996. Edited by A. J. G. Hey and R. W. Allen.

G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 2008 (6th edition, revised by D. R. Heath-Brown and J. H. Silvermann; 1st edition published in 1938).

P. Kaye, R. Laflamme, and M. Mosca. *An introduction to quantum computing*. Oxford University Press, 2007.

T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien. Quantum computers. Nature, 464(4):45–53, 2010.

M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000 (5th printing 2005).

P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5):1484–1509, 1997.

Joachim Stolze and Dieter Suter. *Quantum Computing: a Short Course from Theory to Experiment*. Physics Textbook. Wiley-VCH, 2008. Second, updated and enlarged edition.

A. Sudbery. *Quantum mechanics and the particles of nature. An outline for mathematicians*. Cambridge University Press, 1988 (reprinting, with corrections, of 1986 edition).

L. A. Takhtajan. *Quantum mechanics for mathematicians*, volume 95 of Graduate Studies in Mathematics. American Mathematical Society, 2008.