QUANTUM COMPUTATION AND INFORMATION

Amílcar Sernadas,[1] Paulo Mateus[1] and Yasser Omar[2]

[1] *CLC, Dep. Matemática, IST, UTL*
Av. Rovisco Pais, 1049-001 Lisboa, Portugal
{acs,pmat}@math.ist.utl.pt

[2] *CEMAPRE, Dep. Matemática, ISEG, UTL*
Rua do Quelhas 6, 1200-781 Lisboa, Portugal
yomar@iseg.utl.pt

Abstract After a very brief survey of the key milestones and open problems in quantum computation and information, the research effort at IST-UTL is outlined, namely, the goals, ongoing tasks and results of the QuantLog project. In order to illustrate some key issues in quantum computation, the problem of minimizing the number of qubits in quantum automata is presented in detail at a level appropriate for non-specialists.

Keywords: Quantum Computation, Quantum Information, Quantum Logic.

1. INTRODUCTION

It seems unavoidable to use quantum resources in information processing and communication for three kinds of reasons. First, the continuing process of miniaturization of computer circuits will in due course lead to scales where quantum effects must be taken into account. Second, as noticed by Feynman [**37**], the fact that many quantum phenomena cannot be efficiently simulated with classical computers suggests that we should look at those phenomena as possible computation tools. Third, entanglement seems to be a natural for solving synchronization problems between distant agents.

Two key results confirmed these ideas. In 1991, Ekert proposed a perfectly secure quantum protocol for sharing a private classical key using public channels [**35**]. In 1994, Shor proposed a polynomial-time quantum algorithm for prime factorization [**71**]. Curiously, Shor's algorithm also has a great impact in security, namely in e-business, because the classical public key systems now in use rely precisely on the fact that prime factorization cannot be

efficiently achieved with classical computers. Afterwards, research in quantum computation and information was accelerated in several fronts: hardware for quantum computation (still in its infancy with very small laboratory prototypes); hardware for quantum enhanced secure communication (with some products already in the market); quantum algorithms (with a few interesting results, namely in searching); quantum security protocols (with several breakthroughs), quantum information theory (key theorems already established), and quantum complexity theory (with some results, but key problems still open). Section 2 contains a very brief survey of these developments.

At IST-UTL, QuantLog project (FCT FEDER POCI/MAT/55796/2004, January 1, 2005 - December 31, 2007) brought together researchers from Mathematics, Physics and Computer Science in order to address some of the open problems in quantum computation, information and logic. At this early stage of the effort, some significant results should already be mentioned: extension of classical logic for reasoning about quantum systems [**54**]; quantum algorithm for pattern matching in genomic sequences [**50**]; and compositionality of quantum security protocols [**6**]. Section 3 outlines the goals, ongoing tasks and results of the project.

Quantum automata are used in Section 4 to illustrate some key issues in quantum computation at a level appropriate for non-specialists.

Finally, in Section 5, some of the most important open problems in the area are revisited, including those currently being addressed at IST-UTL.

2. VERY BRIEF SURVEY

Information is encoded in physical systems and these are described by the laws of physics. Such laws can roughly be divided into two classes: classical physics, which describes the world at our scale, and quantum physics, which describes the world at the atomic and sub-atomic scales[1]. For most of mankind's history, information was encoded in systems that obeyed the laws of classical physics, such as stone, paper, electromagnetic waves or hard disks. And, despite the fact that one of the most important scientific revolutions of the early 20^{th} century was the understanding and control over atoms and their constituents, only in the last couple of decades did the idea to encode information directly in quantum systems, such as atoms, electrons or photons, emerge. This led to a new type of information and a new area of science: quantum information.

By the middle of the 20^{th} century all the ingredients necessary to consider this new type of information were available: Claude Shannon proposed (classical) information theory in 1948 [**68**] and quantum mechanics was an established and successful theory since at least the 30's. Yet, it took a few decades

more before the advent of quantum information. What were then the key ideas that led to it?

With hindsight, the advent of quantum information was inevitable. First, there is a technological problem. With the current trend of miniaturization in electronic chips, it is predicted that in a few decades the number of electrons per transistor will be so little that quantum effects will have to be taken into account: the device can no longer be described by classical physics, nor can the information it processes. From this perspective, the quantum computer appears as the natural consequence of the miniaturization of current (classical) computers. Yet, an apparently very different problem, dissipation of heat, also led people to consider quantum systems to process information: since quantum dynamics is reversible in time by its very nature, Paul Benioff proposed in the early 1980's a quantum Turing machine [**12, 13**] as a way to do computation without dissipating any energy. In fact, miniaturization is also increasing the problem of dissipation as we put more and more devices per unit of surface in microchips, as we can observe in the increasingly sophisticated cooling systems that we find in our laptops, but a quantum computer will be naturally free from such problems.

There was also an efficiency problem. Given the huge limitations that the use of classical computers impose on the efficient simulation of the time evolution of quantum systems, which in general can be in many different superpositions of states, Richard Feynman proposed a computer based on the laws of quantum physics as a natural and efficient way to simulate the dynamics of such systems [**37**]. A few years later, in 1985, David Deutsch effectively launched quantum computation by showing that a quantum computer could solve a particular (and quite academic) problem faster than any classical computer [**32**]. But the most significant step probably came from Peter Shor, who in 1994 showed that it was possible to factorize integers efficiently using a quantum algorithm [**69, 71**]. The factorization problem is believed to be a very hard problem for classical computers to solve, to the extent that the security of most encrypted internet communications nowadays is based on the assumption that our current computers cannot find the solution of the problem in useful time for sufficiently large numbers. Thus, the construction of a quantum computer, a machine that so far exists only in research laboratories in a rudimentary form that can only perform very trivial tasks, would challenge the security of our private communications and transactions online. Another extremely important contribution by Shor, and independently by Andrew Steane, was the proof of the existence of quantum error correcting codes, allowing for the possibility of performing quantum computation in realistic scenarios where the presence of noise cannot be avoided [**70, 72**]. Furthermore, and possibly also contributing to the implementation effort, there are now other models of quantum computation alternative and fully equivalent to the standard model based

on quantum circuits, initially suggested by David Deutsch in 1985 and shown to require only two-quantum-bit gates by David DiVincenzo in 1995 [**34**]. In 2000 Edward Farhi and collaborators proposed to do quantum computation by adiabatic evolution [**36, 9**], and in 2001 Robert Raussendorf and Hans Briegel proposed a quantum computer based on (irreversible) quantum measurements [**63**], a surprising idea very much in contrast with the (reversible) quantum circuit model, and yet completely equivalent to it. Finally, in must be said that very few significant quantum algorithms have surfaced so far: in 1996 Lov Grover proposed a search algorithm that offers a quadratic speed-up [**40, 41**], and in 2003 Andrew Childs and collaborators came up with an algorithm to find a particular node in a specific graph [**28**], a very academic problem but the only quantum algorithm so far offering a demonstrated exponential speed-up compared to its classical counterpart. Recall that, as mentioned above, it is believed that Shor's algorithm offers an exponential speed-up, but in fact it is not known if there is an efficient classical solution to the factorization problem, nor do we know if **NP** $\subseteq$ **BQP**, that is, if $SAT \in$ **BQP**, where **BQP** is the Bounded-error Quantum Polynomial time complexity class which Shor's algorithm belongs to (see Figure 1 for a map of some relevant complexity classes and their known relationships and problems[2]). In any case, should we have an operating quantum computer nowadays, its main use would be to run Shor's algorithm and thus be able to decrypt many private communications.

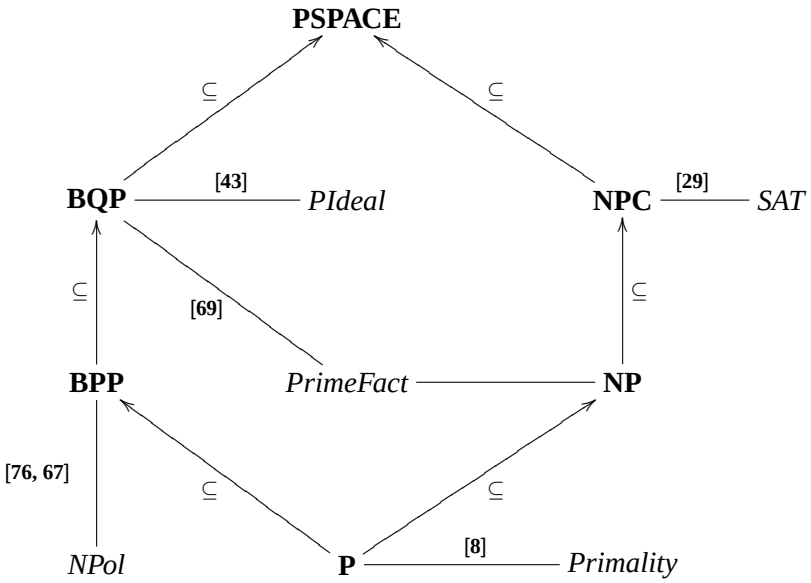

Figure 1. Some relevant complexity classes and problems

Yet, interestingly, the third motivation was precisely the incomparable level of security that quantum information can offer us. In 1935, in an attempt to criticize quantum mechanics, Albert Einstein, Boris Podolsky and Nathan Rosen (EPR) pointed out how this theory allowed for the apparent instantaneous generation of (non-classical) correlations between arbitrarily distant parties, a kind of spooky action at a distance that for them meant that quantum mechanics could not be a complete theory: it needed to be enriched with new features to explain properly such correlations. In the very same year, Erwin Schrödinger identified the existence of states (which he called *entangled states*) offering these strange quantum correlations as the "characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought" [**64**]. Yet, most people were unaware of Schrödinger's reflection and the EPR problem was the source of a long debate on the foundations of quantum theory, a debate that lasted at least until 1981, when Alain Aspect and collaborators, building on previous theoretical work by John Bell [**11**], performed experiments showing that quantum mechanics is indeed a complete theory and that Einstein and his colleagues were wrong [**10**]. In 1991, Artur Ekert revisited the EPR idea of what quantum mechanics was lacking and cunningly understood that it was equivalent to perfect eavesdropping. He then reversed the argument to show that quantum correlations could be used to establish a perfectly secure cryptographic key between two distant parties [**35**], as eavesdropping could be detected. This independent work by Ekert launched the new field of quantum security. Yet, in 1984, Charles Bennett and Gilles Brassard had already proposed a perfectly secure quantum key distribution protocol [**14**], but with almost no impact at the time. Bennett himself was inspired by Stephen Wiesner original ideas in the 1970's to use the unique properties of quantum states for security purposes, as for instance unforgeable quantum money [**74**]. In the early 90's, Bennett and his collaborators also extended the idea that entanglement between two parties could assist in the transmission of information, both classical — as in the *dense coding* scheme where a single quantum two-level system is used to send two bits [**16**], and quantum — as in the *teleportation* protocol to transmit an unknown quantum bit without measuring it [**15**]. The idea of the quantum bit, or *qubit*, as the fundamental unit of quantum information, was introduced in 1993 by Benjamin Schumacher [**65**], who at the same time launched quantum information theory by proving Shannon's Noiseless Coding Theorem [**68**] for quantum channels [**65**]. A few years later, the Holevo-Schumacher-Westmoreland Theorem [**66, 46**] gave us the capacity of a noisy quantum channel for classical information and the fully quantum analog of Shannon's Noisy Channel Coding Theorem [**68**] was finally obtained in 2005, by Igor Devetak [**33**].

These were the key steps leading to the emergence of quantum information as a new area of science, in fact an area that has been attracting very significant

resources over the last decade. This is not that surprising given the revolutionary application that quantum information seems to have the potential to offer. But what has been delivered so far? On the security side, the progress has been quite spectacular, as we now have plug and play quantum key distribution systems available on the market that work in commercial optical fibers for up to 122 km [**39**], with a growing hope that such systems will be able to operate globally in the near future, either by cable or satellite. Regarding the construction of a scalable quantum computer, this is a much harder problem, being tackled with a plethora of different technologies [**59**], and where some significant steps have already been made, despite the infancy of the field: in 2001 a NMR-based machine has been able to run Shor's algorithm with seven quantum bits [**73**], and only in the end of 2005 was it possible to produce and manipulate a quantum byte of entangled particles (in an ion trap) [**42**]. To build a useful quantum computer remains a very difficult challenge and success is not guaranteed. But, in the meantime, there are also several very important challenges at the theoretical level: to find out which problems a quantum computer can help us solve faster, why and its consequences for complexity theory; to extend quantum key distribution protocols to more than two parties and to understand in what other security problems quantum physics can offer us new and better solutions or, on the other hand, better attacks to the current systems; and finally, to study and develop new quantum logics and quantum automata to analyze these novel algorithms and protocols.

3. RESEARCH AT IST-UTL

The interest in quantum computation and information at IST-UTL started a few years ago at the Center for Plasma Physics (CFP) and got momentum with the organization of the very successful International School[3] on Quantum Computation and Information, September 2-7, 2002. A joint (almost weekly) seminar[4], with the Center for Logic and Computation (CLC) and the Center for Physics of Fundamental Interactions (CFIF), was started in September 2003.

In due course, the researchers interested in the seminar put together a research proposal that led to the QuantLog project[5] (FCT FEDER POCI/MAT/55796/2004, January 1, 2005 - December 31, 2007). A dozen faculty members plus some PhD students and postdocs work in the project that addresses some of the challenging open theoretical problems in the area and explores some important applications with emphasis on security.

The project is organized into five tasks: T0) Physics of quantum computation and information – pursuing specific goals in relevant aspects of quantum physics (namely, entanglement in solid state systems) and providing the foundational support for the whole project; T1) Quantum computation – aimed at developing new quantum algorithms (namely in logic), as well as at establish-

ing abstract results in computational complexity. T2) Quantum automata – directed at developing the categorical theory of quantum automata, ultimately aiming at compositional model checking of quantum algorithms and protocols. T3) Logics for quantum reasoning – focused on the development of a new quantum logic endowed with a semantics based on superpositions of classical valuations, having in mind the specification and verification of quantum protocols. T4) Quantum cryptography and security – mainly devoted to applications in cryptography and security, with emphasis on zero-knowledge proof systems.

Cooperation has been established with some leading research groups abroad, namely at the University of Waterloo (Canada), University College, London (UK), Kings College, London (UK), University of Berkley (USA), and University of Pennsylvania, Philadelphia (USA). An intensive guest program brought to Lisbon already more than twenty researchers active in the field for short visits and talks in our QCI seminar.

Exogenous quantum logic

Since a significant part of the project team has a background in logic, it is no surprise that the first significant contributions were in the topic of quantum logic. Based on the simple idea (so called exogenous approach) of taking superpositions of classical models as the models of the envisaged quantum logic, a novel quantum logic (EQPL) was developed for reasoning about the states of collections of qubits [**51, 52, 54**].

This novel approach to quantum reasoning is different from the mainstream approach [**38, 27**]. The latter, as initially proposed by Birkhoff and von Neumann [**17**], focuses on the lattice of closed subspaces of a Hilbert space and replaces the classical connectives by new connectives representing the lattice-theoretic operations. The former adopts superpositions of classical models as the models of the quantum logic, leading to a natural extension of the classical language containing the classical connectives (just as modal languages are extensions of the classical language). Furthermore, EQPL allows quantitative reasoning about amplitudes and probabilities, being in this respect much closer to the possible worlds logics for probability reasoning than to the mainstream quantum logics. Finally, EQPL is designed to reason about finite collections of qubits and, therefore, it is suitable for applications in quantum computation and information. The models of EQPL are superpositions of classical valuations that correspond to unit vectors expressed in the computational basis of the Hilbert space resulting from the tensor product of the independent qubit systems.

Therefore, in EQPL we can express a wide range of properties of states of such a finite collection of qubits. For example, we can impose that some qubits

are independent of (that is, not entangled with) other qubits; we can prescribe the amplitudes of a specific quantum state; we can assert the probability of a classical outcome after a projective measurement over the computational basis; and, we can also impose classical constraints on the admissible quantum states.

A complete axiomatization was given for EQPL in [**54**] (see Figure 2). Later on, a decidable fragment was presented in [**26**] where completeness was recovered with respect to a relaxed semantics over an arbitrary real closed field and its algebraic closure.

Axioms

[CTaut]	$\vdash$	α for each classical tautology α
[QTaut]	$\vdash$	γ for each quantum tautology γ
[Lift$\Rightarrow$]	$\vdash$	$((\alpha_1 \Rightarrow \alpha_2) \sqsupset (\alpha_1 \sqsupset \alpha_2))$
[Eqv$\perp$]	$\vdash$	$(\perp \equiv \perp\!\!\!\perp)$
[Ref$\sqcap$]	$\vdash$	$((\alpha_1 \sqcap \alpha_2) \sqsupset (\alpha_1 \wedge \alpha_2))$
[Sub$\emptyset$]	$\vdash$	$[\emptyset]$
[Sub$\cup$]	$\vdash$	$([G_1] \sqsupset ([G_2] \sqsupset [G_1 \cup G_2]))$
[Sub$\setminus$]	$\vdash$	$([G] \equiv [\mathsf{qB} \setminus G])$
[RCF]	$\vdash$	$\kappa\{\!\{\vec{x}/\vec{t},\ \vec{z}/\vec{u}\}\!\}$ where κ is a valid arithmetical formula, $\vec{x}$, $\vec{z}$, $\vec{t}$ and $\vec{u}$ are sequences of real variables, complex variables, real terms and complex terms respectively
[If$\top$]	$\vdash$	$(\alpha \sqsupset ((\alpha \rhd u_1; u_2) = u_1))$
[If$\perp$]	$\vdash$	$((\boxminus \alpha) \sqsupset ((\alpha \rhd u_1; u_2) = u_2))$
[Empty]	$\vdash$	$(\lvert\top\rangle_{\emptyset\emptyset} = 1)$
[NAdm]	$\vdash$	$((\neg(\wedge A)) \sqsupset (\lvert\top\rangle_{\mathsf{qB}A} = 0))$
[Unit]	$\vdash$	$([G] \sqsupset ((\sum_{A \subseteq G} \lvert\lvert\top\rangle_{GA}\rvert^2) = 1))$
[Mul]	$\vdash$	$(([G_1] \sqcap [G_2]) \sqsupset (\lvert\top\rangle_{G_1 \cup G_2 A_1 \cup A_2} = \lvert\top\rangle_{G_1 A_1} \lvert\top\rangle_{G_2 A_2}))$ where $G_1 \cap G_2 = \emptyset$, $A_1 \subseteq G_1$ and $A_2 \subseteq G_2$
[Prob]	$\vdash$	$((\int \alpha) = (\sum_A \lvert\lvert\alpha\rangle_A\rvert^2))$

Inference rules

[CMP]	$\alpha_1, (\alpha_1 \Rightarrow \alpha_2) \vdash \alpha_2$
[QMP]	$\gamma_1, (\gamma_1 \sqsupset \gamma_2) \vdash \gamma_2$

Figure 2. Axiomatization of EQPL

Other applications and further development of the exogenous approach to enriching logics were presented in [**55, 19**]. The adjective "exogenous" is used as a counterpoint to "endogenous". For instance, in order to enrich some given logic with probabilistic reasoning it may be convenient to tinker with the models of the original logic. This endogenous approach has been used extensively. For example, the domains of first-order structures are endowed with probability measures in [**44**]. Other examples include labeling the accessibility pairs with probabilities in the case of Kripke structures [**45**] for reasoning about probabilistic transition systems. By not tinkering with the original models and only

adding some additional structure on collections of those models as they are, the exogenous approach has the potential for providing general mechanisms for enriching a given logic with some additional reasoning dimension. In the case at hand, the exogenous approach has the advantage of closely guiding the design of the envisaged quantum language around the underlying concepts of quantum physics while keeping the classical connectives.

Current efforts in the quantum logic front of the QuantLog project are directed at reasoning about imperative quantum programs [**25**], as well as at trying to establish a clear bridge between EQPL and the Birkhoff and von Neumann style of quantum logics via an algebraic characterization of EQPL.

Quantum pattern matching

In another direction, a quantum algorithm for pattern matching in very long strings (like genomic sequences) was proposed in [**50**]. The algorithm is based on the modified Grover search algorithm proposed in [**18**] for the case of multiple solutions. It uses the techniques originally introduced by Grover [**41**]: a query operator that marks the state encoding the database element being searched by changing its phase; followed by an amplitude amplification of the marked state. The state can be detected with high probability by iterating this process $\sqrt{N}$ times where N is the size of the database.

- Input: $w \in \Sigma^*$ and $p \in \Sigma^*$
- Output: $m \in \mathbb{N}$
- Quantum variables: $|\psi\rangle \in \mathcal{H}(\{1, \ldots, N\})$
- Classical variables: $r, i, j \in \mathbb{N}$
- Procedure:
  1. choose $r \in [0, \llcorner\sqrt{N - M + 1}\lrcorner]$ uniformly,
  2. set $|\psi\rangle = \sum_{k=1}^{N-M+1} \frac{1}{\sqrt{N-M+1}}|k\rangle$;
  3. for $i = 1$ to r
     (a) choose $j \in [1, M]$ uniformly
     (b) set $|\psi\rangle = T_j^{-1} U_{p_j} T_j |\psi\rangle$;
     (c) set $|\psi\rangle = D|\psi\rangle$
  4. set m to the result of the measurement of $|\psi\rangle$ over the base $\{|1\rangle, \ldots, |N\rangle\}$.

Figure 3. Quantum pattern matching algorithm

The algorithm (see Figure 3) proposed in [**50**] searches for as many distinct patterns as desired in a given unsorted string, and moreover returns the position of the closest substring to a given pattern with high probability in $O(\sqrt{N})$ queries, where N is the size of the string. This means that the time to find the

closest match (a much harder problem than to find the *exact* match, as we shall see) does not depend on the size of the pattern itself, a result with no classical equivalent. Another crucial point is that our quantum algorithm is actually useful and implementable to perform searches in (unsorted) databases. For this, a query function per symbol of the pattern alphabet is needed, which will require a significant (though clearly efficient) pre-processing, but will allow us to perform an arbitrary amount of different searches in a static string. A *compile once, run many* approach yielding a new search algorithm that not only settles the previously existing implementation problems, but even offers the solution of a more general problem, and with a very interesting speed-up.

In the classical setting, the best algorithm for the closest substring problem takes $\mathrm{O}(MN)$ queries where M is the size of the pattern. This result follows from adapting the best known algorithm for approximate pattern matching [**58**], which takes $\mathrm{O}(eN + M)$ where e is the number of allowed errors. One should not compare the closest match to (exact) pattern match, where the problem consists in determining if a certain word (pattern) is a substring of a text. For exact pattern matching it is shown that the best algorithm can achieve $\mathrm{O}(M + N)$ [**58**]. However, in practical cases where data can mutate over time, like DNA, or it is stored in noisy systems, the closest match problem is much more relevant, since in general only approximates of the pattern exist, but nevertheless need to be found.

The full analysis of the proposed quantum algorithm as well as the recipe for its implementation as a quantum circuit are under way. In due course, more complex pattern matching problems will be addressed.

Quantum process algebra in security

In yet another direction of the QuantLog project, work has been done in the area of quantum process algebras. In [**6**] a quantum process algebra was proposed for the design and verification of quantum protocols, with applications in quantum security.

Security protocols are composed by several agents running in parallel, where each agent computes information (bounded by polynomial-time on the security parameter) and exchange it with other agents. In the context of quantum processes, the computation is bounded by quantum polynomial-time and the information exchanged is supported by qubits.

The problem of defining quantum security properties is addressed in [**6**] using a quantum polynomial-time process algebra. This approach is highly inspired in [**56, 48**]. The computational model used to define quantum polynomial terms is based on the logarithmic cost random access machine [**30**]. A hybrid model, using both classic and quantum memory [**47**], is considered and it is shown to be (polynomial-time) equivalent to a uniform family of quan-

tum circuits. Such machines model the computation of each agent, and receive qubits as input and return qubits as output. Thanks to the non-cloning theorem, quantum information can not be copied without prior knowledge of its state. This observation imposes some design options in the process algebra, since it is necessary to know which agent possesses a qubit in order to know who can retrieve some piece of information. In order to deal with this fact, a set of agents is fixed and the qubits are partitioned among them.

Process terms are divided into local and global. An agent is modeled by a local process while a protocol is modeled by a global process, so, a global process corresponds to local processes running in parallel. A semantics based on probabilistic transition systems (which can be easily translated to Markov chains) is provided, and the probabilistic transitions are defined using rules and assuming a uniform scheduler to resolve non-deterministic choices.

Agent observation is defined as a probability distribution over binary words obtained by measuring, at the end of the protocol and on the computational basis, (some of) the agent's qubits. This concept is the key ingredient to establish observational equivalence, that in the context of security protocols is based on computational indistinguishability [**75**]. Intuitively, two process terms are observational equivalent for an agent if, after making all possible reductions to each process, it is impossible to distinguish (in quantum polynomial-time) the qubits of the agent on both processes. Since quantum polynomial-time machines are internalized in the process algebra language, observational equivalence is easily defined and it is shown to be a congruence relation.

One of the most successful ways for defining secure concurrent cryptographic tasks is via process emulation [**1, 24**]. This definitional job boils down to the following: a process realizes a cryptographic task iff it emulates an ideal process that is known to realize such task. Hence, verification of a protocol amounts to checking if it can emulate the ideal protocols. This approach is fully compositional.

Current work on this front of the QuantLog project is focused on applications to designing and verifying concrete quantum security protocols, namely contract signing, as well as on finding quantum attacks to classical cryptosystems, namely zero-knowledge proof systems.

4. FROM QUANTUM BITS TO QUANTUM AUTOMATA

Some of the basic concepts and issues of quantum computation can be easily illustrated around the notion of quantum automaton.

But let us start first with the notion of classical automaton. Classical automata are widely used. In a typical household you will find several automata: refrigerators, washing machines, lifts, et cetera are usually controlled

by automata. A classical finite state automaton has a finite memory (that is, composed of a finite number of bits). The contents of the memory (state) is changed according to the input fed to the automaton. At each state the automaton displays an output. More precisely, a classical automaton is a tuple $(\Sigma, \Gamma, S, s_0, \delta, Z)$ where Σ is the input alphabet (set of input symbols), Γ is the output alphabet (set of output symbols), S is the state space (finite set of states), $s_0 \in S$ is the initial state, $\delta : S \times \Sigma \to S$ is the transition map (returns the next state $\delta(s, \sigma)$ on receiving input σ on state s), and $Z : S \to \Gamma$ is the output map (returns the output $Z(s)$ on state s). For example, in the case of your washing machine, the inputs are the buttons that you press and also the tics of the clock. The outputs are what you can observe in its display plus the commands it is able to issue to the other components of the washing machine (water valves, pumps, heaters, etc).

These days, the memory is implemented using a finite number of (classical) bits. A bit is a (classical) system that can be only in two states: false or true. Let us denote these two states of a bit by $|0\rangle$ and $|1\rangle$, respectively.

It is only natural to introduce the notion of quantum automaton by adding to the classical concept a quantum memory. A quantum memory is to be implemented by a finite number of quantum bits known as qubits. A qubit is a quantum system that can be in any superposition of the states of a (classical) bit. That is, a possible state of a qubit is a vector $\alpha|0\rangle + \beta|1\rangle$ where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. Thus, in general, the state of a qubit is *not* one of the two possible truth values. The state of a qubit is, in general, a "combination" of those two truth values (remember Schrödinger's cat!).

A classical bit is usually implemented with some electronic system: for instance, its state is true if the voltage is greater than +5 Volts, and its state is false if the voltage is less than -5 Volts (any other voltage is considered faulty).

A qubit can be implemented, for example, using the spin of an electron: its state is true if the spin is +1/2, and its state is false if the spin is -1/2. Furthermore, as a quantum system, the spin of the electron can be in any superposition of +1/2 and -1/2.

The postulates of quantum mechanics also prescribe how we can observe the state of a qubit. Given a qubit in the state $\alpha|0\rangle + \beta|1\rangle$, if you measure it with an appropriate apparatus (mathematically described as a Hermitian operator acting on its state space[6]) then the possible outcomes of the measurement are the eigenvalues of that operator. By choosing an operator with eigenvectors $|0\rangle$ and $|1\rangle$ corresponding to distinct eigenvalues, we can decide after the measurement if the result is false or true. This result is random: false will come out with probability $|\alpha|^2$ and true will come out with probability $|\beta|^2$. Thus, quantum systems when observed are random systems.

Quantum systems evolve by the application of unitary operators. For instance, a qubit in state $\alpha|0\rangle + \beta|1\rangle$ will evolve to the state $\beta|0\rangle + \alpha|1\rangle$ if subjected to the Pauli X transformation. The Hadamard transformation when applied to $\alpha|0\rangle + \beta|1\rangle$ results in $\frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$.

Returning to automata, we are now ready to motivate a simple but nevertheless quite useful notion of quantum automaton. Figure 4 depicts the overall structure of such an automaton. The inputs and δ are as in the classical case. But now we also have a quantum component of the memory. At each classical component of the state s, upon input σ the quantum component of the memory is subjected to the unitary transformation $U_{s\sigma}$. Starting at some initial state $(s_0, |\psi_0\rangle)$, after a sequence of inputs w, the automaton reaches the final state $(s_w, |\psi_w\rangle)$. The random output is obtained by applying a suitable Hermitian operator A_{s_w} to $|\psi_w\rangle$.

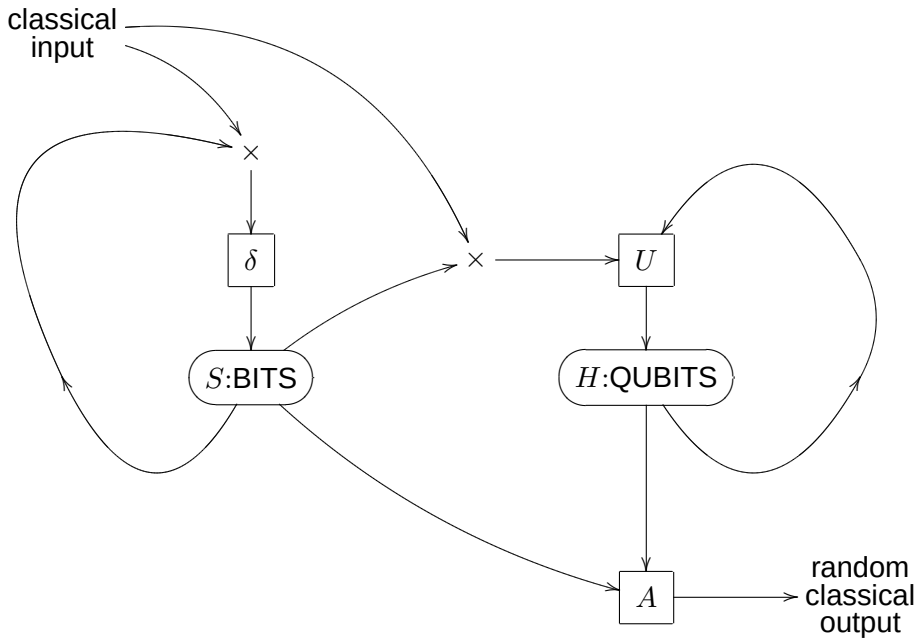

Figure 4. Basic quantum automaton

In short, a quantum automaton is a tuple

$$M = (\Sigma, \Gamma, S, H, s_0, |\psi_0\rangle, \delta, U, A)$$

where: Σ is the input alphabet; $\Gamma \subseteq \mathbb{R}$ is the output alphabet[7]; S is the classical state space; H is the Hilbert space of the quantum states; $s_0 \in S$ is the initial

classical state; $|\psi_0\rangle \in H$ is the initial quantum state; $\delta : S \times \Sigma \to S$ is the classical state transition map; $U = \{U_{s\sigma}\}_{s\in S,\sigma\in\Sigma}$ where each $U_{s\sigma}$ is the quantum state transition operator at s for input σ; and $A = \{A_s\}_{s\in S}$ where each A_s is the measurement operator at s such that $\mathsf{spec}A_s \subseteq \Gamma$. This rather simple notion of quantum automaton subsumes the concepts previously proposed in the literature [**57**].

The behavior of such a quantum automaton M is the map B_M that returns for each sequence w of inputs the probability distribution over Γ of the outputs obtained by measuring $|\psi_w\rangle$ using the Hermitian operator A_{s_w}. Two quantum automata M and M' should be considered equivalent if $B_M = B_{M'}$.

At this stage several interesting problems arise. Given M, can we find an equivalent $M^\bullet$ with minimal dimension of the underlying Hilbert space $H^\bullet$, that is, with minimal number of qubits? The answer is yes. We can even get rid of all qubits! But the price is high: in that case $M^\bullet$ will have a very large classical state space $S^\bullet$. That is, we can replace all qubits with an exponential increase in the number of the (classical) bits. This is yet another instance of a well know effect: we can always simulate quantum machinery with classical machinery but paying a high price.

Thus, we are led to the following reformulation of the qubit minimization problem. Given M, can we find an equivalent $M^\bullet$ with minimal dimension of the underlying Hilbert space $H^\bullet$, that is, with minimal number of qubits, but allowing only a polynomial increase on the number of (classical) bits?

These problems for this kind of quantum automata (and also for more powerful kinds of quantum automata allowing quantum outputs) are the current focus of task T2 of the Quantlog project described in Section 3.

5. OUTLOOK

Notwithstanding the significant steps mentioned in Section 2, some key open issues remain in the field of quantum computation and information before it revolutionizes the way we compute and communicate, namely:

- Usable hardware for quantum computation?
- Long range cable and open air quantum communication and networks?
- Which quantum systems can be efficiently simulated in a classical computer?
- Where is **BQP** in the family of computational complexity classes? Is SAT in **BQP**?
- Further examples (besides Child's graph search) of exponential gains by using quantum computation?

- Can quantum communication achieve exponential gain in communication complexity?
- Besides Shor's quantum Fourier transform and Grover's amplitude amplification, other approaches to the design of quantum algorithms?
- Can quantum resources help in producing tamper-proof devices?
- Which classical cryptosystems will still be secure against quantum attacks?

At IST-UTL, within the context of the QuantLog project described in Section 3, some aspects of the non experimental issues above are being addressed, namely: properties of entanglement in solid state systems [**31**]; particle statistics in quantum information [**61, 60**]; quantum walks and their comparison with random walks [**62**]; quantum algorithms for searching [**49**] and in logic; quantum automata and their minimization and interconnection; quantum transition systems for model checking of quantum systems [**7**]; quantum logic [**51, 52, 54, 53, 55, 26, 19, 25**] for model checking of quantum systems; formal methods in security [**21, 23, 20, 22, 4, 3, 2, 5**]; quantum security [**6**]; and quantum attacks to classical cryptosystems.

ACKNOWLEDGMENTS

The authors wish to express their gratitude to all members of the team of the QuantLog project for helping in this survey of their activities. This work was partially supported by FCT and EU FEDER through POCTI and POCI, namely via POCI/MAT/55796/2004 project.

NOTES

1. Throughout this text, the word *classical* will be used in the sense of *non-quantum*.
2. See also the site http://qwiki.caltech.edu/wiki/Complexity_Zoo by Scott Aaronson.
3. http://www.qubit.org/school2002/
4. http://sem.math.ist.utl.pt/qci/
5. http://clc.math.ist.utl.pt/quantlog.html
6. Hilbert space of dimension 2.
7. Recall that the eigenvalues of a Hermitian operator are real numbers.

REFERENCES

[1] Abadi M, Gordon AD. "A calculus for cryptographic protocols: The Spi Calculus", *Information and Computation*, **vol**. 148 **no**. 1, pp. 1-70, 1999. Full version available as SRC Research Report 149, January 1998.

[2] Adão P, Bana G, Herzog J, Scedrov A. "Soundness and completeness of formal encryption: The cases of key-cycles and partial information leakage", Preprint, CLC, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2005. Submitted for publication.

[3] Adão P, Bana G, Herzog J, Scedrov A. "Soundness of formal encryption in the presence of key-cycles", S. D. C. di Vimercati, P. Syverson, and D. Gollmann (eds.), *Proceedings of the 10th European Symposium on Research in Computer Security (ESORICS)*, **vol**. 3679 of *Lecture Notes in Computer Science*, Springer-Verlag, 2005, pp. 374-396.

[4] Adão P, Bana G, Scedrov A. "Computational and information-theoretic soundness and completeness of formal encryption", *Proceedings of the 18th IEEE Computer Security Foundations Workshop (CSFW)*, IEEE Computer Society Press, 2005, pp. 170-184.

[5] Adão P, Fournet C. "Cryptographically sound implementations for communicating processes", Preprint, CLC, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2006. Submitted for publication.

[6] Adão P, Mateus P. "A process algebra for reasoning about quantum security", *Electronic Notes in Theoretical Computer Science*, to appear. Preliminary version presented at 3rd International Workshop on Quantum Programming Languages, June 30 - July 1, 2005, Chicago, Affiliated Workshop of LICS 2005.

[7] Adão P, Mateus P, Reis T, Viganò L. "Towards a quantitave analysis of security protocols", Preprint, CLC, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2006. Submitted for publication.

[8] Agrawal M, Kayal N, Saxena N. "PRIMES is in P", *Annals of Mathematics*, **vol**. 160 **no**. 2, pp. 781-793, 2004.

[9] Aharonov D, van Dam W, Kempe J, Landau Z, Lloyd S, Regev O. "Adiabatic quantum computation is equivalent to standard quantum computation", *FOCS '04: Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS'04)*, IEEE Computer Society, 2004, pp. 42-51.

[10] Aspect A, Grangier P, Roger G. "Experimental tests of realistic local theories via Bell's theorem", *Physical Review Letters*, **vol**. 47, pp. 460, 1981.

[11] Bell JS. "On the Einstein-Podolsky-Rosen paradox", *Physics*, **vol**. 1, pp. 195, 1964.

[12] Benioff P. "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines", *Journal of Statistical Physics*, **vol**. 22, pp. 563-591, 1980.

[13] Benioff P. "Quantum mechanical models of Turing machines that dissipate no energy", *Physical Review Letters*, **vol**. 48, pp. 1581-1585, 1982.

[14] Bennett CH, Brassard G. "Quantum cryptography: Public key distribution and coin tossing", *Proceedings of IEEE international Conference on Computers, Systems and Signal Processing*, IEEE Press, 1984, pp. 175-179.

[15] Bennett CH, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters W. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", *Physical Review Letters*, **vol**. 70 **no**. 13, pp. 1895-1899, 1993.

[16] Bennett CH, Wiesner SJ. "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states", *Physical Review Letters*, **vol**. 69 **no**. 20, pp. 2881-2884, 1992.

[17] Birkhoff G, von Neumann J. "The logic of quantum mechanics", *Annals of Mathematics*, **vol**. 37 **no**. 4, pp. 823-843, 1936.

[18] Boyer M, Brassard G, Høyer P, Tapp A. "Tight bounds on quantum searching", *Fortschritte der Physik*, **vol**. 46 **no**. 1-5, pp. 493-505, 1998.

[19] Caleiro C, Mateus P, Sernadas A, Sernadas C. "Quantum institutions", Preprint, CLC, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2005. Submitted for publication.

[20] Caleiro C, Viganò L, Basin D. "Deconstructing Alice and Bob", *Electronic Notes in Theoretical Computer Science*, **vol**. 135 **no**. 1, pp. 3-22, 2005. Preliminary version presented at ICALP'05 ARSPA Workshop.

[21] Caleiro C, Viganò L, Basin D. "Metareasoning about security protocols using distributed temporal logic", *Electronic Notes in Theoretical Computer Science*, **vol**. 125 **no**. 1, pp. 67-89, 2005. Preliminary version presented at IJCAR'04 ARSPA Workshop.

[22] Caleiro C, Viganò L, Basin D. "On the expresiveness of a message sequence formalism for security protocols", Preprint, CLC, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2005. Submitted for publication.

[23] Caleiro C, Viganò L, Basin D. "Relating strand spaces and distributed temporal logic for security protocol analysis", *Logic Journal of the IGPL*, **vol**. 13 **no**. 6, pp. 637-664, 2005.

[24] Canetti R. "Universally composable security: A new paradigm for cryptographic protocols", *42nd IEEE Symposium on Foundations of Computer Science (FOCS)*, IEEE Computer Society Press, 2001, pp. 136-145. Full version available at IACR ePrint Archive, Report 2000/067.

[25] Chadha R, Mateus P, Sernadas A. "Reasoning about states of probabilistic sequential programs", Preprint, CLC, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2006. Submitted for publication.

[26] Chadha R, Mateus P, Sernadas A, Sernadas C. "Extending classical logic for reasoning about quantum systems", Preprint, CLC, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2005. Submitted for publication.

[27] Chiara MLD, Giuntini R, Greechie R. *Reasoning in Quantum Theory*, Dordrecht, The Netherlands, Kluwer Academic Publishers, 2004.

[28] Childs AM, Cleve R, Deotto E, Farhi E, Gutmann S, Spielman DA. "Exponential algorithmic speedup by a quantum walk", *STOC'03: Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, ACM Press, 2003, pp. 59-68.

[29] Cook SA. "The complexity of theorem-proving procedures", *STOC'71: Proceedings of the 3rd Annual ACM Symposium on Theory of Computing*, ACM Press, 1971, pp. 151-158.

[30] Cook SA, Reckhow RA. "Time bounded random access machines", *Journal of Computer and System Sciences*, **vol**. 7 **no**. 4, pp. 354-375, 1973.

[31] Costa Jr AT, Bose S, Omar Y. "Entanglement of two impurities through electron scattering", Preprint, CFP, Department of Physics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2005. Submitted for publication.

[32] Deutsch D. "Quantum theory, the Church-Turing principle and the universal quantum computer", *Proceedings of the Royal Society of London A*, **vol**. 400, pp. 97-117, 1985.

[33] Devetak I. "The private classical capacity and quantum capacity of a quantum channel", *IEEE Transactions on Information Theory*, **vol**. 51, pp. 44-55, 2005.

[34] DiVincenzo DP. "Two-bit gates are universal for quantum computation", *Physical Review A*, **vol**. 51, pp. 1015-1022, 1995.

[35] Ekert AK. "Quantum cryptography based on Bell's theorem", *Physical Review Letters*, **vol**. 67 **no**. 6, pp. 661-663, 1991.

[36] Farhi E, Goldstone J, Gutmann S, Sipser M. "Quantum computation by adiabatic evolution", Technical Report quant-ph/0001106, ArXiv, USA, 2000.

[37] Feynman RP. "Simulating Physics with computers", *International Journal of Theoretical Physics*, **vol**. 21, pp. 467, 1982.

[38] Foulis DJ. "A half-century of quantum logic. What have we learned?", *Quantum Structures and the Nature of Reality*, **vol**. 7 of *Einstein Meets Magritte*, Kluwer Acad. Publ., 1999, pp. 1-36.

[39] Gobby C, Yuan ZL, Shields AJ. "Quantum key distribution over 122 km of standard telecom fiber", *Applied Physics Letters*, **vol**. 84 **no**. 19, pp. 3762-3764, 2004.

[40] Grover LK. "A fast quantum mechanical algorithm for database search", *STOC'96: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, ACM Press, 1996, pp. 212-219.

[41] Grover LK. "Quantum mechanics helps in searching for a needle in a haystack", *Physical Review Letters*, **vol**. 79 **no**. 2, pp. 325-328, 1997.

[42] Häffner H, Hänsel W, Roos CF, Benhelm J, al kar D Chek, Chwalla M, Körber T, Rapol UD, Riebe M, Schmidt PO, Becher C, Gühne O, Dür W, Blatt R. "Scalable multiparticle entanglement of trapped ions", *Nature*, **vol**. 438, pp. 643-646, 2005.

[43] Hallgren S. "Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem", *STOC'02: Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, ACM Press, 2002, pp. 653-658.

[44] Halpern JY. "An analysis of first-order logics of probability", *Artificial Intelligence*, **vol**. 46, pp. 311-350, 1990.

[45] Hansson H, Jonsson B. "A logic for reasoning about time and reliability", *Formal Aspects of Computing*, **vol**. 6, pp. 512-535, 1995.

[46] Holevo AS. "The capacity of quantum channel with general signal states", *IEEE Transactions on Information Theory*, **vol**. 44, pp. 269, 1998.

[47] Knill E. "Conventions for quantum pseudocode", Technical Report LAUR-96-2724, Los Alamos National Laboratory, Los Alamos, USA, 1996.

[48] Mateus P, Mitchell J, Scedrov A. "Composition of cryptographic protocols in a probabilistic polynomial-time process calculus", R. Amadio and D. Lugiez (eds.), *CONCUR 2003 - Concurrency Theory*, **vol**. 2761 of *Lecture Notes in Computer Science*, Springer, 2003, pp. 327-349.

[49] Mateus P, Omar Y. "Quantum pattern matching", Preprint, CLC, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2005. ArXiv quant-ph/0508237. Full version of [**50**].

[50] Mateus P, Omar Y. "A quantum algorithm for closest pattern matching", D. Angelakis and M. Christandl (eds.), *Proceedings of NATO ASI Quantum Computation and Information*, IOS Press, in print. Short version of [**49**].

[51] Mateus P, Sernadas A. "Exogenous quantum logic", W. A. Carnielli, F. M. Dionísio, and P. Mateus (eds.), *Proceedings of CombLog'04, Workshop on Combination of Logics: Theory and Applications*, Departamento de Matemática, Instituto Superior Técnico, Lisboa, 2004, pp. 141-149. Extended abstract.

[52] Mateus P, Sernadas A. "Reasoning about quantum systems", J. Alferes and J. Leite (eds.), *Logics in Artificial Intelligence, Ninth European Conference, JELIA'04*, **vol**. 3229 of *Lecture Notes in Artificial Intelligence*, Springer-Verlag, 2004, pp. 239-251.

[53] Mateus P, Sernadas A. "Complete exogenous quantum propositional logic", Technical report, CLC, Department of Mathematics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2005. Extended abstract. Short presentation at LICS 2005, Chicago, USA, June 26-29.

[54] Mateus P, Sernadas A. "Weakly complete axiomatization of exogenous quantum propositional logic", *Information and Computation*, in print. ArXiv math.LO/0503453.

[55] Mateus P, Sernadas A, Sernadas C. "Exogenous semantics approach to enriching logics", G. Sica (ed.), *Essays on the Foundations of Mathematics and Logic*, **vol**. 1 of *Advanced Studies in Mathematics and Logic*, Polimetrica, 2005, pp. 165-194.

[56] Mitchell J, Ramanathan A, Scedrov A, Teague V. "A probabilistic polynomial-time calculus for analysis of cryptographic protocols (Preliminary Report)", *Electronic Notes in Theoretical Computer Science*, **vol**. 45, pp. 1-31, 2001.

[57] Moore C, Crutchfield JP. "Quantum automata and quantum grammars", *Theoretical Computer Science*, **vol**. 237 **no**. 1-2, pp. 275-306, 2000.

[58] Navarro G. "A guided tour to approximate string matching", *ACM Computing Surveys*, **vol**. 33 **no**. 1, pp. 31-88, 2001.

[59] Nielsen MA, Chuang IL. *Quantum Computation and Quantum Information*, Cambridge, UK, Cambridge University Press, 2000.

[60] Omar Y. "Indistinguishable particles in quantum mechanics: An introduction", *Contemporary Physics*, **vol**. 46, pp. 437-448, 2005.

[61] Omar Y. "Particle statistics in quantum information processing", *International Journal of Quantum Information*, **vol**. 3 **no**. 1, pp. 201-205, 2005.

[62] Omar Y, Paunkovic N, Sheridan L, Bose S. "Quantum walk on a line with two entangled particles", Preprint, CFP, Department of Physics, Instituto Superior Técnico, 1049-001 Lisboa, Portugal, 2004. Submitted for publication.

[63] Raussendorf R, Briegel HJ. "A one-way quantum computer", *Physical Review Letters*, **vol**. 86 **no**. 22, pp. 5188-5191, 2001.

[64] Schrödinger E. "Die gegenwartige Situation in der Quantenmechanik", *Naturwissenschaften*, **vol**. 23, pp. 807-812, 823-823, 844-849, 1935. English translation: John D Trimmer, Proceedings of the American Philosophical Society, 124, 323-38 (1980), Reprinted in Quantum Theory and Measurement, p. 152 (1983).

[65] Schumacher B. "Quantum coding", *Physical Review A*, **vol**. 51, pp. 2738-2747, 1995.

[66] Schumacher B, Westmoreland M. "Sending classical information via noisy quantum channels", *Physical Review A*, **vol**. 56, pp. 131138, 1997.

[67] Schwartz JT. "Fast probabilistic algorithms for verification of polynomial identities", *Journal of the ACM*, **vol**. 27 **no**. 4, pp. 701-717, 1980.

[68] Shannon CE. "A mathematical theory of communication", *Bell System Technical Journal*, **vol**. 27, pp. 379, 623, 1948.

[69] Shor PW. "Algorithms for quantum computation: Discrete logarithms and factoring", S. Goldwasser (ed.), *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, IEEE Computer Society, 1994, pp. 124-134.

[70] Shor PW. "Scheme for reducing decoherence in quantum computer memory", *Physical Review A*, **vol**. 52, pp. R2493, 1995.

[71] Shor PW. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM Journal on Computing*, **vol**. 26 **no**. 5, pp. 1484-1509, 1997. Presented at FOCS'94.

[72] Steane AM. "Error correcting codes in quantum theory", *Physical Review Letters*, **vol**. 77 **no**. 5, pp. 793-797, 1996.

[73] Vandersypen LMK, Steffen M, Breyta G, Yannoni CS, Sherwood MH, Chuang IL. "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance", *Nature*, **vol**. 414, pp. 883-887, 2001.

[74] Wiesner S. "Conjugate coding", *SIGACT News*, **vol**. 15 **no**. 1, pp. 78-88, 1983. Original manuscript written circa 1970.

[75] Yao AC. "Theory and applications of trapdoor functions", *23rd IEEE Symposium on Foundations of Computer Science (FOCS)*, IEEE Computer Society, 1982, pp. 80-91.

[76] Zippel R. "Probabilistic algorithms for sparse polynomials", *EUROSAM '79: Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*, Springer-Verlag, 1979, pp. 216-226.