A new model of a Quantum Automaton (QA), working with qubits is proposed. The quantum states of the automaton can be pure or mixed and are represented by density operators. This is the appropriated approach to deal with measurements and dechorence.

The linearity of a QA and of the partial trace super-operator, combined with the properties of invariant subspaces under unitary transformations, are used to minimize the dimension of the automaton and, consequently, the number of its working qubits.

The results here developed are valid whether the state set of the QA is finite or not.

There are two main results in this paper: 1) We show that the dimension reduction is possible whenever the unitary transformations, associated to each letter of the input alphabet, obey a set of conditions. 2) We develop an algorithm to find out the equivalent minimal QA and prove that its complexity is polynomial in its dimension and in the size of the input alphabet.
1 Introduction

In order to understand computation in a quantum context, it might be useful to introduce as many concepts as possible from the classical computation theory to the quantum case.

One of these basic concepts concerns the functioning of finite automata in classical systems. To extend these concepts from classical to quantum systems, several models have been proposed [1, 2, 4, 5], most of them dealing with language recognition. This kind of automata is usually referred to as acceptors, in the sense that they are designed to indicate, by giving a yes or no output, whether a given input sequence does or does not possess the proper characteristics.

In this article we propose a new model for a quantum automaton which acts as a transducer [6]. This QA is prepared in a given initial quantum state, then a classical device reads an input string of letters and apply the corresponding transformations to the quantum part. After all the letters in the string are read, the QA is observed (measured). Finally, the output of the quantum measurement is written in an exterior classical "tape". In this sense, our QA is similar to the measured-once Quantum Finite Automata (QFA) model introduced by [1], where the measurements are made only after a sequence of letters is read, and it differs from the measured-many QFA model introduced by [2, 7] that is observed after reading each letter. Since the outputs of this QA are probabilities, it can be seen as some kind of extension of the probabilistic transducers [8, 9]. Let us stress that, our QA does not have necessarily a finite state set and it is not used for purposes of language recognition. One important application of transducers is in the measurement, control and identification of systems.

The study of such problems starts with the minimal-state equivalent automaton which suggests us that an important issue to take into account, when a given QA is defined, is how to minimize it. As far as we know such a question was never addressed in the context of QA.

The main purpose of this article is to study the minimization procedure of a QA which differs from the procedure used with classical automata.
The physical support of the QA that we are proposing in this paper is a system of \( n \) two-state quantum particles which encode information in the form of quantum bits, *qubits*. Each qubit is a unit vector of a 2-dimensional Hilbert space. Beside the formal reasons mentioned above, the minimization of a QA is an important question to be addressed because qubits are a very expensive resource.

The minimization problem can be studied in two complementary ways. The first one, concerns the minimization of the dimension of the underlying Hilbert space, which consists in looking for an equivalent automaton working with the smallest number of qubits. Once the dimension minimization is achieved, another question can be asked, namely the possibility of minimizing the cardinality of the QA state set.

Most authors represent the states of a quantum automaton by *pure states*. In general, a quantum system is not in a pure state. This may be due to the fact that we have only partial information about the system, or that the system is not isolated from the rest of the Universe, so it is not in a well defined pure state. In such cases we say that the system is in a *mixed state* which is represented by a *density operator*. The density operator is the most general and powerful way of expressing the state of a quantum system, namely when quantum measurements are performed [10, 11, 12], therefore we adopt this formalism to describe the states of a quantum automata.

Another advantage of describing the states of a QA by density operators, is to deal with quantum measurements performed in subsystems of a larger quantum system. The approach developed in this paper to minimize the dimension of the QA uses the operation of *tracing out* that transforms density operators of a Hilbert space in density operators of another Hilbert space of smaller dimension. The transformed density operators are named *reduced density operators*.

A QA is a special case of automata, this is, a QA is a linear automaton since its quantum states are vectors of a Hilbert space and the transition and output maps are linear transformations. Based on this linearity, we apply some known results of the theory of invariant subspaces to derive the necessary and sufficient conditions that the unitary evolution operators must obey, in order to minimize its dimension.
This article is organized as follows: in section 2, the physics background is presented and the physical notation, used in quantum systems, is introduced. In section 3, the definition of our quantum automaton is presented and its functioning is explained. The conditions for reduction of its dimension are derived in section 4. The minimization algorithm is developed and its complexity is computed in section 5. Finally, the conclusions are presented in section 6.

2 Physics background

A quantum physical system in a pure state is described by a unit vector in a Hilbert space, i.e., a vector space with an inner product. In the Dirac notation, the pure state is denoted by $|\psi\rangle$. The quantum automaton, that we are considering, works with n-qubits which can be physically realized by $n$ two-state particles. The Hilbert space of such a system is $\mathcal{H}_2^n = \mathbb{C}^{(0,1)^n}$, this is a $2^n$ dimensional complex vector space. $\mathcal{H}_2^n$ is a tensor product of $n$ Hilbert spaces, each one associated to a qubit: $\mathcal{H}_2^n = \bigotimes_{j=1}^n \mathcal{H}_2(j)$ where $\mathcal{H}_2(j)$ is the 2-dimensional Hilbert space of qubit $j$. For each $\mathcal{H}_2(j)$ we choose a special basis set, called computational basis, consisting of two orthonormal states $|i_j\rangle, (i_j = 0, 1)$. A basis set for $\mathcal{H}_2^n$ is $\{\bigotimes_{j=1}^n |i_j\rangle, i_j = 0, 1\}$. A general pure state of n-qubits is a vector superposition of the type: $|\Psi\rangle = \sum_{i_1,...,i_n=0}^1 \psi_{i_1,...,i_n} \bigotimes_{j=1}^n |i_j\rangle$, where $\sum_{i_1,...,i_n=0}^1 |\psi_{i_1,...,i_n}|^2 = 1$. The transposed-complex conjugate of $|\Psi\rangle$ is denoted by $\langle \Psi |$. The inner product between $|\Psi\rangle$ and $|\Phi\rangle$ is denoted by $\langle \Phi | |\Psi\rangle = \sum_{i_1,...,i_n=0}^1 \psi_{i_1,...,i_n} \phi^*_{i_1,...,i_n}$. We define $|\Psi\rangle \langle \Phi |$ to be the linear operator from $\mathcal{H}_2^n \rightarrow \mathcal{H}_2^n$, known as the outer product of two vectors of $\mathcal{H}_2^n$, whose matricial representation, in the above mentioned computational basis, is $\bigotimes_{j=1}^n \bigotimes_{k=1}^n \langle i_j | |\Psi\rangle \langle \Phi | i_k\rangle$.

According to the postulates of quantum mechanics, the operations that we can perform in a quantum system are represented by completely positive maps [10, 14, 15]. To our QA we are going to apply: a) unitary transformations, represented by unitary operators $U$ acting in $\mathcal{H}_2^n$: $U : |\Psi\rangle \rightarrow |\Psi\rangle' = U |\Psi\rangle$. The unitary transformations preserve the norm of the vectors in $\mathcal{H}_2^n$. b) measurements of a given physical quan-
tity $A$ [13]. Such a quantity is represented by an hermitian operator $A$ in $\mathcal{H}_2^n$, named observable quantity. The measurements can be performed in one or more qubits. The possible outcomes of these measurements are given by the eigenvalues $a_k$ (always real) of the operator $A$. The measurements can be performed in one or more qubits. The possible outcomes of these measurements are given by the eigenvalues $a_k$ (always real) of the operator $A$. The set of vectors, $\{ | a_k^i \rangle \}$, constitute an orthonormal basis set in $\mathcal{H}_2^n$, obeying the eigenvalue equation: $A | a_k^i \rangle = a_k | a_k^i \rangle$; $0 < k < n$; $0 < i < g_k$, and $Tr$ stands for the trace of an operator. After a measurement, the quantum state of the system changes according to the outcome $a_k$ becoming, $| \Psi' \rangle = P_k | \Psi \rangle / \sqrt{\langle \Psi | P_k | \Psi \rangle}$.

We have already mentioned that the most general state of a quantum system is not a pure state but rather a mixed state. We say that the system is in a mixed state, and assign with the system a probability distribution $\{ p_r, | \psi_r \rangle \}$, meaning that the system is in the pure state $| \psi_r \rangle$, with the probability $p_r$. A straightforward way of describing such a state is by using density operators $\rho$ defined by $\rho = \sum_r p_r | \psi_r \rangle \langle \psi_r |$. The density operators are:

- **a.** Linear operators of $\mathcal{H}_2^n \to \mathcal{H}_2^n$;
- **b.** Hermitian, $\rho = \rho^*$;
- **c.** Semi definite positive, i.e., for any vector $| \Psi \rangle \in \mathcal{H}_2^n$, $\langle \Psi | \rho | \Psi \rangle \geq 0$;
- **d.** The trace, $Tr\{ \rho \}$ = $\sum_k \sum_i \langle a_k^i | \rho | a_k^i \rangle = 1$.

The set $\mathcal{L}_{\mathcal{H}_2^n}$, of all linear operators of $\mathcal{H}_2^n \to \mathcal{H}_2^n$ is a vector space. Given any two vectors $A$ and $B$ of $\mathcal{L}_{\mathcal{H}_2^n}$ we can define a inner product function by $\langle A, B \rangle = Tr\{ A^\dagger B \}$, called the Hilbert-Schmidt inner product. With this inner product function, the vector space $\mathcal{L}_{\mathcal{H}_2^n}$, becomes a Hilbert space. To any unitary operator, $U : | \Psi \rangle \to | \Psi' \rangle = U | \Psi \rangle$ on $\mathcal{H}_2^n$, we can assign another unitary operator, $\tilde{U} : A \to \tilde{A} = \tilde{U}(A) = UAU^\dagger$ on $\mathcal{L}_{\mathcal{H}_2^n}$. Operators like $\tilde{U}$, that transform operators into other operators are called super-operators.

An important application of the density operators formalism is as a descriptive tool for subsystems of a composite quantum system. In fact, most physical systems are constituted by two or more parts (subsystems). Let us assume that the observable quantity $A(1)$ measures only part (1), of a system, for instance the part composed by the $n_1$ first qubits and call part (2) to the remaining $n_2$ qubits, this is $\mathcal{H}_2^n = \mathcal{H}_2^{n_1} \otimes \mathcal{H}_2^{n_2}$.

The observable quantities $A(1)$ on a subsystem (1) can be extended to a composite
system (1) + (2) as follows [13]: \( \tilde{A}(1) = A(1) \otimes 1(2) \), where \( \tilde{A}(1) \) denotes the corresponding observable for the same physical measurement, performed on the composite system and \( 1(2) \) is the identity operator in \( \mathcal{H}_2^{n_2} \). The action of this operator on the vector, \( |\Psi(1)\rangle \otimes |\Psi(2)\rangle \) is defined by,

\[
\tilde{A}(1)[|\Psi(1)\rangle \otimes |\Psi(2)\rangle] = [A(1)|\Psi(1)\rangle] \otimes [1(2)|\Psi(2)\rangle]
\]

The spectrum of \( \tilde{A}(1) \) in \( \mathcal{H}_2^n \) is the same as the spectrum of \( A(1) \) in \( \mathcal{H}_2^{n_1} \), but with all the eigenvalues degenerated in \( \mathcal{H}_2^n \), even if none of them is degenerated in \( \mathcal{H}_2^{n_1} \). The probability \( P_k \) of obtaining the outcome \( a_k \), when the observable \( \tilde{A}(1) \) is measured over part (1) of the system is given by

\[
P_k = \text{Tr}\{\tilde{P}_k(1)\rho\}
\]

where \( \tilde{P}_k(1) = P_k(1) \otimes 1(2) \) and \( P_k(1) \) is the projector operator on the eigenspace \( E_k \).

A natural question we can ask is, would it be possible to define a density operator for subsystem (1), that gives the correct probabilities \( P_k \) for the outcomes of the observable \( A(1) \)?

It can be shown [14, 15] that there is a unique transformation of \( \mathcal{L}_{\mathcal{H}_2^n} \) into \( \mathcal{L}_{\mathcal{H}_2^{n_1}} \) which gives rise to the correct description of observable quantities for subsystem (1). This transformation, called trace out or partial trace and denoted \( \text{Tr}_{\mathcal{B}}\{\cdot\} \), is a completely positive map of \( \mathcal{L}_{\mathcal{H}_2^n,\mathcal{H}_2^{n_1}} \) which is the space of all linear operators: \( \mathcal{L}_{\mathcal{H}_2^n} \rightarrow \mathcal{L}_{\mathcal{H}_2^{n_1}} \). It is defined for any pair of finite dimensional Hilbert spaces \( \mathcal{L}_{\mathcal{H}_2^n} \) and \( \mathcal{L}_{\mathcal{H}_2^{n_1}} \), with \( n_1 < n \).

The image of the partial trace of a density operator \( \rho \in \mathcal{L}_{\mathcal{H}_2^n} \) is denoted by \( \rho^1 = \text{Tr}_{\mathcal{B}}\{\rho\} \) and is named reduced density operator for subsystem (1), whose matrix elements are

\[
\rho^1(i,j) = \sum_{k=n_1+1}^n \langle k|\rho|k \rangle = \sum_{k=n_1+1}^n \rho(ik,jk).
\]

It means that we are averaging over \( \mathcal{H}_2^{n_2} \). Any quantum operator that does not operate on \( \mathcal{H}_2^{n_2} \) commutes with the partial trace. The reduced density operators have the same properties as the density operators. Let (A) to be a subsystem of \( n_A \) qubits, containing the first \( n_1 \) qubits and let (B) to be the remaining \( n_B \) qubits, then \( n_A = n - n_B \). The partial trace has the following property:

\[
P_k = \text{Tr}\{\tilde{P}_k(1)\rho\} = \text{Tr}_A\{\tilde{P}_k(1)\rho^A\} = \text{Tr}_1\{P_k(1)\rho^1\}.
\] (2)

Where \( \rho^A = \text{Tr}_B\{\rho\} \) is the reduced density operator of subsystem (A) and \( \text{Tr}_B\{\cdot\} \) is the partial trace over subsystem (B). This equality shows that it is enough to know the reduced
density operator $\rho^1$ (or $\rho^A$) in order to compute the probabilities of all the outcomes of a measurement over subsystem (1).

3 A quantum automaton

We say that a quantum system of $n$ qubits works as a quantum automaton $\mathcal{M} = \langle \mathcal{H}_2^n, \rho_0, \Sigma, \mathcal{U}, Q, \tilde{A}(1), \Omega \rangle$ when the following conditions are fulfilled:

1. $\mathcal{H}_2^n$ is the underlying Hilbert space of dimension $2^n$.
2. $\rho_0 \in \mathcal{L}_{\mathcal{H}_2^n}$ is the density operator of the initial quantum state of the $n$ qubits.
3. $\Sigma = \{\sigma\}$ is a finite set of input symbols (the input alphabet).
4. $Q$ is the set of reachable states given by: $Q = \{\rho_w : w \in \Sigma^*\}$, with $\rho_w = \tilde{U}_w(\rho_0) = \mathcal{U}_w \rho_0 \mathcal{U}_w^\dagger$ and where the family $\{\mathcal{U}_w\}_{w \in \Sigma^*}$ of unitary operators of $\mathcal{H}_2^n$ is built as follows: i) $\mathcal{U} = \{\mathcal{U}_\sigma\}_{\sigma \in \Sigma}$, is a finite set of unitary operators indexed upon $\sigma \in \Sigma$; ii) $\mathcal{U}_e = \mathbf{1}(n)$; and iii) $\mathcal{U}_w \sigma = \mathcal{U}_\sigma \mathcal{U}_w$.
5. $\delta : \Sigma \times Q \rightarrow Q$ is the transition map defined by

$$\delta(\sigma, \rho_w) = \rho_{w \sigma} = \tilde{U}_\sigma(\rho_w) \tag{3}$$

6. $\tilde{A}(1)$ is the observable quantity to be measured. The possible outcomes of a measurement of $\tilde{A}(1)$ are its eigenvalues $a_k$: $\text{Spec}\tilde{A}(1) = \{a_k : \tilde{A}(1)(|a_k^i\rangle \otimes \mathbf{1}(2)) = a_k(|a_k^i\rangle \otimes \mathbf{1}(2))\}$. The diagonal representation of the observable is $\tilde{A}(1) = \sum_k a_k \tilde{P}_k(1)$, where $\tilde{P}_k(1) = \sum_{i_k=1}^{g_k} |a_k^i\rangle \langle a_k^i| \otimes \mathbf{1}(2)$ is the projector into the eigenspace $\mathcal{E}_k$ of $\tilde{A}(1)$.
7. $\Omega$ is a set of output symbols (the output alphabet) whose elements are defined by the following output map:
8. $\omega : Q \rightarrow \Omega$

$$\omega(w, a_k) = \text{Tr}\{\tilde{P}_k(1) \rho_w\} \tag{4}$$

For each $w \in \Sigma^*$, the set $\Omega_w = \{\omega(w, a_k) : a_k \in \text{Spec}\tilde{A}(1)\}$ is the unique probability measure for the state $\rho_w$ and the output alphabet, $\Omega = \{\Omega_w, w \in \Sigma^*; \sum_k \omega(w, a_k) = 1\}$, is a set of probability measures.
The physical performance of this QA is as follows: a classical exterior device can read the symbols $\sigma \in \Sigma$ stored in an external classical "tape". Then it applies the corresponding gate, represented by the unitary operator $U_\sigma$, to the quantum state $\rho_w \in L_{H_n^2}$, of the $n$ two-state particles where the amount of information is stored. The dimension of the QA $\mathcal{M}$, denoted by $\text{dim}[\mathcal{M}]$, is the dimension of its quantum states $\rho_w$: $\text{dim}[\mathcal{M}] = 2^n \times 2^n = N$. After each input string of length $w$, the observable $\tilde{A}(1)$ is measured and the corresponding output is given by the probability $\omega(w, a_k) = \text{Tr}\{\tilde{P}_k(1)\rho_w\}$, which is stored in an exterior classical device.

The concepts of equivalent states and of equivalent automata can also be defined for a QA as follows.

Two states $\rho_{w_i}$ and $\rho_{w_j}$ of the state set $Q$ of a QA $\mathcal{M}$, are said to be equivalent, and we write $\rho_{w_i} \simeq \rho_{w_j}$ iff $\omega(\tilde{U}_w(\rho_{w_i}), a_k) = \omega(\tilde{U}_w(\rho_{w_j}), a_k)$ for every $w \in \Sigma^*$. More precisely, two states $\rho_{w_i}, \rho_{w_j} \in Q$ are equivalent, iff for every $a_k \in \text{Spec}\tilde{A}(1)$ and for every $w \in \Sigma^*$:

$$\text{Tr}\{\rho_{w_i}\tilde{P}_k(1)\} = \text{Tr}\{\rho_{w_j}\tilde{P}_k(1)\}$$

$$\text{Tr}\{\tilde{U}_w(\rho_{w_i})\tilde{P}_k(1)\} = \text{Tr}\{\tilde{U}_w(\rho_{w_j})\tilde{P}_k(1)\}.$$  \hfill (5)

We define a quantum behavior of a QA $\mathcal{M}$ over the signature $(\Sigma, \Omega)$, as a map $\beta_M(w) : \Sigma^* \rightarrow \Omega(\rho_w)$ for every $w \in \Sigma^*$. Furthermore, two QA $\mathcal{M}$ and $\mathcal{M}_A$, over the same signature are said to be equivalent and we write $\mathcal{M} \simeq \mathcal{M}_A$, when they have the same observable quantity $\tilde{A}(1)$ and the same behavior. The equivalence between quantum automata is a bit more restrictive than between classical ones. The reason is because the output alphabet of a QA is determined by the probabilities of the outcomes of the measurements of an observable quantity $\tilde{A}(1)$, therefore all equivalent QA must have in common this observable. In the present case, where the QA works with qubits, we cannot replace it by another QA with the same signature, if it doesn’t work with qubits. Moreover, there is no QA equivalent to $\mathcal{M}$ with less than $n_1$ qubits, since the observable quantity must always be $\tilde{A}(1)$.

The fact that the dimension of the underlying Hilbert space of a QA is finite doesn’t imply that the cardinality, or size, of its state set $Q$ is finite. When the cardinal of $Q$ is
finite we call the QA a *Quantum Finite Automaton*. In such a case the output alphabet is also finite.

The unitary operators $U_\sigma$ should have some properties in order that a QA might be also a QFA.

**Proposition 1:** The number of states $\rho_l = U_l^\dagger \rho_0 U_l^\dagger$ ($l \in \mathbb{N}$), generated by a unitary operator $U$ of $\mathcal{H}_2^n$, is finite iff there is a $p \in \mathbb{N}$ and $p \leq 2^n \times 2^n$, such that $U^p = 1$. In this case the unitary operator $U$ has $p$ different imaginary eigenvalues $u_j = e^{i2\pi j/p}$, with $1 \leq j \leq p$, and the set generated by $U$ is a finite group.

**Proof:** The finite number of states of the QA is the result of the well known properties of any group of cyclic unitary operators. Q.E.D.

**Corollary 1:** Let $\mathcal{M}$ be a QA. If there is at least a $\sigma \in \Sigma$ such that the set generated by the unitary operator $U_\sigma$ is not a finite group then the QA $\mathcal{M}$ is not finite.

**Corollary 2:** If for each $\sigma \in \Sigma$ the set generated by $U_\sigma$ is finite and if: $U_\sigma U_\sigma' = U_{\sigma'} U_{\sigma}$ for every $\sigma, \sigma' \in \Sigma$, then $\{U_w\}_{w \in \Sigma^*}$ is a finite commutative group, and the QA $\mathcal{M}$ is finite.

## 4 Dimension reduction

Let us consider a QA, $\mathcal{M} = \langle \mathcal{H}_2^n, \rho_0, \Sigma, \mathcal{U}, Q, \hat{A}(1), \Omega \rangle$, composed by two subsystems (1) and (2) working with $n_1$ and $n_2$ qubits, respectively. The total number of qubits of the QA $\mathcal{M}$ is $n = n_1 + n_2$. The observable quantity of the QA is $\hat{A}(1) = A(1) \otimes 1(2)$. Measuring this physical quantity corresponds to “inquiring” only about part (1) of the total system. A natural question we can ask is: In which conditions would it be possible to replace the QA $\mathcal{M}$ by another equivalent QA $\mathcal{M}_A$, using only $n_A$ ($n_1 \leq n_A < n$), qubits? Such a QA would obviously have a smaller dimension than the original one. Moreover, if $n_A = \bar{n}$ is the least number of qubits such that $\mathcal{M}_A \simeq \bar{\mathcal{M}}$ is equivalent to $\mathcal{M}$ then, $\bar{\mathcal{M}}$ is the automaton with the minimal dimension or saying in other words, $\bar{\mathcal{M}}$ is the QA working with the minimal number of qubits.
What is usually understood by the minimization process of a classical automaton is the minimization of the cardinality of its state set. However, this question can only be addressed if the QA is also a QFA. Instead, we are going to show that given a QA $M$, with a finite or infinite number of states, it is always possible to determine whether its dimension is minimal.

A QA is a special case of automata, this is, a QA is a linear automaton since its states are vectors in a Hilbert space and the transition and output maps are linear transformations. One of the distinct advantages of linear automata is that their behavior can be studied by analytical rather than the enumerative techniques used in general automata.

The procedure to minimize the cardinality of a QFA follows the usual approach developed for classical automata, which consists in looking for equivalent states and the corresponding equivalence classes, however there are some specificities for quantum systems that we will present in a future work.

4.1 Disentangled subsystems

It was mentioned in section 2, that the unique operation on a system that gives rise to the correct description of an observable quantity referred to one of its subsystems, is the partial trace over the remaining subsystems. This property will be the keystone in the process of dimension reduction of a QA.

Theorem 1: Let $M = \langle \mathcal{H}_2^n, \rho_0, \Sigma, U, Q, \tilde{A}(1), \Omega \rangle$ be a QA whose initial state $\rho_0$ can be expressed in the form $\rho_0 = \rho_0^A \otimes \rho_0^B$, where $\rho_0^A$ is the reduced density operator of part (A) of the system, working with $n_A$ qubits and containing subsystem (1), and $\rho_0^B$ is the reduced density operator of the remaining part (B) of the system, working with $n_B = n - n_A$ qubits. If all unitary transformations $\tilde{U}_\sigma \in \mathcal{U}$, had the form $\tilde{U}_\sigma = \tilde{U}_\sigma^A \otimes \tilde{U}_\sigma^B$ (where $\tilde{U}_\sigma^A$ and $\tilde{U}_\sigma^B$ are unitary transformations in $\mathcal{L}_{\mathcal{H}_2^n A}$ and $\mathcal{L}_{\mathcal{H}_2^n B}$, respectively), then the QA $M_A = \langle \mathcal{H}_2^{n_A}, \rho_0^A, \Sigma, U_A, Q_A, \tilde{A}(1), \Omega \rangle$ is equivalent to $M$, and

1 - $\mathcal{H}_2^{n_A}$ is the underlying Hilbert space with the minimal dimension $2^{n_A}$.
2 - $\rho_0^A = Tr_B\{\rho_0\}$ is the initial state.
3 - The input alphabet, $\Sigma = \{\sigma\}$, is the same as in QA $M$. 
4. $Q_A = \{ \rho_w^A : w \in \Sigma_* \}$ with $\rho_w^A = Tr_B(\rho_w) = \tilde{U}_w^A(\rho_0^A) = U_w^A \rho_0^A U_w^A$, and $\{ U_w^A \}_{w \in \Sigma_*}$ is a family of unitary operators of $\mathcal{H}_w^A$ built as follows: i) $U_w^A = 1(A)$; ii) $U_A = \{ U^A_\sigma \}_{\sigma \in \Sigma}$, is a finite set of unitary operators indexed upon $\sigma \in \Sigma$ and iii) $U^A_{\sigma w} = U^A_\sigma U^A_w$.

5. $\delta_A : \Sigma \times Q_A \to Q_A$ such that $\delta_A(\sigma, \rho_w^A) = \tilde{U}_\sigma^A(\rho_w^A)$

6. The output function $\omega_A : Q \to \Omega$ is defined by $\omega_A(\rho_w^A, a_k) = Tr_A(\tilde{P}_k(1) \rho_w^A) = \omega(\rho_w, a_k)$.

7. $\omega_A : Q_A \to \Omega$ such that $\omega_A(\rho_w^A, a_k) = Tr_A(\tilde{P}_k(1) \rho_w^A)$ and $\Omega = \{ \Omega_w ; w \in \Sigma_* ; \sum_k \omega_A(w, a_k) = 1 \}$, with $\Omega_w = \{ \omega_A(\rho_w, a_k) : a_k \in SpecA \}$, is the same as in QA $\mathcal{M}$.

Proof: Using the properties of the partial trace operator:

$\rho_w^A = Tr_B(\rho_0) = Tr_B(\tilde{U}_\sigma(\rho_0)) = Tr_B(\tilde{U}_\sigma^A(\rho_0^A) \tilde{U}_\sigma^B(\rho_0^B)) = \tilde{U}_\sigma^A(\rho_0^A)$.

Using eq.(2), we obtain: $\omega_A(\rho_w^A, a_k) = Tr_A(\tilde{P}_k(1) \rho_w^A) = Tr(\tilde{P}_k(1) \rho_w) = \omega(\rho_w, a_k)$.

Q.E.D.

Theorem 1 says that if part (A) is initially disentangled from part (B) of the system and, if the unitary transformations preserve this disentanglement, then each subsystem (A) and (B) follows its own dynamics behaving as two separated systems. In this situation we can forget subsystem (B) and consider the QA restricted to subsystem (A), because $\mathcal{M} \simeq \mathcal{M}_A$. The equivalent QA $\mathcal{M}_A$ is named a sober QA. Theorem 1 is a sufficient condition for dimension reduction.

In the next sections we are going to use some known properties of invariant subspaces under unitary transformations, in order to derive the classes of equivalent quantum states.

4.2 Linear transformations and invariant subspaces

Let $\tilde{T} : \mathcal{L}_{\mathcal{H}_w^A} \to \mathcal{L}_{\mathcal{H}_w^A}$ to be the linear transformation defined by $\tilde{T} = Tr_B(\cdot \cdot)$. Let $\mathcal{K} = ker(\tilde{T})$ and $\mathcal{I} = Im(\tilde{T})$, to be the kernel and the image spaces of the transformation $\tilde{T}$. In Appendix A it is shown that, $Im(\tilde{T}) = \mathcal{L}_{\mathcal{H}_w^A}$, therefore $\tilde{T}$ is a linear transformation onto $\mathcal{L}_{\mathcal{H}_w^A}$. Let $\mathcal{Q} \subset \mathcal{L}_{\mathcal{H}_w^A}$ be the subspace orthogonal to $\mathcal{K}$, i.e. $\mathcal{L}_w^A = \mathcal{Q} \oplus \mathcal{K}$, then $dim[\mathcal{L}_w^A] = dim[\mathcal{Q}] + dim[\mathcal{K}]$, where $dim[\cdot]$ means dimension of a vector space. It is also true that $dim[\mathcal{L}_w^A] = dim[\mathcal{I}] + dim[\mathcal{K}]$. and we conclude that $dim[\mathcal{Q}] = dim[\mathcal{I}]$.

Since the spaces $\mathcal{Q}$ and $\mathcal{I}$ have the same dimension they are isomorphic (1st theorem of
is any vector in $L$ is, the matrix elements of the super-operator $\bar{U}$, therefore, if the images of the basis vectors are known, the image of any vector can be determined. The image of the basis-$B^Q \cup B^K$, under $\bar{U}$ is,

$$\bar{U}(B^Q_j) = \sum_{i=1}^{q} \bar{u}^Q_{ij} B^Q_i + \sum_{i=1+q}^{d} \bar{u}^Q_{ij} B^K_i ; j = 1, ..., q$$

(10)

$$\bar{U}(B^K_j) = \sum_{i=1}^{q} \bar{u}^K_{ij} B^Q_i + \sum_{i=1+q}^{d} \bar{u}^K_{ij} B^K_i ; j = q + 1, ..., d$$

(11)

where,

$$\bar{u}^Q_{ij} = (B^Q_i, \bar{U}(B^Q_j)) = Tr\{B^Q_i \bar{U}(B^Q_j)\} ; i = 1, ..., q; \ j = 1, ..., q$$

(12)

$$\bar{u}^K_{ij} = (B^K_i, \bar{U}(B^K_j)) = Tr\{B^K_i \bar{U}(B^K_j)\} ; i = q + 1, ..., d ; j = q + 1, ..., d$$

(13)

$$\bar{u}^Q_{ij} = (B^K_i, \bar{U}(B^Q_j)) = Tr\{B^K_i \bar{U}(B^Q_j)\} ; i = q + 1, ..., d ; j = 1, ..., q$$

(14)

$$\bar{u}^K_{ij} = (B^Q_i, \bar{U}(B^K_j)) = Tr\{B^Q_i \bar{U}(B^K_j)\} ; i = 1, ..., q ; j = q + 1, ..., d$$

(15)

are the matrix elements of the super-operator $\bar{U}$ in the basis-$B^Q \cup B^K$. 

The properties of any unitary transformation $\bar{U}$ are completely determined by its effect on the basis-$B^Q \cup B^K$. Thus, if

$$Z = \sum_{j=1}^{q} z_j B^Q_j + \sum_{j=1+q}^{d} z_j B^K_j.$$ 

(8)

is any vector in $L$, the image of $Z$ under $\bar{U}$ is

$$\bar{U}(Z) = \sum_{j=1}^{q} z_j \bar{U}(B^Q_j) + \sum_{j=1+q}^{d} z_j \bar{U}(B^K_j).$$

(9)

therefore, if the images of the basis vectors are known, the image of any vector can be determined.
Replacing $\bar{U}(B_j^Q)$ and $\bar{U}(B_j^K)$ given by (10) and (11) into eq.(9), we obtain

$$\bar{U}(Z) = \sum_{j=1}^{q} \{ \sum_{j=1}^{q} \bar{u}_{ij}^{QQ} z_j + \sum_{j=1+q}^{d} \bar{u}_{ij}^{KK} z_j \} B_j^Q + \sum_{j=1+q}^{d} \{ \sum_{j=1}^{q} \bar{u}_{ij}^{QQ} z_j + \sum_{j=1+q}^{d} \bar{u}_{ij}^{KK} z_j \} B_j^K$$

(16)

A possible relation between the subspaces $Q$ and $K$ of $L_{\mathcal{H}_2}$ and the linear transformation $\bar{U}$, is invariance. We say that $Q$ (or $K$) is invariant under $\bar{U}$ if, for every $X \in Q$ (or, for every $Y \in K$) implies $\bar{U}(X) \in R$ (or $\bar{U}(Y) \in K$). We also say that $Q$ (or $K$) is invariant under a set of linear transformations $\bar{U}_{\sigma}$ ($\sigma \in \Sigma$), if it is invariant under each member of the set. When two spaces, say $Q$ and $K$, such that $Q \oplus K = L_{\mathcal{H}_2}$, are both invariant under $\bar{U}$, then we say that $\bar{U}$ is reduced (decomposed) by the pair $(Q, K)$. The following proposition [16] defines the structure of the matrix representing a unitary transformation $\bar{U}$ under which $Q$ (or $K$) is invariant.

**Proposition 2:** Let $L_{\mathcal{H}_2} = Q \oplus K$ be the direct sum of the subspaces $Q$ and $K$. If $K$ (or $Q$) is invariant under a unitary operator $\bar{U}$, so is the complementary subspace $Q$ (or $K$). Then, the unitary transformation $\bar{U}$ is reduced by the pair $(Q, K)$ and the matrix representation of $\bar{U}$ in the basis-$B^Q \cup B^K$ is

$$\bar{U} = \begin{pmatrix} \bar{U}^{QQ} & 0 \\ 0 & \bar{U}^{KK} \end{pmatrix}$$

(17)

where the block diagonal matrices

$$\bar{U}^{QQ} = [\bar{u}_{ij}^{QQ}]_{i=1,...,q; j=1,...,q}$$

(18)

$$\bar{U}^{KK} = [\bar{u}_{ij}^{KK}]_{i=q+1,...,d; j=q+1,...,d}$$

(19)

are unitary matrices, and the off diagonal blocks are

$$\bar{U}^{QK} = [\bar{u}_{ij}^{QK}]_{i=q+1,...,d; j=1,...,q} = 0$$

(20)

$$\bar{U}^{KQ} = [\bar{u}_{ij}^{KQ}]_{i=1,...,q; j=q+1,...,d} = 0$$

(21)

Whenever $\bar{U}$ is reduced by the pair $(Q, K)$ then, $\bar{U} = \bar{U}^{QQ} \oplus \bar{U}^{KK}$ is the direct sum of the unitary transformations $\bar{U}^{QQ}$ and $\bar{U}^{KK}$ defined on the subspaces $Q$ and $K$, respectively. The transformation $\bar{U}^{QQ}$ describes what $\bar{U}$ does on $Q$ and the transformation $\bar{U}^{KK}$ describes what $\bar{U}$ does on $K$. 
Proposition 3: Let $K \in \mathcal{L}_{\mathcal{H}_2^n}$ to be invariant under the unitary transformations $\bar{U}_a$ and $\bar{U}_b$. Then $K$ is also invariant under the transformation $\bar{U}_a \bar{U}_b$.

Proof: The product of diagonal matrices is also a diagonal matrix. QED.

What will the action of a unitary super-operator $\bar{U}$ on a general vector $Z \in \mathcal{L}_{\mathcal{H}_2^n}$ be?

Applying the linear super-operator $\bar{T} = Tr_B\{\cdot\}$ to both sides of this eq.(8), and denoting by $B^I_j = \bar{T}(B^Q_j); j = 1, \ldots q$, we obtain

$$Z^A = \sum_{j=1}^q z_j B^I_j = \sqrt{2^{n-n_A}} \sum_{j=1}^q z_j B^I_j$$ (22)

The set $B^I = \{B^I_j; j = 1, \ldots q\}$ is an orthonormal basis set of $\mathcal{L}_{\mathcal{H}_2^n}$ (Appendix A), and $Z^A = Tr_B\{Z\} \in \mathcal{L}_{\mathcal{H}_2^n}$ is the image of $Z$.

The image of $Z$ under $\bar{U}$ is $\tilde{Z} = \bar{U}(Z)$ given by eq.(9). Applying $\bar{T}$ to both sides of it, we end up with,

$$\tilde{Z}^A = \sqrt{2^{n-n_A}} \sum_{i=1}^q \left( \sum_{j=1}^q \bar{u}^Q_{ij} z_j + \sum_{i=q+1}^d \bar{u}^K_{ij} z_j \right) B^I_i$$ (23)

where $\tilde{Z}^A = \bar{T}(\tilde{Z})$.

We would like to know if there is a unitary super-operator $\bar{U}^A : \mathcal{L}_{\mathcal{H}_2^n} \rightarrow \mathcal{L}_{\mathcal{H}_2^n}$, such that for every state $Z \in \mathcal{L}_{\mathcal{H}_2^n}$:

$$\bar{U}^A \bar{T}(Z) = \bar{T} \bar{U}(Z)$$ (24)

The action of any super-operator $\bar{U}^A$ on any $Z^A \in \mathcal{L}_{\mathcal{H}_2^n}$ is,

$$\bar{U}^A(Z^A) = \sqrt{2^{n-n_A}} \sum_{i=1}^q \left[ \sum_{j=1}^q \bar{u}^A_{ij} z_j \right] B^I_i$$ (25)

where $\bar{u}^A_{ij} = \left( B^I_i, \bar{U}^A(B^I_j) \right)$ are the elements of $\bar{U}^A$ relative to the $B^I$-basis. Replacing (25) and (23) in eq.(24) and recalling that $B^I$ is a set of linearly independent vectors, we obtain

$$\sum_{j=1}^q \left( \bar{u}^A_{ij} - \bar{u}^Q_{ij} \right) z_j - \sum_{j=q+1}^d \bar{u}^K_{ij} z_j = 0; \quad \forall i=1, \ldots q$$ (26)

This is a system of $q$ linear equations, where the unknowns are the $q^2$ elements $\bar{u}^A_{ji}$ of matrix $\bar{U}^A$. There are $(q^2 - q)$ linearly independent non-trivial solutions. We can choose
freely \((q^2 - q)\) numbers \(u_{ji}^A\) and the remaining \(q\) values being uniquely determined. Each of these solutions will depend on the components \(z_j\) of the vector \(\mathbf{Z}\), except when the coefficients of every \(z_j\), in eq.(26), are simultaneously null, i.e.,

\[
\begin{align*}
\bar{u}_{ij}^A &= \bar{u}_{ij}^{QQ} & i &= 1, \ldots, q; \ j = 1, \ldots, q \\
\bar{u}_{ij}^{KQ} &= 0; & i &= 1, \ldots, q; \ j = q + 1, \ldots, d
\end{align*}
\]

Comparing these conditions with the statement of Proposition 2, we conclude that the invariance of subspace \(Q\), under the action of the super-operator \(\bar{U}\), is a necessary condition for the existence of an operator \(\bar{U}^A \in \mathcal{L}_{\mathcal{H}_2^a}\), obeying eq.(24). In such case \(\bar{U}^A = \bar{U}^{QQ}\), and the matrix \(\bar{U}^{QQ} = [u_{ij}^{QQ}]_{i=1,\ldots,q;j=1,\ldots,q}\) is unitary.

The following proposition summarizes these results.

**Proposition 4.** Let \(K \subset \mathcal{L}_{\mathcal{H}_2^a}\) to be the kernel of the linear partial trace transformation \(\bar{T} : \mathcal{L}_{\mathcal{H}_2^a} \to \mathcal{L}_{\mathcal{H}_2^a}^\prime\). \(K\) is invariant under the unitary operator \(\bar{U} : \mathcal{L}_{\mathcal{H}_2^a} \to \mathcal{L}_{\mathcal{H}_2^a}^\prime\) iff \(\bar{U}^{KQ} = 0\) (or \(\bar{U}^{QK} = 0\)). Then \(\bar{U} = \bar{U}^{QQ} \oplus \bar{U}^{KK}\) and there is a unitary transformation \(\bar{U}^A = \bar{U}^{QQ} : \mathcal{L}_{\mathcal{H}_2^a} \to \mathcal{L}_{\mathcal{H}_2^a}^\prime\), such that, for every \(\mathbf{Z} \in \mathcal{L}_{\mathcal{H}_2^a}\), \(\bar{U}^A \bar{T}(\mathbf{Z}) = \bar{T}\bar{U}(\mathbf{Z})\).

### 4.3 Condition for dimension reduction

Applying the transformation \(\bar{T} = Tr_B\{\cdot\}\) to each state of the state set \(Q = \{\rho_w = \bar{U}_w(\rho_0) : w \in \Sigma^*\}\) of the QA \(\mathcal{M}\), we obtain the set \(Q_A = \{\rho_w^A = Tr_B\{\rho_w\} : w \in \Sigma^*\}\), where \(\rho_w^A\) are the reduced density operators in \(\mathcal{L}_{\mathcal{H}_2^a}\). In particular, the initial state \(\rho_0\) is mapped into \(\rho_0^A = Tr_B\{\rho_0\}\). The set \(Q_A\) will be a set of reachable states of a QA \(\mathcal{M}_A\), iff there is a family of operators \(U_A = \{U_w^A : w \in \Sigma^*\}\), such that \(\rho_w^A = U_w^A\rho_0^A(U_w^A)^\dagger\). We have shown in Proposition 4 that when \(\bar{U}_w^{QK} = 0\), then \(\bar{U}_w = \bar{U}_w^{QQ} \oplus \bar{U}_w^{KK}\) and there is a unitary operator \(\bar{U}_w^A = \bar{U}_w^{QQ}\). By Proposition 3, \(\bar{U}_w = \bar{U}_w^{QQ} \oplus \bar{U}_w^{KK}\) \((w \in \Sigma^*)\) iff \(\bar{U}_w^{KQ} = 0\), for every \(\sigma \in \Sigma\).

Moreover, the quantum automata \(\mathcal{M}\) and \(\mathcal{M}_A\) will be equivalent, if they have the same behavior. The probability of obtaining an outcome \(a_k\) when the QA \(\mathcal{M}\) is in the state \(\rho_w\) is:

\[
\omega(\rho_w, a_k) = Tr\{\bar{P}_k(1)\rho_w\} = Tr_A\{\bar{P}_k(1)\rho_w^A\} = \omega_A(\rho_w, a_k),
\]

where we used
eq. (2). This last equality shows that the quantum automata $\mathcal{M}$ and $\mathcal{M}_A$ have the same behavior: $\beta_\mathcal{M}(w) = \beta_{\mathcal{M}_A}(w) : \Sigma^* \rightarrow \Omega$, for every $w \in \Sigma^*$.

The results that we have been deriving can be summarized in the following theorem.

**Theorem 2:** A tuple $\mathcal{M}_A = (H_2^{n_A}, \rho_0^A, \Sigma, U_A, Q_A, \hat{A}(1), \Omega)$, with $n_A < n$ and whose state set $Q_A = \{\rho_w^A = Tr_B(U_w(\rho_0)) : w \in \Sigma^*\}$ is a QA equivalent to the QA $\mathcal{M}$, iff $\hat{U}_\sigma^{QQ} = 0$ for every unitary operator $\hat{U}_\sigma \in \Sigma$. In such a case, $\hat{U}_\sigma = \hat{U}_\sigma^{QQ} \oplus \hat{U}_\sigma^{KK}$:

1. $H_2^{n_A}$ is the underlying Hilbert space with dimension $2^{n_A} < 2^n$.
2. $\rho_0^A = Tr_B(\rho_0) \in L_{H_2^{n_A}}$ is the initial state.
3. The input alphabet, $\Sigma = \{\sigma\}$, is the same as in QA $\mathcal{M}$.
4. The state set $Q_A = \{\rho_w^A : w \in \Sigma^*\}$ with $\rho_w^A = Tr_B(\rho_w) = \hat{U}_\sigma^{QQ}(\rho_w) = \hat{U}_\sigma^{A}(\rho_0^A) = U_w\rho_0 U_w^\dagger$, where $\{U_w^A\}_{w \in \Sigma^*}$ is a family of unitary operators of $H_2^{n_A}$ built as follows: i) $U_A = \{U_w^A\}_{w \in \Sigma}$, is a finite set of unitary operators indexed upon $\sigma \in \Sigma$, ii) $U_\sigma^A = 1(A)$; and iii) $U_{\sigma w}^A = U_{\sigma}^A U_{w}^A$.
5. The transition map $\delta_A : \Sigma \times Q_A \rightarrow Q_A$ such that $\rho^A_{w \sigma} = \delta_A(\sigma, \rho_w^A) = \hat{U}_\sigma^A(\rho_w^A)$.
6. The output function $\omega_A : Q \rightarrow \Omega$ is defined by $\omega_A(\rho_w^A, a_k) = Tr_A(\hat{P}_k(1)\rho_w^A) = \omega(\rho_w, a_k)$.
7. The output set, $\Omega = \{\Omega_w; w \in \Sigma^*; \sum_k \omega_A(w, a_k) = 1\}$, with $\Omega_w = \{\omega_A(w, a_k) : a_k \in Spec A\}$, is the same as in QA $\mathcal{M}$.

This theorem tells us how to built the physical support of the equivalent automaton $\mathcal{M}_A$. It is a system of $n_A(n_1 < n_A < n)$ two-state quantum particles prepared in a quantum state $\rho_0^A = Tr_B(\rho_0)$, and submitted to quantum gates represented by the set of unitary operators $U_A = \{U_w^A\}_{w \in \Sigma}$ such that $\hat{U}_\sigma^A(\rho_w^A) = U_{\sigma w}^A \rho_w^A U_{w}^A$ and $\hat{U}_\sigma^A = \hat{U}_\sigma^{QQ}$. The probabilities of the possible outcomes of a measurement of the observable $\hat{A}(1) = A(1) \otimes 1(B)$, performed on the first $n_1$ of the $n_A$ two-state particles, give the output symbols of the smaller QA $\mathcal{M}_A$, with dimension $2^{n_A} \times 2^{n_A}$.

If there is at least one input $\sigma \in \Sigma$ such that $\hat{U}_\sigma^{QQ} \neq 0$, then there is no QA with dimension $2^{n_A} \times 2^{n_A}$, equivalent to $\mathcal{M}$. 
5 Minimization algorithm

Theorem 2 says that a QA $\mathcal{M}_A$, working with $n_A < n$ is equivalent to the initial QA $\mathcal{M}$ iff the kernel of the partial trace transformation is invariant under all the unitary operators $\bar{U}_\sigma$, with $\sigma \in \Sigma$. However, it does not say whether $n_A$ is the minimum number of qubits $\bar{n}$. In this section we present an algorithm to determine the minimal QA.

Usually, the density matrices $\rho$ and the unitary operators $U_\sigma$, are expressed in terms of the computational Dirac basis-$\mathcal{B}_d(n)$ of $L_{H_2^n}$, (Appendix A), rather than in terms of the basis-$\mathcal{B}_Q \cup \mathcal{B}_K$, that is needed to check the invariance of subspace $K$ under the operators $\bar{U}_\sigma$. Therefore, the first step of the algorithm consists in constructing two orthonormal basis sets for the subspaces $Q$ and $K$, as explained in Appendix A.

We assume that the $n_1$ first qubits of the QA $\mathcal{M}$ belong to subsystem (1) where the observable $\tilde{A}(1)$ is going to be measured and that we have already checked if the conditions of Theorem 1 are verified. If so we obtain the corresponding sober automaton.

Given a QA $\mathcal{M} = \langle H_2^n, \rho_0, \Sigma, U, Q, \tilde{A}(1), \Omega \rangle$ over a finite signature $\langle \Sigma, \Gamma \rangle$, we compute the QA $\bar{\mathcal{M}} = \langle H_2^n, \bar{\rho}_0, \Sigma, \bar{U}, \bar{Q}, \tilde{A}(1), \Omega \rangle$, working with the minimal number of qubits $\bar{n}$, as follows:

1. Replace each Dirac vector $\otimes_{j=1}^n v_{i_j, i'_j}$; $i_j, i'_j = 0, 1$, of the Dirac computational basis set $\mathcal{B}_d^C(n)$ by the $2^n \times 2^n$ matrix $B_r$, $r = 2^n(l - 1) + l'$, whose elements are all null except the element $b_{l,l'}$, that is equal to 1 and obtain the ordered computational basis set $\mathcal{B}_d^C(n) = \{B_r, r = 1, ..., 2^n \times 2^n\}$.

2. Do $n_A = n_1$.

3. Replace each Dirac vector $\otimes_{j=1}^{n_A} v_{i_j, i'_j} \in \mathcal{B}_d^C(n_A)$; $i_j, i'_j = 0, 1$, of the Dirac computational basis set $\mathcal{B}_d^C(n_A)$, by the $2^{n_A} \times 2^{n_A}$ the matrix $B_r^A$, $r = 2^{n_A}(l - 1) + l'$, whose elements are all null except the element $b_{l,l'}$, that is equal to 1 and obtain the ordered computational basis set $\mathcal{B}_d^C(n_A) = \{B_r^A, r = 1, ..., 2^{n_A} \times 2^{n_A}\}$.

4. Compute $\bar{T}(B_r)$ for $r = 1, ..., 2^n \times 2^n$. If $\bar{T}(B_r) = 0$ add the vector $B_r$ to the set $S_0$. If $\bar{T}(B_r) = B_j^1$, with $j = 1, ..., 2^{n_A} \times 2^{n_A}$, add $B_r$ to the set $S_j$. 
5. With vectors of each set $S_j = \{B_{rk}(j) : \mathbf{T}(B_{rk}(j)) = B^1_j; \, k = 1, \ldots, 2^{n-n_A}\}$, $j = 1, \ldots, 2^{n_A} \times 2^{n_A}$, obtain the following linear combinations: $B^Q_j = \frac{1}{\sqrt{2^{n-n_A}}} \sum_{k=1}^{2^{n-n_A}} B_{rk}(j)$ and build the set $B^Q = \{B^Q_j : j = 1, \ldots, 2^{n_A} \times 2^{n_A}\}$.

6. With the vectors of each set $S_j$, $j = 1, \ldots, 2^{n_A} \times 2^{n_A}$, obtain the following linear combinations: $B_{1j} = \sum_{k=1}^{2^{n-n_A}} c_k B_{rk}(j)$ where $c_k = \frac{1}{\sqrt{2^{n-n_A}-1}}$ for $k = 1, \ldots, 2^{n-n_A} - 1$ and $c_{2^{n-n_A}} = -1$.

7. Compute the vectors $B_{1j}$ corresponding to all cyclic permutations of the coefficients $c_k$ ($k > 1$) in eq.(31), and build the $2^{n_A} \times 2^{n_A}$ sets $C_j = \{B_{1j}; l = 1, \ldots, 2^{n-n_A} - 1\}$ with $j = 1, \ldots, 2^{n_A} \times 2^{n_A}$.

8. Apply the Gram-Schmidt algorithm to each set $C_j$ in order to obtain a set of orthonormal vectors $C^\perp_j$.

9. Apply an appropriate ordering algorithm to the vectors given by (32) to obtain an ordered set of orthonormal vectors $B^K = \{B^K_r; r = 2^{n_A} \times 2^{n_A} + 1, \ldots, 2^n \times 2^n\}$ and build $B^C = B^Q \cup B^K$.

10. Write the transition matrix $\mathbf{C}$ from the basis $B^C_j(n)$ to the basis $B^C$.

11. For each $U'_\sigma \in U$ compute $\bar{u}_{ij}(\sigma) = Tr\{B^C_j U'_\sigma B^C_{1i} U'_{\sigma}^\dagger\}$ with $i, j = 1, \ldots, 2^n \times 2^n$.

12. Build the matrices $\bar{U}'_{\sigma} = [\bar{u}_{ij}(\sigma)]$, $i, j = 1, \ldots, 2^n \times 2^n$, $\sigma \in \Sigma$.

13. For each $\sigma \in \Sigma$ compute $\bar{U}_{\sigma} = \mathbf{C}^{-1} \bar{U}'_{\sigma} \mathbf{C}$

14. For each $\sigma \in \Sigma$ compute $\bar{u}^{QK}_{ij}(\sigma) = Tr\{B^K_{1i} U_{\sigma} B^Q_{j} U_{\sigma}^\dagger\}$, $i = 2^{n_A} \times 2^{n_A} + 1, \ldots, 2^n \times 2^n$ and $j = 1, \ldots, 2^{n_A} \times 2^{n_A}$.

15. If there is at least one $\bar{u}_{ij}(\sigma)^{QK} \neq 0$, go to 17. If for every $\sigma \in \Sigma$ and for every $i = 1, \ldots, 2^{n_A} \times 2^{n_A}, j = 2^{n_A} \times 2^{n_A} + 1, \ldots, 2^n \times 2^n$, $\bar{u}^{QK}_{ij}(\sigma) = 0$, go to 16.

16. For each $\sigma \in \Sigma$ build the matrices $\bar{U}^{QQ}_{\sigma} = [\bar{u}^{QQ}_{ij}(\sigma)] = Tr\{\bar{U}_{\sigma}^\dagger(B^Q_j)B^Q_{i}\}; i, j = 1, \ldots, 2^{n_A} \times 2^{n_A}$, go to 20.

17. Do $n_A = n_A + 1$.

18. If $n_A = n$, go to 21. If not, go to 3.
19. The initial QA $\mathcal{M}$, is the minimal one.

20. Write $\bar{n} = n_A$.

21. Compute $\bar{\rho}_0 = T_{r_B}\{\rho_0\}$.

22. Write the set $\bar{\mathcal{U}} = \{ \bar{U}^{QQ}_\sigma; \sigma \in \Sigma \}$.

23. The QA $\bar{\mathcal{M}} = \langle \mathcal{H}_2^{\bar{n}}, \bar{\rho}_0, \Sigma, \mathcal{U}, \bar{Q}, \bar{\mathcal{A}}(1), \Omega \rangle$, with $\bar{n} < n$ qubits, is the minimal one.

The complexity of this algorithm is computed in terms of the dimension of the initial QA $\mathcal{M}$, and of the dimension of the QA $\mathcal{M}_A$ which are $\text{dim}[\mathcal{M}] = 2^n \times 2^n = N$ and $\text{dim}[\mathcal{M}_A] = 2^{n_A} \times 2^{n_A} = N_A$ respectively. Another variable playing a role in the computation of the complexity of the algorithm, is the size $|\Sigma|$ of the input alphabet, since it gives the number of unitary operators $U_\sigma$ (gates) to be computed in the $\mathcal{B}^{C} = \mathcal{B}^{Q} \cup \mathcal{B}^{K}$-basis. The cardinality of the state set $Q$, doesn’t play any role in the minimization algorithm. The dimensions of the observable $\bar{\mathcal{A}}(1)$ and the size $|\Omega|$ of the output set, are irrelevant variables in the algorithm.

**Theorem 3:** Given a QA $\mathcal{M}$ over a signature $(\Sigma, \Omega)$, the minimization algorithm requires $O(p(|\Sigma|, \text{dim}[\mathcal{M}])))$ arithmetic operations.

**Proof:** Here is the detailed analysis of the algorithm (bounding for each step the worst case execution time in terms of arithmetic operations):

1 - $O(N^2)$ since the cost of ordering $N$ objects is quadratic and the cost of computing the matrix representation of $N$ vectors $\bigotimes_{j=1}^{n} v_{i_ji_j'}; i_j, i_j' = 0, 1$ is $N$.

2 - $O(1)$ since this is the cost of a constant.

3 - $O(N_A^2)$ since the cost of ordering $N_A$ objects is quadratic and the cost of computing the matrix representation of $N_A$ vectors $\bigotimes_{j=1}^{n_A} v_{i_ji_j'}; i_j, i_j' = 0, 1$ is $N_A$.

4 - $O(N^{3/2}N_A^{-1/2})$ since the body of the cycle is running $O(N)$ times and each run computes the partial trace $\bar{T}\{\mathcal{B}_r\}$ with the cost $O((N/N_A)^{1/2})$.

5 - $O(N)$ since this is the cost of a sum of vectors of dimension $N$.

6 - $O(N)$ for the same reason as in 5.
7 - $O((NN_A)^{1/2})$ since $O((N/N_A)^{1/2})$ is the cost of a permutation of $(N/N_A)^{1/2}$ objects and there are $N_A$ permutations to compute.

8 - $O(N^{3/2}N_A^{1/2})$ since $O(N^2(N/N_A)^{1/2})$ is the cost of applying the Gram-Schmidt process to a set of $(N/N_A)^{1/2}$ vectors of dimension $N$ each, and this process is repeated for each of the $N_A$ sets $C_j$.

9 - $O((N - N_A)^2)$ since the cost of the ordering algorithm is quadratic in the number of objects and this is the number of vectors in the set given by eq.(30).

10 - $O(N^2)$ since each of the $N$ vectors of the $B'^C_d$-basis has $N$ coefficients, being $N^2$ the dimension of the super-operator $\bar{C}$.

11 - $O(N^5)$ since there are $N^2$ operations corresponding to two loops, being the cost of the body of each loop $O(N^3)$. The body of each loop computes the matrix product $\{B'^C_d U'^C_d B'^C_d U'^C_d\}$ that has a cubic cost, followed by the computation of its trace that has cost $O(N)$.

12 - $O(|\Sigma|N^5)$ since the body of the cycle is running $O(|\Sigma|)$ times and the cost of each run is $O(N^5)$.

13 - $O(|\Sigma|N^6)$ since the body of the cycles is running $O(|\Sigma|)$ times and the cost of each run is cubic (product of matrices) in the dimension of the super-operators $\bar{C}$ which is $N^2$.

14 - $O(|\Sigma|(N - N_A)N^3)$ the same reason as in step 12.

15 - $O(|\Sigma|N^2)$ since the body of the cycles is running $O(|\Sigma|N^2)$ times and the cost of each run is $O(1)$.

16 - $O(|\Sigma|N_AN^3)$ the same reason as in step 12.

17 - $O(|\Sigma|\log(N/N_A)N^6)$ since the body of the cycle is running $O(\log(N/N_A))$ times and the cost of each run is $O(|\Sigma|N^6)$.

18, 19 and 20 - $O(1)$ since this is the cost of a constant.

21 - $O(N^{3/2}N_A^{-1/2})$, the same reason as in step 4.

22 and 23 - $O(1)$ since this is the cost of a constant.
In conclusion: all steps of the minimization algorithm requires a polynomial number of arithmetic operations in $|\Sigma|$, $N = \text{dim}[\mathcal{M}]$, $N_A = \text{dim}[\mathcal{M}_A]$ and the $\text{dim}[\mathcal{M}_A] \leq \text{dim}[\mathcal{M}]$. QED.

6 Conclusion

In this paper a new model for a QA working with qubits was proposed and the problem of minimizing its dimension was solved.

The quantum states of the QA were represented by density operators which is a powerful approach to deal with measurements concerning only part of a quantum system. The linearity of the automaton and of the partial trace super-operator were used to derive the conditions for dimension reduction. It was shown that this is possible, if the kernel of the partial trace transformation is invariant under each of the unitary transformations associated to each letter of the input alphabet.

It was also developed a minimization algorithm and it was shown that its complexity is polynomial in the size of the input alphabet and in the dimension of the QA.

Let us stress again that the minimization of the dimension of a QA and the minimization of the cardinality of its state set are different issues. While the dimension minimization can be addressed whether the QA is finite or not, the cardinality minimization is only possible if the automaton is a QFA. This problem will be studied in a future work.

Finally, we refer the possibility that the minimization technique here developed, can be adapted to other kind of automata, namely Quantum Cellular Automata that implement quantum computation on qubits using spins [17, 18].

Appendix A

The computational basis set for $\mathcal{L}_{\mathcal{H}_2^n}$ is an orthonormal basis set. In the Dirac notation it is expressed by $\mathcal{B}_d^\epsilon(n) = \left\{ \otimes_{k=1}^n v_{i_ki'_k}; i_k, i'_k = 0, 1 \right\}$ with $v_{i_ki'_k} = |i_k\rangle\langle i'_k|$ and $\text{dim}[\mathcal{B}_d^\epsilon(n)] = \ldots$
The set $\mathcal{B}_d^C(n)\setminus\mathcal{B}_d^C(n_A)$ we associate to each vector $\bigotimes_{k=1}^{n_A} v_{i_k,i_k'} \in \mathcal{B}_d^C(n_A) ; i_k,i_k' = 0,1$, (which is the Dirac computational basis for the image space $\mathcal{L}_{\mathcal{N}_2^{n_A}}$) we associate to each vector $\bigotimes_{j=1}^{n_A} v_{i_j,i_j'} \in \mathcal{B}_d^C(n_A) ; i_k,i_k' = 0,1$, a $2^{n_A} \times 2^{n_A}$ matrix $\mathcal{B}_j^I$, whose elements are all null except the element $b_{i,i'}$, that is equal to 1 and where $r = 2^{n_A}(l-1)+l'$. Call $\mathcal{B}_j^I = \{ \mathcal{B}_j^I \mid r = 1, ..., 2^{n_A} \times 2^{n_A} \}$ to the ordered computational basis-set of the image space $\mathcal{L}_{\mathcal{N}_2^{n_A}}$.

The image of any vector of the basis $\mathcal{B}_d^C(n)$ by the transformation $\tilde{T} = Tr_B \{ . \}$ is,

$$\tilde{T} \left( \bigotimes_{k=1}^{n_A} v_{s_k,s_k'} \bigotimes_{k=n_A+1}^{n} v_{s_k,s_k'} \right) = \bigotimes_{k=1}^{n_A} v_{s_k,s_k'} Tr_B \left\{ \bigotimes_{k=n_A+1}^{n} v_{s_k,s_k'} \right\} \quad (29)$$

Computing the partial trace we obtain,

$$\tilde{T} \left( \bigotimes_{k=1}^{n_A} v_{s_k,s_k'} \bigotimes_{k=n_A+1}^{n} v_{s_k,s_k'} \right) = \begin{cases} 0 & \text{if } \exists j : s_k \neq s_k' \\ \bigotimes_{k=1}^{n_A} v_{s_k,s_k'} & \text{if } \forall k : s_k = s_k' \end{cases}$$

Let us denote by $S_0 = \{ \mathcal{B}_{r_k} : \tilde{T}(\mathcal{B}_{r_k}) = 0 \mid k = 1, ..., 2^n(2^n-2^{n_A}) \}$ the set of all vectors of $\mathcal{B}_d^C(n)$ transformed by $\tilde{T}$ into zero. Let us denote by $S_j = \{ \mathcal{B}_{r_k}(j) : \tilde{T}(\mathcal{B}_{r_k}(j)) = \mathcal{B}_j^I \mid k = 1, ..., 2^{n-n_A} \}$ the set of the vectors of $\mathcal{B}_d^C(n)$ with the same image $\mathcal{B}_j^I$. There are $2^{n-n_A}$ vectors $\mathcal{B}_{r_k}(j) \in \mathcal{B}_d^C(n)$ and there are $2^{n_A} \times 2^{n_A}$ sets $S_j$.

A straightforward way of obtaining an orthonormal basis set for the subspace $\mathcal{Q}$ consists in taking the following linear combinations of all vectors $\mathcal{B}_{r_k}(j) \in S_j$:

$$\mathcal{B}_j^Q = \frac{1}{\sqrt{2^{n-n_A}}} \sum_{k=1}^{2^{n-n_A}} \mathcal{B}_{r_k}(j) \quad (30)$$

The set $\mathcal{B}_j^Q = \{ \mathcal{B}_j^Q : j = 1, ..., 2^{n_A} \times 2^{n_A} \}$ is an ordered set of orthonormal vectors and constitute a basis set for the subspace $\mathcal{Q}$. In fact, applying the super-operator $\tilde{T}$ to both sides of eq.(30) the result is the vector $\mathcal{B}_j^Q = \frac{1}{\sqrt{2^{n-n_A}}} \mathcal{B}_j^I$.

With the vectors of the sets $S_j$ and $S_0$ it is possible to build up an orthonormal basis set for the kernel subspace $\mathcal{K}$, complementary to $\mathcal{Q}$. It is simple algebra to prove that the
following linear combination of all vectors $B_{rk}(j) \in S_j$

$$B_{1j} = \sum_{k=1}^{2^n-n_A} c_k B_{rk}(j)$$  \hspace{1cm} (31)

with $c_k = \frac{1}{2^n-n_A-1}$; $k = 1, \ldots, 2^{n-n_A} - 1$ and $c_{2^{n-n_A}} = -1$, is applied on 0 by the super-operator $\bar{T}$.

Making all the cyclic permutations of the last $2^{n-n_A} - 1$ coefficients $c_k$ of eq.(31) it is possible to generated $2^{n-n_A} - 1$ different vectors $B_{lj}$ with $l = 1, \ldots, 2^{n-n_A} - 1$. The vectors of each set $C_j = \{B_{lj}; l = 1, \ldots, 2^{n-n_A} - 1\}; (j = 1, \ldots, 2^n \times 2^n)$, are orthogonal to the vectors of the basis-$\mathcal{B}^Q$ and to the vectors of the set $S_0$.

The vectors of each set $C_j$ are not mutually orthogonal. They can be transformed in an set of orthonormal vectors, $C_j^{\perp}$, by applying to each set $C_j$ the Gram-Schmidt algorithm.

Giving all these properties of the vector sets $S_0$ and $C_j^{\perp}$, it is now clear that the following union of sets

$$S_0 \cup_{j=1}^{2^n \times 2^n} C_j^{\perp}$$  \hspace{1cm} (32)

is an orthonormal basis set for the kernel subspace $\mathcal{K}$. Applying an appropriate ordering algorithm to the vectors given by (32) we obtain an ordered set of orthonormal vectors $\mathcal{B}^K = \{B^K_r; r = 2^n \times 2^n + 1, \ldots, 2^n \times 2^n\}$.

Let $\mathcal{B}^C = \{B^C_r; r = 1, \ldots, 2^n \times 2^n\}$ be the ordered orthonormal computational basis set in $\mathcal{L}_{H_L^2}$. This basis set is related to the orthonormal basis set $\mathcal{B}^Q \cup \mathcal{B}^K$ through the equations

$$B^C_i = \sum_{s=1}^{2^n \times 2^n} \bar{c}^Q_{si} B^Q_s; \hspace{1cm} B^K_i = \sum_{s=1}^{2^n \times 2^n} \bar{c}^K_{si} B^Q_s$$  \hspace{1cm} (33)

where $\bar{c}^Q_{si}$; $(i = 1, \ldots, 2^n \times 2^n; s = 1, \ldots, 2^n \times 2^n)$ and $\bar{c}^K_{si}$ $(i = 2^n \times 2^n + 1, \ldots, 2^n \times 2^n; s = 1, \ldots, 2^n \times 2^n)$ are the elements of the transition matrix $\bar{C}$ from the basis-$\mathcal{B}^C$ to the basis-$\mathcal{B}^Q \cup \mathcal{B}^K$. The action of $\bar{U}$ relative to the $\mathcal{B}^C$-basis is

$$\bar{U}'(B_j) = \sum_{i=1}^{2^n \times 2^n} \bar{u}'_{ij} B_i$$  \hspace{1cm} (34)
where \( \bar{u}_{ij}' = (\bar{U}'(B_j), B_i) = Tr\{\bar{U}'(B_j)B_i\} \) are the elements of \( \bar{U} \) relative to this basis set. If \( \bar{U}' \) is the matrix of the super-operator \( \bar{U} \) relative to the \( B^C \)-basis, then

\[
\bar{U} = \bar{C}^{-1}\bar{U}'\bar{C}
\]

is the matrix of the same super-operator relative to the basis-\( B^Q \cup B^K \). The matrix \( \bar{U} \) given by eq.(35), is the one that must be used to compute the matrices \( \bar{U}^{QQ} \) and \( \bar{U}^{KQ} \) of eqs.(18) and (21).
References

[1] C. Moore and J. Crutchfield. Quantum automata and quantum grammars. *Theoretical Computer Science*, 237, pages 275-306 (2000).

[2] A. Kondacs and J. Watrous. On the power of quantum finite state automata. *In Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, pages 66-75 (1997).

[3] A. Ambainis and R. Freivalds. 1-way quantum finite automata: strenghts, weaknesses and generalizations. *In Proceedings of 39th Annual Symposium of Foundations of Computer Science*, pages 332-3341, (1998).

[4] H. Nishimura and T. Yamakami. An application of quantum finite automata to quantum proof systems. quant-ph/0410040.

[5] A. Ambainis and A. Kikusts, Exact results for accepting probabilities of quantum automata, quant-ph/0109136v2.

[6] T. L. Booth. *Sequential machines and automata theory*, John Wiley and Sons (1967).

[7] A. Ambainis and J. Watrous. Two-way finite automata with quantum and classical states. *Theoretical Computer Science*, 287 (1), pages 299-311 (2002).

[8] A. Paz. *Introduction to probabilistic automata*, Academic Press, New York (1971).

[9] M. O. Rabin. Probabilistic Automata. *Info. Control*, 6, pages 230-245 (1963).

[10] D. Aharonov, A. Kitaev and N. Nisan. Quantum circuits with mixed states, *In Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 20-30 (1998), also in quant-ph9806029.

[11] A. Ambainis, A. Nayak, A. TA-Shma and U. Vazirani. Dense quantum coding and quantum finite automata, *In Proceedings of the 31th Annual ACM Symposium on Theory of Computing*, pages 376-383 (1999). Also in quant-ph/9804043 v2.
[12] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacker. On quantum coding for ensembles of mixed states, quant-ph/0008024 (2000).

[13] C. Cohen-Tannoudji, B. Diu, F. Laloë Quantum Mechanics I, Academic Press, New York (1996).

[14] John Preskill, Lecture Notes for Physics 229: Quantum Information and Computation, California Institute of Technology. Available at http://theory.caltech.edu/people/preskill/ph229, (1998).

[15] K. Kellig and K. Kraus, Comm. Mathematical Phy., 16, 142, (1970). M. A. Nielsen and I. L. Chuang Quantum Computation and Quantum Information, Cambridge University Press, U.K. (2002).

[16] P. R. Halmos, Finite-dimensional vector-spaces, Springer-Verlag, New-York (1987).

[17] D. J. Shepherd, T. Franz and R. F. Werner, Phys. Rev. Lett. 97, 020502 (2006).

[18] B. Schumacher and R. F. Werner, quant-ph/0505174v1 (2004).