Applied Mathematics & Information Sciences – An International Journal ©2011 NSP

Irreversibility in Quantum Computational Logics

Giuseppe Sergioli, Roberto Giuntini, Francesco Paoli Department of Education, University of Cagliari *Email Address: paoli@unica.it*

Received June 22, 2009; Revised March 21, 2010; Accepted May 02, 2010

In this paper we discuss an approach to quantum computation where the basic information units (qubits and quregisters) are replaced by density operators and the restriction to unitary operators as logical gates is lifted through the introduction of the more general concept of *quantum operation* ([17], [1]). This perspective is especially suited to provide a physical description of open systems. In particular, we illustrate the advantages of this approach over the standard one and show that it can account for two important irreversible transformations already considered in the literature: the irreversible conjunction IAND and the fuzzy-like Łukasiewicz disjunction \oplus .

Keywords: Quantum computational logics, quantum operations, irreversible connectives.

1 Introduction

At first sight, it would seem as though irreversibility did not fit in very well with quantum computation: one of the most evident advantages of the latter, when compared to classical computation, is given by the fact that its reversible gates allow us to trace the evolution of a system during the computation process with no loss of information whatsoever. Indeed, investigations in mainstream quantum computation have prevailingly considered computational situations for which this description pattern is adequate ([?], [12], [10]). However, as we will discuss below, there are phenomena that can be hardly accounted for if we keep to the standard paradigm: decoherence, noise, measurements in the middle of a computation - roughly put, any computational process that involves an interaction with an *environment* of sorts - call into play an unavoidable loss of information that renders the process itself irreversible. To conveniently describe such situations, alongside with the kind of processes that are dealt with by the standard approach, a new, more comprehensive perspective has been recently developped in quantum computation (see e.g. [17], [1]). The

Giuseppe Sergioli et al.

aim of this paper is to survey this new approach and to describe some original applications of such.

In particular, in Section 2 we review the basics of the standard approach to quantum computation. In Section 3 and in Section 4 we introduce a different framework, where the basic information units (qubits and quregisters) are replaced by density operators and the restriction to unitary operators as logical gates is lifted in favour of a more liberal attitude which leads to the introduction of the more general concept of *quantum operation*. We also mutually compare both frameworks and contend that the latter has a decisive edge over the former. Section 5 is devoted to the development of a logical perspective on quantum computation. Finally, in Section 6, building upon previous work by our research group, we show that the quantum operations framework can account for two important irreversible transformations already considered in the literature: the irreversible conjunction IAND and the fuzzy-like Łukasiewicz disjunction \oplus . We show, in fact, that the IAND connective is expressible through a quantum operation via Kraus' Theorem, while the Łukasiewicz disjunction can be approximated by means of a special class of quantum operations.

2 The standard approach to quantum computation

In this section we shall try to bridge the current formal models of quantum computational theory [?] - proceeding via quantum gates operating on pure states - and a novel approach according to which:

- the carriers of information need not be pure states, but, more generally, density operators (*qumixes*) ([?], [?]);
- the operations acting thereupon need not be unitary operators ([1], [16], [?], [?]).

It is well-known that in quantum mechanics a physical system is associated to a Hilbert space \mathcal{H} . Any pure state of the system, mathematically represented by a unit vector of \mathcal{H} , is a maximal information quantity, i.e. a piece of information on the physical system that could not be consistently augmented by any further observation.

Let us first consider a simple physical system S whose associated Hilbert space is \mathbb{C}^2 . Let $\mathcal{B} = \{|0\rangle, |1\rangle\}$ be the orthonormal canonical basis of \mathbb{C}^2 . In this simple case, the general form of a pure state $|\psi\rangle$ is

$$a \left| 0 \right\rangle + b \left| 1 \right\rangle$$
,

where a and b are complex numbers which, in virtue of the unitarity hypothesis, must abide by the condition $|a|^2 + |b|^2 = 1$. In the quantum computational parlance, the vector $|\psi\rangle$ is called *qubit* and acts as the quantum counterpart of the classical bit. As dictated by the Born rule, $|a|^2$ yields the probability that $|\psi\rangle$ is detected in the state $|0\rangle$ as the outcome of a possible measure, and dually for $|b|^2$ and $|1\rangle$. Logically speaking, $|0\rangle$ and $|1\rangle$ can be naturally interpreted as meaning "falsity" and "truth", respectively; in accordance with this convention, $|a|^2$ (respectively, $|b|^2$) can be read as the probability that $|\psi\rangle$ is false (respectively, true).

Switching to spherical coordinates, the general form of a qubit $|\psi\rangle$ can be written also as

$$|\psi\rangle = e^{i\xi} \left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

where the global phase factor $e^{i\xi}$ can be omitted since it has no observable effect. By varying the values of θ and ϕ , we are in a position to induce a bijective correspondence between qubits and surface points of the Bloch-Poincaré sphere. This circumstance suggests the geometric representation of Fig. 1.



Figure 2.1: The Bloch-Poincaré sphere.

Observe that orthogonal vectors in \mathbb{C}^2 need not be orthogonal vectors in the Bloch-Poincaré representation: orthogonal vectors in \mathbb{C}^2 , in fact, are geometrically represented by unit vectors having opposite directions.

Scientific investigation, however, often requires a mathematical representation not just of a simple physical system, but rather of a number of physical systems interacting with one another. Suppose, then, that the physical system S is composed by n (sub-)systems, say $S_1, ..., S_n$. Let \mathcal{H}^{S_i} be the Hilbert space associated to S_i , for $1 \le i \le n$. The space \mathcal{H} associated to S will be the tensor product $\mathcal{H}^{S_1} \otimes \cdots \otimes \mathcal{H}^{S_n}$ of the spaces associated to $S_1, ..., S_n$. If $S_i = S_j$ for every i, j, we resort to the notation $\otimes^n \mathcal{H}^{S_i}$ in place of \mathcal{H}^{S_i} Giuseppe Sergioli et al.

 $\otimes \cdots \otimes \mathcal{H}^{S_i}.$

As we have seen, qubits "live" in the space \mathbb{C}^2 . *Quregisters* are the tensor product analogues of qubits: by quregister, in fact, we mean any unit vector in $\otimes^n \mathbb{C}^2$. Quregisters are the quantum counterpart of classical registers - i.e. finite strings of bits.

We will call any unit vector of the form $|\phi\rangle = |x_1, ..., x_n\rangle$ of $\otimes^n \mathbb{C}^2$ an *n*-configuration, where $x_1, ..., x_n$ are variables ranging over the set $\{0, 1\}$. It is not hard to see that one can identify each *n*-configuration with a natural number $i \in [0, 2^n - 1]$, for $i = 2^{n-1}x_1 + 2^{n-2}x_2 + ... + x_n$. Intuitively, any *n*-configuration can be read as a natural number in its binary codification. In other words, one can concisely express a quregister $|\phi\rangle$ as

$$|\phi\rangle = \sum_{j=0}^{2^n - 1} c_j || j\rangle\rangle$$

where c_j is a complex number, $||j\rangle$ is the *n*-configuration corresponding to the number *j*, and $\sum_{j=0}^{2^n-1} |c_j|^2 = 1$. Let $\Re(\otimes^n \mathbb{C}^2)$ be the set of all quregisters of $\otimes^n \mathbb{C}^2$. We denote by

$$\mathfrak{R}:=igcup_{n=1}^{\infty}\left(\mathfrak{R}\left(\otimes^{n}\mathbb{C}^{2}
ight)
ight)$$

the set of all quregisters in \mathbb{C}^2 or in a tensor product of \mathbb{C}^2 . Summing up, a quregister is a pure state either of a simple (2-dimensional) or of a compound physical system.

Like in the classical case, also in quantum computation the evolution of a state is described by the application of a *gate* to a register (alternatively, if we adopt a logical perspective, we can see registers as sentences and gates as logical connectives). In the standard presentation of classical computation, a gate is an *irreversible* function $f : \{0,1\}^n \rightarrow \{0,1\}$: it is not possible to retrieve the values of the inputs by a sheer analysis of the output. In other words, we are in no position to trace a state resulting from the application of a gate back to the initial states to which the gate had been applied. On the other hand, in quantum computation gates are *unitary* operators¹ mapping *n*-tuples of quregisters into quregisters.

Because of the unitarity constraint, quantum gates are always *reversible*. Classical gates, as we have observed, generally fail to be such. Note that, however, any irreversible function $f : \{0,1\}^m \to \{0,1\}^n$ can be transformed into a reversible function $\tilde{f} : \{0,1\}^{m+n} \to \{0,1\}^{n+m}$ such that: $\forall x_1, ..., x_n, x_{n+1}, x_{n+m}$

$$\widetilde{f}(x_1, ..., x_n, x_{n+1}, x_{n+m}) = (x_1, ..., x_n, f(x_{1,..., x_m}) + (x_{m+1} ... x_{m+n}))$$

where $\hat{+}$ is the (*componentwise*) sum modulo 2. By way of example, consider the classical And truth table. It is immediate to see that it represents a typical many-to-one

¹An operator U is unitary whenever $UU^+ = U^+U = \mathbb{I}$, where U^+ is the adjoint of the operator U and \mathbb{I} is the identity operator.

irreversible transformation f:

From f we can obtain its reversible match $\tilde{f}: \{0,1\}^3 \to \{0,1\}^3$, called *classical Toffoli* gate. If we set to 0 the third component of the input, we encode in a reversible way the behaviour of the classical binary conjunction:

Observe that the third coordinate of each input (called the *ancilla bit*) plays no role other than guaranteeing that inputs and outputs have the same lengths.

The quantum generalisation of the classical Toffoli gate (denoted by $T^{(n,m,1)}$) can be naturally defined in the following way:

Definition 2.1. For any $n, m \ge 1$, the *Toffoli* gate is the unitary operator $T^{(n,m,1)}$ such that, for every element $|x_1, ..., x_n\rangle \otimes |y_1, ..., y_m\rangle \otimes |z\rangle$ of the computational basis $\mathcal{B}^{(n+m+1)}^2$ (shortened as $|x\rangle \otimes |y\rangle \otimes |z\rangle$),

$$T^{(n,m,1)}(\ket{x}\otimes\ket{y}\otimes\ket{z})=\ket{x}\otimes\ket{y}\otimes\ket{x_ny_m+z}.$$

For instance, $T^{(1,1,1)}$ trasforms any factorised vector $|x\rangle \otimes |y\rangle \otimes |z\rangle$ into the vector obtained by leaving the first two factors (referred to as the *control bits*) unchanged, while replacing $|z\rangle$ (the *target bit*) by $|xy + z\rangle$.

Similary to the classical case, we can define a quantum version of And in the following way:

$$\{|x_1, ..., x_n\rangle : x_i \in \{0, 1\}\}.$$

²We call *computational basis*, using the symbol $\mathcal{B}^{(n)}$, the orthonormal basis for the space $\otimes^{n} \mathbb{C}^{2}$ given by the set of all *n*-configurations

Definition 2.2. (the quantum And):

And
$$(|\psi\rangle \otimes |\varphi\rangle) = T^{(1,1,1)}(|\psi\rangle \otimes |\varphi\rangle \otimes |0\rangle).$$

Restricting ourselves to $\mathcal{B}^{(3)}$, the computational basis of $\otimes^3 \mathbb{C}^2$, we obtain the following reversible table, where the target bits represent just the values of the classical conjunction truth table:

$ 000\rangle$	\rightarrow	$ 000\rangle$
$ 001\rangle$	\rightarrow	$ 001\rangle$
$ 010\rangle$	\rightarrow	$ 010\rangle$
$ 011\rangle$	\rightarrow	$ 011\rangle$
$ 100\rangle$	\rightarrow	$ 100\rangle$
$ 101\rangle$	\rightarrow	$ 101\rangle$
$ 110\rangle$	\rightarrow	$ 111\rangle$
$ 111\rangle$	\rightarrow	$ 110\rangle$.

3 From quregisters to density operators

The only situations we have been considering so far are cases of applications of quantum gates to pure states which yield, in a reversible way, quregisters as outputs. However, more often than not either we lack a *complete knowledge* about the physical systems we are investigating, or such systems are not isolated from the rest of the universe. Evidently, quregisters are not the appropriate tools for a correct mathematical description of what is going on in such cases as these.

In actual practice, a prepared state seldom corresponds to a pure state. Let us consider the simplest case of an observable (i.e. a self-adjoint operator) A whose spectral decomposition is $\sum_{k=1}^{m} a_k P_{|\psi_k\rangle}$, where $P_{|\psi_k\rangle} := |\psi_k\rangle \langle \psi_k|$ is the projection operator onto the span of $|\psi_k\rangle$. The real numbers a_k represent the possible values that A may assume. If the physical system is in a pure state $|\psi_j\rangle$, the probability of getting the result a_k is $p_k = |\langle \psi_a | \psi \rangle|^2$.

In general, however, the preparing instrument fluctuates in such a way that successive preparations of the system may correspond to different states. Suppose that $|\psi\rangle$ is prepared with relative frequency s_k ($s_k > 0$, $\sum_k s_k = 1$). Then, the probability value p_k should be replaced by the following expression:

$$\sum_{k=1}^{m} s_{k} \left| \left\langle \psi \mid \psi_{k} \right\rangle \right|^{2} = \sum_{k=1}^{m} s_{k} \left\langle \psi \mid \psi_{k} \right\rangle \cdot \left\langle \psi_{k} \mid \psi \right\rangle^{*}$$
$$= \left\langle \psi \right| \sum_{k=1}^{m} s_{k} \left| \psi_{k} \right\rangle \left\langle \psi_{k} \right| \psi \right\rangle$$
$$= \left\langle \psi \mid \rho \mid \psi \right\rangle$$

where

$$\rho = \sum_{k=1}^{m} s_k \left| \psi_k \right\rangle \left\langle \psi_k \right|.$$

It turns out that ρ is a density operator, where:

Definition 3.1. A density operator is a non-negative self-adjoint operator of trace 1.

In quantum computational jargon, a density operator in $\otimes^n \mathbb{C}^2$ is called *qumix*. We will denote the set of all density operators in $\otimes^n \mathbb{C}^2$ by $\mathfrak{D}(\otimes^n \mathbb{C}^2)$. The density operator ρ of our example represents a mixed state of all possible pure states $|\psi_k\rangle$, each with weight equal to s_k . It does no harm to formulate quantum mechanics in terms of density operators only [9], since pure states are special cases of density operators in that every pure state $|\psi_k\rangle$ uniquely determines a density operator $P_{|\psi\rangle}$ (more on that will be said presently). In what follows, we will consider these two alternative but equivalent formulations as different viewpoints on (or rather descriptions of) pure quantum states, calling them, respectively, *quregister world* and *qumix world*. The term "world", as a matter of fact, should be understood as devoid of any metaphysical connotation: the same pure state can be seen as an object in the quregister world (the unit vector $|\psi\rangle$) or as an object in the qumix world (the corresponding projection operator $P_{|\psi\rangle}$).

Why do qumixes matter to quantum computation? As hinted in our Introduction, and as discussed more amply in [1], there are several phenomena (such as measurements in the middle of a computation, noise, or decoherence) that are very difficult or even impossible to account for in the usual unitary approach to the subject. On the other hand, the non-unitary (i.e. irreversible) approach can adequately deal with them. In fact, although quantum computations may allow measurements in the middle of a computation, the state of the computation after such a measurement is a mixed state. Moreover, noise and, in particular, decoherence are serious obstacles for the implementation of quantum computer devices. These phenomena are modelled by non-unitary operations that turn pure states into mixed states.

A set of quregisters can be used in order to generate, by convex combination, the set of all mixed states. Formally:

Theorem 3.1. For every density operator ρ , there exists an orthonormal sequence of quregisters $|\psi_i\rangle$ and a sequence of real numbers λ_i with $\sum_i \lambda_i = 1$, s.t. $\rho = \sum_i \lambda_i P_{|\psi_i\rangle}$.

In general, however, this representation is by no means unique. Actually, a density operator with degenerate eigenvalues can be decomposed in infinitely many ways by using sequences of orthonormal vectors [2].

This failure to admit a unique decomposition entails the untenability of an epistemic interpretation of mixed states. If, in fact, we were to interpret the representation $\lambda P_{|\psi_1\rangle} + (1-\lambda) P_{|\psi_2\rangle}$ of ρ as "the system we are considering is either in the state $|\psi_1\rangle$ or in the state $|\psi_2\rangle$, but we lack a complete knowledge about it", then a different representation $\overline{\lambda}P_{|\overline{\psi_1}\rangle} + (1-\overline{\lambda}) P_{|\overline{\psi_2}\rangle}$ of the same density operator could by full right be interpreted as "the system is either in the state $|\overline{\psi_1}\rangle$ or in the state $|\overline{\psi_2}\rangle$, but we lack a complete knowledge about it", which is absurd. On the contrary, ρ represents a state which is different from $|\psi_1\rangle$, $|\psi_2\rangle, |\overline{\psi_1}\rangle$ or $|\overline{\psi_2}\rangle$.

Let us give a physical exemplification of mixed states. As is well known, the polarisation state of a photon through a density operator is represented as a linear combination of the pure states P_{θ}^{up} and P_{θ}^{down} :

$$\rho = \lambda P_{\theta}^{up} + (1 - \lambda) P_{\theta}^{down},$$

where θ is an arbitrary direction. The possible values of λ induce a bijection between such convex combinations and the real interval [0, 1]; in particular, if λ assumes the extreme values of the interval, ρ collapses onto one of the projection operators P_{θ}^{up} (for $\lambda = 1$) and P_{θ}^{down} (for $\lambda = 0$). From a physical viewpoint, such pure states express the fact that the photon is *completely polarised* in the state P_{θ}^{up} or in the state P_{θ}^{down} , respectively. Of course P_{θ}^{up} and P_{θ}^{down} represent pure states, being projection operators. With the exception of these limiting cases, in all the other linear combinations both coefficients are nonzero physically, this means that our photon is not completely polarised.

It is possible to provide a geometrical insight into the qumix world (at least for qumixes of \mathbb{C}^2) just as we did for the quregister world. Recall from [2] that the Pauli matrices σ_1 , σ_2 and σ_3 and the identity matrix I form a basis for the space of all operators of \mathbb{C}^2 . If we write an operator as a linear combination of these basis elements, its trace coincides with the coefficient of the identity matrix ($\frac{1}{2}$ acts as a normalisation coefficient). Consequently, every density operator ρ of \mathbb{C}^2 can be written as

$$\rho = \frac{1}{2} \left(r_1 \sigma_1 + r_2 \sigma_2 + r_3 \sigma_3 + I \right)$$

with $r_1^2 + r_2^2 + r_3^2 \le 1$. Once again, therefore, we get a bijective correspondence with the Bloch-Poincaré sphere; density operators, however, may correspond not only to surface points of this sphere, but to inner points as well. A simple proof can show that, if we

represent the density operator ρ of \mathbb{C}^2 in the form $\lambda P_{|\psi_1\rangle} + (1 - \lambda) P_{|\psi_2\rangle}$, the idempotency property of projection operators implies that $r_1^2 + r_2^2 + r_3^2 = 1$ whenever $\lambda = 1$ or $\lambda = 0$; in all the remaining cases, on the other hand, $r_1^2 + r_2^2 + r_3^2 < 1$.

In this geometrical perspective, a vector corresponds to a maximal information bit according as it reaches the surface of the sphere or not. In detail: if the length of the vector in the three-dimensional sphere is 1, then we have: i) $r_1^2 + r_2^2 + r_3^2 = 1$; ii) a surface point on the sphere; iii) a pure state; iv) a maximal piece of information. If its length is less than 1, then we have: i) $r_1^2 + r_2^2 + r_3^2 < 1$; ii) an inner point of the sphere; iii) a mixed state; iv) a non-maximal piece of information. For all these reasons, it is appropriate to claim that density operators are generalisations of quregisters: every qubit is a particular case of qumix, and this holds not only for \mathbb{C}^2 but also for tensor product spaces with a finite but otherwise arbitrary number of dimensions.



Figure 3.2: The Bloch-Poincaré sphere and the three-dimensional sphere: two different representations, in \mathbb{C}^2 and \mathbb{R}^3 respectively, of quantum information quantities.

It is easy to see how every unit vector in the Bloch-Poincaré sphere is the counterpart of a projection operator.

4 From quantum gates to quantum operations

In the preceding section we have described the quantum counterpart of classical bits and classical gates and we have pondered the advantages of resorting to density operators rather than unit vectors in the description of some physical systems, such as e.g. open systems. In general, an open physical system can be regarded as the result of the interaction between a principal system and an *environment*. This new resulting system can be finally considered as a closed system. Formally speaking, if ρ is the density operator associated with the principal system and ρ_{env} is the density operator associated with the environment, we represent the compund system-environment state by means of the tensor product state $\rho \otimes \rho_{env}$ ³, because of the fact that ρ and ρ_{env} are coupled with each other. Let us now consider a particular input state $\rho \otimes \rho_{env}$, and let U be a transformation acting on the same system-environment state. If we want to focus on the principal state ρ , we have to *trace out* the environment state by means of an operation ϵ that can be mathematically described as the *partial trace*⁴ over ρ_{env} .

The resulting state ρ' (called *reduced state*) of the principal system after the transformation U has been applied is given by:

$$\epsilon(\rho) = tr_{env}[U(\rho \otimes \rho_{env})U^+] \tag{4.1}$$

where tr_{env} is short for $tr_{\mathcal{H}}$, \mathcal{H} being the space where ρ_{env} "lives". The partial trace is a particular example of *quantum operation*:

Definition 4.1. A quantum operation is a trace preserving, completely positive linear map from linear operators to linear operators in a finite-dimensional Hilbert space, which outputs a density operator whenever it is applied to a density operator. ⁵

All the requirements which collectively make up Definition 4.1 amount to the preservation of some important feature:

- a quantum operation is a map *which outputs a density operator whenever it is applied to a density operator.* Since density operators are self-adjoint, this means that in this case both the inputs and the outputs of a quantum operation have real eigenvalues;
- a quantum operation is a *trace preserving map*: as a consequence, probabilities are preserved;
- a quantum operation is a *linear map*, that is a map which preserves linear combinations. This requirement is crucial since, given that any mixed state can be expressed as a linear combination of pure states, a quantum operation applied to a mixed state will transform a linear combination of states into another linear combination of pure states.
- a quantum operation is a *completely positive map*, and so it preserves positivity, extending it to an arbitrary number of dimensions.

³As Nielsen and Chuang point out [?], although it is not possible, in general, to assume that the system and the environment start in product state, in many cases of practical interest it is reasonable to do so.

⁴Suppose \mathcal{H} and \mathcal{K} are finite-dimensional Hilbert spaces. For any Hilbert space \mathcal{H} let $L(\mathcal{H})$ be the space of linear operators on \mathcal{H} . The *partial trace* over \mathcal{H} is the linear operator $tr_{\mathcal{K}} : L(\mathcal{H} \otimes \mathcal{K}) \to L(\mathcal{H})$ such that for all $P \in L(\mathcal{K})$, and for all $Q \in L(\mathcal{K})$, $tr_V(P \otimes Q) = Ptr(Q)$.

⁵A map A on a n-dimensional Hilbert space \mathcal{H} is completely positive if: i) it is positive, meaning that $0 \leq \langle \psi_i | A | \psi_i \rangle$ for all $| \psi_i \rangle$; ii) for all natural numbers m, the extended map $I_m \otimes A$ (where I_m is the m-dimensional identity matrix) is also positive.

A neat characterisation of quantum operations is due to Kraus [17], who proved the following result (known as *Kraus representation theorem*):

Theorem 4.1. Let A be an operator on $L(\mathcal{H})$. Then A is a quantum operation iff there exist a set of operators $\{A_i\}$ on \mathcal{H} s.t.:

- 1. $\sum_{i} A_i^+ A_i = I;$
- 2. for every density operator ρ , $A(\rho) = \sum_{i} \widehat{A}_{i}(\rho)$, where $\sum_{i} \widehat{A}_{i}(\rho) = \sum_{i} (A_{i}\rho A_{i}^{+})$.

In other words, an operator whose arguments are themselves operators is a quantum operation just in case it is expressible, when applied to density operators, as the sum of extensions of operators which are "similar enough" (in the sense of item 1. in Theorem 4.1) to quantum gates. This result will prove of fundamental importance for the approximation results in the next section.

In the light of what we have just said, let us rewrite Equation 4.1 in terms of such a representation.

Let $|e_k\rangle$ be an orthonormal basis for the finite-dimensional state space of the environment and let $\rho_{env} = |e_0\rangle\langle e_0|$ be the initial state of the environment. Equation 4.1 can be rewritten as

$$\rho' = \epsilon(\rho)$$

= $\sum_{k} \langle e_k U[\rho \otimes |e_0\rangle \langle e_0] U^+ |e_k\rangle$
= $\sum_{k} E_k \rho E_k^+,$

where $E_k = \sum_k \langle e_k | U | e_0 \rangle \langle e_0 |$. Observe that the last equation is a restatement of Equation 4.1 in terms of operators on the principal system Hilbert space only. The elements of the set E_k are known as operation elements for the quantum operation ϵ . From the trace-preserving requirement $(tr(\epsilon(\rho)) = 1)$ it follows that: $1 = tr(\epsilon(\rho)) = tr(\sum_k E_k \rho E_k^+) = tr(\sum_k E_k^+ E_k \rho)$ which imply $\sum_k E_k^+ E_k = I$, that is the so-called *completeness relation* holds. It should be noticed, however, that whenever measurement processes come into play, the trace-preserving requirement generally fails. In these cases we do not have a complete knowledge about the system: formally $tr(\epsilon(\rho)) < 1$, therefore $\sum_k E_k^+ E_k < I$ [17].

The main feature of the operation sum representation is that it characterises the dynamics of the principal system while dispensing us from explicitly considering properties of the environment: all we need to know is which elements of the set of operators E_k act on the principal system alone. For, this representation allows us to choose, among a number of different environment interactions, the one that contains no irrelevant information about Giuseppe Sergioli et al.

other systems. The operation sum representation provides therefore a useful mathematical description of the interaction between system and environment. Still, it would be interesting to gain some insight into the converse problem: given a set of operators E_k , is there any reasonable model of an environmental system and the related dynamics which gives rise to a quantum operation having E_k as its operation elements? Interestingly, Nielsen and Chuang [?] have proved that for any quantum operation ϵ , where E_k are the corresponding operation elements, there exists a model environment E, whose initial state is the pure state $|e_0\rangle$, and model dynamics by a unitary operator U and projector P onto E such that $\epsilon(\rho) = tr_E(PU(\rho \otimes |e_0\rangle\langle e_0|)U^+P)$. In order to properly appreciate the difference between quantum operations and quantum gates, it may be expedient to briefly comment on the main properties of the former. The trace class requirement $(0 \le tr(\epsilon(\rho)) \le 1$ for any ρ) is there because $tr(\epsilon(\rho))$ represents the probability that the measurement outcome described by ϵ occurs given the initial state ρ . Let us just observe that, as a special case, if our quantum operation ϵ is trace-preserving we have that $tr(\epsilon(\rho)) = 1$. The linearity requirement can be easily justified by statistical arguments which rest on Bayes' Theorem [?]. Therefore, to round off our justification of the above definition, all we are committed to do is to give a motivation of the requirement that our map be completely positive. Given an observable U, the expectation value of U with respect to ρ is $tr(\rho U) = \sum_{i} p_i \langle \psi_i | U | \psi_i \rangle$. This observation easily implies that $\langle \psi_i | U | \psi_i \rangle$ must be positive. Why, however, should our map be completely positive? This constraint arises since it is highly desirable that a positive operator U on the principal system should remain positive whenever it is extended to the global system which includes the environment system as well. Let us now briefly recap the most important differences between quantum gates and quantum operations:

- Unlike quantum gates, quantum operations can be applied to mixed states: in fact, quantum operations admit density operators (that are, in general, mixed states) both as inputs and as outputs.
- The quantum operation model *includes* the quantum gate model. In fact, it is possible to extend in a natural way the action of quantum gates to density operators: for all unitary operators U ∈ H we can define an associated map Û from D(H) to D(H) in the following way: for any ρ ∈ D(H), Û(ρ) = UρU⁺. It follows from the fact that for any |ψ⟩, if U|ψ⟩ = |φ⟩ then UP_{|ψ⟩}U⁺ = P_{|φ⟩} that Û is an appropriate extension of U. It turns out that Û is a trace preserving quantum operation, called *unitary quantum operation*. Given a quantum gate U and a qubit |ψ⟩, U|ψ⟩ and Û(P_|ψ⟩) are statistically indistinguishable (i.e. Û|ψ⟩⟨ψ| = |Uψ⟩⟨ψU⁺|)⁶.
- The quantum operation model *properly* includes the quantum gate model. Quantum operations need not be unitary and therefore can represent irreversible physical

⁶It is easy to show that A and \widehat{A} perform the same rotation in the Bloch-Poincaré sphere.

phenomena. An example of non-unitary quantum operation is the partial trace introduced in footnote 4 and another interesting example will be introduced in the next section.

• Finally, a quantum gate is by definition an isometry, whereas a quantum operation generally fails to be norm preserving and may give rise to a loss of information. For example, pure states are not closed under the action of quantum operations. It may happen that a non-unitary quantum operation transform a pure state into a genuine mixed state.

5 Quantum computation: A logical perspective

The *quantum circuit with mixed states approach* has plenty of advantages over its main competitor: as Aharonov, Kitaev and Nisan [1] have proved, although this model is polinomially equivalent in computational power to the standard unitary model, it can solve several problems that cannot be disposed of in the unitary model - e.g. measurements in the middle of computation, noise, decoherence. In fact, the state of a computation after a measurement is generally a mixed state⁷, while quantum noise and decoherence are nonunitary operations as well.

Under this perspective, the quregister world appears even more just a fragment of the wider qumix world. The latter is all the more useful in that, beside providing us with an opportunity to give an account of the physical systems described in the former, it yields as a plus a formal description of irreversible operations on arbitrary mixed states.



In view of the above, it is all too natural to select as a basis for the convex body of density operators $\mathfrak{D}(\otimes^n \mathbb{C}^2)$ the two projection operators $P_{|0\rangle}$ and $P_{|1\rangle}$, here notated for

⁷The state of a system after the measurement is $\frac{M_n|\psi\rangle}{\sqrt{\langle\psi|M_n^+M_n|\psi\rangle}}$, where M_n is the measurement operator, satisfying the *completeness equation [?]:* $\sum_k M_k^+ M_k = I.$

short P_0 and P_1 , respectively. We come to select the class of density operators of the following form⁸:

$$\rho_{\lambda}^{n} = (1 - \lambda)k_{n}P_{o}^{n} + \lambda k_{n}P_{1}^{n}$$

where k_n is the parametrisation factor $\frac{1}{2^{n-1}}$ and $\lambda \in [0, 1] \subset \mathbb{R}$ ([?], [?], [?], [15]). Under this perspective, the probability that a density operator $\rho \in \mathfrak{D}(\otimes^n \mathbb{C}^2)$ is *true* (or *false*) is given by $p(\rho) = trP_1^n(\rho)$ (or $trP_0^n(\rho)$).

Assuming once again the logical perspective, one may wonder what is the import of widening the class of quantum computational connectives as we have done. A remarkable consequence of this liberalisation is the appearance of irreversible quantum computational counterparts of connectives belonging to well-known nonclassical logics. Before mentioning a few cases in point, let us establish a notational convention: henceforth, some quantum gates will be indicated with small Roman letters, while their extensions to density operators will be denoted by capital letters. For example, given the quantum negation gate Not, $NOT\rho$ will denote the operator Not ρ Not.

In the previous sections we have introduced the And gate as an example of reversible gate. Now we define two irreversible connectives:

Definition 5.1. (The irreversible conjunction *IAND*). If σ , τ are density operators,

$$IAND(\sigma,\tau) = \rho_{p(\sigma)p(\tau)}^{1}$$

IAND is irreversible for, if $\sigma \neq \overline{\sigma}, \tau \neq \overline{\tau}$ but $p(\sigma) = p(\overline{\sigma})$ and $p(\tau) = p(\overline{\tau})$, then $IAND(\sigma, \tau) = IAND(\overline{\sigma}, \overline{\tau})$. Some of the properties of IAND are summarised in the next

Lemma 5.1. 1. IAND is associative and commutative;

- 2. $IAND(\rho, P_0) = P_0;$
- 3. $IAND(\rho, P_1) = \rho_{P(\rho)};$
- 4. $p(IAND(\rho, \sigma)) = p(\rho)p(\sigma)$.

Proof. Straightforward application of the definitions.

Another example of irreversible connective is given by a quantum counterpart of the disjunction connective of Łukasiewicz logic [?]:

Definition 5.2. (The Łukasiewicz disjunction). If $\sigma \in \mathfrak{D}(\otimes^n \mathbb{C}^2)$ and $\tau \in \mathfrak{D}(\otimes^m \mathbb{C}^2)$ and θ is truncated sum (i.e. min(x + y, 1), for $x, y \in [0, 1]$),

$$\sigma \oplus \tau = \rho^1_{p(\sigma) \oplus p(\tau)}$$

⁸By P_0^n we refer to the extension of P_0 to the dimension *n*. In other words, $P_0^n = I^{n-1} \otimes P_0$.

The operation \oplus is also clearly irreversible: if $\sigma \neq \overline{\sigma}, \tau \neq \overline{\tau}$ but $p(\sigma) = p(\overline{\sigma})$ and $p(\tau) = p(\overline{\tau})$, then $\sigma \oplus \tau = \overline{\sigma} \oplus \overline{\tau}$. More than that, the unique reversible application of the Łukasiewicz disjunction turns out to arise when $\sigma = P_0^n$ and $\tau = P_0^m$. The following properties are easily seen to hold:

2.
$$p(\sigma \oplus \tau) = p(\sigma) \oplus p(\tau)$$



Figure 5.3: The Łukasiewicz function

6 Approximating irreversible connectives via quantum operations

Leaving aside the IAND for the moment, we remark from the outset that, for a logician, a connective like \oplus is appealing and puzzling at once:

- It is appealing, because it arises naturally within the mixed state approach and enjoys nice algebraic properties: in fact, it has been widely studied from a universal algebraic viewpoint (see for example [?], [?]). Moreover, it represents a promising bridge towards other more or less remote areas of logical research, like fuzzy logic.
- On the other hand, it is puzzling because it does not fit easily within the framework we have been establishing so far: not only it fails to be a quantum gate, but *it is not even a quantum operation*. This is easy to see, since any quantum operation must be in particular an operator, hence linear; and ⊕ is not such. It looks like even the more liberal approach we have adopted is not encompassing enough to let it in.

A justification for this irreversible connective is therefore in order, and the aim of this section is to provide some. The strategy we will follow is due to Hector Freytes and his

collaborators (partly published in [?]), and aims at giving a Stone-Weierstrass type approximation result via quantum operations. The upshot of this theorem is that, although these irreversible fuzzy-like connectives are not themselves quantum operations, they can be probabilistically approximated by means of such.

The Stone-Weierstrass theorem is one of the most celebrated results in complex analysis and general topology. In its simplest version, it says that every continuous complex-valued function on any bounded closed real interval can be approximated by means of polynomial functions (this much is due to Weierstrass; Stone generalised the result to any arbitrary compact Hausdorff space). In a more rigorous fashion, this theorem can be stated as follows:

Theorem 6.1. Let f be a continuous complex-valued function defined on the real interval [a,b]. For every $\epsilon \in \mathbb{R}^+$, there exists a polynomial function P over the complex field \mathbb{C} such that for any $x \in [a,b]$ we have $|f(x) - P(x)| < \epsilon$.

We are now about to examine a version of this theorem (cp. [?] for a more technical and compact presentation), yielding a probabilistical approximation of the connectives defined in Definitions 5.1 and 5.2 by means of polynomial quantum operations. The proofs of all the results contained in the present section are fully developed in [?]. Let us, however, proceed gradually. Our first goal is associating a polynomial quantum operation to each real polynomial; this can be done as follows. A generic real polynomial $P(x_1, ..., x_n)$ in n variables can be written in the form

$$\sum_{j=1}^{m} \prod_{i=1}^{n} a_j x_i^{\alpha_{ij}}$$

where $\max_j \max_i \{\alpha_{ij}\} = \deg(P)$ and $\alpha_{ij} \ge 0$. For example, if we fix $a_1 = 7, a_2 = 6, n = 3, m = 2$, and we let α_{ij} be the i, j entry in the following matrix:

$$\begin{pmatrix} 2 & 3 & 1 \\ 2 & 1 & 2 \end{pmatrix}$$

we obtain the polynomial

$$7x_1^2x_2^3x_3 + 6x_1^2x_2^1x_3^2.$$

We recall from the previous sections that every density operator ρ in \mathbb{C}^2 has the matrix representation $\frac{1}{2}(r_1\sigma_1 + r_2\sigma_2 + r_3\sigma_3 + I)$. Expanding and letting $\alpha = \frac{1-r_3}{2}, \beta = \frac{r_1-ir_2}{2}$, we get

$$\frac{1}{2} \begin{pmatrix} 1+r_3 & r_1-ir_2\\ r_1+ir_2 & 1-r_3 \end{pmatrix} = \begin{pmatrix} 1-\alpha & \beta\\ \beta^* & \alpha \end{pmatrix}$$

Now, matrices of the above form have an interesting property. If $A_1, ..., A_n$ are such matrices, upon replacing each scalar α by a variable x_i $(i \leq n)$, the diagonal elements of

the tensor product matrix

$$A = (\otimes_k A_1) \otimes \cdots \otimes (\otimes_k A_n)$$

are the members of the set

$$D_k(x_1, ..., x_n) = \{(1 - x_1)^{\alpha_1} x_1^{\beta_1}, ..., (1 - x_n)^{\alpha_n} x_n^{\beta_n} : \alpha_i + \beta_i = k, i \in \{1, ..., n\}\}$$

For any set of variables $\{x_1, ..., x_n\}$, monomials in $D_k(x_1, ..., x_n)$ are better behaved than garden variety monomials $\prod_{i=1}^n ax_i^{\alpha_i}$. However, each such monomial can be represented in terms of monomials in $D_k(x_1, ..., x_n)$. In fact, we have the following

Lemma 6.1. Let $\{x_1, ..., x_n\}$ be a set of variables and let $\prod_{i=1}^n a x_i^{\alpha_i}$ be a monomial. Let moreover k be a natural number s.t. $k \ge \sum_{i=1}^n \alpha_i$. Then

$$\prod_{i=1}^{n} a x_i^{\alpha_i} = \sum_{m \in D_k(x_1, \dots, x_n)} \delta_m m \text{ and}$$
$$1 - \prod_{i=1}^{n} a x_i^{\alpha_i} = \sum_{m \in D_k(x_1, \dots, x_n)} \gamma_m m,$$

where $\delta_m, \gamma_m \in \{0, 1\}$.

We now have all the ingredients we need to spell out the crucial definition of *polynomial quantum operation* associated to a polynomial.

Definition 6.1. Let $P(x_1, ..., x_n) = \sum_{j=1}^m \prod_{i=1}^n a_j x_i^{\alpha_{ij}}$ be a polynomial s.t.:

- 1. for every $j \leq m$, $\prod_{i=1}^{n} a_j x_i^{\alpha_{ij}} \in D_k(x_1, ..., x_n)$;
- 2. $0 \le P(x_1, ..., x_n) \le 1$ whenever $x_1, ..., x_n \in [0, 1]^n$.

The polynomial quantum operation P^* associated to P is the function:

$$P^*: \otimes^{nk} \mathfrak{D}(\mathbb{C}^2) arrow \otimes^{nk} \mathfrak{D}(\mathbb{C}^2)$$

Definition 6.2. s.t. for $\sigma_1, ..., \sigma_n$ in $\mathfrak{D}(\mathbb{C}^2)$ we have:

$$P^*((\otimes^k \sigma_1) \otimes \cdots \otimes (\otimes^k \sigma_n)) = (\frac{1}{2^{nk-1}} \otimes^{nk-1} I) \otimes \rho_{P(p(\sigma_1),\dots,p(\sigma_n))}$$

Giuseppe Sergioli et al.

This definition is far less complicated than it might seem at first sight: let us, then, take some of the mystery out of it and see what it boils down to. Let us be given a polynomial Pwhich has the following two characteristics: i) it is the sum of "well-behaved" monomials (by Lemma 6.1, this entails no loss of generality); ii) it outputs values in [0, 1] whenever all of its input values are in [0, 1]. To this polynomial we associate an operator P^* on $\otimes^{nk} \mathfrak{D}(\mathbb{C}^2)$ which, when applied to the argument $(\otimes^k \sigma_1) \otimes \cdots \otimes (\otimes^k \sigma_n)$ (for $\sigma_1, ..., \sigma_n$ in $\mathfrak{D}(\mathbb{C}^2)$), outputs the density operator whose probability of truth (in the above specified sense) is just the result of the application of the polynomial function P to the probabilities of $\sigma_1, ..., \sigma_n$ (appropriately lifted to the space having the "right" dimension via the tensor product with the normalised identity matrix $\frac{1}{2^{nk-1}} \otimes^{nk-1} I$).

The label we used in Definition 6.1 is not a misnomer. In fact, we have as a fundamental result that:

Theorem 6.2. Polynomial quantum operations are quantum operations.

Let us now reflect for a while on a special feature of the connectives IAND and \oplus . Both have the property that, if applied to a given pair of density operators σ, τ , their output is a density operator whose probability of truth is a *binary continuous function* of the probabilities of σ, τ . Abstracting away from these specific examples, we attain the following

Definition 6.3. Let $F : [0,1]^n arrow[0,1]$ be a continuous function. The *continuous quantum connective* associated to F is the function

$$F^*:\otimes^{nk}\mathfrak{D}(\mathbb{C}^2)arrow\mathfrak{D}(\mathbb{C}^2)$$

s.t. for $\sigma_1, ..., \sigma_n$ in $\mathfrak{D}(\mathbb{C}^2)$ we have:

$$F^*((\otimes^k \sigma_1) \otimes \cdots \otimes (\otimes^k \sigma_n)) = \rho_{F(p(\sigma_1),\dots,p(\sigma_n))}.$$

It is clear that, in general, continuous quantum connectives are not quantum operations. Nonetheless, they admit of a Stone-Weierstrass-style probabilistical approximation by means of quantum operations in the following sense: for every continuous quantum connective we can find a polynomial quantum operation which is "probabilistically indistinguishable" from it. More precisely:

Theorem 6.3. Let $F : [0,1]^n \operatorname{arrow}[0,1]$ be a continuous function, let F^* be the continuous quantum connective associated to F, and let $\mu = \min\{\min(1-F), \min(F)\}$. Then there exists a polynomial quantum operation $P^* : \otimes^{nk} \mathfrak{D}(\mathbb{C}^2) \operatorname{arrow} \otimes^{nk} \mathfrak{D}(\mathbb{C}^2)$ (associated to some polynomial function P) s.t. for every $0 < \epsilon \leq \mu$ there exists a constant M such that for every $\sigma = (\otimes^k \sigma_1) \otimes \cdots \otimes (\otimes^k \sigma_n)$ we have that:

$$|p(P^*(\sigma)) - \frac{1}{M}p(F^*(\sigma))| \le \epsilon.$$

We must, however, emphasise a disanalogy between the cases of the connectives IAND and \oplus . While the former complies with the conditions of Theorem 4.1 and can therefore be considered a quantum operation to all intents and purposes, rendering any recourse to Theorem 6.3 unnecessary, the latter fails to be such and can only be approximated by a polynomial quantum operation by means of Theorem 6.3 [?].

acknowledgement

We warmly thank Hector Freytes for his precious feedback concerning the topics of Section 6, as well as for providing the basic insights underlying the work described therein. The first author was funded by Regione Autonoma della Sardegna, PO Sardegna FSE- M.S 2007-2013, L.R. 7/2007.

References

- Aharonov, D., Kitaev, A. and Nisan, N., "Quantum circuits with mixed states", STOC '98: *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, ACM press, 1998, pp. 20-30.
- [2] Beltrametti E., Cassinelli G., *The Logic of Quantum Mechanics*, Vol. XV of *Encyclopedia of Mathematics and its Applications*, Addison-Wesley, Boston, 1981.
- [3] Bruzda W., Cappellini V., Sommers H.-J., Zyczkowski K., "Random quantum operations", *Phys. Lett. A*, 373, 3, 2009, pp. 320-324.
- [4] Cattaneo G., Dalla Chiara M. L., Giuntini R., Leporini R., "An unsharp logic from quantum computation", *International Journal of Theoretical Physics*, 43, 7-8, 2001, pp. 1803-1817.
- [5] Cattaneo G., Dalla Chiara M.L., Giuntini R., Leporini R., "Quantum computational structures", *Mathematica Slovaca*, 54, 2004, pp. 87-108.
- [6] Cignoli R., D'Ottaviano I.M.L., Mundici D., *Algebraic Foundations of Many-Valued Reasoning*, Kluwer, Dordrecht, 1999.
- [7] Dalla Chiara M.L., Giuntini R., Greechie R., *Reasoning in Quantum Theory*, Kluwer, Dordrecht, 2004.
- [8] Dalla Chiara M.L., Giuntini R., Leporini R., "Logics from quantum computation", *International Journal of Quantum Information*, 3, 2, 2005, pp. 293-337.
- [9] de Muynck W.M., Foundations of Quantum Mechanics: An Empiristic Approach, Springer, Berlin, 2002.

- [10] Deutsch D., "Quantum theory, the Church-Turing principle and the universal quantum computer", *Proceedings of the Royal Society of London*, Series A, Mathematical and Physical Sciences, 400, 1818, 1985, pp. 97-117.
- [11] Deutsch D., Barenco A., Ekert A., "Universality in quantum computation", *Computer Bulletin*, 449, 1995, pp. 669-677.
- [12] Feynman R., "Simulating physics with computers", *International Journal of Theoretical Physics*, 21, 6, 1982, pp. 467-488.
- [13] Freytes H., Sergioli G., Aricò A., "Representing continuous T-norms in quantum computation with mixed states", *Journal of Physics A*, Math. Theor. 43, 2010, 465306.
- [14] Giuntini R., Ledda A., Paoli F., "Expanding quasi-MV algebras by a quantum operator", *Studia Logica*, 87, 1, 2007, pp. 99-128.
- [15] Giuntini R., Ledda A., Sergioli G., Paoli F., "Some generalizations of fuzzy structures in quantum computational logic", *International Journal of General Systems*, forthcoming.
- [16] Kitaev A.Y., Shen A., Vyalyi M.N., *Classical and Quantum Computation*, AMS Bookstore, Boston, 2002.
- [17] Kraus K., States, Effects and Operations, Springer, Berlin, 1983.
- [18] Ledda A., Konig M., Paoli F., Giuntini R., "MV algebras and quantum computation", *Studia Logica*, 82, 2, 2006, pp. 245-270.
- [19] Leuchs G., "Partial measurement based quantum operations", *International Conference on Quantum Information*, Optical Society of America, 2008, paper QWD1.
- [20] Nielsen M., Chuang I., *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.
- [21] Reed M., Simon B., *Methods of Modern Mathematical Physics*, Vol. I, Academic Press, New York, 1972.



Giuseppe Sergioli is a post-doc researcher at the University of Cagliari and the topics of his research are quantum computation, quantum communication and quantum Logics. He obtained his M.Sc. in theoretical physics from the University of Catania and was awarded the prize S. Notarrigo by S.I.F. (Societ Italiana di Fisica) for his Master's thesis. He got his Ph.D. in History, Philosophy and Didactics of Science with a thesis entitled: "Reversibility and Universality

in Quantum Computation". He published several papers appeared in international peerreviewed journals of physics, computer science and philosophy. He is co-facilitator for the chairs of Logic, Basic Mathematics and Critical Thinking at the University of Cagliari.



Roberto Giuntini is full professor at the University of Cagliari. His research interests inlulde quantum computation, foundation of physics, logic and universal algebra. He was scientific supervisor for a number of research projects and he got plenty of scientific and academic assignments and he currently is director of I.Q.S.A. (International Quantum Structures Association). He pubblished a large number of books and papers appeared in international pee-rreviewed

journals of physics, logic, universal algebra, computer science and philosophy.



Francesco Paoli is an Associate Professor of Logic at the University of Cagliari. His research interests span a wide range of topics, including mathematical and philosophical logic, universal algebra, the foundations of physics, mathematics education and critical thinking. He published the book Substructural Logics: A Primer (Kluwer, Dordrecht, 2002) and several papers appeared in international peerreviewed journals of mathematics, computer science and philosophy.

He is member of the editorial board of several journals, including Studia Logica and Logica Universalis.