Gianpiero Cattaneo; Maria Luisa Dalla Chiara; Roberto Giuntini; Roberto Leporini
Quantum computational structures

Mathematica Slovaca, Vol. 54 (2004), No. 1, 87--108

Persistent URL: http://dml.cz/dmlcz/136899

Mathematica Slovaca
© 2004
Mathematical Institute
Slovak Academy of Sciences

Math. Slovaca, **54** (2004), No. 1, 87–108

Dedicated to Professor Sylvia Pulmannová on the occasion of her 65th birthday

QUANTUM COMPUTATIONAL STRUCTURES

GIANPIERO CATTANEO* — MARIA LUISA DALLA CHIARA** — ROBERTO GIUNTINI*** — ROBERTO LEPORINI*

(*Communicated by Anatolij Dvurečenskij*)

ABSTRACT. Quantum computation has suggested new forms of quantum logic, called *quantum computational logics* ([CATTANEO, G.—DALLA CHIARA, M. L. —GIUNTINI, R.—LEPORINI, R.: *An unsharp logic from quantum computation.* e-print: quant-ph/0201013]). The basic semantic idea is the following: the meaning of a sentence is identified with a *quregister*, representing a possible *pure state* of a compound physical system, whose associated Hilbert space is an n-fold tensor product $\overset{n}{\otimes}\mathbb{C}^2$. The generalization to density operators, which might be useful to analyse *entanglement-phenomena*, is due to [GUDDER, S.: *Quantum computational logic.* Preprint]. In this paper we study structural properties of density operators systems, where some basic *quantum logical gates* are defined. We introduce the notions of *standard reversible* and *standard irreversible quantum computational structure*. We prove that the second structure is isomorphic with an algebra based on a particular set of complex numbers.

1. Introduction

Quantum computation has recently suggested new forms of quantum logic that have been called *quantum computational logics* ([CDCGL01]). These logics are based on the following semantic idea: unlike orthodox quantum logic ([DCG02]), the *meaning of a sentence* is identified with a *qubit* or a *quregister* (a system of qubits) or, more generally, with a *qumix* (a mixture of quregisters). From a physical point of view, qubits represent possible *pure states* of quantum systems whose associated Hilbert space is $\mathbb{C}^2$. Quregisters represent pure states of compound systems whose associated Hilbert space is an n-fold tensor product $\overset{n}{\otimes}\mathbb{C}^2$, while qumixs correspond to density operators.

2000 Mathematics Subject Classification: Primary 81P68; Secondary 03G12.
Keywords: quantum computation, quantum logic.

The *qubit semantics*, presented in [CDCGL01], takes only in consideration qubits and quregisters. The generalization to qumixs, which might be useful to analyse *entanglement-phenomena*, is due to G u d d e r [Gu03]. In this paper we will study structural properties of qumix systems, where some basic *quantum logical gates* are defined. The logics that are naturally characterized by such structures will be investigated in forthcoming papers.

2. Qubits, quregisters and qumixs

Consider the two-dimensional Hilbert space $\mathbb{C}^2$ (where any vector $|\psi\rangle$ is represented by a pair of complex numbers). Let $\mathcal{B}^{(1)} = \{|0\rangle, |1\rangle\}$ be the canonical orthonormal basis for $\mathbb{C}^2$, where $|0\rangle = (1,0)$ and $|1\rangle = (0,1)$.

DEFINITION 2.1. (Qubit) A *qubit* is a unit vector $|\psi\rangle$ of the Hilbert space $\mathbb{C}^2$.

Recalling the Born rule, any qubit $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ (with $|c_0|^2 + |c_1|^2 = 1$) can be regarded as an *uncertain piece of information*, where the answer *NO* has probability $|c_0|^2$, while the answer *YES* has probability $|c_1|^2$. The two basis-elements $|0\rangle$ and $|1\rangle$ are usually taken as encoding the classical bit-values 0 and 1, respectively. From a semantic point of view, they can be also regarded as the classical truth-values *Falsity* and *Truth*.

An n-qubit system (also called *n-quregister*) is represented by a unit vector in the n-fold tensor product Hilbert space $\bigotimes^n \mathbb{C}^2 := \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n\text{-times}}$ (where $\bigotimes^1 \mathbb{C}^2 := \mathbb{C}^2$). We will use $x, y, \ldots$ as variables ranging over the set $\{0,1\}$. At the same time, $|x\rangle, |y\rangle, \ldots$ will range over the basis $\mathcal{B}^{(1)}$. Any factorized unit vector $|x_1\rangle \otimes \cdots \otimes |x_n\rangle$ of the space $\bigotimes^n \mathbb{C}^2$ will be called an *n-configuration* (which can be regarded as a quantum realization of a classical bit sequence of length n). Instead of $|x_1\rangle \otimes \cdots \otimes |x_n\rangle$ we will simply write $|x_1, \ldots, x_n\rangle$. Recall that the dimension of $\bigotimes^n \mathbb{C}^2$ is 2^n, while the set of all n-configurations $\mathcal{B}^{(n)} = \{|x_1, \ldots, x_n\rangle : x_i \in \{0,1\}\}$ is an orthonormal basis for the space $\bigotimes^n \mathbb{C}^2$. We will call this set a *computational basis* for the n-quregisters. Since any string $x_1, \ldots, x_n$ represents a natural number $j \in [0, 2^n - 1]$ (where $j = 2^{n-1}x_1 + 2^{n-2}x_2 + \cdots + x_n$), any unit vector of $\bigotimes^n \mathbb{C}^2$ can be briefly expressed in the following form: $\sum_{j=0}^{2^n-1} c_j \| j \rangle\!\rangle$, where $c_j \in \mathbb{C}$, $\| j \rangle\!\rangle$ is the n-configuration corresponding to the number j and $\sum_{j=0}^{2^n-1} |c_j|^2 = 1$.

Consider now the two following sets of natural numbers:

$$C_1^{(n)} := \{i : \|i\rangle\rangle = |x_1, \ldots, x_n\rangle \text{ and } x_n = 1\}$$

and

$$C_0^{(n)} := \{i : \|i\rangle\rangle = |x_1, \ldots, x_n\rangle \text{ and } x_n = 0\}.$$

Let us refer to a generic unit vector of the space $\bigotimes^n \mathbb{C}^2$:

$$|\psi\rangle = \sum_{i=0}^{2^n-1} a_i \|i\rangle\rangle .$$

We obtain:

$$|\psi\rangle = \sum_{i \in C_0^{(n)}} a_i \|i\rangle\rangle + \sum_{j \in C_1^{(n)}} a_j \|j\rangle\rangle .$$

Let $P_1^{(n)}$ and $P_0^{(n)}$ be the projections onto the span of $\{\|i\rangle\rangle : i \in C_1^{(n)}\}$ and $\{\|i\rangle\rangle : i \in C_0^{(n)}\}$, respectively. Clearly, $P_1^{(n)} + P_0^{(n)} = I^{(n)}$, where $I^{(n)}$ is the identity operator of $\bigotimes^n \mathbb{C}^2$. Apparently, $P_1^{(n)}$ and $P_0^{(n)}$ are density operators if and only if $n = 1$. Let $k_n = \frac{1}{2^{n-1}}$ be the normalization coefficient such that $k_n P_1^{(n)}$ and $k_n P_0^{(n)}$ are density operators. From an intuitive point of view, $k_n P_1^{(n)}$ can be regarded as a privileged information corresponding to the *Truth*, while $k_n P_0^{(n)}$ corresponds to the *Falsity*. In particular, $P_1^{(1)}$ represents the bit $|1\rangle$, while $P_0^{(1)}$ represents the bit $|0\rangle$. Let $\mathfrak{D}(\bigotimes^n \mathbb{C}^2)$ be the set of all density operators of $\bigotimes^n \mathbb{C}^2$ and let $\mathfrak{D} := \bigcup_{n=1}^{\infty} \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$.

DEFINITION 2.2. (Qumix) A *qumix* is a density operator in $\mathfrak{D}$.

Needless to say, quregisters correspond to particular qumixs that are *pure states* (i.e. projections onto one-dimensional closed subspaces of a given $\bigotimes^n \mathbb{C}^n$). Recalling the Born rule, we can now define the *probability-value* of any qumix.

DEFINITION 2.3. (Probability of a qumix) For any qumix $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$:

$$\mathrm{p}(\rho) = \mathrm{tr}(P_1^{(n)} \rho) .$$

From an intuitive point of view, $\mathrm{p}(\rho)$ represents the probability that the information stocked by the qumix ρ is true. In the particular case where ρ corresponds to the qubit

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle ,$$

we obtain that $\mathrm{p}(\rho) = |c_1|^2$.

For any quregister $|\psi\rangle$, we will write $\mathrm{p}(|\psi\rangle)$ instead of $\mathrm{p}(P_{|\psi\rangle})$, where $P_{|\psi\rangle}$ is the density operator represented by the projection onto the one-dimensional subspace spanned by the vector $|\psi\rangle$.

3. Quantum gates

In quantum computation, *quantum logical gates* (briefly *gates*) are unitary operators that transform quregisters into quregisters. Being unitary, gates represent characteristic *reversible transformations*. The canonical gates (which are studied in the literature) can be naturally generalized to qumixs. Generally, gates correspond to some basic *logical operations* that admit a reversible behaviour. We will consider here the following gates: *negation*, the *square root of negation*, *conjunction* and *disjunction*.

Let us first refer to quregisters.

DEFINITION 3.1. (The negation) For any $n \geq 1$, the *negation* on $\bigotimes^n \mathbb{C}^2$ is the linear operator $\text{NOT}^{(n)}$ such that for every element $|x_1, \ldots, x_n\rangle$ of the computational basis $\mathcal{B}^{(n)}$:

$$\text{NOT}^{(n)}(|x_1, \ldots, x_n\rangle) = |x_1, \ldots, x_{n-1}\rangle \otimes |1 - x_n\rangle .$$

In other words, $\text{NOT}^{(n)}$ inverts the value of the last element of any basis-vector of $\bigotimes^n \mathbb{C}^2$.

Clearly:

$$\text{NOT}^{(n)} = \begin{cases} X & \text{if } n = 1, \\ I^{(n-1)} \otimes X & \text{otherwise,} \end{cases}$$

where X is the "first" Pauli matrix, i.e.,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

DEFINITION 3.2. (The Petri-Toffoli gate) For any $n \geq 1$ and any $m \geq 1$ the *Petri-Toffoli gate* is the linear operator $T^{(n,m,1)}$ defined on $\bigotimes^{n+m+1} \mathbb{C}^2$ such that for every element $|x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z\rangle$ of the computational basis $\mathcal{B}^{(n+m+1)}$:

$$\begin{aligned} &T^{(n,m,1)}(|x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z\rangle) \\ &\quad = |x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |x_n y_m \oplus z\rangle , \end{aligned}$$

where $\oplus$ represents the sum modulo 2.

Clearly:

$$T^{(n,m,1)} := (I^{(n+m)} - P_1^{(n)} \otimes P_1^{(m)}) \otimes I^{(1)} + P_1^{(n)} \otimes P_1^{(m)} \otimes X .$$

One can easily show that both $\text{NOT}^{(n)}$ and $T^{(n,m,1)}$ are unitary operators.

The quantum logical gates we have considered so far are, in a sense, "semi-classical". A quantum logical behaviour only emerges in the case where our gates are applied to superpositions. When restricted to classical registers, such operators turn out to behave as classical (reversible) truth-functions. We will now consider a *genuine quantum gate* that transforms classical registers (elements of $\mathcal{B}^{(n)}$) into quregisters that are superpositions.

DEFINITION 3.3. (The square root of the negation) For any $n \geq 1$, the *square root of the negation* on $\bigotimes^n \mathbb{C}^2$ is the linear operator $\sqrt{\text{NOT}}^{(n)}$ such that for every element $|x_1, \ldots, x_n\rangle$ of the computational basis $\mathcal{B}^{(n)}$:

$$\sqrt{\text{NOT}}^{(n)}(|x_1, \ldots, x_n\rangle) = |x_1, \ldots, x_{n-1}\rangle \otimes \frac{1}{2}\big((1+\mathrm{i})|x_n\rangle + (1-\mathrm{i})|1-x_n\rangle\big)\,.$$

One can easily show that $\sqrt{\text{NOT}}^{(n)}$ is a unitary operator. The basic property of $\sqrt{\text{NOT}}^{(n)}$ is the following:

$$\Big(\forall\,|\psi\rangle \in \bigotimes^n \mathbb{C}^2\Big)\Big(\sqrt{\text{NOT}}^{(n)}\Big(\sqrt{\text{NOT}}^{(n)}(|\psi\rangle)\Big) = \text{NOT}^{(n)}(|\psi\rangle)\Big).$$

In other words, applying twice the square root of the negation means negating.

Clearly:

$$\sqrt{\text{NOT}}^{(n)} := \begin{cases} M & \text{if } n = 1\,, \\ I^{(n-1)} \otimes M & \text{otherwise,} \end{cases}$$

where

$$M := \frac{1}{2}\begin{pmatrix} 1+\mathrm{i} & 1-\mathrm{i} \\ 1-\mathrm{i} & 1+\mathrm{i} \end{pmatrix}.$$

Interestingly enough, the gate $\sqrt{\text{NOT}}^{(n)}$ admits physical models and implementations ([DEL00]). From a logical point of view, $\sqrt{\text{NOT}}^{(n)}$ can be regarded as a "tentative partial negation" (a kind of "half negation") that transforms *precise pieces of information* into *maximally uncertain* ones. For, we have:

$$\mathrm{p}\Big(\sqrt{\text{NOT}}^{(1)}(|1\rangle)\Big) = \frac{1}{2} = \mathrm{p}\Big(\sqrt{\text{NOT}}^{(1)}(|0\rangle)\Big).$$

Consider now the set $\bigcup_{n=1}^{\infty} \bigotimes^n \mathbb{C}^2$ (which contains all quregisters $|\psi\rangle$ "living" in $\bigotimes^n \mathbb{C}^2$ for a given $n \geq 1$). The gates NOT, $\sqrt{\text{NOT}}$ and T can be uniformly

defined on this set in the expected way:

$$\begin{aligned}
\textsc{Not}(|\psi\rangle) &:= \textsc{Not}^{(n)}(|\psi\rangle) && \text{if } |\psi\rangle \in \bigotimes^{n} \mathbb{C}^2 ,\\
\sqrt{\textsc{Not}}(|\psi\rangle) &:= \sqrt{\textsc{Not}}^{(n)}(|\psi\rangle) && \text{if } |\psi\rangle \in \bigotimes^{n} \mathbb{C}^2 ,\\
T(|\psi\rangle, |\varphi\rangle, |\chi\rangle) &:= T^{(n,m,1)}(|\psi\rangle, |\varphi\rangle, |\chi\rangle) && \text{if } |\psi\rangle \in \bigotimes^{n} \mathbb{C}^2 ,\\
& && \quad |\varphi\rangle \in \bigotimes^{m} \mathbb{C}^2 ,\\
& && \quad |\chi\rangle \in \mathbb{C}^2 .
\end{aligned}$$

On this basis, a conjunction AND and a disjunction OR can be defined for any pair of quregisters $|\psi\rangle$ and $|\varphi\rangle$:

$$\begin{aligned}
\textsc{And}(|\psi\rangle, |\varphi\rangle) &:= T(|\psi\rangle, |\varphi\rangle, |0\rangle);\\
\textsc{Or}(|\psi\rangle, |\varphi\rangle) &:= \textsc{Not}(\textsc{And}(\textsc{Not}(|\psi\rangle), \textsc{Not}(|\varphi\rangle))) .
\end{aligned}$$

Clearly, $|0\rangle$ represents an "ancilla" in the definition of AND.

One can easily verify that, when applied to classical bits, NOT, AND and OR behave as the standard Boolean truth-functions.

At first sight, AND and OR may look as *irreversible transformations*. However, it is important to recall that, in this framework, $\textsc{And}(|\psi\rangle, |\varphi\rangle)$ should be regarded as a mere metalinguistic abbreviation for $T(|\psi\rangle, |\varphi\rangle, |0\rangle)$ (where T is reversible). Similarly OR.

The gates considered so far can be naturally generalized to qumixs. When our gates will be applied to density operators, we will write: NOT, $\sqrt{\text{NOT}}$, AND, OR (instead of NOT, $\sqrt{\text{NOT}}$, AND, OR).

DEFINITION 3.4. (The negation) For any qumix $\rho \in \mathfrak{D}(\bigotimes^{n} \mathbb{C}^2)$,

$$\text{NOT}^{(n)}\rho = \textsc{Not}^{(n)}\rho\textsc{Not}^{(n)} .$$

DEFINITION 3.5. (The square-root of the negation) For any qumix $\rho \in \mathfrak{D}(\bigotimes^{n} \mathbb{C}^2)$,

$$\sqrt{\text{NOT}}^{(n)}\rho = \sqrt{\textsc{Not}}^{(n)}\rho\sqrt{\textsc{Not}}^{(n)*} ,$$

where $\sqrt{\textsc{Not}}^{(n)*}$ is the adjoint of $\sqrt{\textsc{Not}}^{(n)}$.

It is easy to see that for any $n \in \mathbb{N}^+$, both $\text{NOT}^{(n)}(\rho)$ and $\sqrt{\text{NOT}}^{(n)}(\rho)$ are qumixs of $\mathfrak{D}(\bigotimes^{n} \mathbb{C}^2)$. Further: $\text{NOT}^{(n)}\text{NOT}^{(n)} = I^{(n)}$.

DEFINITION 3.6. (The conjunction) Let $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$ and $\sigma \in \mathfrak{D}(\bigotimes^m \mathbb{C}^2)$.

$$\mathrm{AND}^{(n,m,1)}(\rho,\sigma) = T^{(n,m,1)}\rho \otimes \sigma \otimes P_0^{(1)} T^{(n,m,1)}\,.$$

Like in the quregister-case, the gates NOT, $\sqrt{\mathrm{NOT}}$, AND, OR can be uniformly defined on the set $\mathfrak{D}$ of all qumixs.

The following theorems describe some basic properties of our gates.

THEOREM 3.1. ([Gu03])

(i) $\mathrm{NOT} k_n P_0^{(n)} \mathrm{NOT} = k_n P_1^{(n)}$;
(ii) $\mathrm{NOT} k_n P_1^{(n)} \mathrm{NOT} = k_n P_0^{(n)}$;
(iii) $\mathrm{p}(\mathrm{NOT}\rho) = 1 - \mathrm{p}(\rho)$.

Consider now the "second" Pauli's matrix:

$$Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}.$$

This matrix can be naturally generalized to an operator $R^{(n)}$ defined on $\bigotimes^n \mathbb{C}^2$ (for any $n \in \mathbb{N}^+$):

$$R^{(n)} := \begin{cases} Y & \text{if } n = 1; \\ I^{(n-1)} \otimes Y & \text{otherwise.} \end{cases}$$

LEMMA 3.1. *For any $n \in \mathbb{N}^+$, the following properties hold:*

(i) $\mathrm{tr}(R^{(n)}) = 0$;
(ii) $\mathrm{tr}(R^{(n)} P_1^{(n)}) = 0$;
(iii) $\mathrm{tr}(R^{(n)} P_0^{(n)}) = 0$.

Proof.

(i) Let $n = 1$. Then $\mathrm{tr}(R^{(1)}) = \mathrm{tr}(Y) = 0$. Let $n > 1$. Then, $\mathrm{tr}(R^{(n)}) = \mathrm{tr}(I^{(n-1)} \otimes Y) = \mathrm{tr}(I^{(n-1)})\,\mathrm{tr}(Y) = 0$.

(ii) If $n = 1$, then $\mathrm{tr}(R^{(1)} P_1^{(1)}) = \mathrm{tr}(Y P_1^{(1)}) = 0$. If $n > 1$, then $\mathrm{tr}(R^{(n)} P_1^{(n)}) = \mathrm{tr}(I^{(n-1)} \otimes Y P_1^{(1)}) = 0$.

(iii) It follows from the fact that $\mathrm{tr}(R^{(1)} P_0^{(1)}) = \mathrm{tr}(Y P_0^{(1)}) = 0$. □

THEOREM 3.2.

(i) $\sqrt{\mathrm{NOT}}\sqrt{\mathrm{NOT}}\rho = \mathrm{NOT}\rho$;
(ii) $\mathrm{p}(\sqrt{\mathrm{NOT}}\rho) = \frac{1}{2} - \frac{1}{2}\mathrm{tr}(R^{(n)}\rho)$;
(iii) $\mathrm{p}(\sqrt{\mathrm{NOT}}\mathrm{NOT}\rho) = \mathrm{p}(\mathrm{NOT}\sqrt{\mathrm{NOT}}\rho)$;
(iv) $(\forall n \in \mathbb{N}^+)\left(\mathrm{p}(\sqrt{\mathrm{NOT}} k_n P_1^{(n)}) = \mathrm{p}(\sqrt{\mathrm{NOT}} k_n P_0^{(n)}) = \frac{1}{2}\right)$.

P r o o f . The proof of (i) is contained in G u d d e r [Gu03].

(ii) Let $n = 1$. Then $\mathrm{p}\big(\sqrt{\mathrm{NOT}}\rho\big) = \mathrm{tr}\big(M^* P_1^{(1)} M\rho\big) = \mathrm{tr}\big(\frac{1}{2}(I^{(1)} - Y)\rho\big) = \frac{1-\mathrm{tr}(R\rho)}{2}$. Let $n > 1$. Then $\mathrm{p}\big(\sqrt{\mathrm{NOT}}\rho\big) = \mathrm{tr}\big(I^{(n-1)} \otimes M^* P_1^{(1)} M\rho\big) = \mathrm{tr}\big(I^{(n-1)} \otimes \frac{1}{2}(I^{(1)} - Y)\rho\big) = \frac{1}{2} - \frac{1}{2}\,\mathrm{tr}\big(R^{(n)}\rho\big)$.

(iii)–(iv) It follows from (ii) and Lemma 3.1(ii)–(iii). □

THEOREM 3.3.

(i) $\mathrm{p}\big(\mathrm{AND}(\rho,\sigma)\big) = \mathrm{p}(\rho)\,\mathrm{p}(\sigma)$;
(ii) $\mathrm{p}\big(\sqrt{\mathrm{NOT}}\big(\mathrm{AND}(\rho,\sigma)\big)\big) = \frac{1}{2}$.

P r o o f .

(i)

$$\begin{aligned}
\mathrm{p}\big(\mathrm{AND}(\rho,\sigma)\big) &= \mathrm{tr}\big(P_1^{(n+m+1)} T^{(n+m+1)} \rho \otimes \sigma \otimes P_0^{(1)} T^{(n+m+1)}\big) \\
&= \mathrm{tr}\big(\big(I^{(n+m)} - P_1^{(n)} \otimes P_1^{(m)}\big)\rho \otimes \sigma \big(I^{(n+m)} - P_1^{(n)} \otimes P_1^{(m)}\big) \\
&\quad \otimes P_1^{(1)} P_0^{(1)} + P_1^{(n)} \rho P_1^{(n)} \otimes P_1^{(m)} \sigma P_1^{(m)} \otimes P_1^{(1)} X P_0^{(1)} X\big) \\
&= \mathrm{tr}\big(\big(I^{(n+m)} - P_1^{(n)} \otimes P_1^{(m)}\big)\rho \otimes \sigma\big)\,\mathrm{tr}\big(P_1^{(1)} P_0^{(1)}\big) \\
&\quad + \mathrm{tr}\big(P_1^{(n)}\rho\big)\,\mathrm{tr}\big(P_1^{(m)}\sigma\big)\,\mathrm{tr}\big(P_1^{(1)} P_1^{(1)}\big) \\
&= \mathrm{p}(\rho)\,\mathrm{p}(\sigma)\,.
\end{aligned}$$

(ii)

$$\begin{aligned}
&\mathrm{p}\big(\sqrt{\mathrm{NOT}}\big(\mathrm{AND}(\rho,\sigma)\big)\big) \\
&= \mathrm{tr}\Big(P_1^{(n+m+1)} \sqrt{\mathrm{NOT}}^{(n+m+1)} T^{(n+m+1)} \rho \otimes \sigma \otimes P_0^{(1)} T^{(n+m+1)} \sqrt{\mathrm{NOT}}^{(n+m+1)*}\Big) \\
&= \mathrm{tr}\big(\big(I^{(n+m)} - P_1^{(n)} \otimes P_1^{(m)}\big)\rho \otimes \sigma\big(I^{(n+m)} - P_1^{(n)} \otimes P_1^{(m)}\big) \otimes P_1^{(1)} M P_0^{(1)} M^* \\
&\quad + P_1^{(n)} \rho P_1^{(n)} \otimes P_1^{(m)} \sigma P_1^{(m)} \otimes P_1^{(1)} M P_1^{(1)} M^*\big) \\
&= \mathrm{tr}\big(\big(I^{(n+m)} - P_1^{(n)} \otimes P_1^{(m)}\big)\rho \otimes \sigma\big)\,\mathrm{tr}\big(P_1^{(1)} M P_0^{(1)} M^*\big) \\
&\quad + \mathrm{tr}\big(P_1^{(n)}\rho\big)\,\mathrm{tr}\big(P_1^{(m)}\sigma\big)\,\mathrm{tr}\big(P_1^{(1)} M P_1^{(1)} M^*\big) \\
&= \big(1 - \mathrm{p}(\rho)\,\mathrm{p}(\sigma)\big)\,\mathrm{p}\big(\sqrt{\mathrm{NOT}} P_0^{(1)}\big) + \mathrm{p}(\rho)\,\mathrm{p}(\sigma)\,\mathrm{p}\big(\sqrt{\mathrm{NOT}} P_1^{(1)}\big) = \frac{1}{2}\,.
\end{aligned}$$

□

4. The standard reversible quantum computational structure

An interesting feature of the qumix system is the following: any real number $\lambda \in [0,1] \subset \mathbb{R}$ uniquely determines a qumix $\rho_\lambda^{(n)}$ (for any $n \in \mathbb{N}^+$):

$$\rho_\lambda^{(n)} := (1-\lambda)k_n P_0^{(n)} + \lambda k_n P_1^{(n)} . \tag{4.1}$$

Clearly, $\rho_\lambda^{(n)} \in \mathfrak{D}\big(\bigotimes^n \mathbb{C}^2\big)$. From an intuitive point of view, $\rho_\lambda^{(n)}$ represents a *mixture of pieces of information* that might correspond to the *Truth* with probability λ.

From the physical point of view, $\rho_\lambda^{(n)}$ corresponds to a particular preparation of the system such that the quantum system is in the state $k_n P_0^{(n)}$ with probability $1-\lambda$ and in the state $k_n P_1^{(n)}$ with probability λ. It is worthwhile recalling that the random polarized states of the photon are represented by the density operator $\rho_{1/2}^{(1)} = \frac{1}{2} I^{(1)}$.

LEMMA 4.1.

(i) $\big(\forall n \in \mathbb{N}^+\big)\big(\forall \lambda \in [0,1]\big)\big(\mathrm{p}\big(\rho_\lambda^{(n)}\big) = \lambda\big)$;

(ii) $\mathrm{p}\big(\sqrt{\mathrm{NOT}}\rho_\lambda^{(n)}\big) = \frac{1}{2}$.

Proof.

(i) Straightforward.

(ii)

$$\begin{aligned}
\mathrm{p}\big(\sqrt{\mathrm{NOT}}\rho_\lambda^{(n)}\big) &= \frac{1}{2} - \frac{1}{2}\operatorname{tr}\big(R^{(n)}\rho_\lambda^{(n)}\big) && \text{(Theorem 3.2(ii))}\\
&= \frac{1}{2} - \frac{1-\lambda}{2^n}\operatorname{tr}\big(R^{(n)}P_0^{(n)}\big) - \frac{\lambda}{2^n}\operatorname{tr}\big(R^{(n)}P_1^{(n)}\big)\\
&= \frac{1}{2}. && \text{(Lemma 3.1(ii)–(iii))}
\end{aligned}$$

□

We will now introduce two interesting relations that can be defined on the set of all qumixs. Both of them turn out to be a preorder-relation. We will speak of *weak* and of *strong preorder*, respectively.

DEFINITION 4.1. (Weak preorder)

$$\rho \leq \sigma \iff \mathrm{p}(\rho) \leq \mathrm{p}(\sigma) .$$

DEFINITION 4.2. (Strong preorder) $\rho \preceq \sigma$ if and only if the following conditions hold:

(i) $\mathrm{p}(\rho) \leq \mathrm{p}(\sigma)$;

(ii) $\mathrm{p}(\sqrt{\mathrm{NOT}}\sigma) \leq \mathrm{p}(\sqrt{\mathrm{NOT}}\rho)$.

Clearly, $\rho \preceq \sigma$ implies $\rho \leq \sigma$, but not the other way around. One immediately shows that both $\leq$ and $\preceq$ are reflexive and transitive, but not antisymmetric. Counterexamples can be easily found in $\mathfrak{D}(\mathbb{C}^2)$.

Consider now the following structure:

$$\left(\mathfrak{D}, \preceq, \mathrm{AND}, \mathrm{NOT}, \sqrt{\mathrm{NOT}}, P_0^{(1)}, P_1^{(1)}, \rho_{1/2}^{(1)}\right). \tag{4.2}$$

We will call such a structure the *standard reversible quantum computational structure* (briefly the *RQC-structure*).

In the following we will generally write I, P_0, P_1 and $\rho_{1/2}$ instead of $I^{(1)}$, $P_0^{(1)}$, $P_1^{(1)}$, $\rho_{1/2}^{(1)}$. From an intuitive point of view, P_0, P_1 and $\rho_{1/2}$ represent privileged pieces of information that are *true*, *false*, *indeterminate*, respectively. Generally, our qumixs fail to satisfy *Duns Scotus law*: P_0 and P_1 are not the *minimum* and the *maximum* element of the RQC-structure. Hence, in this situation, it is interesting to isolate the elements that have a *Scotian* behaviour.

DEFINITION 4.3. (Down and up Scotian qumixs) Let ρ be a qumix of $\mathfrak{D}$.

(i) ρ is *down Scotian* if and only if $P_0 \preceq \rho$;

(ii) ρ is *up Scotian* if and only if $\rho \preceq P_1$;

(iii) ρ is *Scotian* if and only if ρ is both down and up Scotian.

LEMMA 4.2.

(i) $\rho \preceq \sqrt{\mathrm{NOT}}\, P_1$ *if and only if* $\mathrm{p}(\rho) \leq \frac{1}{2}$;

(ii) $\sqrt{\mathrm{NOT}}\, P_0 \preceq \rho$ *if and only if* $\mathrm{p}(\rho) \geq \frac{1}{2}$.

Proof.

(i) Suppose $\rho \preceq \sqrt{\mathrm{NOT}}\, P_1$. By Theorem 3.2(iv), we obtain $\mathrm{p}(\rho) \leq \mathrm{p}(\sqrt{\mathrm{NOT}}\, P_1) = \frac{1}{2}$. Viceversa, suppose $\mathrm{p}(\rho) \leq \frac{1}{2}$. Then, $\mathrm{p}(\rho) \leq \frac{1}{2} = \mathrm{p}(\sqrt{\mathrm{NOT}}\, P_1)$. Now, $\sqrt{\mathrm{NOT}}\sqrt{\mathrm{NOT}}\, P_1 = P_0$. Thus $0 = \mathrm{p}(\sqrt{\mathrm{NOT}}\sqrt{\mathrm{NOT}}\, P_1) \leq \mathrm{p}(\sqrt{\mathrm{NOT}}\rho)$. Hence: $\rho \preceq \sqrt{\mathrm{NOT}}\, P_1$.

(ii) Similar to the proof of (i), via Theorem 3.2(iv). □

THEOREM 4.1.

(i) *ρ is down Scotian if and only if* $\mathrm{p}(\sqrt{\mathrm{NOT}}\rho) \leq \frac{1}{2}$ *if and only if* $\sqrt{\mathrm{NOT}}\rho \preceq \sqrt{\mathrm{NOT}}P_1$.

(ii) *ρ is up Scotian if and only if* $\frac{1}{2} \leq \mathrm{p}(\sqrt{\mathrm{NOT}}\rho)$ *if and only if* $\sqrt{\mathrm{NOT}}P_0 \preceq \sqrt{\mathrm{NOT}}\rho$.

(iii) *ρ is Scotian if and only if* $\mathrm{p}(\sqrt{\mathrm{NOT}}\rho) = \frac{1}{2}$.

(iv) *For all $n \in \mathbb{N}^+$, $k_n P_0^{(n)}$, $k_n P_1^{(n)}$, $\rho_{1/2}^{(n)}$ are Scotian.*

(v) *For any $n \in \mathbb{N}^+$, the set $\mathfrak{D}\big(\bigotimes^n \mathbb{C}^2\big)$ contains uncountably many Scotian density operators.*

P r o o f . The proof of (i)–(ii) follows from Lemma 4.2.

The proof of (iii) follows from (i) and (ii).

(iv) The proof follows from Lemma 4.1 and from (iii).

(v) It is sufficient to show that $\mathfrak{D}\big(\mathbb{C}^2\big)$ contains uncountably many Scotian elements. Let $\lambda \in [-1, 1] \subset \mathbb{R}$. Consider the operator

$$\rho(\lambda) := \frac{1}{2}\begin{pmatrix} 1 & \lambda \\ \lambda & 1 \end{pmatrix}.$$

Clearly, $\rho(\lambda) \in \mathfrak{D}\big(\mathbb{C}^2\big)$. An easy computation shows that $\mathrm{p}\big(\sqrt{\mathrm{NOT}}\rho(\lambda)\big) = \frac{1}{2}$. Thus, by (iii) we can conclude that $\rho(\lambda)$ is Scotian. □

5. An irreversible operation: Łukasiewicz-sum

The gates we have considered so far represent typical *reversible* logical operations. From a logical point of view, it might be interesting to consider also some *irreversible* operations. An important example is represented by a Łukasiewicz-like disjunction.

DEFINITION 5.1. (The Łukasiewicz-disjunction) Let $\tau \in \mathfrak{D}\big(\bigotimes^n \mathbb{C}^2\big)$ and $\sigma \in \mathfrak{D}\big(\bigotimes^m \mathbb{C}^2\big)$.

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

where $\oplus$ in $\mathrm{p}(\tau) \oplus \mathrm{p}(\sigma)$ is the Łukasiewicz "truncated sum" defined on the real interval $[0, 1]$ (i.e. $\mathrm{p}(\tau) \oplus \mathrm{p}(\sigma) = \min\{1, \mathrm{p}(\tau) + \mathrm{p}(\sigma)\}$) ([Za34]).

LEMMA 5.1.

(i)
$$\tau \oplus \sigma = \begin{cases} \rho^{(1)}_{\mathrm{p}(\tau)\oplus\mathrm{p}(\sigma)} & \textit{if } \mathrm{p}(\tau)+\mathrm{p}(\sigma) \leq 1\,, \\ P_1^{(1)} & \textit{otherwise;} \end{cases}$$

(ii) $\mathrm{p}(\tau \oplus \sigma) = \mathrm{p}(\tau) \oplus \mathrm{p}(\sigma)$;
(iii) $\mathrm{p}\big(\sqrt{\mathrm{NOT}}(\tau \oplus \sigma)\big) = \frac{1}{2}$.

Proof.
(i) Straightforward.
(ii) The proof follows from Lemma 4.1(i).
(iii) The proof follows from Lemma 4.1(ii). □

LEMMA 5.2. *Let* $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$.

(i) $\big(\forall n \in \mathbb{N}^+\big)\big(\rho \oplus k_n P_1^{(n)} = P_1^{(1)}\big)$;
(ii) $\big(\forall n \in \mathbb{N}^+\big)\big(\rho \oplus k_n P_0^{(n)} = \rho^{(1)}_{\mathrm{p}(\rho)}\big)$;
(iii) $\rho \oplus \mathrm{NOT}\rho = P_1^{(1)}$.

Proof. Straightforward. □

From Lemma 5.2 it follows that $\mathrm{p}\big(\rho \oplus k_n P_1^{(n)}\big) = 1$, $\mathrm{p}\big(\rho \oplus k_n P_0^{(n)}\big) = \mathrm{p}(\rho)$ and $\mathrm{p}\big(\rho \oplus \mathrm{NOT}\rho\big) = 1$.

6. The standard irreversible quantum computational algebra

The preorder $\preceq$ permits us to define on the set of all qumixs an equivalence relation in the expected way.

DEFINITION 6.1. (The strong equivalence relation)
$$\rho \cong \sigma \iff (\rho \preceq \sigma \ \&\ \sigma \preceq \rho)\,.$$

Clearly, $\cong$ is an equivalence relation. Let
$$[\mathfrak{D}]_{\cong} := \big\{[\rho]_{\cong} : \ \rho \in \mathfrak{D}\big\}\,.$$

We will omit $\cong$ in $[\rho]_{\cong}$ if no confusion is possible.

Unlike the qumixs (which are only preordered by $\preceq$), the equivalence-classes of $[\mathfrak{D}]_{\cong}$ can be partially ordered in a natural way.

DEFINITION 6.2.

$$[\rho] \preceq [\sigma] \iff \rho \preceq \sigma .$$

The relation $\preceq$ (which is well defined) is a partial order.

LEMMA 6.1.

(i) $(\forall n \in \mathbb{N}^+)\left([P_1] = [k_n P_1^{(n)}]\right)$;

(ii) $(\forall n \in \mathbb{N}^+)\left([P_0] = [k_n P_0^{(n)}]\right)$;

(iii) $(\forall n \in \mathbb{N}^+)(\forall \lambda \in [0,1])\left([\rho_\lambda^{(1)}] = [\rho_\lambda^{(n)}]\right)$.

Proof.

(i)–(ii) The proof follows from Theorem 3.2(iv) and from the fact that $(\forall n \in \mathbb{N}^+)\left(\mathrm{p}(P_1^{(1)}) = 1 = \mathrm{p}(k_n P_1^{(n)})\right)$.

(iii) The proof follows from Lemma 4.1. □

On this basis, one can naturally define on the set $[\mathfrak{D}]_{\approxeq}$ a conjunction, a negation, the square root of the negation, a Łukasiewicz-disjunction:

DEFINITION 6.3. Let $\rho \in \mathfrak{D}(\overset{n}{\bigotimes} \mathbb{C}^2)$ and $\sigma \in \mathfrak{D}(\overset{m}{\bigotimes} \mathbb{C}^2)$.

(i) $[\rho]\mathrm{AND}[\sigma] = [\mathrm{AND}(\rho, \sigma)]$;

(ii) $\mathrm{NOT}[\rho] = [\mathrm{NOT}\rho]$;

(iii) $\sqrt{\mathrm{NOT}}[\rho] = [\sqrt{\mathrm{NOT}}\rho]$;

(iv) $[\rho] \oplus [\sigma] = [\rho \oplus \sigma]$.

LEMMA 6.2. *The operations of Definition* 6.3 *are well defined.*

Proof.

(i) Suppose $\rho' \approxeq \rho$ and $\sigma' \approxeq \sigma$. We want to show that $\mathrm{p}(\mathrm{AND}(\rho, \sigma)) = \mathrm{p}(\mathrm{AND}(\rho', \sigma'))$ and $\mathrm{p}(\sqrt{\mathrm{NOT}}(\mathrm{AND}(\rho, \sigma))) = \mathrm{p}(\sqrt{\mathrm{NOT}}(\mathrm{AND}(\rho', \sigma')))$. The proof follows from Theorem 3.3.

(ii) The proof follows from Theorem 3.1(iii) and Theorem 3.2(iii).

(iii) The proof follows from Theorem 3.1(iii) and Theorem 3.2(i).

(iv) Straightforward. □

LEMMA 6.3.

(i) *The operation* AND *is associative and commutative;*

(ii) *The operation* $\oplus$ *is associative and commutative;*

(iii) $\mathrm{NOT}\,\mathrm{NOT}\,[\rho] = [\rho]$;

(iv) $\sqrt{\mathrm{NOT}}\,\sqrt{\mathrm{NOT}}\,[\rho] = \mathrm{NOT}\,[\rho]$;

(v) $\sqrt{\mathrm{NOT}}\,\mathrm{NOT}\,[\rho] = \mathrm{NOT}\sqrt{\mathrm{NOT}}\,[\rho]$.

P r o o f . Straightforward. □

Consider now the structure

$$\left([\mathfrak{D}]_{\approxeq}, \text{AND}, \oplus, \text{NOT}, \sqrt{\text{NOT}}, [P_0]_{\approxeq}, [P_1]_{\approxeq}, [\rho_{1/2}]_{\approxeq}\right). \tag{6.1}$$

We will call such a structure the *standard irreversible quantum computational algebra* (briefly the *IQC-algebra*).

As happens in the case of $\preceq$, also the weak preorder $\leq$ permits us to define an equivalence relation, which will be called *weak equivalence relation.*

DEFINITION 6.4. (Weak equivalence relation)

$$\rho \equiv \sigma \iff (\rho \leq \sigma \ \& \ \sigma \leq \rho).$$

Clearly, $\equiv$ is an equivalence relation. Let

$$[\mathfrak{D}]_{\equiv} := \{[\rho]_{\equiv} : \ \rho \in \mathfrak{D}\}.$$

Also $[\mathfrak{D}]_{\equiv}$ can be partially ordered in a natural way.

DEFINITION 6.5.

$$[\rho]_{\equiv} \leq [\sigma]_{\equiv} \iff \rho \leq \sigma.$$

One can easily show that the relation $\leq$ (which is well defined) is a partial order.

A conjunction, a Łukasiewicz-disjunction, a negation (but not the square root of the negation!) can be naturally defined on $[\mathfrak{D}]_{\equiv}$.

DEFINITION 6.6. Let $\rho \in \mathfrak{D}(\overset{n}{\bigotimes}\mathbb{C}^2)$ and $\sigma \in \mathfrak{D}(\overset{m}{\bigotimes}\mathbb{C}^2)$.

(i) $[\rho]_{\equiv}\text{AND}\,[\sigma]_{\equiv} = \left[\text{AND}(\rho,\sigma)\right]_{\equiv}$;
(ii) $\text{NOT}[\rho]_{\equiv} = [\text{NOT}\rho]_{\equiv}$;
(iii) $[\rho]_{\equiv} \oplus [\sigma]_{\equiv} = [\rho \oplus \sigma]_{\equiv}$.

LEMMA 6.4. *The operations of Definition* 6.6 *are well defined.*

P r o o f .
(i) It is a consequence of Theorem 3.3(i).
(ii) It is a consequence of Theorem 3.1(i).
(iii) Straightforward. □

Unlike $\approxeq$, the relation $\equiv$ is not a congruence with respect to $\sqrt{\text{NOT}}$. In fact, the following situation is possible: $[\rho]_{\equiv} = [\sigma]_{\equiv}$ and $\left[\sqrt{\text{NOT}}\,\rho\right]_{\equiv} \neq \left[\sqrt{\text{NOT}}\,\sigma\right]_{\equiv}$. Consider for example the following unit vectors of $\mathbb{C}^2$: $|\psi\rangle := \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle$ and $|\varphi\rangle := \frac{\sqrt{2}}{2}|0\rangle + \frac{1+i}{2}|1\rangle$.

Let $P_{|\psi\rangle}$ and $P_{|\varphi\rangle}$ be the projections onto the unidimensional spaces spanned by $|\psi\rangle$ and $|\varphi\rangle$, respectively. It turns out that $\mathrm{p}(P_{|\psi\rangle}) = \mathrm{p}(P_{|\varphi\rangle}) = \frac{1}{2}$. Accordingly, $[P_{|\psi\rangle}]_{\equiv} = [P_{|\varphi\rangle}]_{\equiv}$. However, $\mathrm{p}(\sqrt{\mathrm{NOT}}\, P_{|\psi\rangle}) = \frac{1}{2}$ and $\mathrm{p}(\sqrt{\mathrm{NOT}}\, P_{|\varphi\rangle}) = \frac{1}{8} + \left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right)^2 \approx 0.146447$. Consequently, $[P_{|\psi\rangle}]_{\cong} \neq [P_{|\varphi\rangle}]_{\cong}$.

An interesting relation between the weak and the strong preorder is described by the following theorem.

THEOREM 6.1. *For any* $\rho, \sigma \in \mathfrak{D}$*:*

$$[\rho]_{\equiv} \leq [\sigma]_{\equiv} \iff [\rho]_{\cong}\mathrm{AND}\,[P_1]_{\cong} \preceq [\sigma]_{\cong}\mathrm{AND}\,[P_1]_{\cong}\,.$$

Proof. Suppose $\mathrm{p}(\rho) \leq \mathrm{p}(\sigma)$. By Theorem 3.3(i), we obtain

$$\mathrm{p}\big(\mathrm{AND}(\rho, P_1)\big) = \mathrm{p}(\rho) \leq \mathrm{p}(\sigma) = \mathrm{p}\big(\mathrm{AND}(\sigma, P_1)\big)\,. \tag{6.2}$$

By Theorem 3.3(ii),

$$\mathrm{p}\big(\sqrt{\mathrm{NOT}}\,\mathrm{AND}(\rho, P_1)\big) = \frac{1}{2} = \mathrm{p}\big(\sqrt{\mathrm{NOT}}\,\mathrm{AND}(\sigma, P_1)\big)\,. \tag{6.3}$$

Thus, $[\rho]_{\cong}\mathrm{AND}\,[P_1]_{\cong} \preceq [\sigma]_{\cong}\mathrm{AND}\,[P_1]_{\cong}$.

Viceversa, suppose $[\rho]_{\cong}\mathrm{AND}\,[P_1]_{\cong} \preceq [\sigma]_{\cong}\mathrm{AND}\,[P_1]_{\cong}$.

Then,

$$\mathrm{p}(\rho) = \mathrm{p}(\rho)\,\mathrm{p}(P_1) = \mathrm{p}\big(\mathrm{AND}(\rho, P_1)\big) \leq \mathrm{p}\big(\mathrm{AND}(\sigma, P_1)\big) = \mathrm{p}(\sigma)\,. \tag{6.4}$$

□

LEMMA 6.5.

(i) *The structure* $\big([\mathfrak{D}]_{\equiv}, \mathrm{AND}, [P_1]_{\equiv}\big)$ *is an Abelian monoid with neutral element* $[P_1]_{\equiv}$*;*

(ii) $\big([\mathfrak{D}]_{\equiv}, \oplus, [P_0]_{\equiv}\big)$ *is an Abelian monoid with neutral element* $[P_0]_{\equiv}$*;*

(iii) $\mathrm{NOT}\,\mathrm{NOT}\,[\rho]_{\equiv} = [\rho]_{\equiv}$.

Proof. Easy. □

7. The Poincaré irreversible quantum computational structures

We will now restrict our analysis to qumixs living in the two-dimensional space $\mathbb{C}^2$. As is well known, every density operator of $\mathfrak{D}(\mathbb{C}^2)$ has the following matrix representation:

$$\frac{1}{2}(I + r_1 X + r_2 Y + r_3 Z)\,, \tag{7.1}$$

where r_1, r_2, r_3 are real numbers such that $r_1^2 + r_2^2 + r_3^2 \leq 1$ and X, Y, Z are the Pauli matrices:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

It turns out that a density operator $\frac{1}{2}(I + r_1 X + r_2 Y + r_3 Z)$ represents a *pure state* (a qubit) if and only if $r_1^2 + r_2^2 + r_3^2 = 1$. Consequently,

- Pure density operators are in $1:1$ correspondence with the points of the surface of the Poincaré sphere;
- Proper mixtures are in $1:1$ correspondence with the inner points of the Poincaré sphere.

Let ρ be a density operator of $\mathfrak{D}(\mathbb{C}^2)$. We will denote by $\bar{\rho}$ the point of the Poincaré sphere that is univocally associated to ρ.

Let (r_1, r_2, r_3) be a point of the Poincaré sphere. We will denote by $\widehat{(r_1, r_2, r_3)}$ the density operator univocally associated to (r_1, r_2, r_3).

LEMMA 7.1. *Let $\rho \in \mathfrak{D}(\mathbb{C}^2)$ such that $\bar{\rho} = (r_1, r_2, r_3)$. The following conditions hold:*

(i) $\mathrm{p}(\rho) = \frac{1-r_3}{2}$;
(ii) $\mathrm{p}(\sqrt{\mathrm{NOT}}\,\rho) = \frac{1-r_2}{2}$.

Proof. Easy computation. □

An irreversible conjunction can be now naturally defined on the set of all qumixs of $\mathfrak{D}(\mathbb{C}^2)$.

DEFINITION 7.1. (The irreversible conjunction) Let $\tau, \sigma \in \mathfrak{D}(\mathbb{C}^2)$.

$$\mathrm{IAND}(\tau, \sigma) = \rho^{(1)}_{\mathrm{p}(\tau)\,\mathrm{p}(\sigma)}. \tag{7.2}$$

Interestingly enough, the density operator $\mathrm{IAND}(\tau, \sigma)$ can be described in terms of the *partial trace*. Suppose we have a compound physical system consisting of three subsystems, and let

$$\mathcal{H} = \Big(\bigotimes^{n} \mathbb{C}^2\Big) \otimes \Big(\bigotimes^{m} \mathbb{C}^2\Big) \otimes \Big(\bigotimes^{r} \mathbb{C}^2\Big)$$

be the Hilbert space associated to our system. Then, for any density operator ρ of $\mathcal{H}$, there is a unique density operator $\mathrm{tr}_{1,2}(\rho)$ that represents the *partial trace* of ρ on the space $\bigotimes^{r} \mathbb{C}^2$ (associated to the third subsystem). The two operators ρ and $\mathrm{tr}_{1,2}(\rho)$ are statistically equivalent with respect to the third subsystem. In other words, for any self-adjoint operator $A^{(r)}$ of $\bigotimes^{r} \mathbb{C}^2$:

$$\mathrm{tr}\big(\mathrm{tr}_{1,2}(\rho)\, A^{(r)}\big) = \mathrm{tr}\big(\rho\, I^{(n)} \otimes I^{(m)} \otimes A^{(r)}\big).$$

The density operator $\mathrm{tr}_{1,2}(\rho)$, obtained by "tracing out" the first and the second subsystem, is also called the *reduced state* of ρ on the third subsystem.

One can prove that:

$$\mathrm{IAND}(\tau,\sigma) = \mathrm{tr}_{1,2}\big(\mathrm{AND}(\tau,\sigma)\big)\,.$$

In other words, $\mathrm{IAND}(\tau,\sigma)$ represents the reduced state of $\mathrm{AND}(\tau,\sigma)$ on the third subsystem.

An interesting situation arises when both τ and σ are pure states. For instance, suppose that:

$$\tau = P_{|\psi\rangle} \qquad \text{and} \qquad \sigma = P_{|\varphi\rangle}\,,$$

where $|\psi\rangle$ and $|\varphi\rangle$ are proper qubits. Then,

$$\mathrm{AND}(\tau,\sigma) = P_{T^{(1,1,1)}(|\psi\rangle\otimes|\varphi\rangle\otimes|0\rangle)}\,,$$

which is a pure state. At the same time, we have:

$$\mathrm{IAND}(\tau,\sigma) = \mathrm{tr}_{1,2}\Big(P_{T^{(1,1,1)}(|\psi\rangle\otimes|\varphi\rangle\otimes|0\rangle)}\Big),$$

which is a proper mixture. Apparently, when considering only the properties of the third subsystem, we loose some information. As a consequence, we obtain a final state that does not represent a maximal knowledge. As is well known, situations where the state of a compound system represents a maximal knowledge, while the states of the subsystems are proper mixtures, play an important role in the framework of entanglement-phenomena.

LEMMA 7.2.

(i) IAND *is associative and commutative;*
(ii) $\mathrm{IAND}(\rho, P_0) = P_0$;
(iii) $\mathrm{IAND}(\rho, P_1) = \rho_{\mathrm{p}(\rho)}$;
(iv) $\mathrm{p}\big(\mathrm{IAND}(\rho,\sigma)\big) = \mathrm{p}(\rho)\,\mathrm{p}(\sigma)$;
(v) $\mathrm{p}\big(\sqrt{\mathrm{NOT}}\,\mathrm{IAND}(\rho,\sigma)\big) = \frac{1}{2}$.

P r o o f . Easy computation. □

Consider now the structure

$$\Big(\mathfrak{D}(\mathbb{C}^2),\ \mathrm{IAND},\ \oplus,\ \mathrm{NOT},\ \sqrt{\mathrm{NOT}},\ P_0,\ P_1,\ \rho_{1/2}\Big)\,. \tag{7.3}$$

We will call such a structure the *Poincaré irreversible quantum computational algebra* (briefly the *Poincaré IQC-algebra*).

We can now refer to the relation $\restriction\!\cong$, representing the restriction of $\cong$ to $\mathfrak{D}(\mathbb{C}^2)$. For any $\rho \in \mathfrak{D}(\mathbb{C}^2)$, let

$$[\rho]_{\restriction\cong} := \big\{\sigma \in \mathfrak{D}(\mathbb{C}^2) :\ \rho \cong \sigma\big\}\,. \tag{7.4}$$

Further define

$$[\mathfrak{D}(\mathbb{C}^2)]_{\restriction\cong} := \{[\rho]_{\restriction\cong} : \rho \in \mathfrak{D}(\mathbb{C}^2)\}. \tag{7.5}$$

The operations IAND, $\oplus$, NOT, $\sqrt{\text{NOT}}$ and the relation $\preceq$ can be defined on $[\mathfrak{D}(\mathbb{C}^2)]_{\restriction\cong}$ in the expected way.

On this basis we obtain the following quotient-structure

$$\left([\mathfrak{D}(\mathbb{C}^2)]_{\restriction\cong}, \text{IAND}, \oplus, \text{NOT}, \sqrt{\text{NOT}}, [P_0]_{\restriction\cong}, [P_1]_{\restriction\cong}, [\rho_{1/2}]_{\restriction\cong}\right).$$

We will call such a structure the *contracted Poincaré irreversible quantum computational algebra* (briefly the *contracted Poincaré IQC-algebra*).

THEOREM 7.1. *The contracted Poincaré IQC-algebra is isomorphic to the IQC-algebra via the map* $g\colon [\mathfrak{D}(\mathbb{C}^2)]_{\restriction\cong} \to [\mathfrak{D}]_{\cong}$ *such that for all* $\rho \in \mathfrak{D}(\mathbb{C}^2)$*:*

$$g([\rho]_{\restriction\cong}) = [\rho]_{\cong}. \tag{7.6}$$

Further, for any $\rho, \sigma \in \mathfrak{D}(\mathbb{C}^2)$*:* $[\rho]_{\restriction\cong} \preceq [\sigma]_{\restriction\cong}$ *if and only if* $g([\rho]_{\restriction\cong}) \preceq g([\sigma]_{\restriction\cong})$.

Proof. One can readily see that g preserves the operation NOT, $\sqrt{\text{NOT}}$ and $\oplus$. By Theorem 3.3 and Lemma 7.2(iv–v), g preserves also the operation IAND. Clearly, the map g is injective. Let us prove that g is also surjective. To this aim, it is sufficient to show that for any $n \in \mathbb{N}^+$ and for any $\rho \in \mathfrak{D}(\overset{n}{\otimes}\mathbb{C}^2)$, there exists a density operator $\rho' \in \mathfrak{D}(\mathbb{C}^2)$ such that:

(i) $\text{p}(\rho) = \text{p}(\rho')$;

(ii) $\text{p}(\sqrt{\text{NOT}}\rho) = \text{p}(\sqrt{\text{NOT}}\rho')$.

Let $\rho \in \mathfrak{D}(\overset{n}{\otimes}\mathbb{C}^2)$ and let ρ' be the reduced state of ρ on $\mathbb{C}^2$. Accordingly, for any self-adjoint operator A of $\mathbb{C}^2$, we have:

$$\text{tr}(I^{(n-1)} \otimes A\rho) = \text{tr}(A\rho'). \tag{7.7}$$

Thus, $\text{p}(\rho) = \text{tr}(P_1^{(n)}\rho) = \text{tr}(I^{(n-1)} \otimes P_1^{(1)}\rho) = \text{tr}(P_1^{(1)}\rho')$.

We now prove (ii).

$$\begin{aligned}
\text{p}(\sqrt{\text{NOT}}\rho) &= \text{tr}(P_1^{(n)}(I^{(n-1)} \otimes M)\rho(I^{(n-1)} \otimes M^*)) \\
&= \text{tr}(I^{(n-1)} \otimes M^* P_1^{(1)} M\rho) \\
&\overset{(7.7)}{=} \text{tr}(M^* P_1^{(1)} M\rho') \\
&= \text{p}(\sqrt{\text{NOT}}\rho').
\end{aligned}$$

□

8. The complex quantum computational algebra

An interesting algebraic property of the contracted Poincaré IQC-structure is the following: our structure turns out to be isomorphic to a structure based on a particular subset of the set $\mathbb{C}$ of all complex numbers. Let

$$\mathbb{C}_1 := \{(a,b)\colon a,b \in \mathbb{R} \text{ and } (1-2a)^2 + (1-2b)^2 \leq 1\}.$$

Note that for all pairs $(a,b) \in \mathbb{C}_1$, both elements a, b belong to the real interval $[0,1]$.

Let $\underline{0} := (0, \frac{1}{2})$, $\underline{1} := (1, \frac{1}{2})$, $\underline{\frac{1}{2}} := (\frac{1}{2}, \frac{1}{2})$.

The following operations ($\mathrm{IAND}^{\mathbb{C}_1}$, $\mathrm{NOT}^{\mathbb{C}_1}$, $\sqrt{\mathrm{NOT}}^{\mathbb{C}_1}$, $\oplus^{\mathbb{C}_1}$) can be defined on $\mathbb{C}_1$.

DEFINITION 8.1.

(i) $(a_1,a_2)\mathrm{IAND}^{\mathbb{C}_1}(b_1,b_2) = (a_1b_1, \frac{1}{2})$;

(ii) $\mathrm{NOT}^{\mathbb{C}_1}(a_1,a_2) = (1-a_1, 1-a_2)$;

(iii) $\sqrt{\mathrm{NOT}}^{\mathbb{C}_1}(a_1,a_2) = (a_2, 1-a_1)$;

(iv) $(a_1,a_2) \oplus^{\mathbb{C}_1} (b_1,b_2) = \begin{cases} (a_1+b_1, \frac{1}{2}) & \text{if } a_1+b_1 \leq 1; \\ \underline{1} & \text{otherwise.} \end{cases}$

One can easily see that $\mathbb{C}_1$ is closed under the operations of Definition 8.1.

LEMMA 8.1.

(i) *The operations* $\mathrm{IAND}^{\mathbb{C}_1}$ *and* $\oplus^{\mathbb{C}_1}$ *are commutative and associative;*

(ii) $(a_1,a_2)\mathrm{IAND}^{\mathbb{C}_1}\underline{0} = \underline{0}$;

(iii) $(a_1,a_2) \oplus^{\mathbb{C}_1} \underline{0} = (a_1, \frac{1}{2})$;

(iv) $(a_1,a_2)\mathrm{IAND}^{\mathbb{C}_1}\underline{1} = (a_1\ \frac{1}{2})$;

(v) $(a_1,a_2) \oplus^{\mathbb{C}_1} \underline{1} = \underline{1}$;

(vi) $\mathrm{NOT}^{\mathbb{C}_1}\mathrm{NOT}^{\mathbb{C}_1}(a_1,a_2) = (a_1,a_2)$;

(vii) $\sqrt{\mathrm{NOT}}^{\mathbb{C}_1}\mathrm{NOT}^{\mathbb{C}_1}(a_1,a_2) = \mathrm{NOT}^{\mathbb{C}_1}\sqrt{\mathrm{NOT}}^{\mathbb{C}_1}(a_1,a_2)$;

(viii) $\sqrt{\mathrm{NOT}}^{\mathbb{C}_1}\sqrt{\mathrm{NOT}}^{\mathbb{C}_1}(a_1,a_2) = \mathrm{NOT}^{\mathbb{C}_1}(a_1,a_2)$;

(ix) (a_1,a_2) *is a fixed point of* $\mathrm{NOT}^{\mathbb{C}_1}$ *if and only if* (a_1,a_2) *is a fixed point of* $\sqrt{\mathrm{NOT}}^{\mathbb{C}_1}$ *if and only if* $(a_1,a_2) = \underline{\frac{1}{2}}$.

P r o o f. Easy computation. □

DEFINITION 8.2.

$$(a_1,a_2) \preceq (b_1,b_2) \iff (a_1 \leq b_1 \ \&\ b_2 \leq a_2).$$

Consider now the structure $\left(\mathbb{C}_1, \mathrm{IAND}^{\mathbb{C}_1}, \oplus^{\mathbb{C}_1}, \mathrm{NOT}^{\mathbb{C}_1}, \sqrt{\mathrm{NOT}}^{\mathbb{C}_1}, \underline{0}, \underline{1}, \underline{\frac{1}{2}}\right)$. We will call such a structure the *complex quantum computational algebra* (briefly the $\mathbb{C}_1$ *QC-algebra*).

We will prove that the contracted Poincaré IQC-algebra and the $\mathbb{C}_1$ QC-algebra are isomorphic.

Let $(a, b) \in \mathbb{C}_1$ and let $\rho(a, b)$ be the density operator associated to the triple $(0, 1-2b, 1-2a)$. Thus,

$$\rho(a, b) := (0, \widehat{1-2b, 1-2a}) .$$

Hence:

$$\rho(a, b) = \begin{pmatrix} 1-a & -\mathrm{i}\left(\frac{1}{2}-b\right) \\ \mathrm{i}\left(\frac{1}{2}-b\right) & a \end{pmatrix} .$$

LEMMA 8.2.

(i) $\rho\big((a_1, a_2)\mathrm{IAND}^{\mathbb{C}_1}(b_1, b_2)\big) = \mathrm{IAND}\big(\rho(a_1, a_2), \rho(b_1, b_2)\big)$;

(ii) $\rho\big(\mathrm{NOT}^{\mathbb{C}_1}(a_1, a_2)\big) = \mathrm{NOT}\big(\rho(a_1, a_2)\big)$;

(iii) $\rho\Big(\sqrt{\mathrm{NOT}}^{\mathbb{C}_1}(a_1, a_2)\Big) = \sqrt{\mathrm{NOT}}\big(\rho(a_1, a_2)\big)$;

(iv) $\rho\big((a_1, a_2) \oplus^{\mathbb{C}_1} (b_1, b_2)\big) = \rho(a_1, a_2) \oplus \rho(b_1, b_2)$.

P r o o f . Easy computation. □

THEOREM 8.1. *The* $\mathbb{C}_1$ *QC-algebra*

$$\left(\mathbb{C}_1, \mathrm{IAND}^{\mathbb{C}_1}, \oplus^{\mathbb{C}_1}, \mathrm{NOT}^{\mathbb{C}_1}, \sqrt{\mathrm{NOT}}^{\mathbb{C}_1}, \underline{0}, \underline{1}, \underline{\tfrac{1}{2}}\right)$$

is isomorphic to the contracted Poincaré IQC-algebra

$$\left(\left[\mathfrak{D}(\mathbb{C}^2)\right]_{\restriction\cong}, \mathrm{IAND}, \oplus, \mathrm{NOT}, \sqrt{\mathrm{NOT}}, [P_0]_{\restriction\cong}, [P_1]_{\restriction\cong}, [\rho_{1/2}]_{\restriction\cong}\right) .$$

P r o o f . Let h be the map of $\mathbb{C}_1$ into $\left[\mathfrak{D}(\mathbb{C}^2)\right]_{\restriction\cong}$ such that for all $(a, b) \in \mathbb{C}_1$:

$$h\big((a, b)\big) := \left[\rho(a, b)\right]_{\restriction\cong} .$$

That h is a homomorphism follows from Lemma 8.2. We now prove that h is injective. Suppose $(a, b) \neq (c, d)$. Suppose, by contradiction, that $h\big((a, b)\big) = h\big((c, d)\big)$. Then, $\left[\rho(a, b)\right]_{\restriction\cong} = \left[\rho(c, d)\right]_{\restriction\cong}$. Thus,

$$\mathrm{p}\big(\rho(a, b)\big) = \mathrm{p}\big(\rho(c, d)\big) \qquad \text{and} \qquad \mathrm{p}\big(\sqrt{\mathrm{NOT}}\,\rho(a, b)\big) = \mathrm{p}\big(\sqrt{\mathrm{NOT}}\,\rho(c, d)\big) .$$

By Lemma 7.1, we obtain

$$\mathrm{p}\big(\rho(a,b)\big) = a = c = \mathrm{p}\big(\rho(c,d)\big)$$

and

$$\mathrm{p}\big(\sqrt{\mathrm{NOT}}\,\rho(a,b)\big) = b = d = \mathrm{p}\big(\sqrt{\mathrm{NOT}}\,\rho(c,d)\big)\,.$$

Hence: $(a,b) = (c,d)$, which is a contradiction.

We now prove that h is surjective. Let ρ be a density operator of $\mathfrak{D}(\mathbb{C}^2)$ and let (a,b,c) be the point of the Poincaré sphere associated to ρ. Thus, $(a,b,c) = \bar{\rho}$. Take $\big(\frac{1-c}{2}, \frac{1-b}{2}\big) \in \mathbb{C}_1$. By Lemma 7.1, $\big[\rho\big(\frac{1-c}{2}, \frac{1-b}{2}\big)\big]_{\restriction\cong} = [\rho]_{\restriction\cong}$. Consequently, $[\rho]_{\restriction\cong} = h\big(\big(\frac{1-c}{2}, \frac{1-b}{2}\big)\big)$. □

As a consequence of Theorem 7.1 and of Theorem 8.1, we obtain that the IQC-algebra and the $\mathbb{C}_1$ QC-algebra are isomorphic.

REFERENCES

[CDCGL01] CATTANEO, G.—DALLA CHIARA, M. L.—GIUNTINI, R.—LEPORINI, R.: *An unsharp logic from quantum computation.* e-print: quant-ph/0201013.

[DCG02] DALLA CHIARA, M. L.—GIUNTINI, R.: *Quantum logics.* In: Handbook of Philosophical Logic, vol. VI (G. Gabbay, F. Guenthner, eds.), Kluwer, Dordrecht, 2002, pp. 129–228.

[DGLL02] DALLA CHIARA, M. L.—GIUNTINI, R.—LEPORATI, A.—LEPORINI, R.: *Qubit semantics and quantum trees.* quant-ph/0211190.

[DEL00] DEUTSCH, D.—EKERT, A.—LUPACCHINI, R.: *Machines, logic and quantum physics,* Bull. Symbolic Logic **3** (2000), 265–283.

[Gu03] GUDDER, S.: *Quantum computational logic,* Internat. J. Theoret. Phys. **42** (2003), 39–47.

[Pe67] PETRI, C. A.: *Gründsatzliches zur Beschreibung diskreter Prozesse.* In: Proceedings of the 3rd Colloquium über Automatentheorie (Hannover, 1965), Birkhäuser Verlag, Basel, 1967, pp. 121–140 [English version: *Fundamentals of the representation of discrete processes*, ISF Report 82.04 (1982) (translated by H. J. Genrich and P. S. Thiagarajan)].

[To80] TOFFOLI, T.: *Reversible computing.* In: Automata, Languages and Programming. Lecture Notes in Comput. Sci. 85 (J. W. de Bakker, J. van Leeuwen, eds.), Springer, Berlin-Heidelberg-New York, 1980, pp. 632–644 (Also available as Technical Memo MIT/LCS/TM-151, MIT Laboratory for Computer Science, February 1980).

[Za34] ZAWIRSKI, Z.: *Relation of Many-Valued Logic to Probability Calculus*, Poznańskie Towarzystwo Przyjaciół Nauk, Poznań. (Polish)

Received April 10, 2003

* *Dipartimento di Informatica,*
Sistemistica e Comunicazione (DISCo)
Università degli Studi di Milano — Bicocca
Via Bicocca degli Arcimboldi 8
I–20126 Milano
ITALY
E-mail: cattang@disco.unimib.it
leporini@disco.unimib.it

** *Dipartimento di Filosofia*
Università di Firenze
via Bolognese 52
I–50139 Firenze
ITALY
E-mail: dallachiara@unifi.it

*** *Dipartimento di Scienze Pedagogiche*
e Filosofiche
Università di Cagliari
via Is Mirrionis 1
I–09123 Cagliari
ITALY
E-mail: giuntini@unica.it