Elsevier Editorial System(tm) for Fuzzy Sets and Systems
Manuscript Draft

Manuscript Number: FSS-D-16-00679R1

Title: A Many-valued Approach to Quantum Computational Logics

Article Type: SI: LINZ 2016

Keywords: Quantum logics; quantum tomography; logical gates.

Corresponding Author: Dr. Roberto Leporini, PhD

Corresponding Author's Institution: Università degli Studi di Bergamo

First Author: Maria Luisa Dalla Chiara, Prof.

Order of Authors: Maria Luisa Dalla Chiara, Prof.; Roberto Giuntini, Prof.; Roberto Leporini, PhD; Giuseppe Sergioli, PhD

Abstract: Quantum computational logics are special examples of quantum logic where formulas are supposed to denote pieces of quantum information (qubit-systems or mixtures of qubit-systems), while logical connectives are interpreted as reversible quantum logical gates. Hence, any formula of the quantum computational language represents a synthetic logical description of a quantum circuit. We investigate a many-valued approach to quantum information, where the basic notion of qubit has been replaced by the more general notion of qudit. The qudit-semantics allows us to represent as reversible gates some basic logical operations of Lukasiewicz many-valued logics. In the final part of the article we discuss some problems that concern possible implementations of gates by means of optical devices.

Abstract

Quantum computational logics are special examples of quantum logic where formulas are supposed to denote pieces of quantum information (qubit-systems or mixtures of qubit-systems), while logical connectives are interpreted as reversible quantum logical gates. Hence, any formula of the quantum computational language represents a synthetic logical description of a quantum circuit. We investigate a many-valued approach to quantum information, where the basic notion of qubit has been replaced by the more general notion of qudit. The qudit-semantics allows us to represent as reversible gates some basic logical operations of Lukasiewicz many-valued logics. In the final part of the article we discuss some problems that concern possible implementations of gates by means of optical devices.

*Manuscript

A Many-valued Approach to Quantum Computational Logics

M.L. Dalla Chiara[a], R. Giuntini, G. Sergioli[b], R. Leporini[c,*]

[a] *Dipartimento di Lettere e Filosofia, Università di Firenze, via Bolognese 52, I-50139 Firenze, Italy.*
[b] *Dipartimento di Pedagogia, Psicologia, Filosofia, Università di Cagliari, via Is Mirrionis 1, I-09123 Cagliari, Italy.*
[c] *Dipartimento di Ingegneria Gestionale, dell'Informazione e della Produzione, Università di Bergamo, viale Marconi 5, I-24044 Dalmine (BG), Italy.*

Abstract

Quantum computational logics are special examples of quantum logic where formulas are supposed to denote pieces of quantum information (qubit-systems or mixtures of qubit-systems), while logical connectives are interpreted as reversible quantum logical gates. Hence, any formula of the quantum computational language represents a synthetic logical description of a quantum circuit. We investigate a many-valued approach to quantum information, where the basic notion of *qubit* has been replaced by the more general notion of *qudit*. The qudit-semantics allows us to represent as reversible gates some basic logical operations of Łukasiewicz many-valued logics. In the final part of the article we discuss some problems that concern possible implementations of gates by means of optical devices.

Keywords: Quantum logics, quantum tomography, logical gates.

1. Introduction

The mathematical formalism of quantum theory has inspired the development of different forms of non-classical logics, called *quantum logics*. In

*Corresponding author

Email addresses: dallachiara@unifi.it (M.L. Dalla Chiara), giuntini@unica.it, giuseppe.sergioli@gmail.com (R. Giuntini, G. Sergioli), roberto.leporini@unibg.it (R. Leporini)

many cases the semantic characterizations of these logics are based on special classes of algebraic structures defined in a Hilbert-space environment. The prototypal example of quantum logic (created by Birkhoff and von Neumann) can be semantically characterized by referring to the class of all Hilbert-space lattices, whose support is the set $\mathcal{P}(\mathcal{H})$ of all projections of a Hilbert space $\mathcal{H}$. The question whether the class of all Hilbert-space lattices can be axiomatized by a set of equations is still open. What is known is that the variety of all orthomodular lattices (which gives rise to a semantic characterization of a logic often termed "abstract quantum logic") does not represent a faithful abstraction from the class of all Hilbert-space lattices. A characteristic example of an equation that holds in all Hilbert-space lattices, being possibly violated in orthomodular lattices is the *orthoarguesian law* [1, 3].

Interesting generalizations of Birkhoff and von Neumann's quantum logic are the so called *unsharp (or fuzzy) quantum logics* that can be semantically characterized by referring to different classes of algebraic structures whose support is the set of all *effects* of a Hilbert space. According to the standard interpretation of the quantum formalism, any projection $P \in \mathcal{P}(\mathcal{H})$ represents a *sharp physical event* to which any possible state of a physical system S (associated with the space $\mathcal{H}$) assigns a probability-value. Such events are called "sharp" because they satisfy the non-contradiction principle: $P \wedge P^{\perp} = \mathtt{0}$ (the infimum between P and its orthogonal projection $P^{\perp}$ is the null projection $\mathtt{0}$). Effects, instead, represent *unsharp physical events* that may violate the non-contradiction principle.

The set $\mathcal{E}(\mathcal{H})$ of all effects of a Hilbert space $\mathcal{H}$ is defined as the largest set of linear bounded operators E for which a *Born-probability* can be defined. In other words, for any density operator ρ of $\mathcal{H}$ (representing a possible state of a physical system S whose associated Hilbert space is $\mathcal{H}$), we have:

$$\mathtt{Tr}(\rho E) \in [0,1] \text{ (where } \mathtt{Tr} \text{ is the trace-functional).}$$

The number $\mathtt{Tr}(\rho E)$ represents the probability that a quantum system S in state ρ verifies the physical event represented by the effect E. Of course, $\mathcal{E}(\mathcal{H})$ properly includes $\mathcal{P}(\mathcal{H})$. Different kinds of algebraic structures have been induced on the set $\mathcal{E}(\mathcal{H})$, giving rise to various forms of *unsharp quantum logics* [2, 3].

A different approach to quantum logic has been developed in the framework of *quantum computational logics*, inspired by the theory of quantum computation [4]. While sharp and unsharp quantum logics refer to possible structures of physical events, the basic objects of quantum computational logics are *pieces of quantum information*: possible states of quantum systems that can store and transmit the information in question. *Maximal* pieces of information (which cannot be consistently extended to a richer knowledge) correspond to *pure states*, mathematically represented as unit vectors $|\psi\rangle$ of convenient Hilbert spaces. At the same time, pieces of information that do not necessarily express a maximal knowledge correspond to *mixed states* (or *mixtures*), mathematically represented as density operators ρ. Of course any pure state $|\psi\rangle$ corresponds to a special case of a density operator: the projection $P_{|\psi\rangle}$ that projects over the (one-dimensional) closed subspace determined by $|\psi\rangle$.

In this article we will investigate particular examples of quantum computational logics based on a "many-valued approach" to quantum information, where the fundamental notion of *qubit* has been replaced by the more general concept of *qudit*.

2. Qubits and qudits

As is well known, the basic concept of quantum information is the notion of *qubit* (or *qubit-state*): a possible pure state of a single quantum system, mathematically represented as a unit-vector $|\psi\rangle$ of the two-dimensional Hilbert space $\mathbb{C}^2$ (based on the set of all ordered pair of complex numbers). Accordingly, any qubit can be described as a superposition

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

where $|0\rangle = (1,0)$ and $|1\rangle = (0,1)$ (the two elements of the canonical basis of $\mathbb{C}^2$) represent, in this framework, the two classical bits (0 and 1) or, equivalently, the two classical truth-values (*Falsity* and *Truth*). From an intuitive point of view, a qubit $c_0|0\rangle + c_1|1\rangle$ can be regarded as an "uncertain answer" to a given question; an answer that might be false with probability $|c_0|^2$ and might be true with probability $|c_1|^2$.

A natural "many-valued generalization" of qubits is represented by *qudits*: unit-vectors living in a space $\mathbb{C}^d$, where $d \geq 2$. The elements of the canonical basis of $\mathbb{C}^d$ can be regarded as different truth-values, which can be conventionally indicated in the following way:

$|0\rangle = |\frac{0}{d-1}\rangle = (1, 0, \ldots, 0)$
$|\frac{1}{d-1}\rangle = (0, 1, 0, \ldots, 0)$

$$
\begin{aligned}
&|\tfrac{2}{d-1}\rangle = (0,0,1,0,\ldots,0)\\
&\vdots\\
&|1\rangle = |\tfrac{d-1}{d-1}\rangle = (0,\ldots,0,1).
\end{aligned}
$$

While $|0\rangle$ and $|1\rangle$ represent the truth-values *Falsity* and *Truth*, all other basis-elements correspond to *intermediate* truth-values.

A particularly interesting example of a qudit-space is the qutrit-space $\mathbb{C}^3$, where the truth-values are:

$$
\begin{aligned}
&|0\rangle = |\tfrac{0}{2}\rangle = (1,0,0)\\
&|\tfrac{1}{2}\rangle = (0,1,0)\\
&|1\rangle = |\tfrac{2}{2}\rangle = (0,0,1).
\end{aligned}
$$

From a physical point of view, this space can be naturally used to represent the spin-values of bosons. The eigenvalues of the observable $Spin_z$ (the spin in the z-direction, corresponding to the z-component of the angular momentum) can be associated to the elements of the canonical basis; while the spin-observables in all other directions can be associated to different bases of the space.

Like classical bits, qudits represent atomic pieces of information: answers (which, in the quantum case, are generally uncertain) to single questions. At the same time, complex pieces of quantum information can be naturally represented as possible states of composite quantum systems that can store the information in question. Accordingly, by using the quantum-theoretic formalism for the mathematical representation of composite systems (based on tensor-products), any piece of quantum information can be identified with a possible (pure or mixed) state of a quantum system: a density operator ρ living in a tensor-product space

$$\mathcal{H}_d^{(n)} = \underbrace{\mathbb{C}^d \otimes \ldots \otimes \mathbb{C}^d}_{n-times}, \text{ where } n \geq 1.$$

While d represents the number of truth-values, n represents the number of the components of the quantum system that stores the information ρ.

The canonical basis of $\mathcal{H}_d^{(n)}$ (whose elements are called *registers*) is the following set:

$$\left\{ |v_1,\ldots,v_n\rangle : |v_1\rangle,\ldots,|v_n\rangle \text{ are elements of the canonical basis of } \mathbb{C}^d \right\}$$

(where $|v_1, \ldots, v_n\rangle$ is an abbreviation for the tensor product $|v_1\rangle \otimes \ldots \otimes |v_n\rangle$). A *quregister* of $\mathcal{H}_d^{(n)}$ is a pure state, represented by a unit-vector $|\psi\rangle$ (or, equivalently, by the corresponding density operator $P_{|\psi\rangle}$).

In any space $\mathcal{H}_d^{(n)}$, each truth-value $|\frac{j}{d-1}\rangle$ determines a corresponding *truth-value projection* $P^{(n)}_{\frac{j}{d-1}}$, whose range is the closed subspace spanned by the set of all registers $|v_1, \ldots, v_n\rangle$ where $v_n = \frac{j}{d-1}$. From an intuitive point of view, $P^{(n)}_{\frac{j}{d-1}}$ represents the property "having the truth-degree $\frac{j}{d-1}$". In particular, $P_0^{(n)}$ and $P_1^{(n)}$ represent the *Falsity-property* and the *Truth-property*, respectively. On this basis, one can naturally apply the Born-rule and define for any state ρ (of $\mathcal{H}_d^{(n)}$) the probability that ρ satisfies the property $P^{(n)}_{\frac{j}{d-1}}$:

$$\mathrm{p}_{\frac{j}{d-1}}(\rho) := \mathtt{Tr}\Big(\rho \, P^{(n)}_{\frac{j}{d-1}}\Big).$$

The *probability tout court* of ρ can be then defined as the weighted mean of all truth-degrees.

Definition 1. The probability of a density operator ρ of $\mathcal{H}_d^{(n)}$.

$$\mathrm{p}^{(d)}(\rho) := \frac{1}{d-1} \sum_{j=1}^{d-1} j \, \mathrm{p}_{\frac{j}{d-1}}(\rho).$$

We have:

$$\mathrm{p}^{(d)}(\rho) = \mathtt{Tr}\Big(\rho \, (\mathtt{I}^{(n-1)} \otimes E)\Big),$$

where $\mathtt{I}^{(n-1)}$ is the identity operator (of $\mathcal{H}^{(n-1)}$) and E is the effect (of $\mathbb{C}^d$) represented by the following matrix:

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & \frac{1}{d-1} & 0 & \cdots & 0 \\ 0 & 0 & \frac{2}{d-1} & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

In the particular case where ρ corresponds to the qubit $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$, we obtain that $\mathrm{p}^{(2)}(\rho) = |c_1|^2$.

Due to the properties of the quantum-theoretic formalism, pieces of quantum information turn out to satisfy the characteristic *holistic* features of quantum states. Generally quantum information *flows* from a *whole* to its *parts*, and not the other way around, as happens either in classical information or in the semantics of many important logics (like classical logic, intuitionistic logic or standard fuzzy logics).

Consider a quregister $|\psi\rangle$ representing the pure state of a composite quantum system S consisting of n subsystems $S_1, \ldots, S_n$ (say, an n-electron system), and let $\mathcal{H}_d^{(k_1+\ldots+k_n)}$ be the Hilbert space associated to S. According to the quantum formalism $|\psi\rangle$ determines the *reduced states*

$$Red^{(1)}_{[k_1,\ldots,k_n]}(P_{|\psi\rangle}), \ldots, Red^{(n)}_{[k_1,\ldots,k_n]}(P_{|\psi\rangle})$$

of the subsystems $S_1, \ldots, S_n$. Generally, the state $|\psi\rangle$ of the global system S cannot be represented as the *factorized state* corresponding to the tensor-product of the states of the subsystems $S_1, \ldots, S_n$. We may have:

$$P_{|\psi\rangle} \neq Red^{(1)}_{[k_1,\ldots,k_n]}(P_{|\psi\rangle}) \otimes \ldots \otimes Red^{(n)}_{[k_1,\ldots,k_n]}(P_{|\psi\rangle}).$$

It may also happen that the states of all subsystems are one and the same proper mixture (while $|\psi\rangle$ is a pure state). Consequently, the states of the parts of S turn out to be *indistinguishable*. Furthermore, the information about the global system is more precise than the information about its parts. In such a case $|\psi\rangle$ is called an *entangled* pure state. Entanglement-phenomena (which have for a long time been described as mysterious and potentially paradoxical) represent today a powerful resource in quantum information; they are currently used, for instance, in quantum teleportation-experiments and in quantum cryptography.

3. Quantum logical gates

Quantum information is processed by *quantum logical gates* (briefly, *gates*) that transform pure and mixed pieces of quantum information in a reversible way. When applied to quregisters of a qudit-space $\mathcal{H}_d^{(n)}$ a gate is a *unitary operator* $G^{(n)}$: a reversible map that transforms all vectors of the space, preserving their length. At the same time, any unitary operator $G^{(n)}$ can be canonically extended to a *unitary operation* ${}^{\mathfrak{D}}G^{(n)}$ that transforms all density operators ρ of the space in a reversible way. We have:

$${}^{\mathfrak{D}}G^{(n)}(\rho) := G^{(n)} \rho \, G^{(n)^\dagger},$$

where $G^{(n)^\dagger}$ is the adjoint of $G^{(n)}$. In the particular case where ρ is a pure state $P_{|\psi\rangle}$, we obtain:

$$^{\mathfrak{D}}G^{(n)}(P_{|\psi\rangle}) = P_{G^{(n)}|\psi\rangle}.$$

For the sake of simplicity, we will call *gate* either a unitary operator $G^{(n)}$ or the corresponding unitary operation $^{\mathfrak{D}}G^{(n)}$.

Why is reversibility so important in quantum computation? The reason depends on the form of Schrödinger's equation, where unitary operators play an essential role. And, from a physical point of view, any quantum computation can be described as the time-evolution of a particular quantum system that transforms a given information-input into an information-output.

In the semantics of classical logic and of many important non-classical logics (including Birkhoff and von Neumann's quantum logic) the basic logical operations are generally dealt with as irreversible operations. In the (two-valued) classical semantics negation only is defined as a reversible truth-function:

$$v' := 1 - v, \text{ for any truth-value } \ v \in \{0, 1\}\,.$$

A the same time, both the conjunction $\sqcap$ and the disjunction $\sqcup$ are defined as irreversible truth-functions (for any pair of truth-values u, v):

$$u \sqcap v := \min(u, v);\ \ u \sqcup v := (u' \sqcap v')' = \max(u, v).$$

For our aims it is expedient to recall what happens in the semantics of many-valued Łukasiewicz logics (which represent special examples of fuzzy logics). In this case the set $\mathbf{TV}$ of truth-values is identified either with the real interval $[0, 1]$ or with a finite subset thereof (conventionally indicated as a set $\left\{\frac{0}{d-1}, \frac{1}{d-1}, \ldots, \frac{d-1}{d-1}\right\}$, where $d \geq 2$). The negation is defined like in the classical case:

$$v' := 1 - v, \text{ for any truth-value } \ v \in \mathbf{TV}.$$

At the same time the conjunction is split into two different irreversible operations, the *min-conjunction* $\sqcap$ (also called *lattice-conjunction*) and the *Lukasiewicz-conjunction* $\odot$:

$$u \sqcap v := \min(u, v),\ \ u \odot v := \max(0, u + v - 1), \text{ for any } \ u, v \in \mathbf{TV}.$$

While $\sqcap$ and $\odot$ are the same operations in the two-valued semantics, when $d > 2$ our two conjunctions turn out to satisfy different semantic properties.

The min-conjunction gives rise to possible violations of the non-contradiction principle. We may have:

$$v \sqcap v' \neq 0.$$

Hence, contradictions are not necessarily false, as happens in the case of most fuzzy logics whose basic aim is modeling ambiguous and unsharp semantic situations. At the same time, $\sqcap$ behaves as a lattice-operation in the truth-value partial order $(\mathbf{TV}, \leq)$. The Łukasiewicz-conjunction, instead, is generally non-idempotent. We may have:

$$v \odot v \neq v.$$

Apparently, one is dealing with a kind of conjunction that can be usefully applied to model semantic situations where "repetita iuvant!"("repetitions are useful!").

As expected, the two conjunctions $\sqcap$ and $\odot$ allow us to define two different kinds of disjunctions (via de Morgan-law):

$$u \sqcup v := (u' \sqcap v')' = \max(u, v); \quad u \oplus v := (u' \odot v')' = \min(1, u + v).$$

All these logical operations (which are usually dealt with as irreversible) can be simulated in the many-valued approach to quantum information by means of convenient (reversible) gates. Let us first consider pure pieces of quantum information: quregisters living in some qudit-spaces. In such a case, gates correspond to particular examples of unitary operators.

The logical negation has a natural gate-counterpart: the unitary operator $\mathtt{NOT}^{(n)}$, which is defined in any qudit-space $\mathcal{H}_d^{(n)}$, where $d \geq 2$ and $n \geq 1$.

Definition 2. The negation-gate of $\mathcal{H}_d^{(n)}$.
The negation-gate of $\mathcal{H}_d^{(n)}$ is the linear operator $\mathtt{NOT}^{(n)}$ that is defined for every element of the canonical basis of as follows:

$$\mathtt{NOT}^{(n)}|v_1, \ldots, v_n\rangle := |v_1, \ldots, v_{n-1}\rangle \otimes |1 - v_n\rangle.$$

In the particular case of $\mathcal{H}_d^{(1)} = \mathbb{C}^d$ we obtain:

$$\mathtt{NOT}^{(1)}|v\rangle := |1 - v\rangle.$$

Thus, $\mathtt{NOT}^{(1)}$ behaves as the standard fuzzy negation.

How to deal, in this framework, with the irreversible conjunctions $\sqcap$ and $\odot$? A reversible counterpart for these operations can be obtained by using two special versions of a gate that plays an important role in quantum computation: the *Toffoli-gate*. Let us first recall the definition of the Toffoli-gate for qubit-spaces.

Definition 3. The Toffoli-gate of a qubit-space.
For any $m, n, p \geq 1$, the Toffoli-gate $\mathtt{T}^{(m,n,p)}$ of the qubit-space $\mathcal{H}_2^{(m+n+p)}$ is the linear operator that is defined for every element of the canonical basis as follows:
$\mathtt{T}^{(m,n,p)}|u_1, \ldots, u_m, v_1, \ldots, v_n, w_1, \ldots w_p\rangle :=$
$|u_1, \ldots, u_m, v_1, \ldots, v_n, w_1, \ldots, w_{p-1}\rangle \otimes |(u_m \cdot v_n) \widehat{+}_2 \, w_p\rangle,$
where $\widehat{+}_2$ is the addition modulo 2.

Apparently the smallest qubit-space where the Toffoli-gate is defined is the space $\mathcal{H}_2^{(3)}$. In this case we have:

$$\mathtt{T}^{(1,1,1)}|u, v, w\rangle = |u, v, (u \cdot v) \widehat{+}_2 \, w\rangle.$$

The Toffoli-gate can be generalized to qudit-spaces in different ways. We will consider here two different gates that will be called the *Toffoli-gate* and the *Toffoli-Łukasiewicz gate*, respectively.

Definition 4. The Toffoli-gate of a qudit-space.
For any $m, n, p \geq 1$, the Toffoli-gate $\mathtt{T}^{(m,n,p)}$ of the qudit-space $\mathcal{H}_d^{(m+n+p)}$ is the linear operator that is defined for every element of the canonical basis as follows:
$\mathtt{T}^{(m,n,p)}|u_1, \ldots, u_m, v_1, \ldots, v_n, w_1, \ldots w_p\rangle :=$
$|u_1, \ldots, u_m, v_1, \ldots, v_n, w_1, \ldots, w_{p-1}\rangle \otimes |(u_m \sqcap v_n) \widehat{+}_d \, w_p\rangle,$
where $\widehat{+}_d$ is the addition modulo d.

Definition 5. The Toffoli-Łukasiewicz gate of a qudit-space.
For any $m, n, p \geq 1$, the Toffoli-Łukasiewicz gate $\mathtt{TŁ}^{(m,n,p)}$ of the qudit-space $\mathcal{H}_d^{(m+n+p)}$ is the linear operator that is defined for every element of the canonical basis as follows:
$\mathtt{TŁ}^{(m,n,p)}|u_1, \ldots, u_m, v_1, \ldots, v_n, w_1, \ldots w_p\rangle :=$
$|u_1, \ldots, u_m, v_1, \ldots, v_n, w_1, \ldots, w_{p-1}\rangle \otimes |(u_m \odot v_n) \widehat{+}_d \, w_p\rangle.$

Clearly, $\mathtt{T}^{(m,n,p)}$ and $\mathtt{TŁ}^{(m,n,p)}$ are the same gate when $d = 2$.

By using the unitary operations ${}^{\mathfrak{D}}\mathtt{T}^{(m,n,p)}$ and ${}^{\mathfrak{D}}\mathtt{TŁ}^{(m,n,p)}$ (which correspond to the unitary operators $\mathtt{T}^{(m,n,p)}$ and $\mathtt{TŁ}^{(m,n,p)}$, respectively) one can now define two different kinds of reversible conjunctions for any (pure or mixed) state of a qudit-space.

Definition 6. The Toffoli-conjunction in a qudit-space.
For any $m, n \geq 1$ and for any density operator ρ of a qudit-space $\mathcal{H}_d^{(m+n)}$ the Toffoli-conjunction $\mathtt{AND}^{(m,n)}$ is defined as follows:

$$\mathtt{AND}^{(m,n)}(\rho) := {}^{\mathfrak{D}}\mathtt{T}^{(m,n,1)}(\rho \otimes P_{|0\rangle}).$$

Definition 7. The Toffoli-Łukasiewicz conjunction in a qudit-space.
For any $m, n \geq 1$ and for any density operator ρ of a qudit-space $\mathcal{H}_d^{(m+n)}$ the Toffoli-Łukasiewicz conjunction $\mathtt{ŁAND}^{(m,n)}$ is defined as follows:

$$\mathtt{ŁAND}^{(m,n)}(\rho) := {}^{\mathfrak{D}}\mathtt{TŁ}^{(m,n,1)}(\rho \otimes P_{|0\rangle}).$$

In the definition of both conjunctions the projection $P_{|0\rangle}$ (which corresponds to the bit 0) plays the role of an *ancilla*, which is transformed by the gates ${}^{\mathfrak{D}}\mathtt{T}^{(m,n,1)}$ and ${}^{\mathfrak{D}}\mathtt{TŁ}^{(m,n,1)}$ into the final truth-value of the conjunction.

In the particular case of density operators corresponding to registers of $\mathcal{H}_2^{(2)}$ we obtain:

$$\mathtt{AND}^{(1,1)}(P_{|u,v\rangle}) = P_{\mathtt{T}^{(1,1,1)}|u,v,0\rangle}.$$

Hence:

$$\mathtt{AND}^{(1,1)}(P_{|u,v\rangle}) = \begin{cases} P_{|u,v,1\rangle}, & \text{if } u = v = 1; \\ P_{|u,v,0\rangle}, & \text{otherwise.} \end{cases}$$

(In agreement with the classical truth-table of conjunction).

In the general case, both the Toffoli and the Toffoli-Łukasiewicz conjunctions represent *holistic* forms of conjunction that reflect the characteristic holistic features of the quantum-theoretic formalism. Let $|\psi\rangle$ be a quregister of a space $\mathcal{H}_d^{(m+n)}$. We may have:

$$\mathtt{AND}^{(m,n)}(P_{|\psi\rangle}) \neq \mathtt{AND}^{(m,n)}(Red^{(1)}_{[m,n]}(P_{|\psi\rangle}) \otimes Red^{(2)}_{[m,n]}(P_{|\psi\rangle}));$$

$$\mathtt{ŁAND}^{(m,n)}(P_{|\psi\rangle}) \neq \mathtt{ŁAND}^{(m,n)}(Red^{(1)}_{[m,n]}(P_{|\psi\rangle}) \otimes Red^{(2)}_{[m,n]}(P_{|\psi\rangle})).$$

In other words, the conjunction over a *global* piece of information (consisting of two parts) does not generally coincide with the conjunction of the two separate parts. Interesting counterexamples arise with entangled quregisters. Consider, for instance, the following (entangled) *Bell-state*:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle).$$

We have:

$$\mathtt{T}^{(1,1,1)}(|\psi\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|0,0,0\rangle + |1,1,1\rangle).$$

Hence,

$$\mathtt{AND}^{(1,1)}(P_{|\psi\rangle}) = P_{\frac{1}{\sqrt{2}}(|0,0,0\rangle+|1,1,1\rangle)},$$

which is a pure state. At the same time,

$$Red^{1}_{[1,1]}(P_{|\psi\rangle}) = Red^{2}_{[1,1]}(P_{|\psi\rangle}) = \frac{1}{2}\mathtt{I}^{(1)}.$$

Thus,
$\mathtt{AND}^{(1,1)}(Red^{(1)}_{[1,1]}(P_{|\psi\rangle}) \otimes Red^{(2)}_{[1,1]}(P_{|\psi\rangle})) =$
${}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}(Red^{(1)}_{[1,1]}(P_{|\psi\rangle}) \otimes Red^{(2)}_{[1,1]}(P_{|\psi\rangle}) \otimes P_{|0\rangle}),$
which is a proper mixture.

The gates Negation, Toffoli and Toffoli-Łukasiewicz are also called "semiclassical gates", because they are unable to "create" superpositions. Whenever the information-input is a register, also the information-output will be a register. Quantum computation, however, cannot help referring also to "genuine quantum gates" that can transform classical inputs (represented by registers) into genuine superpositions. And it is needless to stress how superpositions play an essential role in quantum computation, being responsible for the characteristic parallel structures that determine the speed and the efficiency of quantum computers.

Let us first recall the definition of two important genuine quantum gates of the qubit-space $\mathcal{H}^{(1)}_2 = \mathbb{C}^2$.

Definition 8. The Hadamard-gate of $\mathcal{H}^{(1)}_2$.
The Hadamard-gate (also called *square-root of identity*) is the linear operator $\sqrt{\mathtt{I}}^{(1)}$ that is defined for every element of the canonical basis of $\mathcal{H}^{(1)}_2$ as follows:

$$\sqrt{\mathtt{I}}^{(1)}|v\rangle := \frac{1}{\sqrt{2}}((-1)^v|v\rangle + |1-v\rangle).$$

Definition 9. The square-root of negation of $\mathcal{H}_2^{(1)}$.
The square-root of negation is the linear operator $\sqrt{\mathtt{NOT}}^{(1)}$ that is defined for every element of the canonical basis of $\mathcal{H}_2^{(1)}$ as follows:

$$\sqrt{\mathtt{NOT}}^{(1)}|v\rangle := \frac{1}{2}((1+i)|v\rangle + (1-i)|1-v\rangle),$$

where i is the imaginary unit.

Apparently, both $\sqrt{\mathtt{I}}^{(1)}$ and $\sqrt{\mathtt{NOT}}^{(1)}$ transform classical pieces of information (corresponding to the truth-values *Falsity* and *Truth*) into genuine superpositions. We have:

$$\sqrt{\mathtt{I}}^{(1)}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \;\; \sqrt{\mathtt{NOT}}^{(1)}|0\rangle = \frac{1}{2}\Big((1+i)|0\rangle + (1-i)|1\rangle\Big).$$

$$\sqrt{\mathtt{I}}^{(1)}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle); \;\; \sqrt{\mathtt{NOT}}^{(1)}|1\rangle = \frac{1}{2}\Big((1-i)|0\rangle + (1+i)|1\rangle\Big).$$

In this way, all certain answers (*Falsity* or *Truth*) are transformed into maximally uncertain answers that assign probability-value $\frac{1}{2}$ either to the *Falsity* or to the *Truth*.

The gates $\sqrt{\mathtt{I}}^{(1)}$ and $\sqrt{\mathtt{NOT}}^{(1)}$ satisfy the following characteristic properties that have suggested their names ("square-root of identity" and "square-root of negation"):

$$\sqrt{\mathtt{I}}^{(1)}\sqrt{\mathtt{I}}^{(1)} = \mathtt{I}^{(1)}; \;\; \sqrt{\mathtt{NOT}}^{(1)}\sqrt{\mathtt{NOT}}^{(1)} = \mathtt{NOT}^{(1)}.$$

Both $\sqrt{\mathtt{I}}^{(1)}$ and $\sqrt{\mathtt{NOT}}^{(1)}$ can be generalized to any qubit-space $\mathcal{H}_2^{(n)}$.

Definition 10. The Hadamard-gate and the square-root of negation of $\mathcal{H}_2^{(n)}$.

1. The Hadamard-gate is the linear operator $\sqrt{\mathtt{I}}^{(n)}$ that is defined for every element of the canonical basis of $\mathcal{H}_2^{(n)}$ as follows:

$$\sqrt{\mathtt{I}}^{(n)}|v_1,\ldots,v_n\rangle := |v_1,\ldots,v_{n-1}\rangle \otimes \frac{1}{\sqrt{2}}\Big((-1)^{v_n}|v_n\rangle + |1-v_n\rangle\Big).$$

2. The square-root of negation is the linear operator $\sqrt{\mathtt{NOT}}^{(n)}$ that is defined for every element of the canonical basis of $\mathcal{H}_2^{(n)}$ as follows:

$$\sqrt{\mathtt{NOT}}^{(n)}|v_1,\ldots,v_n\rangle := |v_1,\ldots,v_{n-1}\rangle \otimes \frac{1}{2}\Big((1+i)|v_n\rangle + (1-i)|1-v_n\rangle\Big).$$

How can $\sqrt{\mathtt{I}}^{(n)}$ and $\sqrt{\mathtt{NOT}}^{(n)}$ be generalized to qudit-spaces? A natural generalization of the Hadamard-gate for the space $\mathcal{H}_d^{(1)} = \mathbb{C}^d$ is represented by the *Vandermonde-operator*, which generalizes the Walsh-Hadamard matrix used for discrete Fourier transforms.

Definition 11. The Vandermonde-gate of $\mathcal{H}_d^{(1)}$.
The Vandermonde-gate is the linear operator $\mathtt{V}^{(1)}$ that is defined for every element $|\frac{k}{d-1}\rangle$ of the canonical basis of $\mathcal{H}_d^{(1)}$ as follows:

$$\mathtt{V}^{(1)}\left|\frac{k}{d-1}\right\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^{j\,k}\left|\frac{j}{d-1}\right\rangle,$$

where $\omega = e^{\frac{2\pi i}{d}}$.

Lemma 1. *The gate $\mathtt{V}^{(1)}$ of $\mathcal{H}_d^{(1)}$ satisfies the following conditions:*

1) $\mathtt{V}^{(1)} = \sqrt{\mathtt{I}}^{(1)}$, *if $d = 2$.*
2) $\mathtt{V}^{(1)}\mathtt{V}^{(1)}\mathtt{V}^{(1)}\mathtt{V}^{(1)} = \mathtt{I}^{(1)}$.
3) $\mathtt{V}^{(1)}$ *transforms each element of the canonical basis of $\mathcal{H}_d^{(1)}$ into a superposition of all basis-elements, assigning to each basis-element the same probability-value.*

Conditions 1)- 3) of Lemma 1 clearly show that $\mathtt{V}^{(1)}$ represents a "good" generalization of the Hadamard-gate for the qudit-space $\mathbb{C}^d$. In particular, condition 2) explains the reason why $\mathtt{V}^{(1)}$ is also termed the "fourth root of identity".

Another possible generalization of the Hadamard-gate to qudit-spaces is an operator that will be called the *Hadamard-gate restricted to the first two truth-values*, indicated by $\sqrt{\mathtt{I}}_{[2]}^{(1)}$. Unlike $\mathtt{V}^{(1)}$, which transforms all basis-elements into genuine superpositions, the gate $\sqrt{\mathtt{I}}_{[2]}^{(1)}$ only acts on the first two basis-elements $\left(|\frac{0}{d-1}\rangle, |\frac{1}{d-1}\rangle\right)$.

Definition 12. The Hadamard-gate restricted to the first two truth-values of $\mathcal{H}_d^{(1)}$.
The Hadamard-gate restricted to the first two truth-values is the linear operator $\sqrt{\mathtt{I}}_{[2]}^{(1)}$ that is defined for every element $|v\rangle$ of the canonical basis of $\mathcal{H}_d^{(1)}$ as follows:

$$\sqrt{\mathtt{I}}_{[2]}^{(1)}|v\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + |\frac{1}{d-1}\rangle), & \text{if } v = 0; \\ \frac{1}{\sqrt{2}}(|0\rangle - |\frac{1}{d-1}\rangle), & \text{if } v = \frac{1}{d-1}; \\ |v\rangle, \text{ otherwise.} \end{cases}$$

Of course, for the qubit-space $\mathbb{C}^2$ we have:

$$\sqrt{\mathtt{I}}_{[2]}^{(1)} = \sqrt{\mathtt{I}}^{(1)}.$$

In a similar way, the (restricted) square-root of negation can be generalized to any qudit-space.

Definition 13. The square-root of negation restricted to the first two truth-values of $\mathcal{H}_d^{(1)}$.
The square-root of negation restricted to the first two truth-values is the linear operator that is defined for every element $|v\rangle$ of the canonical basis of $\mathcal{H}_d^{(1)}$ as follows:

$$\sqrt{\mathtt{NOT}}_{[2]}^{(1)}|v\rangle := \begin{cases} \frac{1}{2}((1+i)|0\rangle + (1-i)|\frac{1}{d-1}\rangle), & \text{if } v = 0; \\ \frac{1}{2}((1-i)|0\rangle + (1+i)|\frac{1}{d-1}\rangle), & \text{if } v = \frac{1}{d-1}; \\ |v\rangle, \text{ otherwise.} \end{cases}$$

The three gates $\mathtt{V}^{(1)}$, $\sqrt{\mathtt{I}}_{[2]}^{(1)}$ and $\sqrt{\mathtt{NOT}}_{[2]}^{(1)}$ can be naturally generalized to any qudit-space $\mathcal{H}_d^{(n)}$.

Definition 14. The gates $\mathtt{V}^{(n)}$, $\sqrt{\mathtt{I}}_{[2]}^{(n)}$, $\sqrt{\mathtt{NOT}}_{[2]}^{(n)}$ of $\mathcal{H}_d^{(n)}$.
Let $|v_1, \ldots, v_n\rangle$ be an element of the canonical basis of $\mathcal{H}_d^{(n)}$.

1) $\mathtt{V}^{(n)}|v_1, \ldots, v_n\rangle := |v_1, \ldots, v_{n-1}\rangle \otimes \mathtt{V}^{(1)}|v_n\rangle$.
2) $\sqrt{\mathtt{I}}_{[2]}^{(n)}|v_1, \ldots, v_n\rangle := |v_1, \ldots, v_{n-1}\rangle \otimes \sqrt{\mathtt{I}}_{[2]}^{(1)}|v_n\rangle$.
3) $\sqrt{\mathtt{NOT}}_{[2]}^{(n)}|v_1, \ldots, v_n\rangle := |v_1, \ldots, v_{n-1}\rangle \otimes \sqrt{\mathtt{NOT}}_{[2]}^{(1)}|v_n\rangle$.

4. Representing quantum information in Bloch-hyperspheres

It is customary to represent the density operators of the qubit-space $\mathbb{C}^2$ as vectors of the three-dimensional Bloch-sphere $\mathbf{BS}^{[3]}$ of radius 1. Let $\mathfrak{D}(\mathbb{C}^2)$ represent the set of all density operators of $\mathbb{C}^2$. For any $\rho \in \mathfrak{D}(\mathbb{C}^2)$, the corresponding Bloch-vector $\mathbf{b}^\rho$ is determined as follows:

$$\mathbf{b}^\rho = (b_1^\rho, b_2^\rho, b_3^\rho),$$

where $b_1^\rho = \mathtt{Tr}(\rho\, \boldsymbol{\sigma}_1)$, $b_2^\rho = \mathtt{Tr}(\rho\, \boldsymbol{\sigma}_2)$, $b_3^\rho = \mathtt{Tr}(\rho\, \boldsymbol{\sigma}_3)$. The operators $\boldsymbol{\sigma}_1$, $\boldsymbol{\sigma}_2$, $\boldsymbol{\sigma}_3$ are the three Pauli-matrices that are defined as follows:

$$\boldsymbol{\sigma}_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \; \boldsymbol{\sigma}_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \; \boldsymbol{\sigma}_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Viceversa, for any Bloch-vector $\mathbf{b} = (b_1, b_2, b_3)$ the corresponding density operator $\rho^{\mathbf{b}}$ is determined by the following matrix:

$$\frac{1}{2} \begin{bmatrix} 1 + b_3 & b_1 - ib_2 \\ b_1 + ib_2 & 1 - b_3 \end{bmatrix}.$$

We have:

$$\rho^{\mathbf{b}^\rho} = \rho; \;\; \mathbf{b}^{\rho^{\mathbf{b}}} = \mathbf{b}.$$

Via the Bloch-representation, any density operator ρ of $\mathbb{C}^2$ can be canonically represented as a combination of four unitary operators (of $\mathbb{C}^2$): the identity operator $\mathtt{I}^{(1)}$ and the three Pauli-matrices. For any ρ we have:

$$\rho = \frac{1}{2}(\mathtt{I}^{(1)} + b_1^\rho \boldsymbol{\sigma}_1 + b_2^\rho \boldsymbol{\sigma}_2 + b_3^\rho \boldsymbol{\sigma}_3).$$

The Pauli-representation can be generalized to any qudit-space. Let us first introduce the *generalized Pauli-matrices* of a space $\mathbb{C}^d$ (with $d \geq 2$).[1] For the sake of simplicity, in the following, we will also write $|j\rangle$ instead of $|\frac{j}{d-1}\rangle$.

[1]We recall that $|\psi\rangle\langle\varphi|$ denotes the linear operator A that satisfies the following condition for any vector $|\chi\rangle$: $A|\chi\rangle = \langle\varphi|\chi\rangle|\psi\rangle$, where $\langle\varphi|\chi\rangle$ is the inner product of $|\varphi\rangle$ and $|\chi\rangle$.

Definition 15. The generalized Pauli-matrices of $\mathbb{C}^d$.
Let j, k, l be three natural numbers such that: $1 \le j \le d^2 - 1$ and $0 \le k < l \le d - 1$. The generalized Pauli-matrices $\boldsymbol{\sigma}_j$ of $\mathbb{C}^2$ are defined as follows:

$$\boldsymbol{\sigma}_j = \begin{cases} |k\rangle\langle l| + |l\rangle\langle k|, \\ \qquad \text{if } j \le \frac{d(d-1)}{2} \text{ and } j = \frac{k(1-k)}{2} + (d-2)k + l; \\ -i|k\rangle\langle l| + i|l\rangle\langle k|, \\ \qquad \text{if } \frac{d(d-1)}{2} < j \le d(d-1) \text{ and } j = \frac{d(d-1)+k(1-k)}{2} + (d-2)k + l; \\ \sqrt{\frac{2}{l(l+1)}}\Big(\sum_{k=0}^{l-1} |k\rangle\langle k| - l|l\rangle\langle l|\Big), \\ \qquad \text{if } j > d(d-1) \text{ and } j = d(d-1) + l. \end{cases}$$

As expected, in the particular case of the space $\mathbb{C}^2$ the three generalized Pauli-matrices $\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \boldsymbol{\sigma}_{2^2-1}$ turn out to coincide with the three standard Pauli-matrices.

Like in the qubit-case, any density operator $\rho \in \mathfrak{D}(\mathbb{C}^d)$ can be canonically represented as a combination of the identity operator and of the generalized Pauli-matrices $\boldsymbol{\sigma}_1, \ldots, \boldsymbol{\sigma}_j, \ldots, \boldsymbol{\sigma}_{d^2-1}$. We have:

$$\rho = \frac{1}{d}\Big(\mathtt{I}^{(1)} + \sqrt{\frac{d(d-1)}{2}} \sum_{j=1}^{d^2-1} b_j \boldsymbol{\sigma}_j\Big),$$

where $b_j = \sqrt{\frac{d}{2(d-1)}}\mathtt{Tr}(\rho\,\boldsymbol{\sigma}_j) \in \mathbb{R}$.

On this basis, any density operator ρ of $\mathbb{C}^d$ can be associated to a vector

$$\mathbf{b}^\rho = (b_1^\rho, \ldots, b_j^\rho, \ldots, b_{d^2-1}^\rho)$$

of the (real) Bloch-hypersphere $\mathbf{BHS}_{\mathbb{R}}^{[d^2-1]}$, whose radius is 1 and whose dimension is $d^2 - 1$. Notice that, unlike the case of $\mathbb{C}^2$, not all vectors of the hypersphere $\mathbf{BHS}_{\mathbb{R}}^{[d^2-1]}$ correspond to density operators.

Another interesting representation of the density operators of $\mathbb{C}^d$ can be obtained in terms of the Weyl-operators (which have been used in quantum teleportation-experiments and in the study of the geometry of entanglement).

Definition 16. The Weyl-operators of $\mathbb{C}^d$.
Let j be a natural number such that $0 \le j \le d^2 - 1$. The Weyl-operators $\mathtt{W}_j$ of $\mathbb{C}^d$ are defined as follows:

$$\mathtt{W}_j = \sum_{m=0}^{d-1} \omega^{km} |m\rangle\langle m \,\hat{+}_d\, j|,$$

where $\omega = e^{\frac{2\pi i}{d}}$, $k = \lfloor \frac{j}{d} \rfloor$ (the integer part of $\frac{j}{d}$).

In the case of the qubit-space $\mathbb{C}^2$ we obtain:

$$(\mathtt{W}_1, \mathtt{W}_2, \mathtt{W}_3) = (\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_3, i\boldsymbol{\sigma}_2).$$

In some applications an important role is played by the first Weyl-operator $\mathtt{W}_1$, which turns out to be described by the following matrix:

$$\mathtt{W}_1 = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & 0 & \ddots & 0 \\ 0 & 0 & \vdots & \ddots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

As happens in the case of the Pauli-representation, all density operators ρ of $\mathbb{C}^d$ can be canonically represented as combinations of the identity operator and of the Weyl-operators. We have:

$$\rho = \frac{1}{d}\Big(\mathtt{I}^{(1)} + \sqrt{d-1}\sum_{j=1}^{d^2-1} b_j \mathtt{W}_j\Big),$$

where $b_j = \frac{1}{\sqrt{d-1}}\mathtt{Tr}(\rho\, \mathtt{W}_j^\dagger) \in \mathbb{C}$.

On this basis, any density operator $\rho \in \mathfrak{D}(\mathbb{C}^d)$ can be associated to a vector

$$\mathbf{b}^\rho = (b_1^\rho, \ldots, b_j^\rho, \ldots, b_{d^2-1}^\rho)$$

of the complex Bloch-hypersphere $\mathbf{BHS}_{\mathbb{C}}^{[d^2-1]}$, whose radius is 1 and whose dimension is $d^2 - 1$.

In spite of their mathematical interest, both the Pauli and the Weyl-representations turn out to be "non-economical", since they essentially refer to d^2-1 gates, whose implementation might be highly complicated. The following theorem allows us to simplify such situation, showing that the probabilistic behavior of three gates only determines a tomographic reconstruction of any state of $\mathbb{C}^d$. Let $\mathcal{B}(\mathbb{C}^d)$ represent the set of all bounded operators of the space $\mathbb{C}^d$.

Theorem 2. *Let ρ be a density operator of a qudit-space $\mathbb{C}^d$. There exist d^2-1 unitary operators $\mathtt{U}_1, \ldots, \mathtt{U}_{d^2-1}$ (defined on $\mathbb{C}^d$) and a function $f : [0,1]^{d^2-1} \longmapsto \mathcal{B}(\mathbb{C}^d)$ that satisfy the following conditions:*

1) each $\mathtt{U}_j$ (with $1 \le j \le d^2 - 1$) is a finite combination of the three following gates: $\sqrt{\mathtt{I}}^{(1)}_{[2]}$, $\sqrt{\mathtt{NOT}}^{(1)}_{[2]}$, $\mathtt{W}_1$ (defined on $\mathbb{C}^d$).

2) For any sequence $(p_1, \ldots, p_j, \ldots, p_{d^2-1}) \in [0,1]^{d^2-1}$ such that $p_j = \mathtt{p}^{(d)}(\,^{\mathfrak{D}}\mathtt{U}_j(\rho))$, we have:

$$\rho = f(p_1, \ldots, p_j, \ldots, p_{d^2-1})$$

(where $\mathtt{p}^{(d)}$ is the probability-function defined in Section 2).

Proof. (Sketch) It is expedient to distinguish the case where $d = 2$ from the case where $d > 2$.

1) Let $\rho \in \mathfrak{D}(\mathbb{C}^2)$. Consider its Pauli representation and let $\mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}$ the Bloch-vector that corresponds to ρ. Define the operators $\mathtt{U}_1, \mathtt{U}_2, \mathtt{U}_3$ as follows:

$$\mathtt{U}_1 = \sqrt{\mathtt{I}}^{(1)}_{[2]},\ \mathtt{U}_2 = \sqrt{\mathtt{NOT}}^{(1)}_{[2]},\ \mathtt{U}_3 = \mathtt{W}_1.$$

Consider the following three equations:

$$\mathrm{p}^{(2)}(\,^{\mathfrak{D}}\mathtt{U}_1(\rho)) = p_1,\ \mathrm{p}^{(2)}(\,^{\mathfrak{D}}\mathtt{U}_2(\rho)) = p_2,\ \mathrm{p}^{(2)}(\,^{\mathfrak{D}}\mathtt{U}_3(\rho)) = p_3.$$

We have:
$$\frac{1-b_1}{2} = p_1, \frac{1-b_2}{2} = p_2, \frac{1+b_3}{2} = p_3.$$

Hence, $A\mathbf{b} + A\mathbf{c} = \mathbf{p}$, where:

$$A = \begin{bmatrix} -\frac{1}{2} & 0 & 0 \\ 0 & -\frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} \end{bmatrix}, \mathbf{c} = \begin{bmatrix} -1 \\ -1 \\ 1 \end{bmatrix}, \mathbf{p} = \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}.$$

Define $f : [0,1]^3 \to \mathcal{B}(\mathbb{C}^2)$ as follows (for any $e_1, e_2, e_3 \in [0,1]$):

$$f(e_1, e_2, e_3) := \frac{1}{2}\Big(\mathtt{I}^{(1)} + (1-2e_1)\boldsymbol{\sigma}_1 + (1-2e_2)\boldsymbol{\sigma}_2 - (1-2e_3)\boldsymbol{\sigma}_3\Big).$$

We obtain: $\rho = f(p_1, p_2, p_3)$.

2) Let $\rho \in \mathfrak{D}(\mathbb{C}^d)$ (with $d > 2$). For any h such that $1 \leq h \leq d^2 - 1$, define $\mathtt{U}_h$ as follows:

$$\mathtt{U}_h = \mathtt{W}_1^m \sqrt{\mathtt{I}}_{[2]}^{(1)} \mathtt{W}_1^{m\dagger} \mathtt{W}_1^n \sqrt{\mathtt{NOT}}_{[2]}^{(1)} \mathtt{W}_1^{n\dagger},$$

where $\mathtt{W}_1^m = \underbrace{\mathtt{W}_1 \ldots \mathtt{W}_1}_{m-times}$, $\mathtt{W}_1^n = \underbrace{\mathtt{W}_1 \ldots \mathtt{W}_1}_{n-times}$, $m = \lfloor \frac{h}{d} \rfloor$ (the integer part of $\frac{h}{d}$) and $n = h \mod d$ (h modulo d). Consider the following $d^2 - 1$ equations:

$$\mathrm{p}^{(d)}({}^{\mathfrak{D}}\mathtt{U}_h(\rho)) = p_h.$$

We have: $A\mathbf{b} + A\mathbf{c} = \mathbf{p}$, where A, $\mathbf{b}$, $\mathbf{c}$ are matrices defined like in the $\mathbb{C}^2$-case.

Define $f : [0,1]^{d^2-1} \to \mathcal{B}(\mathbb{C}^d)$ as follows (for any $\mathbf{e} \in [0,1]^{d^2-1}$):

$$f(\mathbf{e}) := \frac{1}{d}\Big(\mathtt{I}^{(1)} + \sqrt{\frac{d(d-1)}{2}}(A^{-1}\mathbf{e} - \mathbf{c})^{\mathtt{T}}\boldsymbol{\sigma}\Big).$$

We obtain: $\rho = f(\mathbf{p})$.

5. Many-valued quantum computational logics

Quantum computational logics are special examples of quantum logic based on the following semantic idea: linguistic formulas are supposed to denote pieces of quantum information, while logical connectives are interpreted as particular gates that play an important logical role [4]. Accordingly, any formula of the quantum computational language can be regarded as a synthetic logical description of a quantum circuit. We will consider here a many-valued version of the quantum computational semantics, where, for any choice of a truth-value number d, the *meaning* of any formula α is identified with a density operator ρ living in a qudit-space $\mathcal{H}_d^{(n)}$, whose dimension depends on the linguistic complexity of α.

Let us first introduce the formal language: a "minimal" many-valued quantum computational language $\mathcal{L}$, whose alphabet contains atomic formulas $(\mathbf{q}, \mathbf{q}_1, \mathbf{q}_2, \ldots)$ including two privileged formulas $\mathbf{t}$ and $\mathbf{f}$ that represent the truth-values *Truth* and *Falsity* respectively. The connectives of $\mathcal{L}$ are at least the following: the negation $\neg$ (corresponding to the gate $\mathtt{NOT}^{(n)}$), the ternary Toffoli-connective T (corresponding to the gate $\mathtt{T}^{(m,n,p)}$), the ternary

Toffoli-Łukasiewicz connective $\mathsf{T}_{\text{Ł}}$ (corresponding to the gate $\mathtt{TŁ}^{(m,n,p)}$), the square root of identity $\sqrt{id}$ (corresponding to the gate $\sqrt{\mathtt{I}}^{(n)}$).

The notion of *formula* of $\mathcal{L}$ is inductively defined as follows: 1) atomic formulas are formulas; 2) if α, β, γ are formulas, then $\neg\alpha$, $\sqrt{id}\,\alpha$, $\mathsf{T}(\alpha,\beta,\gamma)$, $\mathsf{T}_{\text{Ł}}(\alpha,\beta,\gamma)$ are formulas. Recalling the definition of the two holistic conjunctions $\mathtt{AND}^{(m,n)}$ and $\mathtt{ŁAND}^{(m,n)}$ (given in Section 3), two binary connectives $\wedge$ and $\wedge_{\text{Ł}}$ can be defined in terms of the two Toffoli-connectives:

$$\alpha \wedge \beta := \mathsf{T}(\alpha,\beta,\mathbf{f});\ \ \alpha \wedge_{\text{Ł}} \beta := \mathsf{T}_{\text{Ł}}(\alpha,\beta,\mathbf{f})$$

(where $\mathbf{f}$ plays the role of a *syntactical ancilla*). On this basis two binary disjunctions ($\vee$ and $\vee_{\text{Ł}}$) can be defined (via de Morgan-law) in the expected way

By *atomic complexity* of a formula α we mean the number $At(\alpha)$ of occurrences of atomic subformulas in α. For instance, the atomic complexity of the formula $\alpha = \mathbf{q}\wedge\neg\mathbf{q} = \mathsf{T}(\mathbf{q},\neg\mathbf{q},\mathbf{f})$ is 3. The number $At(\alpha)$ plays an important semantic role, since it determines, for any choice of a truth-value number d, the *semantic space* $\mathcal{H}_d^{\alpha} = \mathcal{H}_d^{(At(\alpha))}$, where any density operator representing a possible *meaning* of α shall live. We have, for instance, $\mathcal{H}_d^{\mathsf{T}(\mathbf{q},\neg\mathbf{q},\mathbf{f})} = \mathcal{H}_d^{(3)}$.

Any formula α can be naturally decomposed into its parts giving rise to a special configuration, called the *syntactical tree* of α ($STree^{\alpha}$). Roughly, $STree^{\alpha}$ can be represented as a sequence of *levels* consisting of subformulas of α. The *bottom-level* is (α), while all other levels are obtained by dropping, step by step, all connectives occurring in α. Hence, the *top-level* is the sequence of atomic formulas occurring in α. As an example consider again the formula $\alpha = \mathsf{T}(\mathbf{q},\neg\mathbf{q},\mathbf{f})$. In such a case, $STree^{\alpha}$ is the following sequence of *levels*:

$$\begin{aligned} Level_3^{\alpha} &= (\mathbf{q},\mathbf{q},\mathbf{f}) \\ Level_2^{\alpha} &= (\mathbf{q},\neg\mathbf{q},\mathbf{f}) \\ Level_1^{\alpha} &= (\mathsf{T}(\mathbf{q},\neg\mathbf{q},\mathbf{f})) \end{aligned}$$

For any α and for any choice of a truth-value number d, $STree^{\alpha}$ uniquely determines the *gate-tree* of α: a sequence of gates all defined on the space $\mathcal{H}_d^{\alpha}$. As an example, consider again the formula, $\alpha = \mathsf{T}(\mathbf{q},\neg\mathbf{q},\mathbf{f})$. In the syntactical tree of α the second level has been obtained (from the third level) by repeating the first occurrence of $\mathbf{q}$, by negating the second occurrence of $\mathbf{q}$ and by repeating $\mathbf{f}$; while the first level has been obtained (from the second level) by applying the Toffoli-connective. Accordingly, the gate-tree of α can be naturally identified with the following gate-sequence:

$$({}^{\mathfrak{D}}\mathtt{I}^{(1)} \otimes {}^{\mathfrak{D}}\mathtt{NOT}^{(1)} \otimes {}^{\mathfrak{D}}\mathtt{I}^{(1)},\ {}^{\mathfrak{D}}\mathtt{T}^{(1,1,1)}).$$

This procedure can be naturally generalized to any α, whose gate-tree will be indicated by $({}^{\mathfrak{D}}\mathtt{G}^{\alpha}_{n-1}, \ldots, {}^{\mathfrak{D}}\mathtt{G}^{\alpha}_{1})$ (where n is the number of levels of $STree^{\alpha}$).

We consider here a *holistic* version of the quantum computational semantics, where entanglement can be used as a "semantic resource" [5]. Generally, the meaning of a compound formula determines the *contextual* meanings of its parts (and not the other way around, as happens in the case of most *compositional* semantic approaches).

As expected, all basic notions of the many-valued quantum computational semantics depend on the choice of the truth-value number d. The concept of (d-valued) *model* of $\mathcal{L}$ is based on the notion of (d-valued) *holistic map* for $\mathcal{L}$. This is a map $\mathtt{Hol}_d$ that assigns to each level of the syntactical tree of any formula α a density operator living in the semantic space of α. We have:

$$\mathtt{Hol}_d(Level^{\alpha}_k) \in \mathfrak{D}(\mathcal{H}^{\alpha}_d).$$

Suppose that $Level^{\alpha}_k = (\beta_{k_1}, \ldots, \beta_{k_r})$. It is natural to describe $\rho = \mathtt{Hol}_d(Level^{\alpha}_k)$ as a possible state of a composite quantum system consisting of r subsystems. Hence, the *contextual meaning* $(\mathtt{Hol}^{\alpha}_d(\beta_{k_j}))$ of the occurrence β_{k_j} (in $STree^{\alpha}$) can be identified with the reduced state of ρ with respect to the j-th subsystem. Accordingly, we can write:

$$\mathtt{Hol}^{\alpha}_d(\beta_{k_j}) = Red^{(j)}_{[At(\beta_{k_1}),\ldots,At(\beta_{k_r})]}(\rho).$$

The concepts of *model*, *truth* and *logical consequence* (of the d-valued semantics) can be now defined as follows.

Definition 17. Model.
A *model* (or *interpretation*) of the language $\mathcal{L}$ is a holistic map $\mathtt{Hol}_d$ that satisfies the following conditions for any formula α:

1) $\mathtt{Hol}_d$ assigns the same contextual meaning to different occurrences of one and the same subformula of α (in $STree^{\alpha}$).
2) The contextual meanings of the true formula $\mathbf{t}$ and of the false formula $\mathbf{f}$ are the *Truth* $P^{(1)}_1$ and the *Falsity* $P^{(1)}_0$, respectively.

3) $\mathtt{Hol}_d$ preserves the logical form of α by interpreting the connectives of α as the corresponding gates. Accordingly, if $({}^{\mathfrak{D}}\mathtt{G}^{\alpha}_{n-1}, \ldots, {}^{\mathfrak{D}}\mathtt{G}^{\alpha}_{1})$ is the gate-tree of α, then $\mathtt{Hol}_d(Level^{\alpha}_{k}) = {}^{\mathfrak{D}}\mathtt{G}^{\alpha}_{k}(\mathtt{Hol}_d(Level^{\alpha}_{k+1}))$.

On this basis we put:

$$\mathtt{Hol}_d(\alpha) := \mathtt{Hol}_d(Level^{\alpha}_1), \text{ for any formula } \alpha.$$

Notice that any $\mathtt{Hol}_d(\alpha)$ represents a kind of autonomous semantic context that is not necessarily correlated with the meanings of other formulas. Generally we have: $\mathtt{Hol}^{\gamma}_d(\beta) \neq \mathtt{Hol}^{\delta}_d(\beta)$. Thus, one and the same formula may receive different contextual meanings in different contexts.

Definition 18. Truth.
A formula α is called *true* with respect to a model $\mathtt{Hol}_d$ iff $\mathtt{p}^{(d)}(\mathtt{Hol}_d(\alpha)) = 1$.

Definition 19. Logical consequence.
A formula β is called a *logical consequence* of a formula α iff for any formula γ such that α and β are subformulas of γ and for any model $\mathtt{Hol}_d$:

$$\mathtt{p}^{(d)}(\mathtt{Hol}^{\gamma}_d(\alpha)) \leq \mathtt{p}^{(d)}(\mathtt{Hol}^{\gamma}_d(\beta)).$$

Apparently, both *Truth* and *Logical consequence* are, in this semantics, probabilistic notions that essentially depend on the probability-function $\mathtt{p}^d$. For any choice of d, the notion of logical consequence of the d-valued semantics characterizes a special example of logic, called *d-valued holistic quantum computational logic* (indicated by $^{\mathbf{d}}\mathbf{HQCL}$).

All logics $^{\mathbf{d}}\mathbf{HQCL}$ give rise to violations of some important logical implications (which hold for many standard logics).[2] For instance, both conjunctions $\wedge$ and $\wedge_{\text{Ł}}$ are generally non-idempotent, non-commutative and non-associative, although the corresponding truth-value operations ($\sqcap$, $\odot$) do satisfy commutativity and associativity. This can be explained by recalling the contextual behavior of quantum meanings. It may happen that for some context γ:

$$\mathtt{Hol}^{\gamma}_d(\alpha \wedge \beta) \neq \mathtt{Hol}^{\gamma}_d(\beta \wedge \alpha) \text{ and } \mathtt{p}^{(d)}(\mathtt{Hol}^{\gamma}_d(\alpha \wedge \beta)) > \mathtt{p}^{(d)}(\mathtt{Hol}^{\gamma}_d(\beta \wedge \alpha)).$$

[2]Counterexamples in the framework of the qubit-semantics have been described in [5].

Accordingly, different forms of holistic quantum computational logics (also in a first-order version) can be naturally applied to represent semantic phenomena (even far from microphysics), where contextuality, ambiguity and fuzziness play an essential role (as happens in the case of natural languages or in the languages of art) [6, 7].

6. Physical implementations by optical devices

Physical implementations of quantum logical gates represent the basic issue for the technological realization of quantum computers. Among the different choices that have been investigated in the literature we will consider here the case of optical devices, where photon-beams (possibly consisting of single photons) move in different directions. Let us conventionally assume that $|0\rangle$ represents the state of a beam moving along the x-direction, while $|1\rangle$ is the state of a beam moving along the y-direction.

In the framework of this "physical semantics", one-qubit gates (like $\mathtt{NOT}^{(1)}$, $\sqrt{\mathtt{I}}^{(1)}$, $\sqrt{\mathtt{NOT}}^{(1)}$) can be easily implemented. A natural implementation of $\mathtt{NOT}^{(1)}$ can be obtained by a mirror $\mathtt{M}$ that reflects in the y-direction any beam moving along the x-direction, and vice versa. Hence we have:

$$|0\rangle \ \rightarrowtail_{\mathtt{M}} \ |1\rangle; \quad |1\rangle \ \rightarrowtail_{\mathtt{M}} \ |0\rangle$$

(the mirror transforms the state $|0\rangle$ into the state $|1\rangle$, and vice versa).

An implementation of the Hadamard-gate $\sqrt{\mathtt{I}}^{(1)}$ can be obtained by a symmetric $50:50$ beam splitter $\mathtt{BS}$. We have:

$$|0\rangle \ \rightarrowtail_{\mathtt{BS}} \ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \quad |1\rangle \ \rightarrowtail_{\mathtt{BS}} \ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Accordingly, any beam that goes through $\mathtt{BS}$ is split into two components: one component moves along the x-direction, while the other component moves along the y-direction. And the probability of both paths (along the x-direction or along the y-direction) is $\frac{1}{2}$. Also the gate $\sqrt{\mathtt{NOT}}^{(1)}$ can be implemented in a similar way.

Other apparatuses that may be useful for optical implementations of gates are the *relative phase shifters* along a given direction. A particular example is described by the following unitary operator.

Definition 20. The relative phase shifter along the y-direction.
The relative phase shifter along the y-direction is the linear operator $\mathtt{U}_{\mathtt{PS}}$ that is defined for every element of the canonical basis of $\mathbb{C}^2$ as follows:
$\mathtt{U}_{\mathtt{PS}}|v\rangle = c|v\rangle$, where $c = \begin{cases} e^{i\pi}, & \text{if } v = 1; \\ 1, & \text{otherwise.} \end{cases}$

We obtain:

$$\mathtt{U}_{\mathtt{PS}}|\mathtt{0}\rangle = |\mathtt{0}\rangle; \;\; \mathtt{U}_{\mathtt{PS}}|\mathtt{1}\rangle = -|\mathtt{1}\rangle.$$

Let us indicate by PS a physical apparatus that realizes the phase shift described by $\mathtt{U}_{\mathtt{PS}}$.

Relative phase shifters, beam splitters and mirrors are the basic physical components of the *Mach-Zehnder interferometer* (MZI), an apparatus that has played a very important role in the logical and philosophical debates about the foundations of quantum theory. The physical situation can be sketched as follows (Fig. 1).

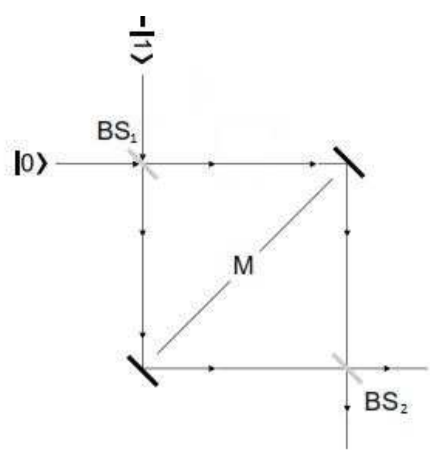

Figure 1: The Mach-Zehnder interferometer

A beam (which may move either along the x-direction or along the y-direction) goes through the relative phase shifter PS of MZI. We have:

$$|0\rangle \;\; \rightarrowtail_{\mathtt{PS}} \;\; |0\rangle; \;\; |1\rangle \;\; \rightarrowtail_{\mathtt{PS}} \;\; -|1\rangle$$

(the phase of the beam changes only in the case where the beam is moving along the y-direction). Soon after the beam goes through the first beam splitter $\mathtt{BS}_1$. As a consequence, it is split into two components: one component moves along the interferometer's arm in the x-direction, the other component moves along the arm in the y-direction. We have:

$$|0\rangle \;\; \rightarrowtail_{\mathtt{BS}_1} \;\; \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \quad -|1\rangle \;\; \rightarrowtail_{\mathtt{BS}_1} \;\; \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle).$$

Then, both components of the superposed beam (on both arms) are reflected by the mirrors $\mathtt{M}$. We have:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \;\; \rightarrowtail_{\mathtt{M}} \;\; \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \;\; \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) \;\; \rightarrowtail_{\mathtt{M}} \;\; \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Finally, the superposed beam goes through the second beam splitter $\mathtt{BS}_2$, which re-composes the two components. We have:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \;\; \rightarrowtail_{\mathtt{BS}_2} \;\; |0\rangle; \;\; \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \;\; \rightarrowtail_{\mathtt{BS}_2} \;\; |1\rangle.$$

Accordingly, $\mathtt{MZI}$ transforms the input $|0\rangle$ into the output $|0\rangle$, while the input $|1\rangle$ is transformed into the output $|1\rangle$.

One is dealing with a result that has for a long time been described as deeply counter-intuitive. In fact, according to a "classical way of thinking" we would expect that the outcoming photons from the second beam splitter should be detected with probability $\frac{1}{2}$ either along the x-direction or along the y-direction.

The Mach-Zehnder interferometer clearly represents a physical implementation of the following quantum logical circuit:

$$\sqrt{\mathtt{I}}^{(1)}\, \mathtt{NOT}^{(1)}\, \sqrt{\mathtt{I}}^{(1)}$$

(called "the Mach-Zehnder circuit"). In the framework of quantum computational logics such circuit can be naturally described by the "Mach-Zehnder formula":

$$\sqrt{id}\,\neg\,\sqrt{id}\,\mathbf{q},$$

where $\mathbf{q}$ is a generic atomic formula. Any interpretation $\mathtt{Hol}_d$ (of the quantum computational language) that assigns to $\mathbf{q}$ a meaning (a qubit living in the space $\mathbb{C}^2$) will determine a meaning for the Mach-Zehnder formula.

While optical implementations of one-qubit gates are relatively simple, trying to implement many-qubit gates may be rather complicated. Consider the case of a gate that plays an important logical and computational role: the Toffoli-gate $\mathtt{T}^{(1,1,1)}$ (defined on the space $\mathcal{H}_2^{(3)} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$).

Mathematically we have:

$$\mathtt{T}^{(1,1,1)}|v_1, v_2, v_3\rangle = \begin{cases} |v_1, v_2, v_1 \sqcap v_2\rangle, & \text{if } v_3 = 0; \\ |v_1, v_2, (v_1 \sqcap v_2)'\rangle, & \text{if } v_3 = 1, \end{cases}$$

where $v_1, v_2, v_3 \in \{0, 1\}$.

The main problem is finding a device that can realize a physical dependence of the target-bit ($v_1 \sqcap v_2$ or $(v_1 \sqcap v_2)'$) from the control-bits (v_1, v_2). A possible strategy is based on an appropriate use of the optical "Kerr-effect": a substance with an intensity-dependent refractive index is placed into a given device, giving rise to an intensity-dependent phase shift.

Let us first give the mathematical definition of a unitary operator that describes a particular form of *conditional phase shift*.

Definition 21. The relative conditional phase shifter
The relative conditional phase shifter of the space $\mathcal{H}_2^{(3)} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ is the unitary operator $\mathtt{U}_{\mathtt{CPS}}$ that is defined for every element of the canonical basis as follows:

$$\mathtt{U}_{\mathtt{CPS}}|v_1, v_2, v_3\rangle = |v_1, v_2\rangle \otimes c|v_3\rangle,$$

where $c = \begin{cases} e^{i\pi}, & \text{if } v_1 = 1,\ v_2 = 1 \text{ and } v_3 = 0; \\ 1, & \text{otherwise.} \end{cases}$.

Let us indicate by CPS a physical apparatus that realizes the phase shift described by the operator $\mathtt{U}_{\mathtt{CPS}}$. Clearly, CPS determines a *conditional* phase shift. For, the phase of a three-beam system in state $|v_1, v_2, v_3\rangle$ is changed only in the case where both control-bits ($|v_1\rangle$, $|v_2\rangle$) are the state $|1\rangle$, while the *ancilla*-bit $|v_3\rangle$ is the state $|0\rangle$. From a physical point of view, such a result can be obtained by using a convenient substance that produces the Kerr-effect.

In order to obtain an implementation of the Toffoli-gate $\mathtt{T}^{(1,1,1,)}$ we will now consider a "more sophisticated" version of the Mach-Zehnder interferometer that will be called "Kerr-Mach-Zehnder interferometer" (indicated by KMZI). Besides the relative phase shifter (PS), the two beam splitters ($\mathtt{BS}_1$, $\mathtt{BS}_2$) and the mirrors (M), the Kerr-Mach-Zehnder interferometer also

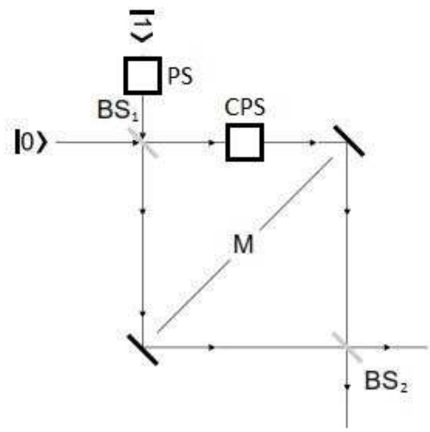

Figure 2: The Kerr-Mach-Zehnder interferometer

contains a relative conditional phase shifter (CPS) that can produce the Kerr-effect (Fig. 2).

While the inputs of the canonical Mach-Zehnder interferometer are single beams (whose states live in the space $\mathbb{C}^2$), the apparatus KMZI acts on composite systems consisting of three beams (S_1, S_2, S_3), whose states live in the space $\mathcal{H}_2^{(3)} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. For the sake of simplicity we can assume that S_1, S_2, S_3 are single photons that may enter into the interferometer-box either along the x-direction or along the y-direction. Let $|v_1, v_2, v_3\rangle$ be the input-state of the composite system $S_1 + S_2 + S_3$. Photons S_1, S_2 (whose states $|v_1\rangle, |v_2\rangle$ represent the control-bits) are supposed to enter into the box along the yz-plane, while photon S_3 (whose state $|v_3\rangle$ is the *ancilla*-bit) will enter through the first beam-splitter $\mathtt{BS}_1$.

Mathematically, the action performed by the apparatus KMZI is described by the following unitary operator (of the space $\mathcal{H}_2^{(3)}$):

$\mathtt{U_{KMZ}} := (\mathtt{I} \otimes \mathtt{I} \otimes \sqrt{\mathtt{I}}^{(1)}) \circ (\mathtt{I} \otimes \mathtt{I} \otimes \mathtt{NOT}^{(1)}) \circ \mathtt{U_{CPS}} \circ (\mathtt{I} \otimes \mathtt{I} \otimes \sqrt{\mathtt{I}}^{(1)}) \circ (\mathtt{I} \otimes \mathtt{I} \otimes \mathtt{U_{PS}})$.

In order to "see" how KMZI is working from a physical point of view, it is expedient to consider a particular example. Take the input $|v_1, v_2, v_3\rangle = |1, 1, 0\rangle$ and let us describe the physical evolution determined by the operator $\mathtt{U_{KMZ}}$ for the system $S_1 + S_2 + S_3$, whose initial state is $|1, 1, 0\rangle$. We have:

$$(\mathtt{I} \otimes \mathtt{I} \otimes \mathtt{U_{PS}})|1, 1, 0\rangle = |1, 1, 0\rangle.$$

The relative phase shifter along the y-direction (PS) does not change the state of photon S_3, which is moving along the x-direction.

$$(\mathtt{I} \otimes \mathtt{I} \otimes \sqrt{\mathtt{I}}^{(1)})|1,1,0\rangle = |1,1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Photon S_3 goes through the first beam splitter $\mathtt{BS}_1$ splitting into two components: one component moves along the interferometer's arm along the x-direction, the other component moves along the arm in the y-direction (like in the case of the canonical Mach-Zehnder interferometer). At the same time, photons S_1 and S_2 (both in state $|1\rangle$) enter into the interferometer-box along the yz-plane.

$$\mathtt{U}_{\mathtt{CPS}}(|1,1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = |1,1\rangle \otimes \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle).$$

The conditional phase shifter $\mathtt{CPS}$ determines a phase shift for the component of S_3 that is moving along the x-direction; because both photons S_1 and S_2 (in state $|1\rangle$) have gone through the substance (contained in $\mathtt{CPS}$) that produces the Kerr-effect.

$$(\mathtt{I} \otimes \mathtt{I} \otimes \mathtt{NOT}^{(1)})(|1,1\rangle \otimes \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle)) = |1,1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Both components of S_3 (on both arms) are reflected by the mirrors.

$$(\mathtt{I} \otimes \mathtt{I} \otimes \sqrt{\mathtt{I}}^{(1)})(|1,1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)) = |1,1,1\rangle.$$

The second beam splitter $\mathtt{BS}_2$ re-composes the two components of the superposed photon S_3.

Consequently, we obtain:

$$\mathtt{U}_{\mathtt{KMZ}}|1,1,0\rangle = |1,1,1\rangle = \mathtt{T}^{(1,1,1)}|1,1,0\rangle.$$

In general, one can easily prove that $\mathtt{U}_{\mathtt{KMZ}}$ and $\mathtt{T}^{(1,1,1)}$ are one and the same unitary operator.

Lemma 3. *For any element $|v_1, v_2, v_3\rangle$ of the canonical basis of the space $\mathcal{H}_2^{(3)}$,*

$$\mathtt{U}_{\mathtt{KMZ}}|v_1, v_2, v_3\rangle = \mathtt{T}^{(1,1,1)}|v_1, v_2, v_3\rangle.$$

Although, from a mathematical point of view, $\mathtt{U_{KMZ}}$ and $\mathtt{T}^{(1,1,1)}$ represent the same gate, physically it is not guaranteed that the apparatus KMZI always realizes its "expected job". All difficulties are due to the behavior of the conditional phase shifter. In fact, the substances used to produce the Kerr-effect generally determine only stochastic results [8]. As a consequence one shall conclude that the Kerr-Mach-Zehnder interferometer allows us to obtain an *approximate* implementation of the Toffoli-gate with an accuracy that is, in some cases, very good.

So far we have considered possible optical implementations of gates in the case of qubit-spaces. The techniques we have illustrated can be also generalized to qudit-spaces. The main idea is using, instead of single beams, systems consisting of many beams (corresponding to different truth-values) that may move either along the x-direction or along the y-direction. The problems concerning physical implementations for the many-valued quantum computational semantics will be investigated in a future article.

7. Acknowledgements

Sergioli's work has been supported by the Italian Ministry of Scientic Research within the FIRB project "Structures and Dynamics of Knowledge and Cognition", Cagliari: F21J12000140001 and of RAS within the project "Modeling the Uncertainty: Quantum Theory and Imaging Processing".

References

[1] R. Greechie, "A non-standard quantum logic with a strong set of states", in E. Beltrametti, B. van Fraassen (eds.), *Current Issues in Quantum Logic*, Plenum, New York, 1981.

[2] A. Dvurečenskij, S. Pulmannová, *New Trends in Quantum Structures*, Kluwer, Dordrecht, 2000.

[3] M.L. Dalla Chiara, R. Giuntini, R. Greechie, *Reasoning in Quantum Theory*, Kluwer, Dordrecht, 2004.

[4] M.L. Dalla Chiara, R. Giuntini, R. Leporini, "Logics from quantum computation", *Int. J. Quantum Inf.* **3**, 293–337, 2005.

[5] M.L. Dalla Chiara, R. Giuntini, R. Leporini, G. Sergioli, "Holistic logical arguments in quantum computation", *Math. Slovaca* **66** (2), 1–22, 2016.

[6] M.L. Dalla Chiara, R. Giuntini, R. Luciani, E. Negri, *From Quantum Information to Musical Semantics*, College Publications, London, 2012.

[7] M.L. Dalla Chiara, R. Giuntini, R. Leporini, G. Sergioli, "A first-order epistemic quantum computational semantics with relativistic-like epistemic effects", *Fuzzy Sets and Systems* **298**, 69–90, 2016.

[8] N. Matsuda, R. Shimizu, Y. Mitsumori, H. Kosaka, K. Edamatsu, "Observation of optical-fibre Kerr nonlinearity at the single-photon level", *Nature Photonics* **3**, 95–98, 2009.

***Revision Note**

We made the corrections suggested by the referees.