Probability in quantum computation and quantum computational logics: a survey

MARIA LUISA DALLA CHIARA, ROBERTO GIUNTINI and GIUSEPPE SERGIOLI

Mathematical Structures in Computer Science / Volume 24 / Special Issue 03 / June 2014 / e240306
DOI: 10.1017/S0960129512000734, Published online: 28 March 2014

Math. Struct. in Comp. Science (2014), vol. 24, iss. 3, e240306, 14 pages.
doi:10.1017/S0960129512000734

Probability in quantum computation and quantum computational logics: a survey

MARIA LUISA DALLA CHIARA[†], ROBERTO GIUNTINI[‡]
and GIUSEPPE SERGIOLI[‡]

[†]*Dipartimento di Filosofia, Università di Firenze, Firenze,*
via Bolognese 52, I-50139 Firenze, Italy
Email: dallachiara@unifi.it
[‡]*Dipartimento di Pedagogia, Psicologia, Filosofia, Università di Cagliari,*
via Is Mirrionis 1, I-09123 Cagliari, Italy
Email: giuntini@unica.it; giuseppe.sergioli@gmail.com

Received 11 February 2011; revised 23 December 2011

Quantum computation and quantum computational logics give rise to some non-standard probability spaces that are interesting from a formal point of view. In this framework, *events* represent quantum pieces of information (*qubits*, *quregisters*, *mixtures of quregisters*), while operations on events are identified with *quantum logic gates* (which correspond to dynamic reversible quantum processes). We investigate the notion of *Shi–Aharonov quantum computational algebra*. This structure plays the role for quantum computation that is played by σ-complete Boolean algebras in classical probability theory.

1. Introduction

The strong parallelism that represents the characteristic feature of quantum computation (QC) is essentially based on a probabilistic behaviour. Intuitively, a quantum computation can be regarded as a *tree* consisting of branches that represent possible computational paths, each associated with a well-determined probability value. A quantum measurement performed at the end of the process determines the 'real' computational result. Some general questions that are currently discussed in this connection are:

(i) What kind of probability is quantum computational probability?
(ii) To what extent can the parallel structures that arise in QC be assimilated into the behaviour of a classical *Probabilistic Turing Machine*?

The second question represents a crucial open problem, which is obviously connected with the validity of the *Church thesis*. The first question has been investigated mathematically. In this article we will sum up some results that have a bearing on *quantum computational logics* (new forms of quantum logic inspired by QC).

2. Probabilistic quantum information

The basic concept in QC is the notion of a *qubit*. Intuitively, a qubit can be regarded as a unit of probabilistic quantum information: a 'quantum perhaps' that assigns a probability

value to the two classical answers *YES* and *NO* (corresponding to the two classical bits 1 and 0, respectively). Consider the two-dimensional Hilbert space $\mathbb{C}^2$, where any vector 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

$$|0\rangle = (1, 0)$$
$$|1\rangle = (0, 1).$$

Definition 2.1 (qubit). A *qubit* is a unit vector

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

of the Hilbert space $\mathbb{C}^2$.

We may also regard the basis elements $|0\rangle$ and $|1\rangle$ as the two classical truth values *false* and *true* 'wedged' by the complex numbers c_0 and c_1. Accordingly, a qubit is a *probabilistic superposition* of the two classical truth values, where *Falsity* has probability $|c_0|^2$ and *Truth* has probability $|c_1|^2$. If the qubit represents the quantum counterpart of the classical bit (describing the pure state of a single particle), the quantum homologue of the classical *register* (corresponding to a system of n particles), is the *n-quregister*, a unit vector of the n-fold tensor product of the space $\mathbb{C}^2$:

$$\bigotimes^n \mathbb{C}^2 := \underbrace{\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2}_{n-times}$$

where $\bigotimes^1 \mathbb{C}^2 := \mathbb{C}^2$. We will use $x, y, \ldots$ as variables ranging over the set $\{0, 1\}$, and $|x\rangle$, $|y\rangle, \ldots$ to range over the basis $\mathcal{B}^{(1)}$. Any factorised unit vector $|x_1\rangle \otimes \cdots \otimes |x_n\rangle$ of the space $\bigotimes^n \mathbb{C}^2$ will represent in this framework a *classical register*, that is, a sequence of n bits. We will also abbreviate $|x_1\rangle \otimes \cdots \otimes |x_n\rangle$ to $|x_1, \ldots, x_n\rangle$. The set

$$\mathcal{B}^{(n)} = \{|x_1, \ldots, x_n\rangle \ : \ x_i \in \{0, 1\}\}$$

of all n-registers is an orthonormal basis for the space $\bigotimes^n \mathbb{C}^2$, which is also called the *computational basis* for the n-quregisters.

Quregisters are pure states, and thus *maximal pieces of information*, that cannot be consistently extended to richer knowledge. In quantum computation, we must also refer to non-maximal pieces of information; these correspond to *mixtures of quregisters*, which are also called *qumixes*, and which are mathematically represented by density operators.

Definition 2.2 (qumix). A *qumix* is a density operator of a Hilbert space $\bigotimes^n \mathbb{C}^2$.

We will write $\mathfrak{D}\left(\bigotimes^n \mathbb{C}^2\right)$ to denote the set of all qumixes of $\bigotimes^n \mathbb{C}^2$, and

$$\mathfrak{D} := \bigcup_{n=1}^{\infty} \mathfrak{D}\left(\bigotimes^n \mathbb{C}^2\right)$$

to denote the set of all possible qumixes. It can be seen that quregisters are special cases of qumixes.

As in the qubit case, we can define a probability function p assigning a probability value $\mathrm{p}(\rho)$ to any qumix ρ. Intuitively, $\mathrm{p}(\rho)$ is the probability that the quantum information stored by ρ corresponds to *true* information. To define the function p, we will first identify in any space $\bigotimes^n \mathbb{C}^2$ two special projections $P_0^{(n)}$ and $P_1^{(n)}$ that will represent the *Falsity* and *Truth* properties, respectively.

In this way, *Falsity* and *Truth* are dealt with as special cases of physical properties to which any density operator assigns a well-determined probability value according to the quantum theoretic formalism. Before defining $P_0^{(n)}$ and $P_1^{(n)}$, we will first distinguish the *true* from the *false* registers in any space $\bigotimes^n \mathbb{C}^2$:

$|x_1, \ldots, x_n\rangle$ is said to be *true* if and only if $x_n = 1$

$|x_1, \ldots, x_n\rangle$ is said to be *false* if and only if $x_n = 0$.

In other words, the last bit of a given register determines its truth value. We can now define *Falsity* and *Truth* naturally as follows.

Definition 2.3 (Falsity and Truth).

(i) The *Falsity* of the space $\bigotimes^n \mathbb{C}^2$ is the projection $P_0^{(n)}$ onto the span of the set of all *false registers*.

(ii) The *Truth* of the space $\bigotimes^n \mathbb{C}^2$ is the projection $P_1^{(n)}$ onto the span of the set of all *true registers*.

By applying the Born rule, the probability function p can be defined as follows.

Definition 2.4 (probability p of a qumix). For any qumix $\rho \in \mathfrak{D}\left(\bigotimes^n \mathbb{C}^2\right)$,

$$\mathrm{p}(\rho) := \mathrm{tr}\left(P_1^{(n)}\rho\right),$$

where tr is the *trace functional*.

Clearly, $\mathrm{p}(\rho)$ represents the probability of the *truth property* for state ρ. We will see how the function p induces a preorder relation on the set $\mathfrak{D}$ of all qumixes.

3. Quantum logic gates as probabilistic processes

Since the probabilistic function p is defined for any qumix, the set $\mathfrak{D}$ of all possible qumixes can also be regarded as the set of all possible *quantum computational events*. What about the algebraic structure of this set? Unlike classical probability theory, the operations defined on quantum computational events have an intrinsic dynamic character and are represented by *quantum logic gates*.

What exactly are quantum logic gates? It is well known that in quantum theory the dynamic evolution of quantum systems is governed by the Schrödinger equation. Accordingly, for any times t_0 and t_1, a pure state $|\psi(t_0)\rangle$ of an object at time t_0 is transformed into another pure state of the same object at time t_1 by means of a unitary operator U, which represents a reversible transformation:

$$|\psi(t_1)\rangle = U(|\psi(t_0)\rangle).$$

Quantum logic gates (which we shall just call *gates* from now on) are special examples of unitary operators that transform quregisters into quregisters in a reversible way. Hence, intuitively, the application of a sequence of gates to an input quregister can be regarded as the dynamic evolution of a quantum object that is processing a given amount of quantum information. By definition, gates are unitary operators whose domains consist of vectors of convenient Hilbert spaces. We will see, however, that they can also be generalised naturally to qumixes.

Intuitively, a quantum information process can be represented naturally as a kind of *quantum epistemic tree* from an initial state of knowledge $\rho(t_o)$ to a final state of knowledge $\rho(t_1)$:

$$\begin{array}{c} \rho(t_1) \\ \Uparrow \\ \vdots \\ \Uparrow \\ \rho(t_0) \end{array}$$

Although the superficial form of a quantum epistemic tree is that of a *linear process*, the deep structure is essentially *parallel* since any qubit $|\psi\rangle$ generally gives rise to a *branching*. A state of knowledge represented by a quantum superposition $|\psi\rangle$ reflects, at the same time, two parallel epistemic paths: the first leads to the answer *YES*, while the second leads to the answer *NO*.

Classical computation theory satisfies a highly desirable property: it can be formulated in terms of a very small set of classical logic gates (Boolean functions), called a *(functionally) universal set of gates*. Generally, classical gates are presented as *irreversible* operations: the same output bits may correspond to different input bits. However, we know that such an irreversible form does not represent an essential feature of classical computation: as shown by Toffoli (Toffoli 1980), every Boolean gate has its own reversible counterpart. The main idea is to consider the input bits of a reversible gate as composed by two parts: a *control* component, which carries over the 'actual' input value, and a *target* component (*ancilla*), whose final value (after the application of the gate) represents the 'actual' output. The price to pay for this is an increase in the computational space due to the number of extra *ancilla* bits needed to make the circuit reversible.

In the irreversible formulation of the gate system, the single gate NAND, or the set consisting of the two gates AND and NOT represent a universal set of gates. In the

reversible version, this role is played by a single gate, the *Toffoli gate* T, which is also called a *controlled-controlled-not* gate.

In quantum computation, gates are identified with unitary operators acting on pure states of a Hilbert space. Since there are uncountably many unitary operators, there is no hope of finding any finite *functionally universal* set of quantum gates. In other words, there is no finite set of quantum gates such that the behaviour of any quantum gate G can be *exactly* reproduced by means of a convenient composition of gates belonging to the set. In spite of this, there are finite sets S of quantum gates such that each S satisfies the following condition: the action of any quantum gate can be mathematically *approximated*, up to an arbitrary accuracy, through appropriate compositions of gates that belong to S (Kitaev 1997). Sets of gates that satisfy such a property are said to be *approximately universal.*

Finding simpler and simpler approximate universal sets of gates represents a crucial step in the attempt to realise concrete quantum computers. An important result obtained by Shi (Shi 2002), and further investigated by Aharonov (Aharonov 2003), has shown that the set whose elements are the (three-qubit) *Toffoli gate* and the (one-qubit) *Hadamard gate* (also called the *squareroot of the identity*) is approximately universal. Unlike the classical reversible case, the Toffoli gate is not sufficient to reproduce the behaviour of all quantum gates. A gate exhibiting a 'genuine' quantum character should be added: the squareroot of the identity comes into play here.

We will now present the mathematical definitions of our gates.

Definition 3.1 (the Toffoli gate). For any $n, m, p \geqslant 1$, the *Toffoli gate* is the linear operator $\mathrm{T}^{(n,m,p)}$ defined on $\bigotimes^{n+m+p} \mathbb{C}^2$ such that for every element

$$|x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z_1, \ldots, z_p\rangle$$

of the computational basis $\mathcal{B}^{(n+m+p)}$,

$$\mathrm{T}^{(n,m,p)}(|x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z_1, \ldots, z_p\rangle) = |x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z_1, \ldots, z_{p-1}, x_n y_m \widehat{+} z_p\rangle,$$

where $\widehat{+}$ represents addition modulo 2.

It is clear that $\mathrm{T}^{(n,m,p)}$ is a unitary operator. On this basis, the Boolean functions AND, NAND, NOT can be defined using Toffoli gates.

Definition 3.2.

— For any $|\psi\rangle \in \bigotimes^n \mathbb{C}^2$ and for any $|\varphi\rangle \in \bigotimes^m \mathbb{C}^2$,

$$\mathrm{AND}(|\psi\rangle, |\varphi\rangle) := \mathrm{T}^{(n,m,1)}(|\psi\rangle \otimes |\varphi\rangle \otimes |0\rangle).$$

— For any $|\psi\rangle \in \bigotimes^n \mathbb{C}^2$ and for any $|\varphi\rangle \in \bigotimes^m \mathbb{C}^2$,

$$\mathrm{NAND}(|\psi\rangle, |\varphi\rangle) := \mathrm{T}^{(n,m,1)}(|\psi\rangle \otimes |\varphi\rangle \otimes |1\rangle).$$

— For any $|\psi\rangle \in \bigotimes^n \mathbb{C}^2$,

$$\mathrm{NOT}(|\psi\rangle) := \mathrm{T}^{(1,1,n)}(|1\rangle, |1\rangle, |\psi\rangle).$$

However, defining the Boolean negation NOT in terms of the Toffoli gate has the shortcoming that it increases the dimension of the Hilbert space. Specifically, if $|\psi\rangle$ belongs to $\bigotimes^n \mathbb{C}^2$, its negation $\mathrm{NOT}(|\psi\rangle)$ belongs to $\bigotimes^{n+2} \mathbb{C}^2$.

For computational purposes, the following independent definition of the negation gate is more economical.

Definition 3.3 (negation). For any $n \geqslant 1$, the *negation* on $\bigotimes^n \mathbb{C}^2$ is the linear operator $\mathrm{Not}^{(n)}$ such that for every element $|x_1, \ldots, x_n\rangle$ of the computational basis $\mathcal{B}^{(n)}$,

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

For classical bits, we immediately get the standard negation truth table:

$$\mathrm{Not}^{(1)}(|0\rangle) = |1\rangle$$
$$\mathrm{Not}^{(1)}(|1\rangle) = |0\rangle.$$

The Toffoli gate represents a classical reversible gate: whenever the input is a classical register, the output will also be a classical register. In other words, the gate cannot 'create' superpositions. The 'genuine' quantum component of the Shi–Aharonov system is represented by the Hadamard gate.

Definition 3.4 (the Hadamard gate). For any $n \geqslant 1$, the *Hadamard gate* on $\bigotimes^n \mathbb{C}^2$ is the linear operator $\sqrt{\mathrm{I}}^{(n)}$ such that for every element $|x_1, \ldots, x_n\rangle$ of the computational basis $\mathcal{B}^{(n)}$,

$$\sqrt{\mathrm{I}}^{(n)}(|x_1, \ldots, x_n\rangle) = |x_1, \ldots, x_{n-1}\rangle \otimes \frac{1}{\sqrt{2}} \left((-1)^{x_n}|x_n\rangle + |1 - x_n\rangle\right).$$

The basic property of $\sqrt{\mathrm{I}}^{(n)}$ is given by

$$\text{for any } |\psi\rangle \in \bigotimes^n \mathbb{C}^2, \quad \sqrt{\mathrm{I}}^{(n)}\left(\sqrt{\mathrm{I}}^{(n)}(|\psi\rangle)\right) = |\psi\rangle.$$

For classical bits, we immediately get

$$\sqrt{\mathrm{I}}^{(1)}(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$\sqrt{\mathrm{I}}^{(1)}(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

In other words, the Hadamard gate transforms maximal certainties into maximal uncertainties, and *vice versa*.

By definition, gates are unitary operators whose domains consist of vectors of convenient Hilbert spaces. At the same time, gates can also be generalised naturally to qumixes. Such generalisations transforming qumixes into qumixes in a reversible way are called *qumix gates*, or *unitary quantum operations* (Aharonov *et al.* 1998).

Let G be a gate of $\bigotimes^n \mathbb{C}^2$. Then the corresponding qumix gate ${}^{\mathcal{D}}\mathrm{G}$ is defined by

$$ {}^{\mathcal{D}}\mathrm{G}(\rho) := \mathrm{G}\rho\mathrm{G}^*, $$

where ρ is a density operator of $\bigotimes^n \mathbb{C}^2$ and G^* is the adjoint of G. Accordingly, we will use ${}^{\mathcal{D}}\mathrm{T}^{(m,n,p)}$ and ${}^{\mathcal{D}}\sqrt{\mathrm{I}}^{(n)}$ to denote the Toffoli and Hadamard qumix gates, respectively.

Some basic probabilistic properties of our classical gates are listed in the following theorem.

Theorem 3.1 (Gudder 2003; Dalla Chiara *et al.* 2005).

$$ \begin{aligned} \mathrm{p}\left({}^{\mathcal{D}}\mathrm{Not}^{(n)}(\rho)\right) &= 1 - \mathrm{p}(\rho) \\ \mathrm{p}\left({}^{\mathcal{D}}\mathrm{AND}(\rho,\sigma)\right) &= \mathrm{p}(\rho)\mathrm{p}(\sigma) \\ \mathrm{p}\left({}^{\mathcal{D}}\mathrm{NAND}(\rho,\sigma)\right) &= 1 - \mathrm{p}(\rho)\mathrm{p}(\sigma). \end{aligned} $$

While negation has a standard probabilistic behaviour, somewhat surprisingly, the conjunction ${}^{\mathcal{D}}\mathrm{AND}$ and its negation ${}^{\mathcal{D}}\mathrm{NAND}$ turn out to behave as *probability functions*: the probability of a conjunction is always the product of the probabilities of the two members. In other words, any pair of quantum computational events seems to behave like a classical pair of independent events. As expected, such non-standard properties give rise to important consequences for the algebraic structure of all quantum computational events.

Theorem 3.2 (Dalla Chiara *et al.* 2009). Let $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$, $\sigma \in \mathfrak{D}(\bigotimes^m \mathbb{C}^2)$ and $\tau \in \mathfrak{D}(\bigotimes^p \mathbb{C}^2)$. Then,

$$ \mathrm{p}\left({}^{\mathcal{D}}\mathrm{T}^{(n,m,p)}(\rho \otimes \sigma \otimes \tau)\right) = (1 - \mathrm{p}(\tau))\mathrm{p}(\rho)\mathrm{p}(\sigma) + \mathrm{p}(\tau)(1 - \mathrm{p}(\rho)\mathrm{p}(\sigma)). $$

As a consequence of Theorems 3.2 and 3.1, the probability value

$$ \mathrm{p}({}^{\mathcal{D}}\mathrm{T}^{(n,m,p)}(\rho \otimes \sigma \otimes \tau)) $$

can be regarded as a kind of weighted sum of $\mathrm{p}({}^{\mathcal{D}}\mathrm{AND}(\rho,\sigma))$ and $\mathrm{p}({}^{\mathcal{D}}\mathrm{NAND}(\rho,\sigma))$, with weights $\mathrm{p}({}^{\mathcal{D}}\mathrm{Not}^{(p)}(\tau))$ and $\mathrm{p}(\tau)$, respectively.

Theorem 3.3. Let $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C})$, $\sigma \in \mathfrak{D}(\bigotimes^m \mathbb{C})$ and $\tau \in \mathfrak{D}(\bigotimes^p \mathbb{C}^2)$. Then,

$$ \mathrm{p}\left({}^{\mathcal{D}}\sqrt{\mathrm{I}}^{(n+m+p)}\left({}^{\mathcal{D}}\mathrm{T}^{(n,m,p)}(\rho \otimes \sigma \otimes \tau)\right)\right) = \mathrm{p}\left({}^{\mathcal{D}}\sqrt{\mathrm{I}}^{(p)}(\tau)\right). $$

4. Probabilistic quantum computational structures

We can now introduce the notion of a *Shi–Aharonov quantum computational algebra*, whose domain is the set of all possible qumixes and whose operations are defined in terms of the Toffoli, negation and Hadamard gates (Dalla Chiara *et al.* 2009). We can say that such a structure plays for quantum computation the role played by σ-complete Boolean algebras in classical probability theory.

Definition 4.1 (the Shi–Aharonov quantum computational algebra). The *Shi–Aharonov quantum computational algebra* is the structure

$$\mathcal{SA} = \left(\mathfrak{D}, \mathbb{T}, \mathbb{N}, \sqrt{\mathbb{I}}, P_0^{(1)}, P_1^{(1)}, \frac{1}{2}I^{(1)}\right),$$

where:

— $\mathfrak{D}$ is the set of all qumixes.

— $\mathbb{T}$ is a ternary operation defined for any $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$, any $\sigma \in \mathfrak{D}(\bigotimes^m \mathbb{C}^2)$ and any $\tau \in \mathfrak{D}(\bigotimes^p \mathbb{C}^2)$ by

$$\mathbb{T}(\rho, \sigma, \tau) := {}^{\mathcal{D}}\mathrm{T}^{(n,m,p)}(\rho \otimes \sigma \otimes \tau).$$

— $\mathbb{N}$ is a unary operation defined for any $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$ by

$$\mathbb{N}(\rho) := {}^{\mathcal{D}}\mathrm{Not}^{(n)}(\rho).$$

— $\sqrt{\mathbb{I}}$ is a unary operation defined for any $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$ by

$$\sqrt{\mathbb{I}}(\rho) := {}^{\mathcal{D}}\sqrt{\mathrm{I}}^{(n)}(\rho).$$

— $P_0^{(1)}$, $P_1^{(1)}$, $\frac{1}{2}I^{(1)}$ (where $I^{(1)}$ is the identity operator of $\mathbb{C}^2$) are three special elements of $\mathfrak{D}(\mathbb{C}^2)$ that represent the privileged true, false and indeterminate qumix, respectively.

The set $\mathfrak{D}$ of all qumixes can be preordered by the relation $\preceq$ defined as follows.

Definition 4.2 (the qumix preorder). For any $\rho, \sigma \in \mathfrak{D}$,

$$\rho \preceq \sigma \text{ iff } \mathrm{p}(\rho) \leqslant \mathrm{p}(\sigma) \text{ and } \mathrm{p}\left(\sqrt{\mathbb{I}}(\rho)\right) \leqslant \mathrm{p}\left(\sqrt{\mathbb{I}}(\sigma)\right).$$

It is easy to see that $\preceq$ is reflexive and transitive. This allows us to define an equivalence relation $\equiv$ on the set $\mathfrak{D}$ in the expected way.

Definition 4.3. $\rho \equiv \sigma$ if and only if $\rho \preceq \sigma$ and $\sigma \preceq \rho$.

Now consider the set

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

For brevity, we will write $[\rho]$ instead of $[\rho]_{\equiv}$. Unlike qumixes, which are only preordered by $\preceq$, the equivalence classes of $[\mathfrak{D}]_{\equiv}$ can be partially ordered in a natural way:

$$[\rho] \preceq [\sigma] \quad \text{iff} \quad \rho \preceq \sigma.$$

We can now consider a quotient structure based on the quotient set $[\mathfrak{D}]_{\equiv}$.

Theorem 4.1. $\equiv$ is a congruence relation with respect to $\mathbb{T}$, $\mathbb{N}$ and $\sqrt{\mathbb{I}}$.

Thanks to Theorem 4.1, we can define the operations $\mathbb{T}$, $\mathbb{N}$ and $\sqrt{\mathbb{I}}$ on $[\mathfrak{D}]_{\equiv}$ in the expected way. Hence, we obtain the following quotient structure:

$$\mathcal{SA}_{\equiv} = \left([\mathfrak{D}]_{\equiv}, \mathbb{T}, \mathbb{N}, \sqrt{\mathbb{I}}, \left[P_0^{(1)}\right], \left[P_1^{(1)}\right], \left[\frac{1}{2}I^{(1)}\right]\right).$$

While $\mathcal{SA}$ is a reversible quantum computational structure, its quotient $\mathcal{SA}_{\equiv}$ is clearly irreversible.

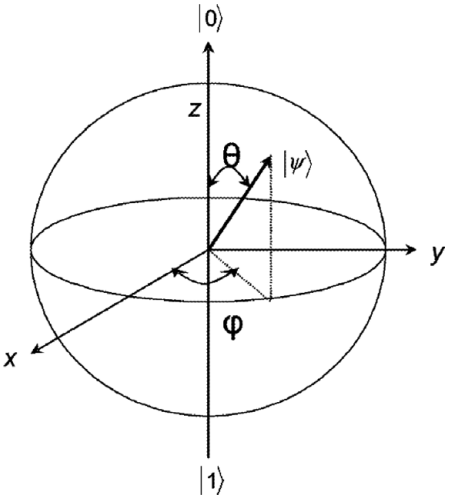

Fig. 1. The Bloch–Poincaré sphere

Interestingly enough, the quotient structure $\mathcal{SA}_{\equiv}$ turns out to be isomorphic to a structure based on a particular set of complex numbers: the closed disc with centre $\left(\frac{1}{2}, \frac{1}{2}\right)$ and radius $\frac{1}{2}$ (Dalla Chiara *et al.* 2009).

It is well known that $\mathfrak{D}\left(\mathbb{C}^2\right)$ is in one-to-one correspondence with the set of all points of the Bloch–Poincaré sphere (of radius 1) – see Figure 1. Consider a qumix τ of $\mathfrak{D}\left(\mathbb{C}^2\right)$ and let (t_1, t_2, t_3) be the point of the Bloch-Poincaré sphere that is uniquely associated to τ. We then have

$$\tau = \frac{1}{2}\begin{pmatrix} 1+t_3 & t_1 - it_2 \\ t_1 + it_2 & 1 - t_3 \end{pmatrix}.$$

It is easy to see that

$$\mathrm{p}(\tau) = \frac{1-t_3}{2}$$
$$\mathrm{p}\left(\sqrt{\mathbb{I}}(\tau)\right) = \frac{1-t_1}{2}.$$

It is clear that the coordinate t_2 has no effect on $\mathrm{p}(\tau)$ and $\mathrm{p}\left(\sqrt{\mathbb{I}}(\tau)\right)$. This suggests a shift down by one dimension. Accordingly, we define the following set of complex numbers:

$$\mathbb{C}_1 := \left\{\left(\mathrm{p}(\tau), \mathrm{p}\left(\sqrt{\mathbb{I}}(\tau)\right)\right) \,:\, \tau \in \mathfrak{D}\left(\mathbb{C}^2\right)\right\}.$$

It is easy to show that

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

On this basis, recalling Theorem 3.2, a Toffoli-like operation ($\mathbb{T}^{\mathbb{C}_1}$), a negation $\mathbb{N}^{\mathbb{C}_1}$ and a Hadamard-like operation ($\sqrt{\mathbb{I}}^{\mathbb{C}_1}$) can be defined naturally on the set $\mathbb{C}_1$.

Definition 4.4 (the pair-Toffoli and the pair-Hadamard).

$$\mathbb{T}^{\mathbb{C}_1}((a_1,a_2),(b_1,b_2)(c_1,c_2)) = ((1-c_1)a_1b_1 + c_1(1-a_1b_1),c_2)$$
$$\mathbb{N}^{\mathbb{C}_1}(a_1,a_2) = (1-a_1,1-a_2)$$
$$\sqrt{\mathbb{I}}^{\mathbb{C}_1}(a_1,a_2) = (a_2,a_1).$$

We now consider the structure

$$\mathcal{C}_1 = \left(\mathbb{C}_1, \mathbb{T}^{\mathbb{C}_1}, \mathbb{N}^{\mathbb{C}_1}, \sqrt{\mathbb{I}}^{\mathbb{C}_1}, \underline{0}, \underline{1}, \underline{1/2}\right), \tag{1}$$

where

$$\underline{0} := \left(0, \frac{1}{2}\right)$$
$$\underline{1} := \left(1, \frac{1}{2}\right)$$
$$\underline{1/2} := \left(\frac{1}{2}, \frac{1}{2}\right).$$

We will call $\mathcal{C}_1$ the *complex Shi–Aharonov quantum computational algebra*.

Theorem 4.2 (Dalla Chiara *et al.* 2009). The complex Shi–Aharonov quantum computational algebra is isomorphic to the quotient of the Shi–Aharonov quantum computational algebra.

It is interesting to compare the quotient structure $\mathcal{SA}_{\equiv}$ of all quantum computational events (or its isomorphic image $\mathcal{C}_1$) with the Boolean event algebras of classical probability spaces. To this end, consider the following reduct structure of $\mathcal{SA}_{\equiv}$:

$$\mathcal{SA}_{\equiv} = \left([\mathfrak{D}]_{\equiv}, \mathrm{AND}, \mathbb{N}, \left[P_0^{(1)}\right], \left[P_1^{(1)}\right]\right),$$

where the conjunction AND is defined on the set $[\mathfrak{D}]_{\equiv}$ in the expected way. We then consider the substructure $\mathcal{SA}_{\equiv}^{\mathfrak{R}}$ of $\mathcal{SA}_{\equiv}$ whose domain consists of all equivalence classes of registers. It is easy to show that $\mathcal{SA}_{\equiv}^{\mathfrak{R}}$ is a two-valued Boolean algebra. Hence, classical quantum computational events have the standard Kolmogorovian behaviour.

What kind of structure is $\mathcal{SA}_{\equiv}$? To sum up, the most significant Boolean properties that are either preserved or possibly violated in this particular case are:

— The conjunction AND is commutative and associative.
— The conjunction AND is not idempotent. Generally,

$$\mathrm{AND}([\rho],[\rho]) \neq [\rho].$$

As happens in fuzzy logics, a non-idempotent conjunction seems to be compatible with concrete situations that may be disturbed by a noise (where *repetita iuvant!*). Consequently, $\mathcal{SA}_{\equiv}$ is not a lattice.

— Although $P_0^{(1)}$ represents a (privileged) *impossible event* such that $\mathrm{p}(P_0^{(1)}) = 0$, the element $\left[P_0^{(1)}\right]$ is not the *minimum* of $\mathcal{SA}_{\equiv}$. In fact, there are some qumixes ρ such that

$P_0^{(1)} \not\leq \rho$. In other words, $\mathcal{SA}_{\equiv}$ does not satisfy the *Duns Scotus principle* (*ex absurdo sequitur quodlibet!*).

— $\left[P_1^{(1)}\right]$ is not a neutral element of $\mathcal{SA}_{\equiv}$. Generally,

$$\mathrm{AND}\left([\rho], \left[P_1^{(1)}\right]\right) \neq [\rho].$$

— The non-contradiction principle can be violated. Generally,

$$\mathrm{AND}([\rho], \mathbb{N}([\rho])) \neq \left[P_0^{(1)}\right].$$

In other words, quantum computational events may be *unsharp* since contradictions are not necessarily impossible!

It is easy to see that our quotient structure $\mathcal{SA}_{\equiv}$ represents a weak example of a *product algebra*

$$(A, ., ', 0, 1)$$

whose standard model is the concrete numerical structure $([0,1], ., ', 0, , 1)$, where . is the real-number product and $x' = 1 - x$. While 1 is a neutral element in any product algebra, we have just seen that in the case of $\mathcal{SA}_{\equiv}$, the element $\left[P_1^{(1)}\right]$ does not satisfy this property.

5. A logical abstraction: quantum computational logics

Quantum computation has recently suggested some new forms of quantum logic, called *quantum computational logics* (**QCL's**), where *meanings* of sentences are identified with quantum information quantities. This provides a mathematical formalism for an abstract *theory of meanings* that can be applied to investigate different kinds of semantic phenomena where *holistic*, *contextual* and *gestaltic* patterns play an essential role (from natural languages to musical compositions).

It is well known that human perception, like thinking, seems to be essentially *synthetic*. We never perceive an object by *scanning* it point by point. Instead, we immediately form a *Gestalt*, that is, a global idea of it. Rational activity also seems to be essentially based on *gestaltic patterns*. Now, *Gestalt thinking* cannot be adequately represented in the framework of classical semantics, which is basically *analytical* and *compositional*: the meaning of a *compound* expression is always determined by the meanings of its *parts*. At the same time, meanings are *non-ambiguous* and *sharp*. All this means that classical semantics is not very applicable to an adequate analysis of natural languages or artistic contexts, where holistic and ambiguous features seem to play a relevant role.

In the semantics of **QCL's** the following conditions are satisfied:

(1) *Global meanings* (which may correspond to a *Gestalt*) are intrinsically *vague* because they leave many relevant properties of the objects under investigation semantically undecided.

(2) Any global meaning determines some *partial meanings*, which are generally vaguer than the global one.

(3) Meanings (*Gestalten*) can be generally represented as *superpositions* of other meanings, possibly associated with probability values.

(4) Meanings (in the same way as *Gestalten*), are dealt with as intrinsically dynamic objects.

In this framework, the *meaning* of any sentence is identified with a quantum information quantity: a quregister or, more generally, a qumix. We will just sketch here the basic intuitive ideas of this semantics[†]. The starting point can be described as a natural generalisation of classical logic. We will refer to an 'information-theoretic' presentation of classical semantics (and classical circuit theory). In this framework, sentences are supposed to denote classical bits (either 1 or 0), while the Boolean connectives (*not*, *and*, *or*) represent classical *logic gates*: functions that allow us to process information. By contrast, the sentences of **QCL′s** are supposed to represent quantum pieces of information that are generally uncertain (qumixes). At the same time, the logical connectives are interpreted as *quantum logic gates*. One can use, for instance, a system of logical connectives that corresponds to the Shi–Aharonov system of gates (negation, Toffoli and Hadamard), which is approximately universal.

In the holistic semantics of **QCL′s**, a *model* (or *interpretation*) of the language is a map $\mathtt{Hol}$ that assigns to any sentence α a qumix that represents the informational meaning of α:

$$\alpha \mapsto \mathtt{Hol}(\alpha).$$

As expected, any model $\mathtt{Hol}$ preserves the logical form of the sentences, by interpreting any connective $\circ$ of the language as a corresponding gate G°. Furthermore, the qumix $\mathtt{Hol}(\alpha)$ lives in a Hilbert space whose dimension depends on the logical form of α. The simplest examples of sentences are *atomic* sentences, which cannot be decomposed into more elementary sentences (say '2 is prime'). Accordingly, the meanings of such sentences live in the simplest Hilbert space: the two-dimensional space $\mathbb{C}^2$. A molecular sentence with n occurrences of atomic sentences can be regarded as a linguistic description of a compound physical system consisting of n particles. In fact, we need n particles to carry the information that is expressed by our molecular sentence. On this basis, it is natural to assume that the meaning of such a sentence lives in the n-fold tensor product of $\mathbb{C}^2$.

The holistic features of our semantics depend on the fact that any model $\mathtt{Hol}$ assigns to any sentence α a *global* meaning that cannot be generally inferred from the meanings assigned by $\mathtt{Hol}$ to the atomic parts of α. What happens here is just the opposite to the standard behaviour of compositional semantics: $\mathtt{Hol}(\alpha)$ determines the meanings of all its parts, which turn out to be essentially *context-dependent*. As a consequence, any sentence may receive different meanings in different contexts. Going from the *whole* to the *parts* is possible here because all logical operations are reversible: we can go back and forth without any dissipation of information!

[†] For technical details, see Dalla Chiara *et al.* (2010).

A fundamental role in this semantic game is played by the notion of *entanglement*, which is mathematically based on the characteristic properties of tensor products. Intuitively, the basic features of an *entangled state* $|\psi\rangle$ can be sketched as follows:

— $|\psi\rangle$ is a maximal information (a pure state) that describes a compound physical system S (say, a two-electron system);
— the information determined by $|\psi\rangle$ about the parts of S is non-maximal. Hence, the states of the whole system is a pure state, while the states of the parts (which are determined by the state of the whole and are usually called *reduced states*) are proper mixtures. It may also happen that the state of the compound system (although representing a maximum of information) describes the parts as essentially indiscernible objects, which cannot satisfy any characteristic individual property. In this way, we get an apparent violation of Leibniz' indiscernibility principle.

Entanglement phenomena can be used naturally to model some typical holistic semantic situations in the framework of our quantum computational semantics. We can consider entangled quregisters that are meanings of molecular sentences. As an example, consider a conjunctive sentence having the form

$$\gamma = \alpha \wedge \beta.$$

The following situation is possible:

— The *meaning* $\mathtt{Hol}(\gamma)$ of the conjunction γ is a quregister, which represents a maximal information (a pure state).
— The meanings of the parts (α, β) are quantum-entangled and cannot be represented by two pure states (two quregisters).

We can say that the *sharp meaning* of the conjunction determines two *ambiguous meanings* for the parts (α, β), which are represented by two mixed states. In other words, *the meaning of the whole determines the meanings of the parts, but not the other way around*. In fact, we cannot go back from the two ambiguous meanings of the parts to the quregister representing the meaning of the whole. The mixed state (that is, the reduced state) representing the ambiguous meaning of α (respectively, β) can be regarded as a kind of *contextual meaning* of α (respectively, β), determined by the *global context*, which corresponds to the quregister $\mathtt{Hol}(\alpha \wedge \beta)$ (the meaning of the conjunction $\alpha \wedge \beta$).

The quantum computational semantics is strongly Hilbert-space dependent. As a consequence, applications to fields far from the quantum world, where Hilbert spaces do not play any significant role, seem to be somewhat unnatural. However, by abstracting from the Hilbert-space formalism, we can develop an abstract version of quantum holistic semantics that is Hilbert space free (Dalla Chiara *et al.* 2010). In this framework, quregisters and qumixes (representing maximal and non-maximal pieces of information, respectively) are dealt with as special kinds of *intensional objects* with growing complexity, which reflects the logical form of possible sentences. Accordingly, an abstract notion of *reduced information* allows us to define *contextual meanings* in an appropriate way (like in the concrete quantum case). This abstract quantum-like semantics seems to represent a flexible tool that might be naturally applied to a number of different fields, including a formal analysis of natural languages and of the languages of art.

References

Aharonov, D. (2003) A simple proof that Toffoli and Hadamard are quantum universal. arXiv:quant-ph/0301040.

Aharonov, D., Kitaev, A. and Nisan, N. (1998) Quantum circuits with mixed states. *STOC '98: Proceedings of the thirtieth annual ACM symposium on Theory of computing*, ACM Press 20–30.

Cattaneo, G., Dalla Chiara, M. L., Giuntini, R. and Leporini, R. (2004) Quantum computational structures. *Mathematica Slovaca* **54** 87–108.

Cignoli, R., D'Ottaviano, I. M. L. and Mundici, D. (2000) *Algebraic Foundations of Many-Valued Reasoning*, Kluwer.

Dalla Chiara, M. L., Giuntini, R. and Leporini, R. (2003) Quantum computational logics: A survey. In: Hendricks, V. F. and Malinowski, J. (eds.) *Trends in Logic: 50 years of Studia Logica*, Kluwer 213–255.

Dalla Chiara, M. L., Giuntini, R. and Leporini, R. (2005) Logics from Quantum Computation. *International Journal of Quantum Information* **3** 293–337.

Dalla Chiara, M. L., Giuntini, R., Freytes, H., Ledda, A. and Sergioli, G. (2009) The algebraic structure of an approximately universal system of quantum computational gates. *Foundations of Physics* **39** (6) 559–572.

Dalla Chiara M. L., Giuntini, R., Ledda, R., Leporini, R. and Sergioli G. (2010) Entanglement as a semantic resource. *Foundations of Physics* **40** (9/10) 1494–1518.

Dawson, C. M. and Nielsen M. A. (2005) The Solovay–Kitaev algorithm. arXiv.org:quant-ph/0505030.

Deutsch, D. (1989) Quantum computational networks. *Proceedings of the Royal Society of London A* **425** 73–90.

Gudder, G. (2003) Quantum computational logics. *International Journal of Theoretical Physics* **42** 39–47.

Kitaev, A. Y. (1997) Quantum Computations: Algorithms and Error correction. *Russian Mathematical Surveys* **52** (6) 1191–1249.

Kraus, K. (1983) *States, effects and operations*, Springer-Verlag.

Ledda, A., Konig, M., Paoli, F. and Giuntini R. (2006) MV algebras and quantum computation. *Studia Logica* **82** (2) 245–270.

Nielsen, M. and Chuang, I. (2000) *Quantum Computation and Quantum Information*, Cambridge University Press.

Shi, Y. (2002) Both Toffoli and controlled-Not need little help to do universal quantum computation. arXiv:quant-ph/0205115.

Toffoli, T. (1980) Reversible computing. In: de Bakker, J. W. and van Leeuwen, J. (eds.) *Automata, Languages and Programming*, Springer 632–644.