International Journal of Theoretical Physics, Vol. 43, Nos. 7/8, August 2004 (© 2004)

An Unsharp Logic From Quantum Computation

Gianpiero Cattaneo,[1] Maria Luisa Dalla Chiara,[2]
Roberto Giuntini,[3] and Roberto Leporini[1,4]

Logical gates studied in quantum computation suggest a natural logical abstraction that gives rise to a new form of *unsharp quantum logic*. We study the logical connectives corresponding to the following gates: the *Toffoli gate*, the NOT and the $\sqrt{\texttt{NOT}}$ (which admit of natural physical models). This leads to a semantic characterization of a logic that we call *quantum computational logic* (QCL).

KEY WORDS: quantum computation; quantum logic.

1. INTRODUCTION

The theory of quantum computation naturally suggests the semantic characterization for a new form of quantum logic, that turns out to have some typical *unsharp* features. According to this semantics, the *meaning* of a sentence is identified with a *system of qubits*, a vector belonging to a convenient Hilbert space, whose dimension depends on the logical complexity of our sentence. At the same time, the *logical connectives* are interpreted as particular *logical gates*.

2. QUANTUM LOGICAL GATES

We will first sum up some basic notions of quantum computation.

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

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

[1] Dipartimento di Informatica, Sistemistica e Comunicazione, Università di Milano—Bicocca, Milano, Italy.
[2] Dipartimento di Filosofia, Università di Firenze, Firenze, Italy.
[3] Dipartimento di Scienze Pedagogiche e Filosofiche, Università di Cagliari, Cagliari, Italy.
[4] To whom correspondence should be addressed at Dipartimento di Informatica, Sistemistica e Comunicazione, Università di Milano—Bicocca, Via Bicocca degli Arcimboldi 8, I-20126 Milano, Italy; e-mail: leporini@disco.unimib.it.

0020-7748/04/0800-1803/0 © 2004 Springer Science+Business Media, Inc.

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

Hence, any *qubit* has the following form:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle,$$

where $a_0, a_1 \in \mathbb{C}$ and $|a_0|^2 + |a_1|^2 = 1$.

We will use $x, y, \ldots$ as variables ranging over the set $\{0, 1\}$. At the same time, $|x\rangle, |y\rangle, \ldots$ will range over the basis $\{|0\rangle, |1\rangle\}$. Furthermore, we will use the following abbreviation: $\otimes^n\mathbb{C}^2 := \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n\text{-times}}$ (where $\otimes$ represents the tensor product).

The set of all vectors having the form $|x_1\rangle \otimes \cdots \otimes |x_n\rangle$ represents an orthonormal basis for $\otimes^n\mathbb{C}^2$ (also called *computational basis*). We will also write $|x_1, \ldots, x_n\rangle$ instead of $|x_1\rangle \otimes \cdots \otimes |x_n\rangle$.

Definition 2.2. n-qubit system (or n-quregister)
An *n-qubit system* (or *n-quregister*) is a unit vector $|\psi\rangle$ in the product space $\otimes^n\mathbb{C}^2$.

Apparently, the computational basis of $\otimes^n\mathbb{C}^2$ can be labeled by binary strings such as

$$|\underbrace{011\ldots10}_{n\text{-times}}\rangle.$$

Since any string $|\underbrace{011\ldots10}_{n\text{-times}}\rangle$ represents a natural number $j \in [0, 2^n - 1]$ in binary notation, any unit vector of $\otimes^n\mathbb{C}^2$ can be shortly expressed in the following form:

$$\sum_{j=0}^{2^n-1} a_j \, \| j\rangle\rangle,$$

where $0 \leq j \leq 2^n - 1$ and $\| j\rangle\rangle$ is the basis-element corresponding to j.

In the following we will call any vector that is either a qubit or an n-qubit system a *quregister*. At the same time, $|0\rangle$ and $|1\rangle$ will be also called *bits*.

We will now introduce some examples of *quantum logical gates*. Generally, a quantum logical gate can be described as a unitary operator, assuming arguments and values in a product-Hilbert space $\otimes^n\mathbb{C}^2$. First of all we will study the so called *Toffoli gate*. It will be expedient to start by analysing the simplest case, where the Hilbert space has the form

$$\otimes^3\mathbb{C}^2 = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2.$$

In such a case, the Toffoli gate will transform the vectors of $\otimes^3\mathbb{C}^2$ into vectors of $\otimes^3\mathbb{C}^2$. In order to stress that our operator is defined on the product space $\otimes^3\mathbb{C}^2$, we will indicate it by $T^{(1,1,1)}$. Since we want to define a unitary operator, it will be sufficient to determine its behavior for the elements of the basis, having the form $|x\rangle \otimes |y\rangle \otimes |z\rangle$ (where $x, y, z \in \{0, 1\}$).

Definition 2.3. The Toffoli gate $T^{(1,1,1)}$
The*Toffoli gate* $T^{(1,1,1)}$ is the linear operator $T^{(1,1,1)} : \otimes^3\mathbb{C}^2 \rightarrowtail \otimes^3 \mathbb{C}^2$ that is defined for any element $|x\rangle \otimes |y\rangle \otimes |z\rangle$ of the basis as follows:

$$T^{(1,1,1)}(|x\rangle \otimes |y\rangle \otimes |z\rangle) = |x\rangle \otimes |y\rangle \otimes |xy \oplus z\rangle,$$

where $\oplus$ represents the sum modulo 2.

From an intuitive point of view, it seems quite natural to "see" the gate $T^{(1,1,1)}$ as a kind of "truth-table" that transforms triples of *zeros* and of *ones* into triples of *zeros* and of *ones*. The "table" we obtain is the following:

$$\begin{array}{ccc}
|0,0,0\rangle & \rightarrowtail & |0,0,0\rangle \\
|0,0,1\rangle & \rightarrowtail & |0,0,1\rangle \\
|0,1,0\rangle & \rightarrowtail & |0,1,0\rangle \\
|0,1,1\rangle & \rightarrowtail & |0,1,1\rangle \\
|1,0,0\rangle & \rightarrowtail & |1,0,0\rangle \\
|1,0,1\rangle & \rightarrowtail & |1,0,1\rangle \\
|1,1,0\rangle & \rightarrowtail & |1,1,1\rangle \\
|1,1,1\rangle & \rightarrowtail & |1,1,0\rangle
\end{array}$$

In the first six cases, $T^{(1,1,1)}$ behaves like the identity operator; in the last two cases, instead, our gate transforms the last element of the triple into the opposite element (0 is transformed into 1 and 1 is transformed into 0).

One can easily show that $T^{(1,1,1)}$ has been well defined for our aims: one is dealing with an operator that is not only linear but also unitary. The matrix representation of $T^{(1,1,1)}$ is the following:

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}$$

By using $T^{(1,1,1)}$, we can introduce a convenient notion of *conjunction*. This conjunction, which will be indicated by AND, is characterized as a function whose arguments are pairs of vectors in $\mathbb{C}^2$ and whose values are vectors of the product space $\otimes^3\mathbb{C}^2$.

Definition 2.4. AND
For any $|\varphi\rangle \in \mathbb{C}^2$ and any $|\psi\rangle \in \mathbb{C}^2$:

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

Let us check that AND represents a good generalization of the corresponding classical truth-function. For the arguments $|0\rangle$ and $|1\rangle$ we obtain the following "truth-table":

$$\begin{array}{lcl}
(|0\rangle, |0\rangle) & \rightarrowtail & T^{(1,1,1)}(|0\rangle \otimes |0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle \otimes |0\rangle \\
(|0\rangle, |1\rangle) & \rightarrowtail & T^{(1,1,1)}(|0\rangle \otimes |1\rangle \otimes |0\rangle) = |0\rangle \otimes |1\rangle \otimes |0\rangle \\
(|1\rangle, |0\rangle) & \rightarrowtail & T^{(1,1,1)}(|1\rangle \otimes |0\rangle \otimes |0\rangle) = |1\rangle \otimes |0\rangle \otimes |0\rangle \\
(|1\rangle, |1\rangle) & \rightarrowtail & T^{(1,1,1)}(|1\rangle \otimes |1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle \otimes |1\rangle
\end{array}$$

One immediately realizes the difference with respect to the classical case. The classical truth-table represents a typical irreversible transformation:

$$\begin{array}{lcl}
(0, 0) & \rightarrowtail & 0 \\
(0, 1) & \rightarrowtail & 0 \\
(1, 0) & \rightarrowtail & 0 \\
(1, 1) & \rightarrowtail & 1
\end{array}$$

The arguments of the function determine the value, but not the other way around. As is well known, irreversibility generally brings about dissipation of information. Mathematically, however, any Boolean function $f : \{0, 1\}^n \rightarrowtail \{0, 1\}^m$ can be transformed into a *reversible* function $\hat{f} : \{0, 1\}^n \times \{0, 1\}^m \rightarrowtail \{0, 1\}^n \times \{0, 1\}^m$ in the following way:

$$\forall u \in \{0, 1\}^n\ \forall v \in \{0, 1\}^m : \hat{f}((u, v)) = (u, v \oplus f(u)),$$

where $\oplus$ is the sum modulo 2 pointwise defined. The function that is obtained by making reversible the irreversible classical "and" corresponds to the Toffoli gate. The classical "and" is then recovered by fixing the third input bit to 0.

Accordingly, the three arguments (0, 0), (0, 1), (1, 0) turn out to correspond to three distinct values, represented by the triples (0, 0, 0), (0, 1, 0), (1, 0, 0). The price we have paid in order to obtain a reversible situation is the increasing of the complexity of our Hilbert space. The function AND associates to pairs of arguments, belonging to the two-dimensional space $\mathbb{C}^2$, values belonging to the space $\otimes^3\mathbb{C}^2$ (whose dimension is 2^3).

All this happens in the simplest situation, when one is only dealing with elements of the basis (in other words, with precise pieces of information). Let us examine the case where the function AND is applied to arguments that are superpositions of the basis-elements in the space $\mathbb{C}^2$. Consider the following *qubit* pair:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle, \quad |\varphi\rangle = b_0|0\rangle + b_1|1\rangle.$$

By applying the definitions of AND and of $T^{(1,1,1)}$, we obtain

$$\mathtt{AND}(|\psi\rangle, |\varphi\rangle) = a_1b_1|1, 1, 1\rangle + a_1b_0|1, 0, 0\rangle + a_0b_1|0, 1, 0\rangle + a_0b_0|0, 0, 0\rangle.$$

This result suggests a quite natural logical interpretation. The four basis-elements that occur in the superposition-vector correspond to the four cases of the truth-table for the classical conjunction:

$$(1, 1, 1), (1, 0, 0), (0, 1, 0), (0, 0, 0).$$

However here, unlike the classical situation, each case is accompanied by a complex number, which represents a characteristic quantum *amplitude*. By applying the "Born rule" we will obtain the following interpretation: $|a_1b_1|^2$ represents the probability-value that both the *qubit*-arguments are equal to $|1\rangle$, and consequently their conjunction is $|1\rangle$. The other three cases admit a similar interpretation.

The logical gate AND refers to a very special situation, characterized by a Hilbert space having the form $\otimes^3\mathbb{C}^2$. However, our procedure can be easily generalized. The Toffoli gate can be defined in any Hilbert space having the form

$$(\otimes^n\mathbb{C}^2) \otimes (\otimes^m\mathbb{C}^2) \otimes \mathbb{C}^2 (= \otimes^{n+m+1}\mathbb{C}^2).$$

Definition 2.5. The Toffoli gate $T^{(n,m,1)}$
The *Toffoli gate* $T^{(n,m,1)}$ is the linear operator

$$T^{(n,m,1)} : (\otimes^n\mathbb{C}^2) \otimes (\otimes^m\mathbb{C}^2) \otimes \mathbb{C}^2 \rightarrowtail (\otimes^n\mathbb{C}^2) \otimes (\otimes^m\mathbb{C}^2) \otimes \mathbb{C}^2,$$

that is defined for any element $|x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z\rangle$ of the computational basis of $\otimes^{n+m+1}\mathbb{C}^2$ as follows:

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

where $\oplus$ represents the sum modulo 2.

On this basis one can immediately generalize our definition of AND.

Definition 2.6. AND

For any $|\varphi\rangle \in \otimes^n \mathbb{C}^2$ and any $|\psi\rangle \in \otimes^m \mathbb{C}^2$:

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

How to deal in this context with the concept of negation? A characteristic of quantum computation is the possibility of defining a plurality of negation-operations: some of them represent good generalizations of the classical negation. We will first consider a function NOT that simply inverts the value of the last elements of any basis-vector. Thus, if $|x_1, \ldots, x_n\rangle$ is any vector of the computational basis of $\otimes^n \mathbb{C}^2$, the result of the application of NOT to $|x_1, \ldots, x_n\rangle$ will be $|x_1, \ldots, 1 - x_n\rangle$.

Consider first the simplest case, concerning the negation of a single *qubit*. In such a case, the function NOT will be a unary function assuming arguments in the space $\mathbb{C}^2$ and values in the space $\mathbb{C}^2$.

Definition 2.7. $\mathtt{NOT}^{(1)}$
For any $|\varphi\rangle = a_0|0\rangle + a_1|1\rangle \in \mathbb{C}^2$:

$$\mathtt{NOT}^{(1)}\,(|\varphi\rangle) := a_1|0\rangle + a_0|1\rangle.$$

One can immediately check that NOT represents a good generalization of the classical truth-table. Consider the basis-elements $|0\rangle$ e $|1\rangle$. In such a case we will obtain

$$\mathtt{NOT}^{(1)}(|1\rangle) = |0\rangle;$$

$$\mathtt{NOT}^{(1)}(|0\rangle) = |1\rangle.$$

The quantum logical gate $\mathtt{NOT}^{(1)}$ can be easily generalized in the following way.

Definition 2.8. $\mathtt{NOT}^{(n)}$
$\mathtt{NOT}^{(n)}$ is the map

$$\mathtt{NOT}^{(n)} : \otimes^n \mathbb{C}^2 \rightarrowtail \otimes^n \mathbb{C}^2$$

s.t. for any $|\psi\rangle = \sum_{j=0}^{2^n-1} a_j |x_{j_1}, \ldots, x_{j_n}\rangle \in \otimes^n \mathbb{C}^2$:

$$\mathtt{NOT}(|\psi\rangle) := \sum_{j=0}^{2^n-1} a_j |x_{j_1}, \ldots, x_{j_{n-1}}, 1 - x_{j_n}\rangle$$

The matrix corresponding to $\mathtt{NOT}^{(1)}$ will be

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The matrix corresponding to $\mathtt{NOT}^{(n)}$ will be the following $2^n \times 2^n$ matrix:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \cdot & \cdot & \cdot & 0 \\ 1 & 0 & 0 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 0 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & 0 & 0 & 1 \\ 0 & \cdot & \cdot & \cdot & 0 & 0 & 1 & 0 \end{pmatrix}$$

We will omit the index n in $\mathtt{NOT}^{(n)}$ if no confusion is possible.

Finally, how to introduce a reasonable disjunction? A gate `OR` can be naturally defined in terms of `AND` and `NOT` via de Morgan.

Definition 2.9. `OR`

For any $|\varphi\rangle \in \otimes^n \mathbb{C}^2$ and $|\psi\rangle \in \otimes^m \mathbb{C}^2$:

$$\mathtt{OR}(|\varphi\rangle, |\psi\rangle) = \mathtt{NOT}\,(\mathtt{AND}\,(\mathtt{NOT}(|\varphi\rangle), \mathtt{NOT}(|\psi\rangle)))\,.$$

The quantum logical gates we have considered so far are, in a sense, "semi-classical." A quantum logical behavior only emerges in the case where our gates are applied to superpositions. When restricted to classical registers, our gates turn out to behave as classical truth-functions. We will now investigate *genuine quantum gates* that may transform classical registers into quregisters that are superpositions.

One of the most significant genuine quantum gates is the *square root of the negation* `NOT`, which will be indicated by $\sqrt{\mathtt{NOT}}$. As suggested by the name, the characteristic property of the gate $\sqrt{\mathtt{NOT}}$ is the following: for any quregister $|\psi\rangle$,

$$\sqrt{\mathtt{NOT}}(\sqrt{\mathtt{NOT}}(|\psi\rangle)) = \mathtt{NOT}(|\psi\rangle).$$

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

Interestingly enough, the gate $\sqrt{\mathtt{NOT}}$ has some interesting physical models (and implementations). As an example, consider an idealized atom with a single electron and two energy levels: a *ground state* (identified with $|0\rangle$) and an *excited state* (identified with $|1\rangle$). By shining a pulse of light of appropriate intensity, duration, and wavelength, it is possible to force the electron to change the energy level. As a consequence, the state (bit) $|0\rangle$ is transformed into the state (bit) $|1\rangle$, and vice versa:

$$|0\rangle \rightarrowtail |1\rangle; \quad |1\rangle \rightarrowtail |0\rangle.$$

We have obtained a typical physical model for the gate NOT. Now, by using a light pulse of half the duration as the one needed to perform the NOT operation, we effect a half-flip between the two logical states. The state of the atom after the half pulse is neither $|0\rangle$ nor $|1\rangle$, but rather a superposition of both states. As observed by Deutsch *et al.* (2000):

> Logicians are now entitled to propose a new logical operation $\sqrt{\mathtt{NOT}}$. Why? Because a faithful physical model for it exists in nature.

Let us now give the mathematical definition of $\sqrt{\mathtt{NOT}}$. We will first consider the simplest case, which refers to the space $\mathbb{C}^2$.

Definition 2.10. $\sqrt{\mathtt{NOT}}^{(1)}$
$\sqrt{\mathtt{NOT}}^{(1)}$ is the map

$$\sqrt{\mathtt{NOT}}^{(1)} : \mathbb{C}^2 \to \mathbb{C}^2$$

such that for any $|\psi\rangle =: a_0|0\rangle + a_1|1\rangle$:

$$\sqrt{\mathtt{NOT}}^{(1)}(|\psi\rangle) := \frac{1}{2}\left[(1+i)a_0 + (1-i)a_1\right]|0\rangle + \frac{1}{2}\left[(1-i)a_0 + (1+i)a_1\right]|1\rangle,$$

where i is the imaginary unit.

It turns out that the matrix associated to $\sqrt{\mathtt{NOT}}^{(1)}$ is

$$\begin{pmatrix} \frac{1}{2}+\frac{i}{2} & \frac{1}{2}-\frac{i}{2} \\ \frac{1}{2}-\frac{i}{2} & \frac{1}{2}+\frac{i}{2} \end{pmatrix}$$

Thus, $\sqrt{\mathtt{NOT}}^{(1)}$ transforms the two bits $|0\rangle$ and $|1\rangle$ into the superposition states $\frac{1}{2}(1+i)|0\rangle + \frac{1}{2}(1-i)|1\rangle$ and $\frac{1}{2}(1-i)|0\rangle + \frac{1}{2}(1+i)|1\rangle$, respectively.

The quantum logical gate $\sqrt{\mathtt{NOT}}^{(1)}$ can be easily generalized in the following way.

Definition 2.11. $\sqrt{\mathtt{NOT}}^{(n)}$
$\sqrt{\mathtt{NOT}}^{(n)}$ is the map

$$\sqrt{\mathtt{NOT}}^{(n)} : \otimes^n\mathbb{C}^2 \rightarrowtail \otimes^n \mathbb{C}^2$$

such that for any $|\psi\rangle = \sum_{j=0}^{2^n-1} a_j|x_{j_1}, \ldots, x_{j_n}\rangle \in \otimes^n\mathbb{C}^2$:

$$\sqrt{\mathtt{NOT}}^{(n)}(|\psi\rangle) := \sum_{j=0}^{2^n-1} a_j|x_{j_1}, \ldots, x_{j_{n-1}}\rangle \otimes \left(\frac{1+i}{2}|x_{j_n}\rangle + \frac{1-i}{2}|1-x_{j_n}\rangle\right).$$

It is easy to see that for any n, $\sqrt{\mathtt{NOT}}^{(n)}$ is a unitary operator such that

$$\sqrt{\mathtt{NOT}}^{(n)}\sqrt{\mathtt{NOT}}^{(n)} = \mathtt{NOT}^{(n)}.$$

The matrix associated to the quantum logical gate $\sqrt{\mathtt{NOT}}$ is the $(2^n) \times (2^n)$ matrix of the form

$$\frac{1}{2}\begin{pmatrix} 1+i & 1-i & \cdot & \cdot & \cdots & \cdot & \cdot \\ 1-i & 1+1 & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & 1+i & 1-i & \cdots & \cdot & \cdot \\ \cdot & \cdot & 1-i & 1+i & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdots & 1+i & 1-i \\ \cdot & \cdot & \cdot & \cdot & \cdots & 1-1 & 1+i \end{pmatrix}$$

We will omit the index n in $\sqrt{\mathtt{NOT}}^{(n)}$ if no confusion is possible.

Theorem 2.1. *For any n, m the following properties hold:*

(i) $T^{(n,m,1)}\sqrt{\mathtt{NOT}}^{(n+m+1)} = \sqrt{\mathtt{NOT}}^{(n+m+1)}T^{(n,m,1)}$;
(ii) $\sqrt{\mathtt{NOT}}^{(n)}\mathtt{NOT}^{(n)} = \mathtt{NOT}^{(n)}\sqrt{\mathtt{NOT}}^{(n)}$.

3. THE PROBABILISTIC CONTENT OF THE QUANTUM LOGICAL GATES

For any quregister one can define a natural *probability-value*, which will play an important role in our quantum computational semantics.

Suppose we have a vector

$$|\varphi\rangle = \sum_{j=0}^{2^n-1} a_j \,\| j\rangle\rangle \in \otimes^n\mathbb{C}^2.$$

Let us first define two particular sets of coefficients that occur in the superposition-vector φ:

$$C^+|\varphi\rangle = \{a_j \;:\; \| j\rangle\rangle = \{x_{j_1}, \ldots, x_{j_{n-1}}, 1\}\},$$

$$C^-|\varphi\rangle = \{a_j \;:\; \| j\rangle\rangle = |x_{j_1}, \ldots, x_{j_{n-1}}, 0\rangle\}.$$

Clearly, the elements of $C^+|\varphi\rangle$ ($C^-|\varphi\rangle$) represent the *amplitudes* associated to the different vector-basis of $\otimes^n\mathbb{C}^2$ ending with 1 (0, respectively). On this basis, we can now define the probability-value of any vector having length less than or equal to 1.

Definition 3.12. The probability-value of a vector
Let $|\psi\rangle = \sum_{j=0}^{2^n-1} a_j \, \| j\rangle\rangle$ be any vector of $\otimes^n \mathbb{C}^2$ such that $\sum_{j=0}^{2^n-1} |a_j|^2 = 1$. Then the probability-value of $|\psi\rangle$ is defined as follows:

$$\mathrm{Prob}(|\psi\rangle) := \sum_{a_j \in C^+|\psi\rangle} |a_j|^2.$$

According to our definition, in order to calculate the probability-value of a quregister $|\psi\rangle$ one has to perform the following operations:

- Consider all the amplitudes a_j that are associated to a basis-element ending with 1;
- Take the squared modules $|a_j|^2$ of all these complex numbers a_j;
- Sum all the real numbers $|a_j|^2$.

One can prove:

Lemma 3.2.

(i) *If* $|\psi\rangle = \sum_{j=0}^{2^n-1} a_j \, \| j\rangle\rangle$ *is any unit vector of* $\otimes^n \mathbb{C}^2$, *then*

$$\sum_{a_j \in C^+|\psi\rangle} |a_j|^2 + \sum_{a_j \in C^-|\psi\rangle} |a_j|^2 = 1.$$

(ii) *Let* $|\psi\rangle = \sum_{j=0}^{2^n-1} a_j \, \| j\rangle\rangle$ *and* $|\varphi\rangle = \sum_{j=0}^{2^n-1} b_j \, \| j\rangle\rangle$ *be any two orthogonal vectors of* $\otimes^n \mathbb{C}^2$ *s.t.* $\| |\psi\rangle + |\varphi\rangle \| \leq 1$ *and* $\forall j (0 \leq j \leq 2^n - 1)$: $a_j b_j = 0$. *Then*

$$\mathrm{Prob}(|\psi\rangle + |\varphi\rangle) = \mathrm{Prob}(|\psi\rangle) + \mathrm{Prob}(|\varphi\rangle).$$

From an intuitive point of view, $\mathrm{Prob}(|\psi\rangle)$ represents "the probability" that the quregister $|\psi\rangle$ (which is a superposition) "collapses" into a classical register whose last element is 1.

The following theorem describes some interesting relations between the probability function Prob and our basic logical gates.

Theorem 3.3. *Let* $|\psi\rangle = \sum_{j=0}^{2^n-1} a_j \, \| j\rangle\rangle$ *and* $|\varphi\rangle = \sum_{k=0}^{2^m-1} b_k \, \| k\rangle\rangle$ *be two unit vectors of* $\otimes^n \mathbb{C}^2$ *(*$\otimes^m \mathbb{C}^2$*, respectively). The following properties hold*

(i) $\mathrm{Prob}(\mathtt{AND}(|\psi\rangle, |\varphi\rangle)) = \mathrm{Prob}(|\psi\rangle)\mathrm{Prob}(|\varphi\rangle)$;
(ii) $\mathrm{Prob}(\mathtt{NOT}(|\psi\rangle)) = 1 - \mathrm{Prob}(|\varphi\rangle)$;
(iii) $\mathrm{Prob}(\mathtt{OR}(|\psi\rangle, \varphi)) = \mathrm{Prob}(|\psi\rangle) + \mathrm{Prob}(|\varphi\rangle) - \mathrm{Prob}(|\psi\rangle)\mathrm{Prob}(|\varphi\rangle$;
(iv) $\mathrm{Prob}(\sqrt{\mathtt{NOT}}(|\psi\rangle)) = \sum_{j \in C^+|\psi\rangle} \mid \frac{1}{2}(1-i)a_{j-1} + \frac{1}{2}(1+i)a_j \mid^2$.

(v) $\text{Prob}(\sqrt{\texttt{NOT}}\,\texttt{NOT}(|\psi\rangle)) = \text{Prob}(\texttt{NOT}\sqrt{\texttt{NOT}}(|\psi\rangle)) = \sum_{j \in C^+|\psi\rangle} |\, \frac{1}{2}(1+i) a_{j-1} + \frac{1}{2}(1-i)a_j \,|^2$.

(vi) $\text{Prob}(\sqrt{\texttt{NOT}}(\texttt{AND}(|\psi\rangle, |\varphi\rangle))) = \frac{1}{2}$.

Condition (i) of Theorem 3 represents a quite unusual property for probabilistic contexts: any pair of quregisters seems to behave here like a classical pair of independent events (so that the probability of their conjunction is the product of the probabilities of both members). At the same time, condition (ii) and (iii) appear to be well behaved with respect to standard probability theory. As a consequence, we obtain

- unlike classical and quantum probability, AND, OR, NOT have a "truth-functional behavior" with respect to the function Prob: the probability of the "whole" is determined by the probabilities of the parts.
- The gate $\sqrt{\texttt{NOT}}$ is not truth-functional. It may happen at the same time that: $\text{Prob}(|\psi\rangle) = \text{Prob}(|\varphi\rangle)$ and $\text{Prob}(\sqrt{\texttt{NOT}}(\psi)) \neq \text{Prob}(\sqrt{\texttt{NOT}}(|\varphi\rangle))$. For example, let $|\psi\rangle := \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle$ and $|\varphi\rangle := \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i)|1\rangle$. Clearly, $\text{Prob}(|\psi\rangle) = \text{Prob}(|\varphi\rangle) = \frac{1}{2}$. However, $\text{Prob}(\sqrt{\texttt{NOT}}(\psi)) = \frac{1}{2}$ and $\text{Prob}(\sqrt{\texttt{NOT}}(|\varphi\rangle)) = \frac{1}{2} - \frac{1}{2\sqrt{2}}$.

As one can easily see, the operators $\texttt{NOT}^{(1)}$ and $\sqrt{\texttt{NOT}}^{(1)}$ have the same set of fixed points. In other words, for any (unit) vector $|\psi\rangle \in \mathbb{C}^2 : \texttt{NOT}^{(1)}(|\psi\rangle) = |\psi\rangle$ iff $\sqrt{\texttt{NOT}}^{(1)}(|\psi\rangle) = |\psi\rangle$. Every vector of the form $\frac{e^{i\vartheta}}{\sqrt{2}}(|0\rangle + |1\rangle)$ turns out to be a fixed point of $\texttt{NOT}^{(1)}$ and, accordingly, of $\sqrt{\texttt{NOT}}^{(1)}$.

4. QUANTUM COMPUTATIONAL SEMANTICS

The starting point of the quantum computational semantics is quite different from the standard quantum logical approach. The meanings of sentences are here represented by quregisters. From an intuitive point of view, one can say that the meaning of a sentence is identified with the *information quantity* encoded by the sentence in question.

Consider a sentential language $\mathcal{L}$ with the following connectives: the *negation* ($\neg$), the *conjunction* ($\curlywedge$), and the *square root of the negation* ($\sqrt{\neg}$). The notion of *sentence* (or *formula*) of $\mathcal{L}$ is defined in the expected way. Let $Form^{\mathcal{L}}$ represent the set of all sentences of $\mathcal{L}$. We will use the following metavariables: **p**, **q**, **r**, ... for atomic sentences and $\alpha, \beta, \gamma, \ldots$ for sentences. The connective *disjunction* ($\curlyvee$) is supposed defined via de Morgan's law:

$$\alpha \curlyvee \beta := \neg(\neg\alpha \curlywedge \neg\beta).$$

We will now introduce the basic concept of our semantics, the notion of *quantum computational realization*: an interpretation of the language $\mathcal{L}$, such that the meaning associated to any sentence is a quregister. As a consequence, the *space of the meanings* corresponds here to a variable Hilbert space (instead of a unique Hilbert space). Any space of this kind will be a product space $\otimes^n \mathbb{C}^2$.

Definition 4.13. Quantum computational realization
A *quantum computational realization* of $\mathcal{L}$ is a function Qub associating to any sentence α a quregister in a Hilbert space $\otimes^n \mathbb{C}^2$ (where n depends on the linguistic form of α):

$$Qub : Form^{\mathcal{L}} \rightarrowtail \bigcup_n \otimes^n \mathbb{C}^2.$$

We will also write $|\alpha\rangle$ instead of $Qub(\alpha)$; and we will call $|\alpha\rangle$ the *information-value* of α. The following conditions are required:

(i) $|\mathbf{p}\rangle$ is a qubit;
(ii) Let $|\beta\rangle \in \otimes^n \mathbb{C}^2$. Then
$|\neg\beta\rangle = \mathtt{NOT}(|\beta\rangle) \in \otimes^n \mathbb{C}^2$;
(iii) Let $|\beta\rangle \in \otimes^n \mathbb{C}^2$, $|\gamma\rangle \in \otimes^m \mathbb{C}^2$. Then:
$|\beta \curlywedge \gamma\rangle = \mathtt{AND}(|\beta\rangle, |\gamma\rangle) \in (\otimes^n \mathbb{C}^2) \otimes (\otimes^m \mathbb{C}^2) \otimes \mathbb{C}^2$;
(iv) Let $|\beta\rangle \in \otimes^n \mathbb{C}^2$. Then
$|\sqrt{\neg}\beta\rangle = \sqrt{\mathtt{NOT}}(|\beta\rangle) \in \otimes^n \mathbb{C}^2$.

Our definition univocally determines, for any sentence α, the Hilbert space $\otimes^n \mathbb{C}^2$ to which $|\alpha\rangle$ belongs. Clearly, n is the number of all occurrences of atomic sentences and of the connective $\curlywedge$ in α. Since the meaning associated to a given sentence partially reflects the logical form of the sentence in question, we can say that our semantics has a typical *intensional* character.

As we have seen, a characteristic of our semantics is to identify the meanings of the linguistic sentences with unit vectors of variable Hilbert spaces. As a consequence, we will obtain that the information-value of a sentence naturally determines a probability-value for that sentence.

Let Qub be a quantum computational realization and let α be any sentence with associated meaning $|\alpha\rangle$. Like all quregisters, also this $|\alpha\rangle$ will have a probability-value, which (according to Definition 3.12.), is determined as follows:

$$\text{Prob}(|\alpha)\rangle := \sum_{a_j \in C^+|\alpha\rangle} |a_j|^2.$$

On this basis, one can naturally define the probability-value of any sentence of our language:

Definition 4.14. The probability-value of α

$$\text{Prob}(\alpha) := \sum_{a_j \in C^+|\alpha\rangle} |a_j|^2.$$

As an example, let us first consider the simplest case, where α is an atomic sentence; in this case, its information-value will belong to the two-dimensional space $\mathbb{C}^2$. Suppose, for instance, that $|\alpha\rangle$ has the form

$$a_0|0\rangle + a_1|1\rangle.$$

Then, the probability-value of α will be

$$\text{Prob}(\alpha) = |a_1|^2.$$

Thus, $\text{Prob}(\alpha) = |a_1|^2$ represents the probability that our *uncertain* information $|\alpha\rangle$ corresponds to the *precise* information $|1\rangle$.

From an intuitive point of view, our definition, clearly, attributes a privileged role to one of the two basic *qubits* (belonging to the basis of $\mathbb{C}^2$): the *qubit* $|1\rangle$. In such a way, $|1\rangle$ is dealt with as the truth-value *True*.

Consider now the case of a molecular sentence α. Its information-value $|\alpha\rangle$ will belong to the space $\otimes^n\mathbb{C}^2$, where n ($\geq$3) depends on the length of α. The dimension of $\otimes^n\mathbb{C}^2$ is 2^n. Hence $|\alpha\rangle$ will generally be a superposition of elements of the basis of $\otimes^n\mathbb{C}^2$. Thus, we will have

$$|\alpha\rangle = \sum_{j=0}^{2^n-1} a_j \, \| j\rangle\rangle,$$

where $\| j\rangle\rangle$ ranges over the basis of $\otimes^n\mathbb{C}^2$.

From the logical point of view, any $\| j\rangle\rangle$ (element of the basis of $\otimes^n\mathbb{C}^2$) represents a possible case of a "reversibile truth-table" for α. For instance, suppose α has the form $\mathbf{p} \curlyvee \mathbf{q}$, where

$$|\mathbf{p}\rangle = a_0|0\rangle + a_1|1\rangle, \;\; |\mathbf{q}\rangle = b_0|0\rangle + b_1|1\rangle.$$

By applying the definitions of quantum computational realization and of `OR`, we will obtain

$$|\mathbf{p} \curlyvee \mathbf{q}\rangle = a_1b_1|1, 1, 1\rangle + a_1b_0|1, 0, 1\rangle + a_0b_1|0, 1, 1\rangle + a_0b_0|0, 0, 0\rangle.$$

We know that the number $|a_1b_1|^2$ represents the probability that both the members of our disjunction are true and that, consequently, the disjunction is true. Similarly in the other cases. In order to calculate the probability of the truth of $\mathbf{p} \curlyvee \mathbf{q}$, it will be sufficient to sum the three probability-values corresponding to the three cases where the final result is *True* (that is the cases of the vectors $|1, 1, 1\rangle$, $|1, 0, 1\rangle$, $|0, 1, 1\rangle$). On this basis, we will be able to assign to the disjunction $\mathbf{p} \curlyvee \mathbf{q}$ the following probability-value:

$$|a_1b_1|^2 + |a_1b_0|^2 + |a_0b_1|^2.$$

We can now define the notions of *truth*, *logical truth*, *consequence* , and *logical consequence*.

Definition 4.15. Truth and logical truth
A sentence α is *true in a realization Qub* ($\models_{Qub} \alpha$) iff $\text{Prob}(\alpha) = 1$.
α is a *logical truth* ($\models \alpha$) iff for any realization *Qub*, $\models_{Qub} \alpha$.

Definition 4.16. Consequence and logical consequence
β is a *consequence of* α *in the realization Qub* ($\alpha \models_{Qub} \beta$) iff $\text{Prob}(\alpha) \leq \text{Prob}(\beta)$;
β is a *logical conseguence* of α ($\alpha \models \beta$) iff for any *Qub*: $\alpha \models_{Qub} \beta$.

Let us call the logic characterized by this semantics *quantum computational logic* (**QCL**).

Some interesting examples of logical consequences that hold in **QCL** are the following:

Theorem 4.4.

(i) $\alpha \models \neg\neg\alpha, \quad \neg\neg\alpha \models \alpha$;
(double negation)
(ii) $\sqrt{\neg}\sqrt{\neg}\alpha \models \neg\alpha, \quad \neg\alpha \models \sqrt{\neg}\sqrt{\neg}\alpha$;
(iii) $\alpha \curlywedge \beta \models \beta \curlywedge \alpha, \quad \alpha \curlyvee \beta \models \beta \curlyvee \alpha$;
(commutativity)
(iv) $\alpha \curlywedge (\beta \curlywedge \gamma) \models (\alpha \curlywedge \beta) \curlywedge \gamma, \quad (\alpha \curlywedge \beta) \curlywedge \gamma \models \alpha \curlywedge (\beta \curlywedge \gamma)$;
(associativity)
(v) $\alpha \curlyvee (\beta \curlyvee \gamma) \models (\alpha \curlyvee \beta) \curlyvee \gamma, \quad (\alpha \curlyvee \beta) \curlyvee \gamma \models \alpha \curlyvee (\beta \curlyvee \gamma)$;
(associativity)
(vi) $\neg(\alpha \curlywedge \beta) \models \neg\alpha \curlyvee \neg\beta, \quad \neg\alpha \curlyvee \neg\beta \models \neg(\alpha \curlywedge \beta)$;
(de Morgan)
(vii) $\neg(\alpha \curlyvee \beta) \models \neg\alpha \curlywedge \neg\beta, \quad \neg\alpha \curlywedge \neg\beta \models \neg(\alpha \curlyvee \beta)$
(de Morgan)
(viii) $\alpha \curlywedge \alpha \models \alpha$.
(semiidempotence 1)
(ix) $\alpha \curlywedge (\beta \curlyvee \gamma) \models (\alpha \curlywedge \beta) \curlyvee (\alpha \curlywedge \gamma)$.
(distributivity 1)

Some logical consequences and some logical truths that are violated in **QCL** are the following:

Theorem 4.5.

(i) $\alpha \not\models \alpha \curlywedge \alpha$;
(semiidempotence 2)
(ii) $\not\models \alpha \curlyvee \neg\alpha$
(excluded middle)

(iii) $\not\models \neg(\alpha \curlywedge \neg\alpha)$;
(noncontradiction)

(iv) $(\alpha \curlywedge \beta) \vee (\alpha \curlywedge \gamma) \not\models \alpha \curlywedge (\beta \curlyvee \gamma)$.
(distributivity)

Proof: (i)–(iii) Take $|\alpha\rangle := \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle$. Then, $\text{Prob}(\alpha) = \frac{1}{2}$, $\text{Prob}(\alpha \curlywedge \alpha) = \frac{1}{4}$, $\text{Prob}(\alpha \curlyvee \neg\alpha) = \text{Prob}(\neg(\alpha \curlywedge \neg\alpha)) = \frac{3}{4}$.
(iv) Take $|\alpha\rangle = |\beta\rangle := \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle$ and $|\gamma\rangle := \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$. Then $\text{Prob}((\alpha \curlywedge \beta) \vee (\alpha \curlywedge \gamma)) = \frac{11}{32} > \frac{10}{32} = \text{Prob}(\alpha \curlywedge (\beta \curlyvee \gamma))$. □

QCL turns out to be a non standard form of quantum logic. Conjunction and disjunction do not correspond to lattice operations, because they are not generally idempotent. Unlike the usual (sharp and unsharp) quantum logics, the weak distributivity principle ($(\alpha \curlywedge \beta) \curlyvee (\alpha \curlywedge \gamma) \models \alpha \curlywedge (\beta \curlyvee \gamma)$) breaks down. At the same time, the strong distributivity ($\alpha \curlywedge (\beta \curlyvee \gamma) \models (\alpha \curlywedge \beta) \curlyvee (\alpha \curlywedge \gamma)$), that is violated in orthodox quantum logic, is here valid. Both the excluded middle and the noncontradiction principles are violated: As a consequence, we have obtained an example of an *unsharp logic*.

The axiomatizability of **QCL** is an open problem.

REFERENCES

Birkhoff, G. and von Neumann, J. (1936). The logic of quantum mechanics. *Annals of Mathematics* **37**, 823–843.

Dalla Chiara, M. L. and Giuntini, R. (2002). Quantum logics. In *Handbook of Philosophical Logic, Vol. 6*, G. Gabbay and F. Guenthner, eds., Kluwer, Dordrecht.

Deutsch, D., Ekert, A., and Lupacchini, R. (2000). Machines, logic and quantum physics. *Bulletin of Symbolic Logic* **6**(3), 265–283.

Preskill, J. (1999). Lecture Notes in Physics. In *Quantum Information and Computation, Vol. 229*, Springer, Berlin.

Ekert, A., Hayden, P., and Inamori, H. (2001). Basic concepts in quantum computation. In *Coeherent Atomic Matter Waves Vol. LXXII of Nato Advanced Study Institute—Les Houches*, R. Kaiser, C. Westbrook, and F. David, eds., Springer-Verlag, Berlin.

Gudder, S. (2000). Quantum languages. In *Current Research in Operational Quantum Logic*, B. Coecke, D. Moore, and A. Wilce, eds., Kluwer, Dordrecht.

Toffoli, T. (1980). Reversible computing. In *Automata, Languages and Programming, Vol. 84*, J. W. de Baker, J. van Leeuwen, eds., Springer, Berlin.