# FROM QUANTUM LOGIC TO QUANTUM COMPUTATIONAL LOGIC

## MICHELE CAPONIGRO AND STEFANO MANCINI

*Physics Department, University of Camerino,*
*Madonna delle Carceri, I-62032 Camerino, Italy*
{*michele.caponigro, stefano.mancini*}*@unicam.it*

**Abstract:** We overview the main concepts of quantum logic ranging from the orthodox formulation to the quantum computational aspects.

## 1. Introduction

Quantum theory is widely accepted as the most successful theory of natural science. One of the most important consequences of the birth of quantum mechanics (QM), especially in its Hilbert space formalism, has been the development of a new kind of logic, called *quantum logic* (QL). The logic underlying classical theory is a Boolean (two-valued) logic, while quantum logic proposed as a logic of quantum mechanics is currently understood as a logic whose truth values are taken from an orthomodular lattice. The major difference relies on distributivity. The first modification of classical logic to quantum logic was proposed by Birkhoff and von Neumann [1] and it is usually referred to this as the orthodox QL. Other quantum logical approaches were developed later on [2, 3]. Recently, the birth of quantum computation and quantum information (see *e.g.* [4]) has renewed the interest on quantum logics leading to novel forms of logic [5–7].

Here, we review the principal elements of quantum logic starting from the orthodox formulation and arriving to the quantum computational logic. The paper is organized as follow. In Section 2 we give some basic notions of QM. In Section 3 we present QM Axiomatic and orthodox QL. Then, in Section 4 we discuss some other approaches. Section 5 is devoted to quantum logic calculus. In Section 6 the quantum computational logic is exposed. Finally, Section 7 is for conclusions.

## 2. Basic notions about quantum mechanics

In the standard formulation [8], QM takes place in Hilbert spaces. A Hilbert space $\mathscr{H}$ is an Euclidean linear strictly positive inner product space (generally over the field of complex numbers $\mathbb{C}$) which is complete with respect to the metric

generated by the inner product, which is separable and which can have finite or infinite dimension. Its elements are vectors.

**Postulate 1.** *Physical states are described by unit norm vectors in $\mathscr{H}$.*

We use the so called Dirac notation $|\psi\rangle$ (called *ket*). Its dual is $\langle\psi|$ (called *bra*). Then, the inner product between two states $|\psi\rangle$ and $|\phi\rangle$ reads $\langle\psi|\phi\rangle \in \mathbb{C}$. As a consequence of the structure of Hilbert space, we have:

**Principle 1.** (Superposition) *If a QM system $S$ can be in a state $|\psi_1\rangle$ and also in a state $|\psi_2\rangle$, then it can be in each linear combination of both $|\psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle$ (with $c_1, c_2 \in \mathbb{C}$).*

Linear operators on $\mathscr{H}$ play an important role. However, since physical *observables* cannot have imaginary values, not all linear operator are good for QM. We must add the requirement that the operators be self-adjoint (Hermitian).

Suppose an observable $\hat{O}$ has eigenvalues $\{o_j\}$ and eigenvectors $\{|b_j\rangle\}$ then the following relations hold

$$\hat{O}|b_j\rangle = o_j|b_j\rangle, \qquad \langle b_j|\hat{O} = o_j\langle b_j|. \tag{1}$$

**Postulate 2.** *The possible measurement results on the observable $O$ are the eigenvalues of the associated self-adjoint operator $\hat{O}$.*

**Postulate 3.** (Born rule) *If the state of a system is $|\psi\rangle$, the probability of having a determinate result (an eigenvalue $o_j$ of an arbitrary observable $\hat{O}$) is given by $\mathrm{Prob} = |c_j|^2$ with $c_j = \langle b_j|\psi\rangle$ being $|b_j\rangle$ the eigenvector of $\hat{O}$ corresponding to $o_j$.*

**Principle 2.** (Uncertainty Principle) *Any two observables $\hat{O}_1$ and $\hat{O}_2$ in $\mathscr{H}$ must satisfy the following inequality:*

$$\Delta(\hat{O}_1)\cdot\Delta(\hat{O}_2) \geq \frac{1}{2}|\langle\psi|[\hat{O}_1,\hat{O}_2]|\psi\rangle|, \tag{2}$$

*for all quantum state $|\psi\rangle$ in $\mathscr{H}$, where $[\hat{O}_1,\hat{O}_2] \equiv \hat{O}_1\hat{O}_2 - \hat{O}_2\hat{O}_1$ is the commutator between $\hat{O}_1$ and $\hat{O}_2$ and $\Delta(\hat{O}_1)$, $\Delta(\hat{O}_2)$ are standard deviations of measurements of $\hat{O}_1$ and $\hat{O}_2$ respectively.*

From this principle it turns out that it is impossible to measure exactly, at the same time, two non-commuting observables.

**Definition 1.** Projectors are one-dimensional (take only values $\{0,1\}$), self-adjoint, idempotent operators.

Formally to each state $|b_k\rangle$ corresponds a projection operator $\hat{P} = |b_k\rangle\langle b_k|$. The action of a projector $\hat{P} = |b_k\rangle\langle b_k|$ on a state $|\psi\rangle$ is $\hat{P}|\psi\rangle = |b_k\rangle\langle b_k|\psi\rangle = c_k|b_k\rangle$ with $c_k \in \mathbb{C}$.

**Postulate 4.** *The dynamics of a system is simply described through a unitary transformation on the system state.*

Suppose a system at time $t_0$ is in the state $|\psi(t_0)\rangle$. For any time $t$ (where either $t \leq t_0$ or $t_0 \leq t$), there exists a unitary operator $U_{[t_0,t]}$ that determines the state of the system at time $t$ as a function of the state of the system at time $t_0$. In other words:

$$|\psi(t)\rangle = U_{[t_0,t]}|\psi(t_0)\rangle. \tag{3}$$

Finally:

**Postulate 5.** *The space of states of a composite system is the tensor product of Hilbert spaces of subsystems.*

The extension of superposition principle to composite systems leads to the concept of *entanglement*. That is, there exist states of the whole system that cannot be factorized into states of the subsystems.

All that we have seen about QM can be rephrased in terms of mixture of states $\{w_j, |\psi_j\rangle\}$ ($w_j$ denotes for the probability for the system to be in the state $|\psi_j\rangle$) by introducing the notion of *density operator*.

**Definition 2.** A density operator $\hat{\rho}$ is a non-negative (Hermitean) trace-one class operator which is also positive semi-definite (that is $\langle \psi | \hat{\rho} | \psi \rangle \geq 0 \ \forall | \psi \rangle \in \mathscr{H}$).

Thus we can represents the mixture $\{w_j, |\psi_j\rangle\}$ by $\hat{\rho} = \sum_j w_j |\psi_j\rangle\langle\psi_j|$.

## 3. Quantum mechanics and quantum logic

As we have seen, basic QM is centered on Hilbert spaces, it associates self-adjoints operators to observables, density operators to states, projectors to propositions, unitary operators to dynamics. But the following problems arise:

- it is possible to specify a determinate Hilbert space only for a finite number of degrees of freedom, while in QM there can also be an infinite number (in the case of continuous observables);
- it is not specified where Hilbert spaces come from; why is there such duality between observables and states?

From these problems arose the search for a more stringent axiomatic approach to QM. Theoretically we have only three elementary possibilities: to take propositions, or observables, or states as primitive elements and try to deduce, in some form, the necessity of the Hilbert spaces. The first possibility was developed very early on by Quantum Logic (the orthodox approach by Birkhoff and von Neumann). It will be analysed hereafter, while other possibilities will be discussed in the next section.

Birkhoff and von Neumann [1] stated that to each proposition $A$ is associated a closed subspace of the Hilbert space, hence the projector $\hat{P}_A$ onto it. The truth or the falsity of the proposition is determined by the eigenvalues of the projector 1 or 0. Logical connectives are: intersection of subspaces (conjunction $\wedge$), direct sum of subspaces (disjunction $\vee$), and orthogonal complement (negation $\neg$). Hilbert subspaces can be supplied by an order relation $\leq$ (the inclusion) to form a lattice.

Birkhoff and von Neumann then realized that what distinguishes classical calculus (Boolean algebra) from the QM one is that *distributivity* is valid in the first case but not in the second. This is a consequence of the fact that not all observables of QM commute.

**Example.** The proposition: 'The electron has a determined momentum value $p$ and position inside or outside of this box' [formally $\hat{P}_p \wedge (\hat{P}_{qB} \vee \hat{P}_{qB'})$] is not equivalent to the proposition 'The electron has momentum $p$ and position inside this box, or its has momentum $p$ and position outside this box' [formally $(\hat{P}_p \wedge \hat{P}_{qB}) \vee (\hat{P}_p \wedge \hat{P}_{qB'})$]. In fact, the second proposition is always false in QM because it violates the Uncertainty Principle.

**Theorem 1.** (Birkhoff/von Neumann) *The QM algebra is not Boolean.*

Though correct this theorem is not integrated into the theory because it is contained by a more general theorem now to be discussed.

Birkhoff and von Neumann thought that modularity, which is weaker than distributivity, was still valid for QM. However, it was pointed out the fact that in this manner the lattice proposed was in fact Boolean. While projective geometries are always modular lattices, for proposition systems in which the maximal element is not a finite union of points, modularity is no longer compatible with other axioms. Then, Jauch [9] proved that in QM only orthomodularity and not modularity is valid.

**Theorem 2.** (Jauch) *QM algebra is a non-modular orthomodular lattice.*

Jauch discovered another important property of QM lattice:

**Theorem 3.** (Jauch) *The QM lattice is atomic and fulfills the covering property.*

It is known that a Boolean algebra is totally reducible (down to the last elements $I, \emptyset$). Therefore, irreducibility signifies the unrestricted validity of *superposition principle*. Each propositional system can be univocally reduced to irreducible ones, so that Boolean algebra is only a limiting case of a more general theory. That is, classical mechanics can be understood as a limiting case of QM. On the other hand, QM though not a Boolean algebra as such, can be understood as a collection of Boolean subalgebras.

**Theorem 4.** *Due to the superposition principle the QM lattice is irriducible, i.e. it is a collection of maximal Boolean subalgebras.*
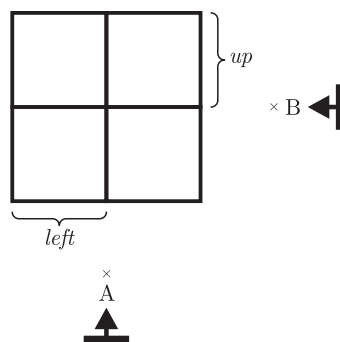


**Figure 1.** An atom in a box can move between quadrants and can emit a photon. A and B represent photon's observers

**Example.** Let us assume that we observe an atom in a box arranged as in Figure 1. The atom can move between the quadrants and can emit a photon. If an observer at point A receives the photon, he can distinguish whether the atom was in the left or in the right half of the box (here we assume macroscopic dimensions of the box and ignore microscopic quantum phenomena allowing the

atom to be in both halves of the box). Similarly, an observer at point B can distinguish the upper and lower half. In the classical case, we may place two observers at points A, B and distinguish four states corresponding to the presence of the atom in particular quadrants. In quantum systems, a simultaneous observation is impossible. Measurements are destructive (they change the state of the system irreversibly). Here a single photon can be observed only once. For the observer placed in A, the elementary observable events are left, right, dark, where left (resp. right) represents the event "the atom is observed in the left (resp. right) half", and dark represents the event "nothing was seen". All observable events form a Boolean algebra

$$\mathscr{A} = \{0, 1, \text{left}, \text{right}, \text{dark}, \text{left}', \text{right}', \text{dark}'\}, \tag{4}$$

where 0, 1 represent the impossible and the sure event, and $'$ denotes the complementation (negation). For the observer in B, the elementary observable events are up, down, dark, where up (resp. down) is the event "the atom is observed in the upper (resp. lower) half". All events observable from B form a Boolean algebra

$$\mathscr{B} = \{0, 1, \text{up}, \text{down}, \text{dark}, \text{up}', \text{down}', \text{dark}'\}. \tag{5}$$

We have no tool to observe the conjunction of left and up and other events which are supposed to exist in the classical probability theory (here we could use the third dimension; an observer at a point outside the plane of Figure 1 could distinguish all quadrants, nevertheless the example can be easily extended to a dimension which is not available). Our system is described by two Boolean algebras, $\mathscr{A}$ and $\mathscr{B}$. Their intersection contains their bounds 0, 1 and also the event dark and its complement (which have the same meaning for both observers, *i.e.* the atom did not emit any photon). All observable events are:

$$\mathscr{L} = \{0, 1, \text{left}, \text{right}, \text{dark}, \text{up}, \text{down}, \text{left}', \text{right}', \text{dark}', \text{up}', \text{down}'\} = \mathscr{A} \cup \mathscr{B}. \tag{6}$$

Every propositional system can be embedded into a projective geometry which is algebraically isomorphic to a linear manifold of some linear vector space with coefficients from a field. QM uses coefficients from a complex field. Now orthocomplementation imposes restrictions on the field of numbers. From here we can derive a definite metric. If the field must contain real numbers there are only three possibilities: real, complex and quaternionic numbers. Jauch adopts the second, from which complex Hilbert spaces. From this it can be derived that the propositional system is $\mathscr{P}(\mathscr{H})$, the ensemble of projectors on a given Hilbert space $\mathscr{H}$.

## 4. Other approaches

### *4.1. Algebraic approach*

Segal [10] assumes *observables* to be primitive and an algebra with natural physical assumtions of linearity, positivity and normalization is constructed. As a consequence there are states which have a place here though not in any classical theory. The aim was to prove the possibility of a QM theory without Hilbert spaces and to show the possibility of deducing Uncertainty principle from an abstract mathematical structure. Hence we arrive at the following

**Theorem 5.** *Hilbert spaces are not necessary for QM.*

The correctness of the theorem is largely independent from the algebraic structure as such, in fact one has successfully constructed a QM in phase space.

The enterprise of Haag and Kastler [11] of constructing an algebra of observables (not intended as operators on Hilbert spaces) can be seen as an attempt to construct

a relativistic QM which presents no local effects. The starting point can be the following

**Principle 3.** *Observables in causally disjoint space-time regions are always compatible.*

Attention must be paid to this concept of disjointedness: it can in no way be interpreted in the sense that without dynamical interaction two systems are completely uncoupled, because in quantum mechanics there can be entanglement.

Another problem is that of representations. On one hand, one should avoid the multiplication of representations in different Hilbert spaces of the same algebra. On the other hand, one should have all the required representations. QL builds an orthomodular lattice by a set of yes/no propositions which turns out to be exactly the lattice which we construct with the set of projectors onto the closed subspaces of Hilbert space. But there are orthomodular lattices which do not have representations with projectors. In order to avoid such problems the necessity arose to use $C^*$ algebras with observables as primitive elements.

One assumes that there are sufficiently many dispersion-free states in order to distinguish the observables using expected values. By their linearity one equips the set of observables with the structure of a real linear space. By assuming associativity one then obtains a $C^*$ algebra. And this turns out to be an algebra of bounded self adjoints operators on a Hilbert space. Thus we have answered not only the question of why Hilbert space are necessary (Theorem 5) but also the question about which Hilbert space is appropriate: different Hilbert spaces can be constructed depending on the states used in the construction. Then, the central theorem becomes

**Theorem 6.** *Two representations are physically equivalent if every neighborhood of any element of one subset of states corresponding to one representation contains an element of the other and vice versa.*

Now the concept of physical equivalence corresponds to that of weak equivalence, hence we can use the theorem:

**Theorem 7.** *Two representations are weakly equivalent iff they have the same kernel.*

As consequence, the relevant object becomes the algebra and not the representation.

### 4.2. Convexity approach

In this approach *states* are taken as primitive [12]. The principal concept is that of *face*.

**Definition 3.** A subset $\mathscr{X}$ pertaining to the convex set of density matrices is said to be a face iff for some weights $w_1, w_2$ and states $\hat{\rho}_1, \hat{\rho}_2$ it is:

$$(\hat{\rho}_1, \hat{\rho}_2 \in \mathscr{X}) \to (w_1\hat{\rho}_1 + w_2\hat{\rho}_2 \in \mathscr{X}), \tag{7}$$

$$(w_1\hat{\rho}_1 + w_2\hat{\rho}_2 \in \mathscr{X}) \to (\hat{\rho}_1, \hat{\rho}_2 \in \mathscr{X}). \tag{8}$$

The first condition says that faces are convex subsets; the latter that faces are convex in the strong way (if a face contains an internal point of a 'segment' then it must contain the whole 'segment'). If the convex sets of density have extreme points (pure

states or kets) then each extreme point is a face. This approach has very important consequences for the problem of open systems, *i.e.* systems with non-unitary time evolution [13].

### *4.3. States-observables approach*

In this case both *states and observables* are taken as primitives. Mackey [14] developed a parallelism between QM and classical probability calculus: observables are the random variables and the states are probability measures. It was tried to extend the discussion by inserting joint probability measures and conditional expectations: but the first exist only if the observables commute, and the second only if observables have discrete spectrum.

The starting point is then the probability of obtaining in the state $\hat{\rho}$ a value in a set $\mathscr{X}$ of real number when an observable $\hat{O}$ is measured: $p(\hat{O},\hat{\rho},\mathscr{X})$. Now we can identify propositions with probabilities and order them by degrees of probability. Hence we write:

$$a \le b \quad \text{if} \quad a(\hat{\rho}) \le b(\hat{\rho}), \qquad \forall \hat{\rho}, \tag{9}$$

which corresponds to the ordering relation of a POSet. The central axiom, which makes $\mathscr{L}$ orthomodular and allows us to see the trace-one class operators as a set of probability measures on $\mathscr{L}$ is the following.

**Postulate 6.** (Makey) *For every pairwise orthogonal sequence* $a_1, a_2, \ldots, \in \mathscr{L}$ *(set of propositions),* $\exists b \in \mathscr{L}$ *such that for every* $\hat{\rho}$ *we have* $b(\hat{\rho}) + a_1(\hat{\rho}) + a_2(\hat{\rho}) + \ldots = 1$.

However, Makey assumed that the POSet $\mathscr{L}$ of all propositions of QM is isomorphic to the POSet of all (closed) subspaces of a separable, infinite-dimensional complex Hilbert space $\mathscr{H}$ in order to create a bridge with ordinary QM. But this axiom is completely ad hoc.

## 5. Quantum mechanics logical calculus

Logic can be understood in a more concrete way: as a calculus which reflects and helps different empirical domains. So understood it is clear that the problem now is: what are the logical connectives and rules which best reflect QM?

The initiator of this approach was Mittelstaedt [15] followed by Hardegree (in [16]). If we want a principle of objectification, we must renounce to the unrestricted availability.

### *5.1. Choice disjunction and negation*

The QM concrete logic $\mathscr{L}_{\mathrm{QM}}$ is closed under the infinitary conjuction but it is not closed under the *exclusion disjunction* (a disjunction that is true iff only one disjoint is true). In fact, due to the superposition principle, $\mathscr{L}_{\mathrm{QM}}$ obeys to a *choice disjunction*, such that if we have closed subsets $\mathscr{X}$ and $\mathscr{X}'$, and we consider their supremum (the smallest subset which includes both), this consists in all linear combinations of $\mathscr{X}$ and $\mathscr{X}'$. Generally, it strictly includes $\mathscr{X} \cup \mathscr{X}'$, *i.e.* there are propositions true in $\mathscr{X} \cup \mathscr{X}'$ but neither in $\mathscr{X}$ nor in $\mathscr{X}'$, which means that the disjunction of some propositions $a, b$ can be true for some states $\hat{\rho}$ but it may be that neither $a$ nor $b$ is true in $\hat{\rho}$.

As a consequence of the choice disjunction, in QM an exclusion negation cannot always be valid. While the formal analogue of the law of excluded middle ($a \vee \neg a$) is still valid in $\mathscr{L}_{\mathrm{QM}}$, *i.e.* every state satisfies $a \vee a^{\perp}$, it is not closed under *exclusion negation*: *i.e.* we have not necessarily $a$ or $a^{\perp}$ (which is a particular realization of the choice disjunction). Hence we have a *choice negation*. Now, although both intuitionistic logic and three-valued logic employ a choice negation, they nevertheless employ a classical choice disjunction.

### 5.2. Truth-value gaps

Thus $\mathscr{L}_{\mathrm{QM}}$ is not bivalent, *i.e.* some projectors need not to have (classical) truth value. But it is not necessary to suppose that $\mathscr{L}_{\mathrm{QM}}$ admits third values: there are simply propositions which are truth-valueless, *i.e.* $\mathscr{L}_{\mathrm{QM}}$ admits truth-value gaps. It is exactly the situation showed by the Kochen-Specker theorem or by the Bell corollary of the Gleason theorem [16].

In conclusion, we have:

**Theorem 8.** (Hardegree) *QM logical calculus is characterized by choice disjunction and choice negation, and consequently it presents truth-value gaps.*

This theorem is in contradiction with the classical assumption that observables always have a determinate value. We can translate it into a propositional calculus. Propositions are represented by projection operators. If the state $\hat{\rho}$ is an eigenvector of some projector $\hat{P}$ then there are only 0,1 as possible values. But if not $\hat{P}$ may be regarded as neither true, nor false at $\hat{\rho}$. In fact we can see this by analysing the case when two observables commute. Let the two observables be expressed in terms of projectors $\hat{P}$, $\hat{P}'$; then we define the commutativity as:

$$\hat{C}(\hat{P},\hat{P}') \equiv (\hat{P} \wedge \hat{P}') \vee (\hat{P} \wedge \hat{P}'^{\perp}) \vee (\hat{P}^{\perp} \wedge \hat{P}') \vee (\hat{P}^{\perp} \wedge \hat{P}'^{\perp}). \tag{10}$$

The operator $\hat{C}$ is the projector onto the subspaces of vectors on which $\hat{P}$ and $\hat{P}'$ commute. In other words, if two observables commute, then we have no value gaps, but both always have a determined value, 0 or 1.

### 5.3. QM implications

Theorem 8 also has a consequence for the structure of QM implication. We can distinguish between the metalanguaged $a \vdash b$ from the objectlanguaged $a \rightarrow b$ and said that the lattice order relation $a \leq b$ corresponds to $a \vdash b$. From the transitivity property derives a weakening law which is not satisfied by counterfactuals. But QM is to a certain extent counterfactual, so that we must reject transitivity. The conditional which has been proposed for QM is the Sasaki arrow $\Rightarrow$ defined by [15]:

$$a \Rightarrow b \equiv a^{\perp} \vee (a \wedge b), \tag{11}$$

which clearly respects the property of orthomodularity (which in turn characterizes QM).

The Sasaki arrow is both residual and locally Boolean, where the last signifies that it agrees with the classical conditional on all Boolean subortholattices of the orthomodular lattice in question. In other words, $a \Rightarrow b = a^{\perp} \vee b$ if we have $a \rightarrow b$. Obviously the Sasaki arrow is different from the classical conditional only under the

assumption (characteristic of QM) that distributivity is not valid; because if it was, then the right hand side of Equation (11) would be equivalent to $(a^\perp \vee a) \wedge (a^\perp \vee b)$, which given that $(a^\perp \vee a)$ is always true (law of tertium non datur), in turn would be equivalent to $a^\perp \vee b$, which is equivalent to a classical implication.

## 6. Quantum computational logic

The development of quantum computation and quantum information [4], has made quantum logic very relevant today. While it is a very specialised subject, quantum logic can provide insights into the workings of nature, and it has already been put to use by Abramsky and Coecke to analyze problems in quantum information [17]. Grinbaum [18, 19] have already proposed a system of information-theoretic axioms from which he derives the formalism of quantum theory. However, it is the theory of logical gates in quantum computation that naturally suggests a new form of logic [5], namely the quantum computational logic (QCL).

The main difference between orthodox quantum logic and quantum computational logic concerns a basic semantic question: How to represent the meanings of the sentences of a given language?

- The answer given by Birkhoff and von Neumann is the following: the meanings of the elementary experimental sentences of quantum theory have to be regarded as determined by convenient sets of states of quantum objects. Since these sets should satisfy some special closure conditions, it turns out that, in the framework of orthodox quantum logic, sentences can be adequately interpreted as closed subspaces of the Hilbert space associated to the physical systems under investigation.
- The answer given in the framework of quantum computational logic is quite different: meanings of sentences are represented by information quantities, a kind of abstract objects that are described in the framework of quantum information theory.

Let us analyze more in details the QCL as proposed in [5]. We first give 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 $\mathbb{C}^2$.

**Definition 4.** A *qubit* is a unit vector $|\psi\rangle$ of the space $\mathbb{C}^2$.

Hence, any *qubit* will have the following form:

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle, \tag{12}$$

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 $\{|0\rangle, |1\rangle\}$. Further 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 also write $|x_1, \ldots, x_n\rangle$ instead of $|x_1\rangle \otimes \cdots \otimes |x_n\rangle$.

**Definition 5.** An *n-qubit system* (or *n-register*) is any 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 labelled by binary strings such as $|\underbrace{011\ldots10}_{n \text{ times}}\rangle$. Since any such string 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:

$$\sum_{j=0}^{2^n-1} a_j |j\rangle. \tag{13}$$

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*.

### 6.1. Quantum logical gates

Generally, a quantum logical gate can be described as a unitary operator, assuming arguments and values in a product-Hilbert space $\otimes^n \mathbb{C}^2$. Then, we can define:

**Definition 6.** The *Toffoli gate* $T^{(n,m,1)}$ is the linear operator

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

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:

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

On this basis one can immediately define `AND`.

**Definition 7.** 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? We will consider a function `NOT` that simply inverts the value of the last elements of any basis-vector.

**Definition 8.** $\mathtt{NOT}^{(n)}$ is the map $\mathtt{NOT}^{(n)} : \otimes^n \mathbb{C}^2 \mapsto \otimes^n \mathbb{C}^2$ such that for any $|\psi\rangle = \sum_{j=0}^{2^n-1} a_j |j\rangle \in \otimes^n \mathbb{C}^2$:

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

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

**Definition 9.** 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 behaviour only emerges in the case where our gates are applied to superpositions. There are however *genuine quantum gates*. One of the

most significant is the *squareroot of the negation* NOT, indicated by $\sqrt{\texttt{NOT}}$. As suggested by the name, the characteristic property of the gate $\sqrt{\texttt{NOT}}$ is the following: for any quregister $|\psi\rangle$,

$$\sqrt{\texttt{NOT}}\sqrt{\texttt{NOT}}|\psi\rangle = \texttt{NOT}|\psi\rangle. \tag{14}$$

As observed in [20] logicians are entitled to propose a new logical operation, $\sqrt{\texttt{NOT}}$, because a faithful physical model for it exists in nature. Mathematically we have

**Definition 10.** $\sqrt{\texttt{NOT}}^{(1)}$ is the map $\sqrt{\texttt{NOT}}^{(1)} : \mathbb{C}^2 \to \mathbb{C}^2$ such that for any $|\psi\rangle =: a_0|0\rangle + a_1 k\text{-}\omega$:

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

where $i$ is the imaginary unit. Moreover, $\sqrt{\texttt{NOT}}^{(n)}$ is the map $\sqrt{\texttt{NOT}}^{(n)} : \otimes^n\mathbb{C}^2 \mapsto \otimes^n\mathbb{C}^2$ such that for any $|\psi\rangle = \sum_{j=0}^{2^n-1} a_j|j\rangle \in \otimes^n\mathbb{C}^2$:

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

### 6.2. 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 a vector

$$|\varphi\rangle = \sum_{j=0}^{2^n-1} a_j|j\rangle \in \otimes^n\mathbb{C}^2. \tag{15}$$

Let us consider two particular sets of coefficients that occur in the superposition-vector $\varphi$:

$$C^+|\varphi\rangle := \{a_j : 1 \le j \le 2^n - 1 \text{ and } j \text{ is odd}\}, \tag{16}$$

$$C^-|\varphi\rangle := \{a_j : 1 \le j \le 2^n - 1 \text{ and } j \text{ is even}\} \cup \{0\}. \tag{17}$$

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).

**Definition 11.** Let $|\psi\rangle = \sum_{j=0}^{2^n-1} a_j|j\rangle$ be any vector of $\otimes^n\mathbb{C}^2$, then its probability-value is:

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

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

As consequence of the relations between the probability function Prob and the basic logical gates we have:

- differently from classical probability (and also from standard quantum probability) AND, OR, NOT have a "truth-functional behaviour" 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: $\mathrm{Prob}(|\psi\rangle) = \mathrm{Prob}(|\varphi\rangle)$ and $\mathrm{Prob}(\sqrt{\texttt{NOT}}(\psi)) \neq \mathrm{Prob}(\sqrt{\texttt{NOT}}(|\varphi\rangle))$.

### 6.3. 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 (where information is of course measured by means of the quantum unit).

Consider a language $\mathscr{L}$ with the following connectives: $\texttt{NOT}$ (negation $\neg$), $\texttt{AND}$ (conjunction $\wedge$) and $\sqrt{\texttt{NOT}}$ ($\sqrt{\neg}$). The disjunction ($\vee$) is supposed defined via de Morgan's law: $\alpha \vee \beta := \neg(\neg\alpha \wedge \neg\beta)$.

To any sentence $\alpha$ is associated a quregister $|\alpha\rangle$ in a Hilbert space $\otimes^n \mathbb{C}^2$ (where $n$ is a function of the length of $\alpha$). In this framework, any sentence $\alpha$ of the language gives rise to a *quantum tree*: a kind of *quantum circuit* that transforms the quregister associated to the atomic subformulas of $\alpha$ into the quregister associated to $\alpha$. The information-value of a sentence naturally determines a probability-value for that sentence, that is

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

Finally, a sentence $\alpha$ is *true* if $\mathrm{Prob}(\alpha) = 1$. Moreover, $\beta$ is a *consequence* of $\alpha$ iff $\mathrm{Prob}(\alpha) \leq \mathrm{Prob}(\beta)$ (the order relation).

The logic characterized by this semantics is the QCL. It 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. Differently from the usual quantum logics, the weak distributivity principle $((\alpha\wedge\beta)\vee(\alpha\wedge\gamma) = \alpha\wedge(\beta\vee\gamma))$ breaks down. At the same time, the strong distributivity $(\alpha\wedge(\beta\vee\gamma) = (\alpha\wedge\beta)\vee(\alpha\wedge\gamma))$, that is violated in orthodox quantum logic, is here valid. Both the excluded middle and the non contradiction principles are violated: as a consequence, we have here an example of an *unsharp logic*.

## 7. Conclusions

Regarding the relation between QL and QM, we can conclude that the former is not very suitable as a model of the latter: the propositions are too abstract a tool, and they do not cover the most interesting developments of the last years.

The great problem of orthodox quantum logic (Birkhoff and von Neumann) is that it is so general that it is not useful as model of QM. We need more axioms than the assumptions made so as to build a bridge to Hilbert spaces. This was the step taken by Varadarajan [21]. But many of the additional axioms have no convincing physical justification. On the other hand, some theorems of QL represent general results whose validity is not confined to this area.

About other approaches we may ask which one is preferable. The importance of the Uncertainty principle can bring to the conclusion that in QM the observables are central. In this sense the algebraic approach would be the best one, and one

would affirm a fundamental dependence of states on observables. But there is at least a property of states which in no way depends from observables: entanglement (resp. factorizability). On the other hand, the impossibility to measure the state of a single system implies that QM cannot only be a theory of states (as the convexity approach wishes). Thus, we have at least two primitive physical entities: observables and states. Finally, QCL though touching recent developments of QM is still far from achieving an axiomatization.

In summary, up to now we have found no model which is satisfactory or complete from all points of view. If this conclusion is sound and confirmed by future developments, then QM cannot be an axiomatic system of theorems. We are therefore forced to develop a concept of science which is more adequate to this situation. The new image of science suggested by this examination is that of a collection of partly independent postulates and theorems and not of a system. One may recall here Gödel's theorem or the choice of an Open Logic, the last justification of which is to be found in the assumption of an operational point of view.

Does this mean that QM is an incomplete theory? If by 'complete' we mean a closed system, then QM is certainly not complete (anyway classical mechanics too was probably not a closed system). If we mean a theory which mirrors every 'element of reality' (semantical completeness), then this is only a mythology which conflicts with the reality of theories' pluralism[1].

But on the other hand QM cannot be an 'incomplete theory' in the sense that there are some physical entities which are in open conflict with the predictions of the theory or which are not at all analysable in the frame of QM, because in that case QM would be a fallacious theory. And surely not in the sense that there are internal contradictions, what would make QM absurd (all recent developments have confirmed the predictions of the theory).

With the advent of quantum information, quantum logic may become more relevant. Ever since research in quantum logic was initiated by Birkhoff and von Neumann, physicists were constantly at odds over what its precise form should be. The emphasis was mostly put on the semantics of quantum logic, in particular on the mathematical structures that underlie quantum theory. What is needed today is a mean of reasoning formally about systems with quantum-mechanical components and procedures, namely, a specialized logic with a formal syntax for describing quantum algorithms, quantum protocols, and their properties (most likely QCL). In order to fulfill this need, one should design a suitable logic using the top-down approach, rather than starting from low-level algebraic structures and their properties [22].

The results gained in quantum logical approaches may offer new insights on the theory of computation [23]. As an example, let us consider the Church-Turing thesis. The realization that the intuitive notion of "effective computation" can be identified with the mathematical concept of" computation by the Turing machine"

---

1. A necessary but insufficient condition of semantical completeness is self-referentiality, *i.e.* the capacity of a theory to furnish also the means of its proofs. This is what happens with the theory of measurement, which on one hand must account for QM phenomena (as objects) and on the other hand is the QM description of the process itself (especially of the apparatus). This is also what happens to a greater extent with the relationship between microphysics and macrophysics.

is based on the fact that the Turing machine is computationally equivalent to some vastly dissimilar formalisms for the same purpose, such as Post systems, $\mu-$recursive functions, $\lambda$-calculus and combinatory logic. Another reason for the acceptance of the Turing machine as a general model of a computation is that the Turing machine is equivalent to its many modified versions that would seem off-hand to have increased computing power. We should note that the equivalence between the Turing machine and its various generalizations as well as other formalisms of computation has been reached in classical Boolean logic. In addition, quantum logic is known to be strictly weaker than Boolean logic. Thus, it is reasonable to doubt that the same equivalence can be achieved when our underlying meta-logic is replaced by quantum logic, and the Church-Turing thesis needs to be reexamined in the realm of quantum logic.

Moreover, we can assert that a certain commutativity of the observables for some basic actions in the Turing machine is a physical support of the Church-Turing thesis in the framework of quantum logic. Thus, there might be a deep connection between the Heisenberg uncertainty principle and the Church-Turing thesis, two of the greatest scientific discoveries in the twentieth century. It is notable that such a connection could be observed via an argument in a nonclassical logic (and it is impossible to be found if we always work within the classical logic). It was argued by D. Deutsch that underlying the Church-Turing thesis there is an implicit physical assertion [24]. There is certainly no doubt about the existence of such a physical assertion. The true problem is: what is it? The answer given by D. Deutsch himself is the following physical principle: "every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means". The analysis on the role of commutativity in computation theory based on quantum logic perhaps indicates that in order to be simulated by a universal computing machine some observables of the physical system are required to possess a certain commutativity.

## *References*

[1] Birkhoff G and von Neumann J 1936 *Ann. Math.* **37** 823
[2] Dalla Chiara M L and Giuntini R 2002 *Quantum Logics*, Kluwer, Amsterdam
[3] Holdsworth and Hooker C A 1983 *A Critical Survey of Quantum Logic. Logic in the 20*th *Century*, Scientia Special Issue, Scientia, Milan, 127–246
[4] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information*, University Press, Cambridge
[5] Dalla Chiara M L, Giuntini R and Leporini R 2005 *Trends in Logic: 50 Years of Studia Logica*, Kluwer, Amsterdam, pp. 213-255
[6] Mateus P and Sernadas A 2004 *Proc. of Workshop on Combination of Logics: Theory and Applications*, Lisbon, pp. 141–149
[7] van der Meyden R and Patra M 2003 *Proc. of Computer Science Logic and 8*th *Kurt Gödel Colloquium*, Wien, pp. 427–440
[8] Dirac P A M 1958 *Principles of Quantum Mechanics*, Clarendon, Oxford
[9] Jauch J M 1968 *Foundations of Quantum Mechanics*, Addison-Wesley, Boston
[10] Segal I E 1947 *Ann. Math.* **48** 930
[11] Haag R and Kastler D 1962 *J. Math. Phys.* **5** 848
[12] Ludwig G 1985 *An Axiomatic Basis for Quantum Mechanics*, Springer, Berlin
[13] Beltrametti E and Cassinelli G 1981 *The Logic of Quantum Mechanics*, Addison-Wesley, Redwood
[14] Mackey G 1957 *The Mathematical Foundations of Quantum Mechanics*, Benjamin, New York

[15] Mittelstaedt P 1978 *Quantum Logic*, DReidel Publ. Co., Dordrecht
[16] Hooker C A 1979 *The Logic-Algebraic Approach to Quantum Mechanics*, Reidel, Dordrecht
[17] Abramsky S and Coecke B 2004 *Proc. 19*th *Annual IEEE Symposium on Logic in Computer Science*, Turku, Finland, pp. 415–425
[18] Grinbaum A 2004 *The Significance of Information in Quantum Theory*, PhD Thesis, Ecole Polytechnique, Paris
[19] Grinbaum A 2005 *Found. Phys. Lett.* **18** 573
[20] Deutsch D, Ekert A and Lupacchini R 2000 *Bull. Symbolic Logic* **3** 265
[21] Varadarajan V S 1985 *Geometry of Quantum Theory*, Springer, Berlin
[22] Mateus P and Sernadas A 2004 *Lecture Notes in Artificial Intelligence* **3229** 239
[23] Ying M S 1994 *J. Symbolic Logic* **59** 830
[24] Deutsch D 1985 *Proc. Roy. Soc. Lond.* **A400** 97