Reasoning about Quantum Systems

P. Mateus and A. Sernadas

CLC, Department of Mathematics, IST,
Av. Rovisco Pais, 1000-149 Lisbon, Portugal

Abstract. A new logic is proposed for reasoning about quantum systems. The logic embodies the postulates of quantum physics and it was designed from the semantics upwards by identifying quantum models with superpositions of classical models. This novel approach to quantum logic is completely different from the traditional approach of Birkhoff and von Neumann. It has the advantage of making quantum logic an extension of classical logic. The key new ingredient of the language of the proposed logic is a rather general modal operator. The logic incorporates probabilistic reasoning (in the style of Nilsson) in order to deal with uncertainty on the outcome of measurements. The logic also incorporates dynamic reasoning (in the style of Hoare) in order to cope with the evolution of quantum systems. A Hilbert calculus for the logic is sketched. A quantum key distribution protocol is specified and analyzed.

1 Motivation and Related Work

A new logic is proposed for modeling and reasoning about quantum systems, embodying all that is stated in the postulates of quantum physics (as presented, for instance, in [1]). The logic was designed from the semantics upwards starting with the key idea of adopting superpositions of classical models as the models of the quantum logic.

This novel approach to quantum logic semantics is completely different from the traditional approach [2, 3] to the problem, as initially proposed by Birkhoff and von Neumann [4] focusing on the lattice of closed subspaces of a Hilbert space. Our semantics has the advantage of closely guiding the design of the language around the underlying concepts of quantum physics while keeping the classical connectives and was inspired by the possible worlds approach originally proposed by Kripke [5] for modal logic. It is also akin to the society semantics introduced in [6] for many-valued logic and to the possible translations semantics proposed in [7] for paraconsistent logic. The possible worlds approach was also used in [8–12] for probabilistic logic. Our semantics to quantum logic, although inspired by modal logic, is also completely different from the alternative Kripke semantics given to traditional quantum logics (as first proposed in [13]) still closely related to the lattice-oriented operations.

Contrarily to traditional quantum logics that replace the classical connectives by new connectives inspired by the lattice-oriented operations, by adopting superpositions of classical models as the models of the quantum logic we are led to a natural extension of the classical language containing the classical connectives (like modal languages are extensions of the classical language). The key new ingredient of our quantum language is a rather general modal operator.

The proposed logic also incorporates probabilistic reasoning (in the style of Nilsson's calculus [8, 9]) since the postulates of quantum physics impose uncertainty on the outcome of measurements. From a quantum state (superposition of classical valuations living in a suitable Hilbert space) it is straightforward to generate a probability space of classical valuations in order to provide the semantics for reasoning about the probabilistic measurements made on that state. Our logic also incorporates dynamic reasoning (in the style of Hoare's calculus [14]) in order to cope with the evolution of quantum systems. Two types of quantum state transitions are considered: unitary transformations and projections. A Hilbert calculus for the logic is sketched having in mind a completeness result obtained elsewhere. As an illustration of the power of the proposed logic, a quantum key distribution protocol is specified and analyzed.

In Section 2, we briefly present the relevant mathematical structures based on the postulates of quantum physics. In Section 3, we present EQPL (exogenous quantum propositional logic) for reasoning about a quantum system in a given quantum state. In Section 4, we extend EQPL to DEQPL (dynamic exogenous quantum propositional logic) for reasoning also about quantum state transitions. Finally, in Section 5, we present and analyze a quantum key distribution protocol.

2 Basic Concepts

In order to materialize the key idea of adopting superpositions of classical models as the models of the envisaged quantum logic, we need to recall the postulates of quantum physics (that we do following closely [1]) and to set up some important mathematical structures.

Postulate 1. Associated to any isolated quantum system is a Hilbert space[1]. The state of the system is completely described by a unit vector $|w\rangle$ in the Hilbert space.

For example, a quantum bit or *qubit* is associated to a Hilbert space of dimension two: a state of a qubit is a vector $\alpha_0|0\rangle + \alpha_1|1\rangle$ where $\alpha_0, \alpha_1 \in \mathbb{C}$ and $|\alpha_0|^2 + |\alpha_1|^2 = 1$. That is, the quantum state is a *superposition* of the two classical states $|0\rangle$ and $|1\rangle$ of a classical bit. Therefore, from a logical point of view, representing the qubit by a propositional constant, a *quantum valuation* is a superposition of the two classical valuations.

[1] Recall that a Hilbert space is a complex vector space with inner product which is complete for the induced norm. It is customary to present its elements using the *ket* Dirac notation $|w\rangle$.

Postulate 2. The Hilbert space associated to a quantum system composed of n independent component systems is the tensor product[2] of the component Hilbert spaces.

For instance, a system composed of two independent qubits is associated to a Hilbert space of dimension four: a state of such a system is a vector $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ where $\alpha_{00}, \alpha_{10}, \alpha_{01}, \alpha_{11} \in \mathbb{C}$ and $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. Again, representing the two qubits by two propositional constants, a *quantum valuation* is a superposition of the four classical valuations. And, so, the Hilbert space of the system composed of two independent qubits is indeed the tensor product of the two Hilbert spaces, each corresponding to a qubit.

The systems we envisage to reason about are composed by a denumerable set of possibly interdependent qubits and, therefore, we fix once and for all the following set of propositional constants $\{\mathbf{p}_k : k \in \mathbb{N}\}$, once for each qubit. In this context, a classical valuation is a map $v : \{\mathbf{p}_k : k \in \mathbb{N}\} \to \{0, 1\}$. We now face the problem of setting up the suitable Hilbert space where the superpositions of such classical valuations will live.

Given a nonempty set V of classical valuations, $\mathcal{H}(V)$ is the following inner product space over $\mathbb{C}$:

- each element is a map $|w\rangle : V \to \mathbb{C}$ such that:
  - $\text{supp}(|w\rangle) = \{v : |w\rangle(v) \neq 0\}$ is countable;
  - $\displaystyle\sum_{v \in \text{supp}(|w\rangle)} ||w\rangle(v)|^2 < \infty$.
- $|w_1\rangle + |w_2\rangle = \lambda v.\, |w_1\rangle(v) + |w_2\rangle(v)$.
- $\alpha|w\rangle = \lambda v.\, \alpha|w\rangle(v)$.
- $\langle w_1|w_2\rangle = \displaystyle\sum_{v \in V} |w_1\rangle(v)\overline{|w_2\rangle(v)}$.

As usual, the inner product induces the norm $|||w\rangle|| = \sqrt{\langle w|w\rangle}$ and, so, the distance $d(|w_1\rangle, |w_2\rangle) = |||w_1\rangle - |w_2\rangle||$. Since $\mathcal{H}(V)$ is complete for this distance, $\mathcal{H}(V)$ is a Hilbert space . Clearly, $\{|v\rangle : v \in V\}$ is an orthonormal basis of $\mathcal{H}(V)$ where $|v\rangle(v) = 1$ and $|v\rangle(v') = 0$ for every $v' \neq v$.

A quantum structure $\mathbf{w}$ is a pair $\langle V, |w\rangle\rangle$ where: V is a nonempty set of classical valuations; and $|w\rangle \in \mathcal{H}(V)$ such that $|||w\rangle|| = 1$. This structure provides the means for reasoning about a quantum system composed of a denumerable set of qubits (one for each $\mathbf{p}_k$) such that by observing it we get a classical valuation in V. The current state of the system is the unit vector $|w\rangle$ (a unit superposition of the observable classical valuations).

[2] Recall that the tensor product of Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ is the Hilbert space composed by the pairs $|w_1\rangle \otimes |w_2\rangle$ such that the following equalities hold for all $\alpha \in \mathbb{C}, |w_1\rangle, |w_1'\rangle \in \mathcal{H}_1$ and $|w_2\rangle, |w_2'\rangle \in \mathcal{H}_2$: $(\alpha(|w_1\rangle \otimes |w_2\rangle)) = ((\alpha|w_1\rangle) \otimes |w_2\rangle) = (|w_1\rangle \otimes (\alpha|w_2\rangle))$; $((|w_1\rangle + |w_1'\rangle) \otimes |w_2\rangle) = ((|w_1\rangle \otimes |w_2\rangle) + (|w_1'\rangle \otimes |w_2\rangle))$; $(|w_1\rangle \otimes (|w_2\rangle + |w_2'\rangle)) = ((|w_1\rangle \otimes |w_2'\rangle) + (|w_1\rangle \otimes |w_2'\rangle))$.

Since we start with the whole system composed of a denumerable set of qubits, we have to use Postulate 2 in the reverse direction: how can we identify an independent subsystem?

Given a set S of propositional constants (qubits), we denote by $V_{[S]}$ the set $\{v|_S : v \in V\}$ and by $V_{]S[}$ the set $\{v|_{S^c} : v \in V\}$. Clearly, $\mathcal{H}(\mathcal{V}) = \mathcal{H}(\mathcal{V}_{[S]}) \otimes \mathcal{H}(\mathcal{V}_{]S[})$ where $\mathcal{V}$ is the set of all classical valuations. But, $\mathcal{H}(V) \subseteq \mathcal{H}(V_{[S]}) \otimes \mathcal{H}(V_{]S[})$ where equality does not hold in general. When it does, we say that the quantum system is composed of two independent subsystems (one with the qubits in S and the other with rest of the qubits). Furthermore, given a unit $|w\rangle \in \mathcal{H}(V)$, if there are unit $|w'\rangle \in \mathcal{H}(V_{[S]})$ and unit $|w''\rangle \in \mathcal{H}(V_{]S[})$ such that $|w\rangle = |w'\rangle \otimes |w''\rangle$ then we say that, in state $|w\rangle$, the qubits in S are not entangled with the qubits not in S and, therefore, that the qubits in S are independent of the other qubits at that state $|w\rangle$.

The two remaining postulates of quantum physics state how the state of the quantum system is changed: either when it is observed or when it evolves by itself without interference.

Postulate 3. Each type of projective measurement or observation that can be made over a quantum system is associated to a Hermitian operator[3] M over its Hilbert space. The possible outcomes of the measurement are the eigenvalues of M. Upon making an observation with M of the system in state $|w\rangle$, the probability of getting an eigenvalue m is given by $\langle w|P_m|w\rangle$ where P_m is the projector onto the eigenspace of M with eigenvalue m. When the outcome m occurs, the quantum system evolves to the state given by $\frac{P_m|w\rangle}{\sqrt{\langle w|P_m|w\rangle}}$.

For the applications we have in mind in quantum computation and information, the most relevant type of measurement is the one corresponding to the identity operator. In this case, the possible outcomes are the classical valuations in V and each v is observed at state $|w\rangle$ with probability $|\langle v|w\rangle|^2$. More precisely, a measurement induces a probability space over the possible outcomes as we proceed to explain after introducing the notion of Nilsson structure[4] that we shall use for providing the semantics of the probabilistic component of the quantum logic.

A *Nilsson structure* $\mathbf{V}$ is a tuple $\langle V, \mathcal{B}, \nu\rangle$ where: V is a non empty set of classical valuations; $\mathcal{B}$ is a σ-algebra over V (that is, $\mathcal{B} \subseteq \wp V$ and $\mathcal{B}$ is closed under complements and countable unions) such that $\{v \in V : v \Vdash \mathbf{p}_k\} \in \mathcal{B}$ for each $k \in \mathbb{N}$; and ν is a map from $\mathcal{B}$ to $[0,1]$ such that $\nu(V) = 1$ and $\nu(\bigcup_{j\in\mathbb{N}} B_j) = \sum_{j\in\mathbb{N}} \nu(B_j)$ whenever $B_{j_1} \cap B_{j_2} = \emptyset$ for every $j_1 \neq j_2 \in \mathbb{N}$. In short, a Nilsson structure is a probability space where outcomes are classical valuations and the extent of every propositional constant is among the events. Such structures provide the semantic basis for several probabilistic logics used for reasoning with uncertainty [8, 12, 9].

[3] Recall that a Hermitian operator H is an operator such that $H = H^*$ where H^* is the adjoint operator of H, that is, the unique operator such that $\langle \psi_1|H\psi_2\rangle = \langle H^*\psi_1|\psi_2\rangle$.

[4] We propose this terminology in recognition of the significance of [8] for the development of probabilistic logic.

As we saw, according to Postulate 3, the stochastic result of observing the system at state $|w\rangle$ is fully described by the Nilsson structure $\mathcal{N}(\mathbf{w}) = \langle V, \wp V, \nu_{|w\rangle}\rangle$ where, for each $U \subseteq V$, $\nu_{|w\rangle}(U) = \sum_{u \in U} |\langle u|w\rangle|^2$.

Postulate 4. Barring measurements, the evolution of a quantum system is described by unitary transformations[5].

Taking into account the applications we have in mind, we can restrict our attention to finite unitary transformations (a transformation is said to be finite if only changes a finite number of components of the argument vector).

It was established in [15] that a finite unitary transformation can be approximated by composing eight basic transformations: identity, Hadamard, phase, $\frac{\pi}{8}$, Pauli X, Y, Z and controlled not. This result helps in choosing the language for denoting such transformations as we shall in Section 4, where we shall provide further information about the basic transformations.

3 Reasoning about a Quantum State

The envisaged quantum logic should first provide the means for reasoning about a given state of a quantum system composed of a denumerable set of qubits (one for each propositional constant $\mathbf{p}_k$) and where the relevant projective observation values are classical valuations. Given the stochastic nature of the outcomes of measurements the logic should incorporate probabilistic reasoning. Therefore, we extended the classical language first with the means for writing probabilistic assertions (loosely inspired by [8–12]) and later with the means for making assertions about superpositions of classical valuations.

This design effort resulted in the (denumerable) quantum language composed of formulae of the form[6]

$$\gamma = \omega_k \curlyvee \varphi \curlyvee (t \leq t) \curlyvee ([S] \lozenge \overrightarrow{\psi : u}) \curlyvee (\boxminus \gamma) \curlyvee (\gamma \sqsupset \gamma)$$

where φ is a classical formula, t is a real term, u is a complex term, S is a non empty recursive set of propositional constants (qubits), and ψ is a classical formula over S. A classical formula φ is of the form

$$\varphi = \xi_k \curlyvee \mathbf{p}_k \curlyvee (\neg \varphi) \curlyvee (\varphi \Rightarrow \varphi).$$

The set of real terms and the set of complex terms are jointly defined as follows

$$\begin{cases} t = \theta_k \curlyvee r \curlyvee (\textstyle\int \varphi) \curlyvee (\textstyle\int \varphi \,|\, \varphi) \curlyvee (t + t) \curlyvee (t\, t) \curlyvee \mathrm{Re}(u) \curlyvee \mathrm{Im}(u) \curlyvee \arg(u) \curlyvee |u| \\ u = \upsilon_k \curlyvee (t + it) \curlyvee te^{it} \curlyvee \overline{u} \curlyvee (u + u) \curlyvee (u\, u) \end{cases}$$

[5] Recall that a unitary transformation (or operator) on a Hilbert space $\mathcal{H}$ is a linear map $U : \mathcal{H} \to \mathcal{H}$ such that $U \circ U^* = I$. It is easy to see that unitary transformations are closed under composition and inverse.

[6] When defining languages, we use the abstract Backus Naur notation [16], but adopting $\curlyvee$ instead of the traditional $|$ in order to avoid confusions with the object language. We also extend the Backus-Naur notation: we write $\overrightarrow{\delta}$ for a finite sequence of elements of the form δ.

where r is a computable real number. The ξ's, ω's, θ's and υ's are schema variables (to be used in rules) that can be the target of substitutions respecting the syntactic categories. An expression is said to be ground if it does not contain any such variable.

The denotation at $\mathbf{w}$ of ground terms is mostly straightforward, but it is worthwhile to mention how the probability terms are interpreted on a given quantum structure $\mathbf{w}$.

Recall the Nilsson structure induced by $\mathbf{w}$ defined in Section 2: $\mathcal{N}(\mathbf{w}) = \langle V, \wp V, \nu_{\mathbf{w}} \rangle$ where, for each $U \subseteq V$, $\nu_{\mathbf{w}}(U) = \sum_{u \in U} |\langle u|w\rangle|^2$.

Clearly, for each ground classical formula φ, its extent at $\mathbf{w}$, $[\varphi]_{\mathbf{w}} = \{v \in V : v \Vdash \varphi\}$, is in $\wp V$. So, we are ready to define the denotation at $\mathbf{w}$ of the probabilistic ground terms:

- $[\![(\int \varphi)]\!]_{\mathbf{w}} = \nu_{\mathbf{w}}([\varphi]_{\mathbf{w}})$;
- $[\![(\int \varphi_2 \,|\, \varphi_1)]\!]_{\mathbf{w}} = \begin{cases} \frac{\nu_{\mathbf{w}}([\varphi_1]_{\mathbf{w}} \cap [\varphi_2]_{\mathbf{w}})}{\nu_{\mathbf{w}}([\varphi_1]_{\mathbf{V}})} & \text{if } \nu_{\mathbf{w}}([\varphi_1]_{\mathbf{w}}) \neq 0 \\ 1 & \text{otherwise} \end{cases}$.

Intuitively, $(\int \varphi)$ gives the probability of getting an outcome (classical valuation) where φ holds, when we observe the quantum system. And $(\int \varphi_2 \,|\, \varphi_1)$ gives the probability of getting an outcome (classical valuation) where φ_2 holds given that φ_1 holds, when we observe the quantum system[7].

The satisfaction of formulae by $\mathbf{w}$ and ground substitution ρ is as follows:

- $\mathbf{w}\rho \Vdash \omega_j$ iff $\mathbf{w}\rho \Vdash \omega_j\rho$;
- $\mathbf{w}\rho \Vdash \varphi$ iff $v \Vdash \varphi\rho$ for every $v \in V$;
- $\mathbf{w}\rho \Vdash (t_1 \leq t_2)$ iff $[\![t_1\rho]\!]_{\mathbf{w}} \leq [\![t_2\rho]\!]_{\mathbf{w}}$;
- $\mathbf{w}\rho \Vdash ([S] \lozenge \psi_1 : u_1, \ldots, \psi_n : u_n)$ iff there are unit $|w'\rangle \in \mathcal{H}(V_{[S]})$ and unit $|w''\rangle \in \mathcal{H}(V_{]S[})$ such that $|w\rangle = |w'\rangle \otimes |w''\rangle$ and there are distinct $v_1, \ldots, v_n \in \text{supp}(|w'\rangle)$ such that $v_k \Vdash \psi_k\rho$ and $|w'\rangle(v_k) = [\![u_k\rho]\!]_{\mathbf{w}}$ for $k = 1, \ldots, n$ (generalized quantum possibility);
- $\mathbf{w}\rho \Vdash (\boxminus \alpha)$ iff $\mathbf{w}\rho \nVdash \alpha$ (quantum negation);
- $\mathbf{w}\rho \Vdash (\alpha_1 \sqsupset \alpha_2)$ iff $\mathbf{w}\rho \nVdash \alpha_1$ or $\mathbf{w}\rho \Vdash \alpha_2$ (quantum implication).

The notion of quantum entailment is introduced as expected: $\Gamma \vDash \delta$ iff, for every quantum structure $\mathbf{w}$ and ground substitution ρ, $\mathbf{w}\rho \Vdash \delta$ whenever $\mathbf{w}\rho \Vdash \gamma$ for each $\gamma \in \Gamma$.

As usual, other (classical and quantum) connectives can be used as abbreviations. Furthermore, we write $(t_1 = t_2)$ for $((t_1 \leq t_2) \sqcap (t_2 \leq t_1))$. The following abbreviations are useful for expressing some important derived concepts:

- $(\lozenge\, \varphi_1 : u_1, \ldots, \varphi_n : u_n)$ for $([\{\mathbf{p}_k : k \in \mathbb{N}\}] \lozenge\, \varphi_1 : u_1, \ldots, \varphi_n : u_n)$;
- $[S]$ for $([S] :)$ — qubits in S are not entangled with those outside S;
- $(\lozenge \varphi)$ for $((\int \varphi) > 0)$ and $(\Box \varphi)$ for $((\int \varphi) = 1)$;

[7] By convention, we imposed this to be one when $(\int \varphi_1)$ is zero.

– $(\bigwedge_F A)$ for $((\wedge_{p_k \in A}\ \mathbf{p}_k) \wedge (\wedge_{p_k \in (F \setminus A)} (\neg\, \mathbf{p}_k)))$ whenever F is a finite set of propositional constants and $A \subseteq F$.

Note that the quantum connectives are still classical but should not be confused with the connectives of classical logic. Indeed, consider the following quantum formulae where φ is a classical formula: (i) $(\varphi \vee (\neg\, \varphi))$; (ii) $(\varphi \sqcup (\boxminus\, \varphi))$; and (iii) $(\varphi \sqcup (\neg\, \varphi))$. Clearly, (i) and (ii) hold in every quantum system for every ground substitution, while (iii) does not hold in general.

The generalized quantum modality is quite powerful and is better understood in the context of a concrete example. Consider the following specification of a state of the quantum system composed of two entangled pairs of qubits where each pair of qubits is at state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$:

– $([\mathbf{p}_0, \mathbf{p}_1]\, \Diamond (\mathbf{p}_0 \wedge \mathbf{p}_1) : \frac{1}{\sqrt{2}}, ((\neg\, \mathbf{p}_0) \wedge (\neg\, \mathbf{p}_1)) : \frac{1}{\sqrt{2}})$;
– $([\mathbf{p}_2, \mathbf{p}_3]\, \Diamond (\mathbf{p}_2 \wedge \mathbf{p}_3) : \frac{1}{\sqrt{2}}, ((\neg\, \mathbf{p}_2) \wedge (\neg\, \mathbf{p}_3)) : \frac{1}{\sqrt{2}})$.

The specified state of the quantum system composed of the four qubits is $\frac{1}{2}|0000\rangle + \frac{1}{2}|0011\rangle + \frac{1}{2}|1100\rangle + \frac{1}{2}|1111\rangle$. This state will be a relevant state of the quantum system discussed in Section 5 for modeling a quantum key distribution protocol. This specification entails the following formulae:

– $([\mathbf{p}_0, \mathbf{p}_1] \sqcap [\mathbf{p}_2, \mathbf{p}_3])$;
– $(\int \mathbf{p}_0) = \frac{1}{2}$;
– $(\int (\mathbf{p}_0 \Leftrightarrow \mathbf{p}_1)) = 1$;
– $(\int (\mathbf{p}_0 \Leftrightarrow \mathbf{p}_2)) = \frac{1}{2}$.

Our ultimate goal was to develop a deduction calculus complete in some useful sense with respect to the above semantics. However, when using only finitary rules, strong completeness is out of question because of quantum entailment is not compact[8].

Despite this negative result, we are able to define a weak complete Hilbert calculus (with respect to an arithmetic oracle)[9]. Here are the interesting axioms for the quantum modality:

SUPP $\vdash (\boxminus\, ([S]\, \Diamond\, \psi : 0))$;

PROJ $\vdash (([S]\, \Diamond\, \psi_1 : u_1, \ldots, \psi_n : u_n) \sqsupset ([S]\, \Diamond\, \psi_k : e^{it} u_k))$ for $k = 1, \ldots, n$;

NORM $\vdash (([S]\, \Diamond\, (\psi \vee \psi') : u) \equiv (([S]\, \Diamond\, \psi : u) \sqcup ([S]\, \Diamond\, \psi' : u)))$;

RPROB $\vdash (([S]\, \Diamond\, \psi_1 : u_1, \ldots, \psi_n : u_n) \sqsupset$
$((|u_1|^2 + \cdots + |u_n|^2) \leq (\int (\psi_1 \vee \ldots \vee \psi_n))))$;

LPROB $\vdash (([F]\, \Diamond\, (\bigwedge_F A) : u) \sqsupset ((\int (\bigwedge_F A)) \leq |u|^2))$;

QMON $\vdash ((\psi_1 \Rightarrow \psi_2) \sqsupset (([S]\, \Diamond\, \psi_1 : u) \leq ([S]\, \Diamond\, \psi_2 : u)))$.

[8] Take $\Gamma = \{((r' \leq (\int \mathbf{p}_1)) \sqcap ((\int \mathbf{p}_1) \leq r'')) : r' < \frac{1}{2} < r''\}$ and $\delta = ((\int \mathbf{p}_1) = \frac{1}{2})$. So, $\Gamma \vDash \delta$, but, clearly, there is no finite $\Gamma_0 \subset \Gamma$ such that $\Gamma_0 \vDash \delta$.

[9] The proof will be presented elsewhere given its size and complexity.

Concerning probabilistic reasoning, the key axioms are as follows:

PM $\vdash ((\int \mathbf{t}) = 1)$;

FA $\vdash (((\int(\neg(\xi_1 \wedge \xi_2))) = 1) \sqsupset ((\int(\xi_1 \vee \xi_2)) = ((\int \xi_1) + (\int \xi_2))))$;

CP $\vdash (((\int \xi_2 \,|\, \xi_1)(\int \xi_1)) = (\int(\xi_1 \wedge \xi_2)))$;

UCP $\vdash (((\int \xi_1) = 0) \sqsupset ((\int \xi_2 \,|\, \xi_1) = 1))$;

PMON $\vdash ((\xi_1 \Rightarrow \xi_2) \sqsupset ((\int \xi_1) \leq (\int \xi_2)))$.

By restricting the quantum language to the probabilistic connectives, we obtain a logic for reasoning with uncertainty. The resulting logic has such nice properties that it is worthwhile to study it by itself.

4 Reasoning about Quantum Evolution

For reasoning about changes in the state of a quantum system (including transitions resulting from projective observations of a single qubit), we need to enrich the language. First, we need transition terms for denoting all such state transitions, of the form

$$Z = \tau_k \curlyvee U \curlyvee P \curlyvee (Z \circ Z)$$

where U is a unitary operator term of the form

$$U = \mathbf{I} \curlyvee \mathbf{H}_k \curlyvee \mathbf{S}_k \curlyvee \left(\frac{\pi}{\mathbf{8}}\right)_k \curlyvee \mathbf{X}_k \curlyvee \mathbf{Y}_k \curlyvee \mathbf{Z}_k \curlyvee \mathbf{cN}^{k_1}_{k_2} \curlyvee U^{-1} \curlyvee (U \circ U)$$

and P is a qubit projective observation transition term of the form

$$P = \mathbf{P}_k^{c|\mathbf{0}\rangle + c|\mathbf{1}\rangle}$$

where c is a complex number of the form $r+ir$ where r is, as before, a computable real number. The eight symbols in U denote the eight basic unitary operators (identity, Hadamard, phase, $\pi/8$, Pauli X, Y, Z, and control not, respectively). As mentioned already at the end of Section 2, any finite, unitary operator can be approximated as close as desired by a finite composition of these basic operators [15]. We also need transition formulae of the form[10]

$$H = \{\gamma\}\, Z\, \{\gamma\} \curlyvee \{\gamma\}\, \Omega Z$$

where γ is a quantum formula as defined in the Section 3.

The denotation $[\![Z]\!]$ of a transition term Z is a partial map from the unit circle of $\mathcal{H}(\mathcal{V})$ to itself (recall that $\mathcal{V}$ is the set of all classical valuations). In the case of every unitary operator term this map is total. Partiality only arises for observation transitions (as illustrated below).

[10] Adapting from the Hoare (pre and post condition) triplets in the logic of imperative programs [14].

Observe that, given $V \subseteq \mathcal{V}$, it may happen that $[\![Z]\!]|w\rangle \notin \mathcal{H}(V)$ even when $|w\rangle \in \mathcal{H}(V)$ and $[\![Z]\!]$ is defined on $|w\rangle$. We must keep this in mind when defining the satisfaction of transition formulae[11]:

- $V\rho \Vdash \{\gamma_1\}\, Z\, \{\gamma_2\}$ iff, for any $|w\rangle \in \mathcal{H}(V)$, if $\langle V, |w\rangle\rangle\rho \Vdash \gamma_1$ then $\langle V, [\![Z]\!]|w\rangle\rangle\rho \Vdash \gamma_2$ whenever $[\![Z]\!]|w\rangle\!\downarrow$ and $[\![Z]\!]|w\rangle \in \mathcal{H}(V)$;
- $V\rho \Vdash \{\gamma\}\, \Omega Z$ iff, for any $|w\rangle \in \mathcal{H}(V)$, if $\langle V, |w\rangle\rangle\rho \Vdash \gamma$ then $[\![Z]\!]|w\rangle\!\downarrow$ and $[\![Z]\!]|w\rangle \in \mathcal{H}(V)$.

That is, $\{\gamma_1\}\, Z\, \{\gamma_2\}$ means that if the quantum system evolves by Z from a state where γ_1 holds to a legitimate state (that is, in $\mathcal{H}(V)$) then γ_2 holds at the resulting state. If the resulting state is not legitimate the transition formula is vacuously satisfied. And $\{\gamma\}\, \Omega Z$ means that the quantum system reaches a legitimate state when it evolves by Z from a state where γ holds.

It is worthwhile to spell out in detail the semantics of the basic unitary operators. To this end, we need the notion of the dual of a valuation on a qubit: $\overline{v}^k$ is the valuation that agrees with v on all propositional symbols barring $\mathbf{p}_k$ and gives the other Boolean value to $\mathbf{p}_k$. For instance:

- $[\![\mathbf{H}_k]\!]|w\rangle(v) = \begin{cases} \frac{1}{\sqrt{2}}(|w\rangle(v) + |w\rangle(\overline{v}^k)) \text{ if } v \nVdash \mathbf{p}_k \\ \frac{1}{\sqrt{2}}(|w\rangle(\overline{v}^k) - |w\rangle(v)) \text{ otherwise} \end{cases};$
- $[\![\mathbf{S}_k]\!]|w\rangle(v) = \begin{cases} |w\rangle(v) \;\; \text{if } v \nVdash \mathbf{p}_k \\ i|w\rangle(v) \text{ otherwise} \end{cases};$
- $[\![\mathbf{cN}^{k_1}_{k_2}]\!]|w\rangle(v) = \begin{cases} |w\rangle(v) \quad\;\; \text{if } v \nVdash \mathbf{p}_{k_1} \\ |w\rangle(\overline{v}^{k_2}) \text{ otherwise} \end{cases}.$

Before describing the semantics of the projective observation operators, we need some notation. Given a set S of propositional constants (qubits), we denote by $I_{[S]}$ the identity operator on $\mathcal{H}(\mathcal{V}_{[S]})$ and by $I_{]S[}$ the identity operator on $\mathcal{H}(\mathcal{V}_{]S[})$. Given $|b\rangle = \alpha_0|\mathbf{0}\rangle + \alpha_1|\mathbf{1}\rangle$ in $\mathcal{H}(2)$ we also need to use the projector along $|b\rangle$, that is, the operator $|b\rangle\langle b|$ on $\mathcal{H}(2)$ defined by the following matrix:

$$\begin{pmatrix} \alpha_0\overline{\alpha_0} & \alpha_0\overline{\alpha_1} \\ \alpha_1\overline{\alpha_0} & \alpha_1\overline{\alpha_1} \end{pmatrix}.$$

Letting $P_k^{|b\rangle}$ be the projector along $|b\rangle$ for qubit k in $\mathcal{H}(\mathcal{V})$ that is given by $I_{[\{\mathbf{p}_0,\ldots,\mathbf{p}_{k-1}\}]} \otimes |b\rangle\langle b| \otimes I_{]\{\mathbf{p}_0,\ldots,\mathbf{p}_k\}[}$, the semantics of the projective observation transition terms is as follows:

- $[\![\mathbf{P}_k^{c_0|\mathbf{0}\rangle+c_1|\mathbf{1}\rangle}]\!]|w\rangle = \frac{P_k^{c_0|\mathbf{0}\rangle+c_1|\mathbf{1}\rangle}|w\rangle}{||P_k^{c_0|\mathbf{0}\rangle+c_1|\mathbf{1}\rangle}|w\rangle||}.$

Observe that $[\![\mathbf{P}_k^{c_0|\mathbf{0}\rangle+c_1|\mathbf{1}\rangle}]\!]$ is undefined at $|w\rangle$ if $||P_k^{c_0|\mathbf{0}\rangle+c_1|\mathbf{1}\rangle}|w\rangle|| = 0$. In particular, $[\![\mathbf{P}_k^{|\mathbf{0}\rangle}]\!]$ is undefined at $|w\rangle$ whenever $|w\rangle \Vdash ((\textstyle\int(\neg\,\mathbf{p}_k)) = 0)$. In fact, it

[11] As usual when dealing with partial maps, we write $[\![Z]\!]|w\rangle\!\downarrow$ for asserting that $[\![Z]\!]$ is defined on $|w\rangle$.

is not possible to observe 0 on $\mathbf{p}_k$ when all valuations in the support of the state of the system satisfy $\mathbf{p}_k$.

The projective observation transition terms play the role of qubit assignments in quantum computation since they impose the superposition of the the target qubit in the resulting state. But, contrarily to classical computation, an assignment to qubit $\mathbf{p}_k$ may also affect other qubits (those that were entangled with $\mathbf{p}_k$), this is a core property of quantum systems where the EPR quantum key distribution protocol relies on.

As an illustration, consider the transition formula

$$\begin{aligned}&\{([\mathbf{p}_0, \mathbf{p}_1] \Diamond(\mathbf{p}_0 \wedge \mathbf{p}_1) : \tfrac{1}{\sqrt{2}}, ((\neg\, \mathbf{p}_0) \wedge (\neg\, \mathbf{p}_1)) : \tfrac{1}{\sqrt{2}})\}\\ &\quad \mathbf{P}^{|\mathbf{1}\rangle}_{\mathbf{p}_0}\\ &\{([\mathbf{p}_1] \Diamond\ \mathbf{p}_1 : 1)\}\end{aligned}$$

This formula states, among other things, that if the qubits are entangled then after observing $\mathbf{p}_0$ taking value one we end up in a state where the other qubit also takes value one.

Given a weak complete axiomatization of EQPL (the logic defined in Section 3), it is straightforward to set up a weak complete axiomatization of DEQPL as defined in this section.

5 Quantum Key Distribution

For illustrating the power of the proposed quantum logic, we specify and reason about the EPR quantum key distribution protocol [17]. This protocol is used for sharing a private classical key (that is, a sequence of n bits) via a public quantum channel (composed of $4n$ qubits).

The quantum system is composed of $12n$ qubits: $2n$ pairs of public channel qubits — $\langle \mathbf{x}_1, \mathbf{x}_2\rangle, \ldots, \langle \mathbf{x}_{4n-1}, \mathbf{x}_{4n}\rangle$; $4n$ private qubits owned by Alice — $\mathbf{aw}_1, \ldots, \mathbf{aw}_{2n}$ for storing channel qubits, $\mathbf{at}_1, \ldots, \mathbf{at}_n$ to be used in a test, and $\mathbf{ak}_1, \ldots, \mathbf{ak}_n$ to be used to generate the key; and, analogously, $4n$ private qubits owned by Bob — $\mathbf{bw}_1, \ldots, \mathbf{bw}_{2n}, \mathbf{bt}_1, \ldots, \mathbf{bt}_n, \mathbf{bk}_1, \ldots, \mathbf{bk}_n$. The protocol runs as follows:

1. A third trusted party sets up each pair of channel qubits at state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.
2. Alice fetches the odd channel qubits and Bob fetches the even channel qubits. Since copying qubits is physically impossible, this is achieved by swapping.
3. Alice and Bob agree on a partition $\langle\{j_1, \ldots, j_n\}, \{j'_1, \ldots, j'_n\}\rangle$ of $\{1, \ldots, 2n\}$. Alice transfers (by swapping) $\mathbf{aw}_{j_k}$ to $\mathbf{at}_k$ and $\mathbf{aw}_{j'_k}$ to $\mathbf{ak}_k$. Bob does the same on his qubits.
4. Alice tests if the qubits **at** and **bt** are still entangled. If this fidelity test fails, she assumes Eve has been eavesdropping and resets the protocol. Otherwise, she projectively measures the **ak** qubits (one by one) and obtains the private classical key shared with Bob. Bob does the same with his qubits in order to obtain the key.

For the sake of economy of presentation, we analyze the protocol for $n = 1$. Barring the test of fidelity, this choice is made without loss of generality. But, in practice, n should be large in order to lower the probability of Eve guessing the key, and, for testing if Eve was eavesdropping while the protocol was running, it is also essential to work with large n (given the statistical nature of the fidelity test). Anyway, it is straightforward to describe and analyze the protocol in the proposed quantum logic for arbitrary n (including proving the soundness of the fidelity test).

Initially all qubits are set to $|0\rangle$ and they constitute an independent closed quantum system. Therefore, the initial state of the protocol fulfills $IC = (((\neg\,\mathbf{x}_1) \wedge (\neg\,\mathbf{x}_2) \wedge \ldots \wedge (\neg\,\mathbf{bk}_1)) \sqcap [\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{bk}_1])$. Each step of the protocol corresponds to a quantum transition on these twelve qubits.

1. Set up each pair of channel qubits at state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ by applying the following composition: $Z_1 = ((\mathbf{cN}^{\mathbf{x}_3}_{\mathbf{x}_4} \circ \mathbf{H}_{\mathbf{x}_3}) \circ (\mathbf{cN}^{\mathbf{x}_1}_{\mathbf{x}_2} \circ \mathbf{H}_{\mathbf{x}_1}))$.
2. Swap the odd channel qubits with the storing channel qubits of Alice by applying the following composition: $((\mathbf{cN}^{\mathbf{x}_3}_{\mathbf{aw}_2} \circ \mathbf{cN}^{\mathbf{aw}_2}_{\mathbf{x}_3} \circ \mathbf{cN}^{\mathbf{x}_3}_{\mathbf{aw}_2}) \circ (\mathbf{cN}^{\mathbf{x}_1}_{\mathbf{aw}_1} \circ \mathbf{cN}^{\mathbf{aw}_1}_{\mathbf{x}_1} \circ \mathbf{cN}^{\mathbf{x}_1}_{\mathbf{aw}_1}))$. Analogously, swap the even channel qubits with the storing channel qubits of Bob by applying the following composition: $((\mathbf{cN}^{\mathbf{x}_4}_{\mathbf{bw}_2} \circ \mathbf{cN}^{\mathbf{bw}_2}_{\mathbf{x}_4} \circ \mathbf{cN}^{\mathbf{x}_4}_{\mathbf{bw}_2}) \circ (\mathbf{cN}^{\mathbf{x}_2}_{\mathbf{bw}_1} \circ \mathbf{cN}^{\mathbf{bw}_1}_{\mathbf{x}_2} \circ \mathbf{cN}^{\mathbf{x}_2}_{\mathbf{bw}_1}))$. Obtain the whole transition by composing the previous two transitions: $Z_2 = ((\mathbf{cN}^{\mathbf{x}_3}_{\mathbf{bw}_1} \circ \mathbf{cN}^{\mathbf{bw}_1}_{\mathbf{x}_3} \circ \mathbf{cN}^{\mathbf{x}_3}_{\mathbf{bw}_1}) \circ ... \circ (\mathbf{cN}^{\mathbf{x}_1}_{\mathbf{aw}_1} \circ \mathbf{cN}^{\mathbf{aw}_1}_{\mathbf{x}_1} \circ \mathbf{cN}^{\mathbf{x}_1}_{\mathbf{aw}_1}))$.
3. Assume that Alice and Bob agree on the partition $\langle\{2\},\{1\}\rangle$ of $\{1, 2\}$. Swap $\mathbf{aw}_2$ with $\mathbf{at}_1$ and $\mathbf{aw}_1$ with $\mathbf{ak}_1$ by applying the following composition: $((\mathbf{cN}^{\mathbf{aw}_1}_{\mathbf{ak}_1} \circ \mathbf{cN}^{\mathbf{ak}_1}_{\mathbf{aw}_1} \circ \mathbf{cN}^{\mathbf{aw}_1}_{\mathbf{ak}_1}) \circ (\mathbf{cN}^{\mathbf{aw}_2}_{\mathbf{at}_1} \circ \mathbf{cN}^{\mathbf{at}_1}_{\mathbf{aw}_2} \circ \mathbf{cN}^{\mathbf{aw}_2}_{\mathbf{at}_1}))$. Analogously, swap $\mathbf{bw}_2$ with $\mathbf{bt}_1$ and $\mathbf{bw}_1$ with $\mathbf{bk}_1$ by applying the following composition: $((\mathbf{cN}^{\mathbf{bw}_1}_{\mathbf{bk}_1} \circ \mathbf{cN}^{\mathbf{bk}_1}_{\mathbf{bw}_1} \circ \mathbf{cN}^{\mathbf{bw}_1}_{\mathbf{bk}_1}) \circ (\mathbf{cN}^{\mathbf{bw}_2}_{\mathbf{bt}_1} \circ \mathbf{cN}^{\mathbf{bt}_1}_{\mathbf{bw}_2} \circ \mathbf{cN}^{\mathbf{bw}_2}_{\mathbf{bt}_1}))$. Obtain the whole transition by composing the previous two transitions: $Z_3 = ((\mathbf{cN}^{\mathbf{bw}_1}_{\mathbf{bk}_1} \circ \mathbf{cN}^{\mathbf{bk}_1}_{\mathbf{bw}_1} \circ \mathbf{cN}^{\mathbf{bw}_1}_{\mathbf{bk}_1}) \circ \cdots \circ (\mathbf{cN}^{\mathbf{aw}_2}_{\mathbf{at}_1} \circ \mathbf{cN}^{\mathbf{at}_1}_{\mathbf{aw}_2} \circ \mathbf{cN}^{\mathbf{aw}_2}_{\mathbf{at}_1}))$.
4. The fidelity test corresponds to verifying if the qubits associated to $\mathbf{at}_1$ and $\mathbf{bt}_1$ are entangled. This test amounts to checking whether $((\int \mathbf{at}_1) = \frac{1}{2})$ and $((\int(\mathbf{at}_1 \Leftrightarrow \mathbf{bt}_1)) = 1)$[12] hold. Finally, Alice and Bob obtain the shared key by measuring $\mathbf{ak}_1$ and $\mathbf{bk}_1$ via the following projectors: $\mathbf{P}^{|\mathbf{0}\rangle}_{\mathbf{ak}_1}$, $\mathbf{P}^{|\mathbf{1}\rangle}_{\mathbf{ak}_1}$, $\mathbf{P}^{|\mathbf{0}\rangle}_{\mathbf{bk}_1}$ and $\mathbf{P}^{|\mathbf{1}\rangle}_{\mathbf{bk}_1}$.

In what concerns the analysis of the protocol, barring the soundness of the fidelity test, there are only two properties to be checked: correctness and perfect security. The protocol is said to be correct if Alice and Bob end up with the same key. The protocol is said to be perfectly secure if: (i) the key is generated with uniform distribution and (ii) the probability of Eve eavesdropping a key

[12] In practice, these probabilities are estimated using several projections, but the details of this procedure are out of the scope of this paper. Clearly, here it is essential to have a large n.

of size n without being detected is $O(2^{-n})$. We do not consider (ii) since that depends on proving the soundness of the fidelity test.

Verifying correctness corresponds to checking whether the following formulae are valid:

- $\{IC\}\, \Omega\, (\mathbf{P}^{|\mathbf{0}\rangle}_{\mathbf{bk}_1} \circ \mathbf{P}^{|\mathbf{0}\rangle}_{\mathbf{ak}_1} \circ Z_3 \circ Z_2 \circ Z_1)$;
- $\{IC\}\, \Omega\, (\mathbf{P}^{|\mathbf{1}\rangle}_{\mathbf{bk}_1} \circ \mathbf{P}^{|\mathbf{1}\rangle}_{\mathbf{ak}_1} \circ Z_3 \circ Z_2 \circ Z_1)$;
- $\{IC\}\, (\mathbf{P}^{|\mathbf{0}\rangle}_{\mathbf{bk}_1} \circ \mathbf{P}^{|\mathbf{1}\rangle}_{\mathbf{ak}_1} \circ Z_3 \circ Z_2 \circ Z_1)\, \{\mathbf{fff}\}$;
- $\{IC\}\, (\mathbf{P}^{|\mathbf{1}\rangle}_{\mathbf{bk}_1} \circ \mathbf{P}^{|\mathbf{0}\rangle}_{\mathbf{ak}_1} \circ Z_3 \circ Z_2 \circ Z_1)\, \{\mathbf{fff}\}$.

The first two formulae assert that the quantum state reached when Alice and Bob obtain the same key is legitimate. The other formulae assert that if Bob and Alice obtain different keys then falsum holds. We sketch how to obtain the validity of the third formula. First, it is easy to see that $\{IC\}\, (Z_3 \circ Z_2 \circ Z_1)\, \{\delta\}$ holds, where $\delta \equiv ([\mathbf{ak}_1, \mathbf{bk}_1] \lozenge (\mathbf{ak}_1 \wedge \mathbf{bk}_1) : \frac{1}{\sqrt{2}}, ((\neg\, \mathbf{ak}_1) \wedge (\neg\, \mathbf{bk}_1)) : \frac{1}{\sqrt{2}})$. This happens, because Z_1 entangles $\mathbf{x}_1$ with $\mathbf{x}_2$, Z_2 swaps them with $\mathbf{aw}_1$ and $\mathbf{bw}_1$ and, finally, Z_3 swaps $\mathbf{aw}_1$ with $\mathbf{ak}_1$ and $\mathbf{bw}_1$ with $\mathbf{bk}_1$. Furthermore, by noticing that $\{\delta\}\, \mathbf{P}^{|\mathbf{1}\rangle}_{\mathbf{ak}_1}\, \{\mathbf{ak}_1 \wedge \mathbf{bk}_1\}$ and $\{\mathbf{ak}_1 \wedge \mathbf{bk}_1\}\, \mathbf{P}^{|\mathbf{0}\rangle}_{\mathbf{bk}_1}\, \{\mathbf{fff}\}$ we reach the desired conclusion.

Finally, note that verifying whether the key is generated with uniform distribution corresponds to checking if $\{IC\}\, (Z_3 \circ Z_2 \circ Z_1)\, \{\delta'\}$ holds where

$$\delta' \equiv ((\textstyle\int \mathbf{ak}_1) = \frac{1}{2}) \sqcap ((\textstyle\int (\neg\, \mathbf{ak}_1)) = \frac{1}{2}).$$

This validity is straightforward, since $\{IC\}\, (Z_3 \circ Z_2 \circ Z_1)\, \{\delta\}$ and $(\delta \sqsupset \delta')$.

6 Concluding Remarks and Acknowledgments

The key idea of identifying quantum models with superpositions of classical valuations provided us with a working semantics for a powerful quantum logic extending classical and probabilistic logic (like modal logic extends classical logic).

The resulting logic is promising and interesting in itself, but further work is necessary, namely towards a clarification of the relationship to the traditional quantum logics. In this respect it should be stressed that our quantum logic has classical implication capable of internalizing the notion of quantum entailment (both MP and MTD hold), contrarily to traditional quantum logics where the notion of implication is a big problem.

Assessing the effective role of the chosen basis for $\mathcal{H}(V)$ is also an interesting line of research. Indeed, the definition of EQPL satisfaction strongly relies upon using the orthonormal basis $\{|v\rangle : v \in V\}$. One wonders if we can relax the semantics, while preserving the intended entailment, in order to be able to deal with classical formulae when we do not know V but we are just given a Hilbert space isomorphic to $\mathcal{H}(V)$.

The authors wish to express their deep gratitude to the regular participants in the QCI Seminar who suffered early presentations of this work and gave very useful feedback that helped us to get over initial difficulties and misunderstandings of quantum physics.

This work was partially supported by FCT and FEDER through POCTI, namely via FibLog 2001/MAT/37239 Project and within the recent QuantLog initiative of CLC.

References

1. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2000)
2. Foulis, D.J.: A half-century of quantum logic. What have we learned? In: Quantum Structures and the Nature of Reality. Volume 7 of Einstein Meets Magritte. Kluwer Acad. Publ. (1999) 1–36
3. Chiara, M.L.D., Giuntini, R., Greechie, R.: Reasoning in Quantum Theory. Kluwer Academic Publishers (2004)
4. Birkhoff, G., von Neumann, J.: The logic of quantum mechanics. Annals of Mathematics **37** (1936) 823–843
5. Kripke, S.A.: Semantical analysis of modal logic. I. Normal modal propositional calculi. Zeitschrift für Mathematische Logik und Grundlagen der Mathematik **9** (1963) 67–96
6. Carnielli, W.A., Lima-Marques, M.: Society semantics and multiple-valued logics. In: Advances in Contemporary Logic and Computer Science (Salvador, 1996). Volume 235 of Contemporary Mathematics. AMS (1999) 33–52
7. Carnielli, W.A.: Possible-translations semantics for paraconsistent logics. In: Frontiers of Paraconsistent Logic (Ghent, 1997). Volume 8 of Studies in Logic and Computation. Research Studies Press (2000) 149–163
8. Nilsson, N.J.: Probabilistic logic. Artificial Intelligence **28** (1986) 71–87
9. Nilsson, N.J.: Probabilistic logic revisited. Artificial Intelligence **59** (1993) 39–42
10. Bacchus, F.: Representing and Reasoning with Probabilistic Knowledge. MIT Press Series in Artificial Intelligence. MIT Press (1990)
11. Bacchus, F.: On probability distributions over possible worlds. In: Uncertainty in Artificial Intelligence, 4. Volume 9 of Machine Intelligence and Pattern Recognition. North-Holland (1990) 217–226
12. Fagin, R., Halpern, J.Y., Megiddo, N.: A logic for reasoning about probabilities. Information and Computation **87** (1990) 78–128
13. Dishkant, H.: Semantics of the minimal logic of quantum mechanics. Studia Logica **30** (1972) 23–32
14. Hoare, C.: An axiomatic basis for computer programming. Communications of the ACM **12** (1969) 576–583
15. DiVincenzo, D.P.: Two-bit gates are universal for quantum computation. Physics Reviews A **51** (1995) 1015–1022
16. Naur, P.: Revised report on the algorithmic language Algol 60. The Computer Journal **5** (1963) 349–367
17. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, IEEE (1984) 175–179