# Extending classical logic for reasoning about quantum systems

Amílcar Sernadas

Departamento de Matemática - Instituto Superior Técnico
Security and Quantum Information Group - Instituto de Telecomunicações
Universidade de Lisboa

Logic Colloquium, Évora
July 24, 2013

FCT & EU FEDER PEst-OE/EEI/LA0008/2013
EU FP7 GA 318287 LANDAUER

# Abstract

A brief presentation of the (essence of) EQPL (†),
a decidable (‡) conservative extension of propositional logic
for reasoning about the state of a quantum system,

including:
- key design options (starting from the QM postulates);
- syntax, semantics, (complete) axiomatization;
- decidability;
- practical impact so far.

(†) Joint work with Paulo Mateus.
(‡) Joint work also with Rohit Chadha and Cristina Sernadas.

# Work environment

## Transdisciplinary team at IST since 2004

- Physicists;
- Mathematical logicians;
- Computer scientists;
- Information theoreticians (recent addition).

## PhD Program in Physics and Mathematics of Information

Just starting with FCT support for 10 new scholarships per year.

# From classical to quantum reasoning

## Birkhoff and von Neumann (1936)

Algebraic semantics

| | | |
|---|---|---|
| CPL | $\rightarrow$ | QPL |
| Boolean algebra | $\rightarrow$ | complete lattice of closed subspaces of the Hilbert space at hand with orthogonal complement |

## Exogenous approach (2006)

Valuation semantics

| | | |
|---|---|---|
| CPL | $\rightarrow$ | EQPL |
| valuation | $\rightarrow$ | superposition of valuations |

# Key design options

## A matter of cats

Is the cat awake or asleep?
Is the cat indoors or outdors?

NO CAT WAS HARMED IN THE PREPARATION OF THIS TALK OR WILL BE HARMED DURING THE TALK.

# The classical cat

## Either awake or asleep and either indoors or outdoors

Four classical valuations:

$$|00\rangle = \begin{cases} \textbf{awake} \mapsto 0 \\ \textbf{indoors} \mapsto 0 \end{cases} \qquad |10\rangle = \begin{cases} \textbf{awake} \mapsto 1 \\ \textbf{indoors} \mapsto 0 \end{cases}$$

$$|01\rangle = \begin{cases} \textbf{awake} \mapsto 0 \\ \textbf{indoors} \mapsto 1 \end{cases} \qquad |11\rangle = \begin{cases} \textbf{awake} \mapsto 1 \\ \textbf{indoors} \mapsto 1 \end{cases}$$

Classical valuation space:

$$\mathcal{V} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

# The quantum cat

## Somewhere between asleep outdors and awake indoors...

Each quantum valuation is a unit superposition of classical valuations:

$$|\psi\rangle = z_{00}|00\rangle + z_{01}|01\rangle + z_{10}|10\rangle + z_{11}|11\rangle$$

with amplitudes (the $z$'s) in $\mathbb{C}$ and such that $||\psi|| = 1$

Quantum valuation space:

$\mathcal{H}_1^{\mathbb{C}}(\mathcal{V})$ = the surface of the unit sphere of

$\mathcal{H}^{\mathbb{C}}(\mathcal{V})$ = the Hilbert space over $\mathbb{C}$ freely generated from $\mathcal{V}$

= $\text{span}^{\mathbb{C}}(\mathcal{V})$ pt $\mathcal{V}$ is finite as in the case at hand.

# RECALL

## QM Postulate 1

*The state space of an isolated quantum system is the surface of the unit sphere of a Hilbert space over $\mathbb{C}$.*

## QM Postulate 2

*The Hilbert space of a quantum system composed of a finite number of independent components is the tensor product of the component Hilbert spaces.*

# If awakeness and whereabouts are independent

## not all superposition are possible

$$\mathcal{H}^{\mathbb{C}}(\mathcal{V}) = \mathcal{H}^{\mathbb{C}}(\mathcal{V}_{[\mathbf{awake}]}) \otimes \mathcal{H}^{\mathbb{C}}(\mathcal{V}_{[\mathbf{indoors}]})$$

$$|\psi\rangle = |\psi'\rangle \otimes |\psi''\rangle$$

$$|\psi'\rangle \in \mathcal{H}_1^{\mathbb{C}}(\mathcal{V}_{[\mathbf{awake}]}) =$$
$$\mathcal{H}_1^{\mathbb{C}}(\{|00\rangle|_{\mathbf{awake}}, |01\rangle|_{\mathbf{awake}}, |10\rangle|_{\mathbf{awake}}, |11\rangle|_{\mathbf{awake}}\}) =$$
$$\mathcal{H}_1^{\mathbb{C}}(\{\mathbf{awake} \mapsto 0, \mathbf{awake} \mapsto 1\})$$

$$|\psi''\rangle \in \mathcal{H}_1^{\mathbb{C}}(\mathcal{V}_{[\mathbf{indoors}]}) =$$
$$\mathcal{H}_1^{\mathbb{C}}(\{\mathbf{indoors} \mapsto 0, \mathbf{indoors} \mapsto 1\})$$

# If awakeness and whereabouts are not independent

## the two qubits may be entangled

$$\mathcal{H}^{\mathbb{C}}(\mathcal{V}) \neq \mathcal{H}^{\mathbb{C}}(\mathcal{V}_{\textbf{[awake]}}) \otimes \mathcal{H}^{\mathbb{C}}(\mathcal{V}_{\textbf{[indoors]}})$$

$|\psi\rangle \neq |\psi'\rangle \otimes |\psi''\rangle$ is possible

for instance

$$|\psi\rangle = \sqrt{\frac{1}{2}}\,|00\rangle + \sqrt{\frac{1}{2}}\,|11\rangle = \sqrt{\frac{1}{2}}\,(|00\rangle + |11\rangle)$$

(a state with maximum entanglement — a Bell state)

# The probabilistic result of observing a quantum cat

## From amplitudes to probabilities

If the quantum cat is in state

$$|\psi\rangle = \sqrt{\frac{1}{3}}\,(|00\rangle + i\,|01\rangle + |11\rangle)$$

the distribution of the random outcome of the logical projective observation of its awakeness is as follows:

$$\mu^{\mathbf{awake}}_{|\psi\rangle} = \begin{cases} (\mathbf{awake} \mapsto 0) \mapsto \frac{2}{3} \\ (\mathbf{awake} \mapsto 1) \mapsto \frac{1}{3} \end{cases}$$

# RECALL

## QM Postulate 3

*Every measurable physical quantity of an isolated quantum system is described by an observable acting on its Hilbert space.*

# FURTHERMORE

## QM Postulate 4 (discrete case)

*The only possible outcomes of the measurement of a physical quantity are the eigenvalues of its observable.*

*When the physical quantity is measured on a system at state* $|\psi\rangle$ *using observable* $A$ *with countable spectrum* $E^A$*,*
*the resulting outcomes are random with distribution*

$$\mu^A_{|\psi\rangle} = e \mapsto ||Proj_e|\psi\rangle||^2 : E^A \to [0,1].$$

When outcome $e$ is observed, the state of the system becomes the unit vector obtained by normalizing $Proj_e|\psi\rangle$.

# EN PASSANT

## Statistical ensembles

Hence, when measurements are made along the way, for dealing with the evolution of the system one needs to work with mixed states (probabilistic mixtures of superpositions).

Such mixed states are better represented by density operators.

Changes to the system correspond to superoperators that subsume both unitary transformations and measurements in the realm of density operators.

NOT TODAY :-)

# Observing some of a finite number of qubits

## Logical projective measurement of $F \subseteq Q$

$$A^F = \left( \sum_{v \in \mathcal{V}_{[F]}} |v\rangle\langle v| \right) \otimes \mathsf{Id}_{]F[}$$

$$E^F = \mathcal{V}_{[F]}$$

$$\mathcal{E}^F_v = v \otimes \mathsf{span}^{\mathbb{C}}(\mathcal{V}_{]F[})$$

where

$\mathcal{V}_{[F]} =$ set of $Q$-valuations restricted to $F$

$\mathcal{V}_{]F[} =$ set of $Q$-valuations restricted to $Q \setminus F$

# By the way...

**Non-deterministic cat**

Non-empty set of valuations.

A quantum cat induces a non-deterministic cat:

$$V = \text{support of } |\psi\rangle$$

**Probabilistic cat**

Random valuation.

Measuring qubits of a quantum cat results in a probabilistic cat.

# EQPL

# EQPL overview

## Signature

$$Q = \text{finite set of qubit symbols}$$

## Semantics

Each quantum valuation is a unit superposition of classical valuations over $Q$:

$$|\psi\rangle \in \mathcal{H}_1^{\mathbb{C}}(2^Q)$$

In fact, we need a bit more of structure...

## Language

Rich enough to express:

- classical constraints;
- independence of some qubits from the other qubits;
- probabilities of measurement outcomes;
- amplitudes of the quantum state at hand.

Only
for reasoning about the state of a quantum system.

Extensions required
for reasoning about the evolution of a quantum system
taking also into account QM Postulate 5.

# EQPL syntax

## Classical formulas

$$\alpha \;:=\; \mathbb{ff} \mid q \mid (\alpha \Rightarrow \alpha)$$

## Real and complex terms ($F \subseteq G \subseteq Q$)

$$t \;:=\; x \mid 0 \mid 1 \mid (t+t) \mid (t\,t) \mid \mathrm{Re}(u) \mid \mathrm{Im}(u) \mid |u| \mid (\textstyle\int \alpha)$$
$$u \;:=\; z \mid \langle F|G\rangle \mid (t+it) \mid \overline{u} \mid (u+u) \mid (u\,u) \mid (\alpha \rhd u;\, u)$$

## Quantum formulas ($G \subseteq Q$)

$$\gamma \;:=\; \alpha \mid (t \leq t) \mid [G] \mid \mathbb{FF} \mid (\gamma \sqsupset \gamma)$$

## Other connectives as abbreviations

| Classical | Quantum |
|---|---|
| $\neg$ | $\boxminus$ |
| $\wedge$ | $\sqcap$ |
| $\vee$ | $\sqcup$ |
| $\Leftrightarrow$ | $\equiv$ |

For instance,

$$(\neg\,\alpha) \quad \text{for} \quad (\alpha \Rightarrow \mathsf{ff})$$

$$(\boxminus\,\gamma) \quad \text{for} \quad (\gamma \sqsupset \mathsf{FF})$$

## Modalities as abbreviations of probabilistic assertions

$$(\Diamond\, \alpha) \quad \text{for} \quad (0 < (\textstyle\int \alpha))$$

$$(\Box\, \alpha) \quad \text{for} \quad (1 = (\textstyle\int \alpha))$$

## Other useful abbreviations in applications ($F \subseteq G \subseteq Q$)

$\left(\bigwedge_G F\right)$ for $\left(\left(\bigwedge_{q\in F} q\right) \wedge \left(\bigwedge_{q\in G\setminus F} (\neg\, q)\right)\right)$

$\langle F \supset \alpha | G\rangle$ for $\left(\left(\left(\bigwedge_G F\right) \Rightarrow \alpha\right) \rhd \langle F|G\rangle;\, 0\right)$

$(\Diamond^u_{[G]}\, \alpha)$ for $\left([G] \sqcap (0 < |u|) \sqcap \left(\bigsqcup_{F\subseteq G} (\langle F \supset \alpha | G\rangle = u)\right)\right)$

in the superposition of independent component $G$
there is a valuation making $\alpha$ true with amplitude $u$

## Examples assuming $\mathbf{awake}, \mathbf{indoors}, \mathbf{running} \in Q$

1. $(\mathbf{running} \Rightarrow \mathbf{awake})$
2. $[\mathbf{awake}, \mathbf{indoors}, \mathbf{running}]$
3. $(\boxminus [\mathbf{awake}])$
4. $((\Diamond\, \mathbf{awake}) \sqcap (\Diamond(\neg\, \mathbf{awake})))$
5. $\left(\left(\int \mathbf{awake}\right) = \frac{1}{9}\right)$
6. $\left(\Diamond^{i\frac{1}{3}}_{[\mathbf{awake},\mathbf{running}]}\, \mathbf{running}\right)$

# EQPL (relaxed) semantics

## Quantum structure over $Q$

$$w = (\mathcal{K}, V, \mathcal{S}, |\psi\rangle, \zeta)$$

replacing $\mathbb{C}$ by $\mathcal{K}^\bullet$

(the algebraic closure of the ordered real closed field $\mathcal{K}$).

## Quantum structure over $Q$: $w = (\mathcal{K}, V, \mathcal{S}, |\psi\rangle, \zeta)$

$\mathcal{K}$ ordered real closed field

$\emptyset \neq V \subseteq 2^Q$ (admissible valuations)

$\mathcal{S}$ partition of $Q$ (independent components)

$|\psi\rangle = \{|\psi\rangle_S\}_{S \in \mathcal{S}}$ with each $|\psi\rangle_S \in \mathcal{H}_1^{\mathcal{K}\bullet}(2^S)$

$$|\psi\rangle_\emptyset = 1$$

$$|\psi\rangle_{S_1 \cup \cdots \cup S_n} = |\psi\rangle_{S_1} \otimes \cdots \otimes |\psi\rangle_{S_n}$$

such that $\langle v|\psi\rangle_Q = 0$ whenever $v \notin V$

$\zeta = \{\zeta_G^F\}_{F \subseteq G \subseteq Q}$ with each $\zeta_G^F \in \mathcal{K}^\bullet$

such that $\zeta_G^F = \langle v_G^F|\psi\rangle_G$ whenever $G \in \mathrm{Alg}(\mathcal{S})$

$$\text{where} \quad v_G^F(q) = \begin{cases} 1 & \text{if } q \in F \\ 0 & \text{if } q \in G \setminus F \end{cases}$$

## Denotation of terms by $w$ and $\rho$

$$
\begin{aligned}
[\![x]\!]_{w\rho} &= \rho(x) \\
[\![t_1 + it_2]\!]_{w\rho} &= [\![t_1]\!]_{w\rho} + i_{\mathcal{K}\bullet}\, [\![t_2]\!]_{w\rho} \\
[\![(\int \alpha)]\!]_{w\rho} &= \sum_{v \Vdash^{\mathsf{c}} \alpha} ||\langle v|\psi\rangle||^2 \\
[\![z]\!]_{w\rho} &= \rho(z) \\
[\![\langle F|G\rangle]\!]_{w\rho} &= \zeta_G^F \\
[\![(\alpha \rhd u_1;\ u_2)]\!]_{w\rho} &= \begin{cases} [\![u_1]\!]_{w\rho} & \text{if } V \Vdash^{\mathsf{c}} \alpha \\ [\![u_2]\!]_{w\rho} & \text{otherwise} \end{cases} \\
&\ldots
\end{aligned}
$$

## Satisfaction of quantum formulas by $w$ and $\rho$

$$
\begin{array}{lll}
w\rho \Vdash \alpha & \text{iff} & V \Vdash^{\mathsf{c}} \alpha \\
w\rho \Vdash (t_1 \leq t_2) & \text{iff} & [\![t_1]\!]_{w\rho} \leq_{\mathcal{K}^\bullet} [\![t_2]\!]_{w\rho} \\
w\rho \Vdash [G] & \text{iff} & G \in \mathsf{Alg}(\mathcal{S}) \\
w\rho \nVdash \mathbb{F} & & \\
w\rho \Vdash (\gamma_1 \sqcap \gamma_2) & \text{iff} & w\rho \nVdash \gamma_1 \text{ or } w\rho \Vdash \gamma_2 \\
\ldots & &
\end{array}
$$

## Quantum connectives do not collapse into classical connectives

For instance:

$$
\begin{array}{lcl}
(\neg\,\alpha) & \models & (\boxminus\,\alpha) \\
(\boxminus\,\alpha) & \not\models & (\neg\,\alpha) \\
 & \not\models & ((\boxminus\,\alpha) \sqsupset (\neg\,\alpha)) \\
(\alpha_1 \Rightarrow \alpha_2) & \models & (\alpha_1 \sqsupset \alpha_2) \\
(\alpha_1 \sqsupset \alpha_2) & \not\models & (\alpha_1 \Rightarrow \alpha_2)
\end{array}
$$

But quantum tautologies are still valid. For example:

$$
\begin{array}{lcl}
 & \models & (\gamma \sqsupset \gamma) \\
 & \models & (\gamma \vee (\boxminus\,\gamma))
\end{array}
$$

# EQPL axiomatization

## Inference rules

CMP $\quad \alpha_1, (\alpha_1 \Rightarrow \alpha_2) \vdash \alpha_2$

QMP $\quad \gamma_1, (\gamma_1 \sqsupset \gamma_2) \vdash \gamma_2$

## Axioms

CTaut $\quad \vdash \alpha$ for each classical tautology $\alpha$

QTaut $\quad \vdash \gamma$ for each quantum tautology $\gamma$

ACORCF $\quad \vdash \kappa^{\vec{x},\vec{z}}_{\vec{t},\vec{u}}$ for each instance $\kappa^{\vec{x},\vec{z}}_{\vec{t},\vec{u}}$ of a theorem $\kappa$ of the ACORCF theory

$$\kappa := (a \leq a) \mid \mathbb{F} \mid (\kappa \sqsupset \kappa)$$
$$a := x \mid 0 \mid 1 \mid (a + a) \mid (a\, a) \mid \mathrm{Re}(b) \mid \mathrm{Im}(b) \mid |b|$$
$$b := z \mid (b + ib) \mid \overline{b} \mid (b + b) \mid (b\, b)$$

## Axioms (cont)

| | |
|---|---|
| Lift $\Rightarrow$ | $\vdash ((\alpha_1 \Rightarrow \alpha_2) \sqsupset (\alpha_1 \sqsupset \alpha_2))$ |
| Clps $\mathbb{FF}$ | $\vdash (\mathbb{ff} \equiv \mathbb{FF})$ |
| Ref $\sqcap$ | $\vdash ((\alpha_1 \sqcap \alpha_2) \sqsupset (\alpha_1 \wedge \alpha_2))$ |

## Axioms (cont)

$$\mathsf{Ind}\,\emptyset \qquad \vdash [\emptyset]$$

$$\mathsf{Ind}\,\cup \qquad \vdash ([G_1] \sqsupset ([G_2] \sqsupset [G_1 \cup G_2]))$$

$$\mathsf{Ind}\,\setminus \qquad \vdash ([G] \equiv [Q \setminus G])$$

## Axioms (cont)

Empty $\quad \vdash (\langle \emptyset | \emptyset \rangle = 1)$

NAdm $\quad \vdash \left( \left( \neg \left( \bigwedge_{G} F \right) \right) \sqsupset (\langle F | G \rangle = 0) \right)$

Unit $\quad \vdash \left( [G] \sqsupset \left( \left( \sum_{F \subseteq G} |\langle F | G \rangle|^2 \right) = 1 \right) \right)$

Prod $\quad \vdash (([G_1] \sqcap [G_2]) \sqsupset (\langle F_1 \cup F_2 | G_1 \cup G_2 \rangle = (\langle F_1 | G_1 \rangle \langle F_2 | G_2 \rangle)))$

provided that $G_1 \cap G_2 = \emptyset$

## Axioms (conc)

$$\text{If tt} \qquad \vdash (\alpha \sqsupset ((\alpha \rhd u_1;\ u_2) = u_1))$$

$$\text{If ff} \qquad \vdash ((\boxminus \alpha) \sqsupset ((\alpha \rhd u_1;\ u_2) = u_2))$$

$$\text{Prob} \qquad \vdash \left( \left( \int \alpha \right) = \sum_{F \subseteq Q} |\langle F \sqsupset \alpha | Q \rangle|^2 \right)$$

## Metatheorems

- MTD:

$$\Gamma, \gamma_1 \vdash \gamma_2 \text{ iff } \Gamma \vdash (\gamma_1 \sqsupset \gamma_2).$$

- MTRA:

$$\text{If } \Gamma, \gamma \vdash \mathbb{F} \text{ then } \Gamma \vdash (\boxminus \gamma).$$

- PSQEF:

$$\vdash ((\gamma_1 \equiv \gamma_2) \sqsupset (\gamma \equiv \gamma'))$$

provided that $\gamma'$ is obtained by replacing zero or more q-occurrences of $\gamma_1$ by $\gamma_2$ in $\gamma$.

- PSCEF:

$$\vdash ((\alpha_1 \Leftrightarrow \alpha_2) \sqsupset (\gamma \equiv \gamma'))$$

provided that $\gamma'$ is obtained by replacing zero or more occurrences of $\alpha_1$ by $\alpha_2$ in $\gamma$.

# Main results

# Main results

**Conservativeness of the extension CPL $\hookrightarrow$ EQPL**

$$\models^{\mathsf{c}} \alpha \text{ iff } \models \alpha$$

**Soundness and completeness of EQPL**

$$\models \gamma \text{ iff } \vdash \gamma$$

**Decidability of EQPL**

$$\emptyset^{\vdash} \text{ is decidable}$$

Strong versions of these results also hold.

# Outline of the proof of weak completeness and decidability

## Fagin–Halpern–Megiddo technique (1990)

Originally proposed for a probabilistic logic (simpler than the probabilistic fragment of EQPL):

- Key idea:
  Reduce any formula to a disjunction of systems of linear inequations over the real numbers where each variable represents the probability of a classical molecular formula.
- Model exists iff at least one of the systems has a solution.
- Decidability results from the algorithmic nature of the model construction.

## What else was neeed for EQPL

Significant revamp of the FHM technique
in order to cope with the novel aspects of EQPL:

- non-deterministic semantics of quantum connectives;
- classical formulae mixed with arithmetic (in)equations and non-entanglement constraints;
- amplitude terms besides probability terms;
- quantum structures instead of probability spaces.

Maximal extension technique used thrice:

- for removing alternative terms;
- for constructing the set $V$ of admissible valuations;
- for building the partition $\mathcal{S}$ of the set $Q$ of qubits.

# Further developments and practical impact

# Extensions and probabilistic ramifications

## Dynamics of quantum systems

- Linear-time temporal EQPL.
- Branching-time temporal EQPL.
- Hoare calculus over EQPL.

QM Postulate 5 (discrete case)
*Excluding measurements, each state transition of an isolated quantum system is described by a unitary transformation.*

## Dynamics of probabilistic systems

Unexpected significant contribution to the field of verification of probabilistic imperative programs (Hoare calculus).

# Applications

## Model checking of quantum protocols

- Warwick quantum model checker.
- Linear-time temporal extension of EQPL.
- Subspace of stabilizer states in $\mathcal{H}^{\mathcal{K}^\bullet}(2^Q)$.

S. J. Gay, R. Nagarajan, and N. Papanikolaou,
*QMC: A model checker for quantum systems*.
Proceedings of the 20th International Conference on Computer Aided Verification (**CAV'08**), Princeton, USA. A. Gupta and S. Malik, editors. Vol. 5123 LNCS, Springer, 2008, pp. 543–547.

# Outlook

## Ongoing and future work on quantum logic

- Axiomatization of stabilizer semantics.
- Quantum Hoare calculus over density operators.
- More general extensions for reasoning about the dynamics of quantum systems.
- Linear algebra techniques in classical, non-deterministic, probabilistic and quantum program verification.
- Planning
  under (probabilistic or quantum) uncertainty.
- Knowledge representation
  with (probabilistic or quantum variants of) description logic.
- FOL theory of quantum systems.

## Ongoing and future work (not directly related but maybe still worth mentioning here)

- Kolmogorov complexity of computable functions.
- Quantum Turing machines with classical control.
- Robust notions of:
  - quantum universal function;
  - quantum Kolmogorov complexity.
- Applications to distinguishability of quantum states.
- Quantum Kolmogorov complexity of computable unitary transformations.
- Quantum Turing reducibility.

# Sources

## For more details on EQPL

- P. Mateus and A. Sernadas, *Weakly complete axiomatization of exogenous quantum propositional logic*, **Information and Computation**, vol. 204 (2006), no. 5, pp. 771–794.
- R. Chadha, P. Mateus, A. Sernadas, and C. Sernadas, *Extending classical logic for reasoning about quantum systems*, **Handbook of Quantum Logic and Quantum Structures: Quantum Logic** (D. Gabbay K. Engesser and D. Lehmann, editors), Elsevier, 2009, pp. 325–372.