

Decidable Quantum Reasoning

Rohit Chadha, Paulo Mateus, Amilcar Sernadas and Cristina Sernadas

Security and Quantum Information Group (SQIG)
IT and IST, Portugal

<http://wslc.math.ist.utl.pt/ftp/pub/SernadasA/05-CMSS-quantlog07.pdf>

Exogenous Quantum Propositional Logic

Quantum security

- Quantum adversary – factorization, discrete log, Shor 97.
- Quantum protocols – key distribution, Bennett & Brassard 84.

Traditional quantum logic – Birkhoff & von Neumann 36

- New propositional connectives.
- Qualitative reasoning only.

The exogenous semantics approach – EQPL

P. Mateus & A. Sernadas, *Inf. & Comp.* 06

- Quantum logic as an extension of classical logic.
- Quantum model = superposition of classical models!
- Quantitative reasoning about amplitudes and probabilities.
- Inspired by probabilistic logics (Nilsson 86, Fagin & Halpern & Megiddo 90, ...).

Quantum mechanics

Postulate 1

The state space of an isolated quantum system is the surface of the unit sphere of a Hilbert space.

- Classical system – n-bit system has 2^n states (valuations).
- Quantum system (superposition principle) – state of a n-qubit system is a unit vector in \mathbb{C}^{2^n} . The coordinates are called *amplitudes*.

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.

- Amplitudes multiply.

EQPL

P. Mateus & A. Sernadas, *Inf. & Comp.* 06
Design

- Model is superposition of 2^n possible valuations.
- Components modeled as partitions of qubits in the model. Language contains sub-system formulas for components.
- Models contain amplitudes of component systems. Terms in language representing amplitudes.

Completeness

- Completeness achieved relative to an undecidable oracle.
- Oracle used to reason about real computable numbers and exponential functions.

Decidability

R. Chadha, P. Mateus, C. Sernadas & A. Sernadas

To appear in Handbook of Quantum Logic

- Restrict language (drop real computable numbers and exponential functions).
- Replace Oracle by decision procedure for real closed fields. Inspired by Fagin & Halpern & Megiddo 90.
- $O(\mu^{2^{2^n}}, 2^{O(2^{2^n})})$ – μ is the complexity of the formula.
- Currently working on efficient sub-logics.

Towards Dynamic EQPL

Sound Hoare logic

R. Chadha, P. Mateus & A. Sernadas, MFPS 06

- Designed using the remaining postulates of quantum mechanics that govern observation and evolution of quantum systems.
- Verified toy examples – quantum one-time pad and quantum teleportation.