Towards a quantum probabilistic logic

Carlos Tavares

High-Assurance Software Laboratory/INESC TEC

ctavares@inesctec.pt

January 12, 2018

Overview

Quantum logic

- Quantum logic was firstly published in 1936 [Birkhoff and Von Neumann, 1936]
- Objects are results of experiments in quantum physics
  - p = "the particle has momentum in the interval [0, +1/6]"
  - q = "the particle is in the interval [1, 1]"
  - r = "the particle is in the interval [1, 3]"
  - p and (q or r) = true
  - (p and q) or (p and r) = false
- Propositions p correspond to subsets of the phase space
  - In the case of quantum physics the phase space is the Hilbert space, and the possible results correspond to Closed linear subspaces, as observables correspond to Hermitic operators $(O = O^\dagger)$

Quantum logic

- Measurements are projections
- A logic can be built upon algebraic operations over such spaces (unions, intersections, complements)

$$\varphi ::= p \mid \perp \mid \sim \varphi \mid \varphi \wedge \varphi \mid \varphi \sqcup \varphi \tag{1}$$

- The main issue is *Complentarity*: the Measurement of the system changes the system state
    - The lattice of propositions is not distributive, hence no natural notion of implication

Quantum programs

What are quantum programs ?

$$p : H \to H \tag{2}$$

Restrictions:

- Transitions are unitary $U.U^{\dagger} = I$
- Measurements spoil the system state $O^{\dagger} = O$
- No cloning theorem - Quantum Information cannot be copied! $\cancel{x = y}$, $\cancel{x = x + 1}$

Advantages:

- Quantum parallelism!
  - $O\left|\Psi\right\rangle = O\sum_n \left|\Psi_n\right\rangle = O\left|\Psi_1\right\rangle + O\left|\Psi_2\right\rangle + \ldots + O\left|\Psi_n\right\rangle$

Quantum Dynamic logic

Dynamic logic: "The logic of Quantum Programs" Baltag & Smets [Baltag and Smets, 2004, Baltag et al., 2014]
Syntax:

$$\varphi ::= p|\varphi \vee \varphi|\neg\varphi|[\pi]\varphi|K_I\varphi|P^{\geq r}\varphi \tag{3}$$

$$\pi ::= unitary|\varphi?|\pi;\pi|\pi \cup \pi \tag{4}$$

(unitary includes Hadamard, CNOT, X, Y, Z, Rotational Gates, Toffoli gates)

Quantum Dynamic logic

Modalities:

- $[\pi]\varphi$ - φ holds on the successful execution of program π
- $K_I\varphi$ - φ holds in a sub-system of the current quantum state. This is what makes this logic an epistemic logic.
- $P^{\geq r}\varphi$ - The condition φ holds with a probability greater than r. This is what makes the logic a probabilistic one.

$\perp ::= \varphi \wedge \neg\varphi$	$< \pi > \varphi := \neg[\pi]\neg\varphi$	$A\varphi := \neg E \neg\varphi$
$\top := \neg\perp$	$\diamond\varphi :=< \varphi? > \top$	$p^{<R}\varphi := \neg p^{\geq r}\varphi$
$\sim \varphi := [\varphi?]\perp$	$:= \neg \diamond \neg\varphi$	$p^{>r}\varphi := \neg p^{\leq R}\varphi$
$\varphi \sqcup \psi :=\sim (\sim \varphi \wedge \sim \psi)$	$E\varphi := \diamond\diamond\varphi$	$p\varphi$
$\varphi \vee \psi := \neg(\neg\varphi \wedge \neg\psi)$	$p^{\leq r}\varphi := p^{>(1-r)} \sim \varphi$	
$[\phi?^{\geq r}]\psi := p^{\geq r}\varphi \to [\varphi?]\psi$	$\varphi \to \psi := \neg(\varphi \wedge \neg\psi)$	

Quantum Dynamic logic

Semantics:

- Modalities
  - $[\![p]\!]$ - $[\![p]\!] \subseteq \Sigma$, corresponds to a closed linear subspace of H
  - $[\![\varphi \vee \Psi]\!]$ - $s \in [\![\varphi \vee \Psi]\!]$ iff either $s \in [\![\varphi]\!]$, or $s \in [\![\Psi]\!]$ so that $[\![\varphi \vee \Psi]\!] = [\![\varphi]\!] \cup [\![\Psi]\!]$
  - $[\![\neg\varphi]\!]$ - $s \in [\![\neg\varphi_q]\!]$ iff $s \notin [\![\varphi_q]\!]$, so that $[\![\neg\varphi_q]\!] = \Sigma \backslash [\![\varphi_q]\!]$, the Boolean complement of $[\![\varphi_q]\!]$
  - $[\![[\varphi?]\Psi]\!]$ - $\{s | Proj_{[\![\phi]\!]}(v) \in [\![\bar{\Psi}]\!]$ for all $v \in s\} = \widetilde{Proj_{[\![\varphi]\!]}}[[\![\bar{\varphi}]\!]]$
  - $[\![[\varphi?]\Psi]\!]$ - $\neg[\![\varphi]\!] \sqcup ([\![\varphi]\!] \cap [\![\Psi]\!])$

Quantum Dynamic logic

- $[\![K_I\varphi]\!] \Longleftrightarrow t \in [\![\varphi]\!]$, for every $t \sim_I s \Longleftrightarrow U(s) \in [\![\varphi]\!]$ for every I-Remote U
  - Indistinguishability:

$$s{\sim}_I t \Longleftrightarrow s_I = t_I \Longleftrightarrow tr_{N/I}(p_v) = tr_{N/I}(p_w) \qquad (5)$$

    for unitary $w, v \in t$
  - Indistinguishability (I-Remote):

$$s{\sim}_I t \Longleftrightarrow t = U(s) \qquad (6)$$

    for some I-remote U $(U : H \to H, U = Id_I \otimes U_{N/I})$
- $[\![P^r\varphi]\!]$ - $\langle v|Proj_{[\![\varphi]\!]}|v\rangle \geq r$ for all unit vectors $v \in s$

Quantum Dynamic logic

Quantum programs: $[\![u]\!]$ - $[\![u]\!] : \Sigma \to \Sigma$, corresponds to a unitary transformation in H

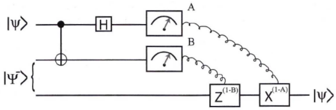
- Dynamic Modalities
  - $[\![[\pi_q]\varphi_q]\!]$ - $s \in [\![[\pi_q]\varphi_q]\!] \iff t \in [\![\varphi]\!]$ whenever $s \xrightarrow{\pi} t$
  - $s \xrightarrow{[\![u]\!]} t = \{s | [\![u]\!](s) \in [\![\varphi]\!]\} = [\![u]\!]^{-1}[\![\varphi]\!]$
  - $s \xrightarrow{[\![\varphi_q?]\!]} t = \{s | Proj_{[\![\varphi]\!]}(v) \in [\![\Psi]\!]$ for all $v \in s\}$
  - $s \xrightarrow{[\![\pi_q;\pi_q]\varphi_q]\!]} t = [\![[\pi_1][\pi_2]\varphi]\!]$
  - $s \xrightarrow{[\![\pi_q \cup \pi_q]\!]} t = [\![[\pi_1]\varphi \wedge [\pi_2]\varphi]\!]$

Quantum Dynamic logic

Hilbert Calculus

- Hilbert calculus is different between the two logics [Baltag and Smets, 2004], [Baltag et al., 2014]. Both are normal
- [Baltag and Smets, 2004] has characteristic axioms for quantum gates, entanglement, general quantum axioms

Proof of teleportation protocol



$$\pi = \bigcup_{x,y \in \{0,1\}} CNOT_{1,2}; H_1; (x_1 \wedge y_2)?; X_3^y; Z_3^x \tag{7}$$

$$\vdash \varphi_1 \wedge \beta_{00}^{2,3} \rightarrow [\pi]\varphi_3 \tag{8}$$

Quantum Dynamic logic

Proof:

$$
\begin{array}{l}
\vdash \varphi_1 \to \varphi_1 \\
\hline
\vdash \varphi_1 \to [Z_1^x; X_1^y; X_1^y; Z_1^x]\varphi_1 \\
\hline
\vdash \varphi_1 \wedge id_{2,3} \to [(Z_1^x; X_1^y)_{1,2}?]; [X_3^y; Z_3^x]\varphi_3 \\
\hline
\vdash \varphi_1 \wedge \beta_{00}^{2,3} \to \beta_{1,2}^{x,y}; [X_3^y; Z_3^x]\varphi_3 \\
\hline
\vdash \varphi_1 \wedge \beta_{00}^{2,3} \to [\bigcup_{x,y\in\{0,1\}} CNOT_{1,2}; H_1; (x_1 \wedge y_2)?; X_3^y; Z_3^x]\varphi_3
\end{array}
$$

Proof of Grover algorithm [Baltag et al., 2014]

$$
\begin{aligned}
QSA := {} & Ora(O) \wedge CState(p) \wedge A\left(p \wedge 0_n \to [O]1_n\right) \wedge A\left(p \wedge 1_n \to [O]0_n\right) \wedge \underline{\mathbf{0}} \wedge 1_n \\
& \to [H_0; \cdots; H_n][O; H_0; \cdots; H_{n-1}; P; H_0; \cdots; H_{n-1}]^k P^{>0.5} p.
\end{aligned}
$$

The quantum probabilistic logic

Objective:

Design a logic that can reason about actual quantum-probabilistic programs in practice

Motivation:

Quantum algorithms may require classical post-processing. Example: Shor algorithm

State of the art:

Several logics for quantum programs: Adams [Adams et al., 2014], Ying [Ying, 2011], Mateus [Mateus and Sernadas,]
Baltag & Smets [Baltag et al., 2014]

The quantum probabilistic logic

Phases are an issue?

- The phase is necessary to reason about the Shor algorithm: Rotational gates
- Global and local phases

$$|\Psi\rangle = -|\Psi\rangle\,; |0\rangle + |1\rangle \neq |0\rangle - |1\rangle\,; \tag{9}$$

- Phase arithmetics

$$e^{i\theta_1} * e^{i\theta_2} = e^{i\theta_1 + \theta_2} \tag{10}$$

- Deal with limits (wishfull thinking) $\sum_0^\infty e^{i\theta} = e^{i\phi}$

A possible solution is to adopt a simpler logic targeted to deal with the known structures in quantum algorithms!

The quantum probabilistic logic ii

A dynamic logic for quantum-probabilistic programs (combine with [Kozen, 1981]):
A programming language:

$$term ::= const | var | var + var | var * var | var - var | var / var$$

$$\pi_p ::= x := term | x := rnd | x := meas(\pi_q) | (\varphi_p?) | \pi_p ; \pi_p | a\pi_p + b\pi_p | \pi_p *$$

$$\pi_q ::= unitary | \varphi_q ? | \pi_q ; \pi_q | \pi_q \cup \pi_q$$

The quantum probabilistic logic ii

Modalities

$$\varphi_p ::= f|\varphi_p + \varphi_p|r\varphi_p| < \pi_p > \varphi_p|\varphi_p.\varphi_p \tag{11}$$

$$\phi_p = \varphi_p <= \varphi_p|\varphi_p \to \varphi_p \tag{12}$$

$$\varphi_q ::= p_q|\varphi_q \vee \varphi_q|\neg\varphi_q|[\pi]\varphi_q|K_I\varphi_q|P^{\geq r}\varphi_q \tag{13}$$

Interactions between modalities?

The quantum probabilistic logic ii

Logic is hierarchic?
What if the language was something as follows:

$$\pi ::= g_q | (x := term)_p | (x := rnd)_p | (\varphi?)_{p,q} | (\pi)_{p,q}; (\pi)_{p,q} | \pi_{q,p} \cup \pi_{q,p} \tag{14}$$

i.e. if both processes could interact with each other? Could we model noise with this?

Conclusions

Potential applications

- Quantum algorithms always involve interaction with the classical world. Ex: Shor algorithm
- A quantum-probabilistic logic may be used in quantum processes that involve noise

Future interesting lines of work:

- Find software tools to make this logic applicable in practice
- Use Higher-order categories in the probabilistic side. Inspiration: [Heunen et al., 2017]
- Use quantitative reasoning in dealing with language developed in this work. Inspiration: [Mardare et al., 2016]

References I

Adams, R., Alpàr, G., Balasch Masoliver, J., Batina, L., Chmielewski, Ł., Papachristodoulou, L., Schwabe, P., Tunstall, M., Batina, L., Hermans, J., et al. (2014).
Qpel: Quantum program and effect language.
In *QPL 2014: Proceedings 11th workshop on Quantum Physics and Logic*, volume 1, pages 236–252. EPTCS.

Baltag, A., Bergfeld, J., Kishida, K., Sack, J., Smets, S., and Zhong, S. (2014).
Plqp & company: Decidable logics for quantum algorithms.
International Journal of Theoretical Physics, 53(10):3628–3647.

Baltag, A. and Smets, S. (2004).
The logic of quantum programs.
Proc. QPL, pages 39–56.

References II

Birkhoff, G. and Von Neumann, J. (1936).
The logic of quantum mechanics.
Annals of mathematics, pages 823–843.

Heunen, C., Kammar, O., Staton, S., and Yang, H. (2017).
A convenient category for higher-order probability theory.
arXiv preprint arXiv:1701.02547.

Kozen, D. (1981).
Semantics of probabilistic programs.
Journal of computer and system sciences, 22(3):328–350.

Mardare, R., Panangaden, P., and Plotkin, G. (2016).
Quantitative algebraic reasoning.
In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 700–709. ACM.

References III

Mateus, P. and Sernadas, A.
Reasoning about quantum systems.
Springer.

Ying, M. (2011).
Floyd–hoare logic for quantum programs.
ACM Transactions on Programming Languages and Systems (TOPLAS), 33(6):19.

Questions ?