Axiomatizing Probabilistic Logic of Quantum Programs

Jort Bergfeld and Joshua Sack

Amsterdam, 2014 April 1

Motivation and Background

Quantum Algorithms and Protocols: use logic for a better understanding.

Probabilistic Logic of Quantum Programs

We involve a logic that expresses

- probabilities of outcomes of quantum tests
- effects of quantum tests and unitary operations
- separation operations that characterize subsystems.

and is decidable: PLQP & company by Baltag et al 2014

In this talk, we

- provide a sound proof system
- use it to prove that "leader election protocol" is correct

Structures for reasoning about quantum systems

Hilbert spaces are commonly used:

- Quantum states are one-dimensional subspaces.
- Probabilities of outcomes of tests characterized by inner product of vector representatives of the states $\frac{|\langle x,y\rangle|^2}{|x||y|}$.
- Composite systems are constructed from the tensor product of Hilbert spaces (subsystems)

In this talk, we

- Involve finite dimensional Hilbert spaces
- Build each structure from the set of states for a basis of the Hilbert space
- Involve agents, each corresponding to a basis of a *subsystem*

Bases and states

Let $\mathcal{H}$ be a Hilbert space with an orthonormal basis

$$\vec{B} = \{\vec{b_1}, \ldots, \vec{b_n}\}.$$

For every state (one dimensional space) s, there is a unit vector $\vec{s}$ in state s, such that

1. there exists an $i \in N$ such that
   1. $\langle \vec{s}, \vec{b_j} \rangle = 0$ for all $j < i$, and
   2. $\langle \vec{s}, \vec{b_i} \rangle \in (0, 1]$,
2. $|\langle \vec{s}, \vec{b_k} \rangle|^2 \in [0, 1]$, and
3. $\sum_{k \in N} |\langle \vec{s}, \vec{b_k} \rangle|^2 = 1$.

The function $\langle \vec{s}, \cdot \rangle : \vec{B} \to \mathbb{C}$ characterizes s.

The function $|\langle \vec{s}, \cdot \rangle|^2 : \vec{B} \to [0, 1]$ is a probability mass function.

Complex probability mass function

$B = \{b_i \mid i \in N\}$ a finite totally ordered set (called basis states).

$f : B \to \mathbb{C}$ is called a complex probability mass function on B if

1. there exists an $i \in N$ such that
   1. $f(b_j) = 0$ for all $j < i$, and
   2. $f(b_i) \in (0, 1]$,
2. $|f(b_k)|^2 \in [0, 1]$, and
3. $\sum_{k \in N} |f(b_k)|^2 = 1$.

F_B is the set of all complex probability mass functions on B.

Complex probability mass functions are states

Proposition

Given a set of basis states

$$B = \{b_1, \ldots, b_n\}$$

there is a Hilbert space $\mathcal{H}$ *with orthonormal basis*

$$\{\vec{b}_1, \ldots, \vec{b}_n\}$$

such that for any complex probability mass function $s : B \to \mathbb{C}$, *there is a vector* $\vec{s}$, *such that for each* i, $s(b_i) = \langle \vec{s}, \vec{b}_i \rangle$.

As the complex probability mass function s uniquely identifies the state (one dimensional subspace) generated by $\vec{s}$, we identify s with that state.

Generating structure from F_B

Define $S := F_B$ (all complex probability mass functions)

- inner product $\mu(s,t) := \sum_{i \in n} s(b_i)\overline{t(b_i)}$ for all $s, t \in S$, $\overline{z}$ is the complex conjugate of $z \in \mathbb{C}$
- nonorthogonality relation $R = \{(s,t) \in S \times S \mid \mu(s,t) \neq 0\}$,
- orthocomplement $\sim X := \{s \in S \mid (s,x) \notin R \text{ for all } x \in X\}$, for any set $X \subseteq S$,
- testable properties $\mathcal{T} := \{P \subseteq S \mid P = \sim\sim P\}$,
- P-test relation $R_P := \{(s,t) \in R \mid t \in P \text{ and } |\mu(s,u)|^2 \leq |\mu(s,t)|^2 \text{ for all } u \in P\}$,
- unitary operators $\mathcal{U} := \{U : S \to S \mid U \text{ is a permutation and } \mu(s,t) = \mu(Us, Ut) \text{ for all } s, t \in S\}$,
- unitary relation $R_U := \{(s,t) \in S \times S \mid t = Us\}$.

Tensor product

Definition (Tensor product)

The tensor product of state bases $B = \{b_1, \ldots, b_n\}$ and $C = \{c_1, \ldots, c_m\}$ is

$$B \otimes C = \{b_i c_j \mid b_i \in B, c_j \in C\}$$

The elements of $B \otimes C$ are totally ordered by the dictionary order.

Separability

Definition (Separable and entangled states)

A complex probability mass function $f \in F_{B\otimes C}$ is separable (into B and C) if there exist $s \in F_B$ and $t \in F_C$, such that $f(bc) = s(b)t(c)$ for all $b \in B$ and $c \in C$. We write $f = s \otimes t$.

If f is not separable we call f entangled.

Definition (Separable Unitaries)

A unitary operator U if $F_{B\otimes C}$ is separable if there exists unitaries U_B and U_C, such that for all $s \in F_B$ and $t \in F_C$, $U(s \otimes t) = U_B(s) \otimes U_C(t)$. We then write $U = U_B \otimes U_C$.

Multi-agent models

Let $\mathcal{A} = \{0, 1, \ldots, N-1\}$ be a finite set of agents.
Let Prop be a set of atomic propositions.

Definition (multi-agent probabilistic quantum model (PQM))

- An $\mathcal{A}$-PQF (probabilistic quantum frame) is a pair $F = (B, \{B_i\}_{i \in \mathcal{A}})$, where B is a basis of states and B_i is a two-state basis for each $i \in \mathcal{A}$, such that $B = \bigotimes_{i \in \mathcal{A}} B_i$.
- Then an $\mathcal{A}$-PQM (probabilistic quantum model) is a pair (F, V), such that $F = (B, \{B_i\}_{i \in \mathcal{A}})$ is an $\mathcal{A}$-PQF and $V : \text{Prop} \to \mathcal{P}(F_B)$ is a valuation.

Given a subset $I \subseteq \mathcal{A}$ of agents, let

- $B_I = \bigotimes_{i \in I} B_i$
- $S_I = F_{B_I}$
- If s is separable over B_I and $B_{\mathcal{A} \setminus I}$, let s_I denote the complex probability mass function such that there exists $s_{\mathcal{A} \setminus I}$ such that $s = s_I \otimes s_{\mathcal{A} \setminus I}$.

Language

Let $\mathcal{A} = \{0, 1, \ldots, N-1\}$ be a finite set of agents.
Let Prop be a (countable) set of atomic propositions.

$$\phi ::= \top_I \mid p \mid t \geq \rho \mid \neg\phi \mid \phi \wedge \phi \mid \Box\phi \mid [\alpha]\phi$$
$$\alpha ::= \top_I \mid \phi? \mid U \mid U^\dagger \mid \alpha \cup \alpha \mid \alpha; \alpha$$
$$t ::= \rho \Pr(\phi) \mid t + t$$

where $p \in \text{Prop}$, $U \in \mathcal{U}$, $I \subseteq \mathcal{A}$ and $\rho \in \mathbb{R}$.

- Language "$\mathcal{L}$" is defined to the the set of all such ϕ
- Set "Terms" is defined to be the set of all terms t

$\top_I$ means "I-separable"
$[\top_I]$ ranges over the "I-subsystem" (is equivalent to $K_{\mathcal{A}\setminus I}$)

Semantics

Let $((B, \{B_i\}_{i\in\mathcal{A}}), V)$ be an $\mathcal{A}$-PQM, and let $S = F_B$. We define

- an extended valuation $[\![\cdot]\!] : \mathcal{L} \to \mathcal{P}S$, and
- for each $s \in S$, $[\![\cdot]\!]_s$: Terms $\to \mathbb{R}$:

$$
\begin{aligned}
[\![\top_I]\!] &:= \{s \in S \mid s = s_I \otimes s_{\mathcal{A}\setminus I} \text{ for some } s_I \in S_I \text{ and } s_{\mathcal{A}\setminus I} \in S_{\mathcal{A}\setminus I}\},\\
[\![p]\!] &:= V(p),\\
[\![t \geq \rho]\!] &:= \{s \in S \mid [\![t]\!]_s \geq \rho\}\\
[\![\neg\phi]\!] &:= S \setminus [\![\phi]\!],\\
[\![\phi \wedge \psi]\!] &:= [\![\phi]\!] \cap [\![\psi]\!],\\
[\![\Box\phi]\!] &:= \{s \in S \mid R(s) \subseteq [\![\phi]\!]\} \text{ (R is non-orthogonality relation)}\\
[\![[\alpha]\phi]\!] &:= \{s \in S \mid R_\alpha(s) \subseteq [\![\phi]\!]\} \text{ (R_α is defined on next slide).}\\
[\![\rho\,\mathrm{Pr}(\phi)]\!]_s &:= \rho \sum_{t\in R_P(s)} |\mu(s,t)|^2, \text{ where } P = {\sim}{\sim}[\![\phi]\!],\\
[\![t_1 + t_2]\!]_s &:= [\![t_1]\!]_s + [\![t_2]\!]_s
\end{aligned}
$$

More semantics

Here R_α can be inductively defined by

$$
\begin{aligned}
R_{\top_I} &:= \{(s,t) \mid t = (U_I \otimes \mathrm{Id}_{\mathcal{A}\setminus I})(s) \text{ for some } U_I \in \mathcal{U}_I\},\\
R_{\phi?} &:= R_P, \text{ where } P = {\sim}{\sim}[\![\phi]\!],\\
R_U &:= R_U,\\
R_{U^\dagger} &:= R_U^c,\\
R_{\alpha\cup\beta} &:= R_\alpha \cup R_\beta, \text{ and}\\
R_{\alpha;\beta} &:= R_\alpha ; R_\beta.
\end{aligned}
$$

Probabilistic abbreviations

$$
\begin{array}{lcl}
\sum_{k=1}^{n} a_k \Pr(\phi_k) & := & a_1 \Pr(\phi_1) + \cdots + a_n \Pr(\phi_n) \\
\rho \sum_{k=1}^{n} a_k \Pr(\phi_k) & := & \sum_{k=1}^{n} \rho a_k \Pr(\phi_k) \\
t < \rho & := & \neg t \geq \rho \\
t \leq \rho & := & -t \geq -\rho \\
t = \rho & := & t \geq \rho \wedge t \leq \rho \\
t_1 \geq t_2 & := & t_1 - t_2 \geq 0
\end{array}
$$

Abbreviations

$$
\begin{array}{lcll}
\sim\phi & := & \Box\neg\phi & \text{(orthocomplement)} \\
\phi \vee \psi & := & \neg(\neg\phi \wedge \neg\psi) & \text{(disjunction)} \\
\phi \sqcup \psi & := & \sim(\sim\phi \wedge \sim\psi) & \text{(quantum join)} \\
\mathsf{A}\phi & := & \Box\Box\phi & \text{(global universal)} \\
\mathsf{E}\phi & := & \Diamond\Diamond\phi & \text{(global existential)} \\
(\phi \leq \psi) & := & \mathsf{A}(\phi \to \psi) & \\
(\phi = \psi) & := & \mathsf{A}(\phi \leftrightarrow \psi) & \\
\phi \perp \psi & := & \phi \leq \sim\psi & \text{(orthogonal)} \\
T(\phi) & := & \sim\sim\phi = \phi & \text{(testable)} \\
\phi_I & := & \top_I \wedge \langle \top_{N\setminus I} \rangle \phi & (I\text{-component}) \\
\phi =_I \psi & := & (\phi \leq \top_I) \wedge (\psi \leq \top_I) \wedge (\phi_I = \psi_I) & (I\text{-equivalent}) \\
I(\phi) & := & (\phi = \phi_I) & (I\text{-local}) \\
\langle \phi? \rangle_{=\rho} \psi & := & \Pr(\phi) = \rho \wedge \langle \phi? \rangle \psi & \\
\langle \phi? \rangle_{>\rho} \psi & := & \Pr(\phi) > \rho \wedge \langle \phi? \rangle \psi &
\end{array}
$$

Example: Leader Election Protocol

Example

- Setting: There are N agents.
- Goal: Each should have an equal $(1/N)$ chance of being chosen to be the leader.
- Strategy: Prepare a quantum state that has equal probability of collapsing into any of N basis elements when measured.
- Solution: This state is the W-state in a 2^N-dimensional Hilbert space (a subsystem for each agent).
  - The basis for the 2^N-dimensional space is the product of the bases $\{0_k, 1_k\}$, for each of the N agents.
  - The k-th agent is associated with the basis element $\mathfrak{b}_k = (0_0 \otimes \cdots \otimes 0_{k-1} \otimes 1_k \otimes 0_{k+1} \otimes \cdots \otimes 0_{N-1})$.
  - The W-state is an equally weighted superposition of the $\mathfrak{b}_k$.

E. D'Hondt and P. Panangaden,
The Computational Power of the W and GHZ States,
Quantum Information and Computation 6 (2006), 173–83.

Expressing the Leader Election Protocol

Let $\mathcal{A} = \{0, 1, \ldots, N-1\}$ be a finite set of agents.

$$\text{Basis}(\mathcal{B}) := (\bigsqcup_{i \in 2^N} b_i = \top) \wedge \bigwedge_{i \neq j} (b_i \perp b_j).$$

$$\text{Separable}(\mathcal{B}) := \bigwedge_{i \in 2^N} (b_i \leq \bigwedge_{a \in \mathcal{A}} \top_a).$$

Let $\mathcal{W} = \{W_i \mid i \in \{0, \ldots, N\}\} \subseteq \mathcal{B}$.
Think of W_N as $(0_0 \otimes \cdots \otimes 0_{N-1})$.

$$\text{QLE}(\mathcal{W}) := \bigwedge_{a \in \mathcal{A}} \left[((W_a)_a \neq_a (W_N)_a) \wedge \bigwedge_{b \in \mathcal{A} \setminus a} ((W_a)_b =_b (W_N)_b) \right].$$

The correctness of the quantum leader election is expressed by

$$\text{Basis}(\mathcal{B}) \wedge \text{Separable}(\mathcal{B}) \wedge \text{QLE}(\mathcal{W}) \rightarrow \text{E} \bigwedge_{a \in \mathcal{A}} (\Pr(W_a) = \frac{1}{N}).$$

Duality result

Theorem

Each quantum dynamic frame is dual to a Piron lattice.

A quantum dynamic frame is a special Kripke frame that satisfies

- Atomicity,
- Intersection,
- Orthocomplement,
- Adequacy,
- Repeatability,
- Partial functionality,
- Self-adjointness,
- Proper superposition,
- Cover law.

Duality result

Theorem

Each quantum dynamic frame is dual to a Piron lattice.

A quantum dynamic frame is a special Kripke frame that satisfies

- Atomicity,
- Intersection,
- Orthocomplement,
- Adequacy,
- Repeatability,
- Partial functionality,
- Self-adjointness,
- Proper superposition,
- Cover law.

Some axioms

We base some axioms on the properties of quantum dynamic frame.

Adequacy

For all $P \in \mathcal{T}$ and for all $s \in P$ we have $s \xrightarrow{P?} s$.

$$p \to (q \to \langle p? \rangle q)$$

Orthocomplement

$s \in {\sim}P$ iff $s \nrightarrow t$ for all $t \in P$.

$$\langle p? \rangle \top \leftrightarrow \Diamond p \qquad (= \neg{\sim}p)$$

Some axioms

We base some axioms on the properties of quantum dynamic frame.

Adequacy

For all $P \in \mathcal{T}$ and for all $s \in P$ we have $s \xrightarrow{P?} s$.

$$p \to (q \to \langle p? \rangle q)$$

Orthocomplement

$s \in {\sim}P$ iff $s \nrightarrow t$ for all $t \in P$.

$$\langle p? \rangle \top \leftrightarrow \Diamond p \qquad (= \neg{\sim}p)$$

Some rules

1. $\phi, \phi \to \psi \implies \psi$ *Modus ponens*
2. $\phi \implies [\alpha]\phi, \Box\phi$ *Necessitation*
3. $\phi \to [p?]\psi \implies \phi \to \Box\psi$ if $p \notin \phi, \psi$
4. $\phi \implies \phi^\sigma$ *Uniform substitution*
   for some $\sigma : \text{Prop} \to \mathcal{L}$

$$\Box(p \to q) \to (\Box p \to \Box q)$$

Reflexivity

Lemma

$$\vdash p \to \Diamond p \qquad (p \to \neg\sim p)$$

Proof.

1. $p \to (\top \to \langle p? \rangle \top)$
2. $\langle p? \rangle \top \leftrightarrow \Diamond p$
3. $p \to \langle p? \rangle \top$
4. $p \to \Diamond p$

Reflexivity

Lemma

$$\vdash p \to \Diamond p \qquad (p \to \neg\sim p)$$

Proof.

1. $p \to (\top \to \langle p? \rangle \top)$
2. $\langle p? \rangle \top \leftrightarrow \Diamond p$
3. $p \to \langle p? \rangle \top$
4. $p \to \Diamond p$

Reflexivity

Lemma

$$\vdash p \to \Diamond p \qquad (p \to \neg\sim p)$$

Proof.

1. $p \to (\top \to \langle p? \rangle \top)$
2. $\langle p? \rangle \top \leftrightarrow \Diamond p$
3. $p \to \langle p? \rangle \top$
4. $p \to \Diamond p$

Reflexivity

Lemma

$$\vdash p \to \Diamond p \qquad (p \to \neg\sim p)$$

Proof.

1. $p \to (\top \to \langle p? \rangle \top)$
2. $\langle p? \rangle \top \leftrightarrow \Diamond p$
3. $p \to \langle p? \rangle \top$
4. $p \to \Diamond p$

Quantum join with orthocomplement

Lemma

$$\vdash \sim(p \wedge \sim p)$$

Proof.

1. $p \to \neg\sim p$
2. $(p \wedge \sim p) \to (\neg\sim p \wedge \sim p)$
3. $(p \wedge \sim p) \to \bot$
4. $\neg(p \wedge \sim p)$
5. $\Box\neg(p \wedge \sim p)$
6. $\sim(p \wedge \sim p)$

Quantum join with orthocomplement

Lemma

$$\vdash \sim(p \wedge \sim p)$$

Proof.

1. $p \to \neg\sim p$
2. $(p \wedge \sim p) \to (\neg\sim p \wedge \sim p)$
3. $(p \wedge \sim p) \to \bot$
4. $\neg(p \wedge \sim p)$
5. $\Box\neg(p \wedge \sim p)$
6. $\sim(p \wedge \sim p)$

Quantum join with orthocomplement

Lemma

$$\vdash \sim(p \wedge \sim p)$$

Proof.

1. $p \to \neg\sim p$
2. $(p \wedge \sim p) \to (\neg\sim p \wedge \sim p)$
3. $(p \wedge \sim p) \to \bot$
4. $\neg(p \wedge \sim p)$
5. $\Box\neg(p \wedge \sim p)$
6. $\sim(p \wedge \sim p)$

Quantum join with orthocomplement

Lemma

$$\vdash \sim(p \wedge \sim p)$$

Proof.

1. $p \to \neg\sim p$
2. $(p \wedge \sim p) \to (\neg\sim p \wedge \sim p)$
3. $(p \wedge \sim p) \to \bot$
4. $\neg(p \wedge \sim p)$
5. $\Box\neg(p \wedge \sim p)$
6. $\sim(p \wedge \sim p)$

Quantum join with orthocomplement

Lemma

$$\vdash \sim(p \wedge \sim p)$$

Proof.

1. $p \to \neg\sim p$
2. $(p \wedge \sim p) \to (\neg\sim p \wedge \sim p)$
3. $(p \wedge \sim p) \to \bot$
4. $\neg(p \wedge \sim p)$
5. $\Box\neg(p \wedge \sim p)$
6. $\sim(p \wedge \sim p)$

Quantum join with orthocomplement

Lemma

$$\vdash \sim(p \wedge \sim p)$$

Proof.

1. $p \to \neg\sim p$
2. $(p \wedge \sim p) \to (\neg\sim p \wedge \sim p)$
3. $(p \wedge \sim p) \to \bot$
4. $\neg(p \wedge \sim p)$
5. $\Box\neg(p \wedge \sim p)$
6. $\sim(p \wedge \sim p)$

Some axioms

Partial functionality

If $s \xrightarrow{P?} t$ and $s \xrightarrow{P?} u$, then $t = u$.

$$\langle p? \rangle q \to [p?]q$$

Self-adjointness

If $s \xrightarrow{P?} t \to u$, then there exists a v such that $u \xrightarrow{P?} v \to s$.

$$p \to [q?]\Box\langle q? \rangle \Diamond p$$

Some axioms

Partial functionality

If $s \xrightarrow{P?} t$ and $s \xrightarrow{P?} u$, then $t = u$.

$$\langle p? \rangle q \to [p?]q$$

Self-adjointness

If $s \xrightarrow{P?} t \to u$, then there exists a v such that $u \xrightarrow{P?} v \to s$.

$$p \to [q?]\Box\langle q? \rangle \Diamond p$$

Symmetry

Lemma

$$\vdash p \to \Box\Diamond p \qquad (p \to {\sim}{\sim} p)$$

Proof.

1. $\top \to (p \to \langle \top ? \rangle p)$
2. $p \to \langle \top ? \rangle p$
3. $\langle \top ? \rangle p \to [\top ?] p$
4. $p \to [\top ?] p$
5. $[\top ?] p \to p$
6. $\langle \top ? \rangle p \to p$
7. $p \to [\top ?] \Box \langle \top ? \rangle \Diamond p$
8. $p \to \Box\Diamond p$

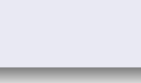
Symmetry

Lemma

$$\vdash p \to \Box\Diamond p \qquad (p \to {\sim}{\sim} p)$$

Proof.

1. $\top \to (p \to \langle \top ? \rangle p)$
2. $p \to \langle \top ? \rangle p$
3. $\langle \top ? \rangle p \to [\top ?] p$
4. $p \to [\top ?] p$
5. $[\top ?] p \to p$
6. $\langle \top ? \rangle p \to p$
7. $p \to [\top ?] \Box \langle \top ? \rangle \Diamond p$
8. $p \to \Box\Diamond p$



Symmetry

Lemma

$$\vdash p \to \Box\Diamond p \qquad (p \to {\sim}{\sim} p)$$

Proof.

1. $\top \to (p \to \langle \top ? \rangle p)$
2. $p \to \langle \top ? \rangle p$
3. $\langle \top ? \rangle p \to [\top ?] p$
4. $p \to [\top ?] p$
5. $[\top ?] p \to p$
6. $\langle \top ? \rangle p \to p$
7. $p \to [\top ?] \Box \langle \top ? \rangle \Diamond p$
8. $p \to \Box\Diamond p$

Symmetry

Lemma

$$\vdash p \to \Box\Diamond p \qquad (p \to {\sim}{\sim}p)$$

Proof.

1. $\top \to (p \to \langle \top ? \rangle p)$
2. $p \to \langle \top ? \rangle p$
3. $\langle \top ? \rangle p \to [\top ?] p$
4. $p \to [\top ?] p$
5. $[\top ?] p \to p$
6. $\langle \top ? \rangle p \to p$
7. $p \to [\top ?] \Box \langle \top ? \rangle \Diamond p$
8. $p \to \Box\Diamond p$

Symmetry

Lemma

$$\vdash p \to \Box\Diamond p \qquad (p \to {\sim}{\sim}p)$$

Proof.

1. $\top \to (p \to \langle \top ? \rangle p)$
2. $p \to \langle \top ? \rangle p$
3. $\langle \top ? \rangle p \to [\top ?] p$
4. $p \to [\top ?] p$
5. $[\top ?] p \to p$
6. $\langle \top ? \rangle p \to p$
7. $p \to [\top ?] \Box \langle \top ? \rangle \Diamond p$
8. $p \to \Box\Diamond p$

Symmetry

Lemma

$$\vdash p \to \Box\Diamond p \qquad (p \to {\sim}{\sim} p)$$

Proof.

1. $\top \to (p \to \langle \top ? \rangle p)$
2. $p \to \langle \top ? \rangle p$
3. $\langle \top ? \rangle p \to [\top ?] p$
4. $p \to [\top ?] p$
5. $[\top ?] p \to p$
6. $\langle \top ? \rangle p \to p$
7. $p \to [\top ?] \Box \langle \top ? \rangle \Diamond p$
8. $p \to \Box\Diamond p$

Symmetry

Lemma

$$\vdash p \to \Box\Diamond p \qquad (p \to {\sim}{\sim}p)$$

Proof.

1. $\top \to (p \to \langle \top ? \rangle p)$
2. $p \to \langle \top ? \rangle p$
3. $\langle \top ? \rangle p \to [\top ?] p$
4. $p \to [\top ?] p$
5. $[\top ?] p \to p$
6. $\langle \top ? \rangle p \to p$
7. $p \to [\top ?] \Box \langle \top ? \rangle \Diamond p$
8. $p \to \Box\Diamond p$

Symmetry

Lemma

$$\vdash p \to \Box\Diamond p \qquad (p \to {\sim}{\sim}p)$$

Proof.

1. $\top \to (p \to \langle \top ? \rangle p)$
2. $p \to \langle \top ? \rangle p$
3. $\langle \top ? \rangle p \to [\top ?] p$
4. $p \to [\top ?] p$
5. $[\top ?] p \to p$
6. $\langle \top ? \rangle p \to p$
7. $p \to [\top ?] \Box \langle \top ? \rangle \Diamond p$
8. $p \to \Box\Diamond p$

Axioms for basic single-agent PQM properties

M1	$\langle p? \rangle \phi \rightarrow \Diamond \phi$
M2	$\Diamond p \leftrightarrow \langle p? \rangle \top$
M3	$T(p) \rightarrow [p?]p$
M4	$T(p) \rightarrow \neg p \leftrightarrow \langle \sim p? \rangle \top$
M5	$\langle p? \rangle q \rightarrow [p?]q$
M6	$p \rightarrow (q \rightarrow \langle p? \rangle q)$
M7	$p \rightarrow [q?] \Box \langle q? \rangle \Diamond p$
M8	$\Diamond \Diamond \Diamond p \rightarrow \Diamond \Diamond p$
M9	$T(p) \wedge T(q) \wedge \Diamond p \wedge \Box(p \rightarrow \Diamond(p \wedge q))] \rightarrow \langle p? \rangle q$
M10	$\langle U \rangle p \leftrightarrow [U]p$
M11	$p \leftrightarrow [U; U^{\dagger}]p$
M12	$p \leftrightarrow [U^{\dagger}; U]p$
M13	$\langle U \rangle \Diamond p \leftrightarrow \Diamond \langle U \rangle p$

Some provable formulas

1. $p \to \Diamond p \quad (p \to \neg\sim p)$
2. $p \to \Box\Diamond p \quad (p \to \sim\sim p)$
3. $T(\sim p) \quad (\sim\sim\sim p \to \sim p)$
4. $p \to p \sqcup q$
5. $(p \to q) \to (\sim q \to \sim p)$
6. $T(p) \wedge T(q) \to T(p \wedge q)$
7. $p \perp q \leftrightarrow q \perp p$
8. $r \perp p \wedge r \perp q \leftrightarrow r \perp (p \sqcup q)$

Some provable formulas

1. $p \to \Diamond p \quad (p \to \neg\sim p)$
2. $p \to \Box\Diamond p \quad (p \to \sim\sim p)$
3. $T(\sim p) \quad (\sim\sim\sim p \to \sim p)$
4. $p \to p \sqcup q$
5. $(p \to q) \to (\sim q \to \sim p)$
6. $T(p) \wedge T(q) \to T(p \wedge q)$
7. $p \perp q \leftrightarrow q \perp p$
8. $r \perp p \wedge r \perp q \leftrightarrow r \perp (p \sqcup q)$

Some provable formulas

1. $p \to \Diamond p \quad (p \to \neg\sim p)$
2. $p \to \Box\Diamond p \quad (p \to \sim\sim p)$
3. $T(\sim p) \quad (\sim\sim\sim p \to \sim p)$
4. $p \to p \sqcup q$
5. $(p \to q) \to (\sim q \to \sim p)$
6. $T(p) \wedge T(q) \to T(p \wedge q)$
7. $p \perp q \leftrightarrow q \perp p$
8. $r \perp p \wedge r \perp q \leftrightarrow r \perp (p \sqcup q)$

Some provable formulas

1. $p \to \Diamond p \quad (p \to \neg\sim p)$
2. $p \to \Box\Diamond p \quad (p \to \sim\sim p)$
3. $T(\sim p) \quad (\sim\sim\sim p \to \sim p)$
4. $p \to p \sqcup q$
5. $(p \to q) \to (\sim q \to \sim p)$
6. $T(p) \wedge T(q) \to T(p \wedge q)$
7. $p \perp q \leftrightarrow q \perp p$
8. $r \perp p \wedge r \perp q \leftrightarrow r \perp (p \sqcup q)$

Some provable formulas

1. $p \to \Diamond p \quad (p \to \neg\sim p)$
2. $p \to \Box\Diamond p \quad (p \to \sim\sim p)$
3. $T(\sim p) \quad (\sim\sim\sim p \to \sim p)$
4. $p \to p \sqcup q$
5. $(p \to q) \to (\sim q \to \sim p)$
6. $T(p) \wedge T(q) \to T(p \wedge q)$
7. $p \perp q \leftrightarrow q \perp p$
8. $r \perp p \wedge r \perp q \leftrightarrow r \perp (p \sqcup q)$

Some provable formulas

1. $p \to \Diamond p \quad (p \to \neg\sim p)$
2. $p \to \Box\Diamond p \quad (p \to \sim\sim p)$
3. $T(\sim p) \quad (\sim\sim\sim p \to \sim p)$
4. $p \to p \sqcup q$
5. $(p \to q) \to (\sim q \to \sim p)$
6. $T(p) \wedge T(q) \to T(p \wedge q)$
7. $p \perp q \leftrightarrow q \perp p$
8. $r \perp p \wedge r \perp q \leftrightarrow r \perp (p \sqcup q)$

Some provable formulas

1. $p \to \Diamond p \quad (p \to \neg\sim p)$
2. $p \to \Box\Diamond p \quad (p \to \sim\sim p)$
3. $T(\sim p) \quad (\sim\sim\sim p \to \sim p)$
4. $p \to p \sqcup q$
5. $(p \to q) \to (\sim q \to \sim p)$
6. $T(p) \wedge T(q) \to T(p \wedge q)$
7. $p \perp q \leftrightarrow q \perp p$
8. $r \perp p \wedge r \perp q \leftrightarrow r \perp (p \sqcup q)$

Axioms for inequalities

I1	$t \geq \beta \leftrightarrow t + 0P_a(\phi) \geq \beta$
I2	$\sum_{k=1}^{n} \alpha_k P_a(\phi_k) \geq \beta \rightarrow \sum_{k=1}^{n} \alpha_{j_k} P_a(\phi_{j_k}) \geq q\beta$ for any permutation $j_1, \ldots, j_n$ of $1, \ldots, n$
I3	$\sum_{k=1}^{n} \alpha_k P_a(\phi_k) \geq \beta \wedge \sum_{k=1}^{n} \alpha'_k P_a(\phi_k) \geq \beta' \rightarrow \sum_{k=1}^{n} (\alpha_k + \alpha'_k) P_a(\phi_k) \geq (\beta + \beta')$
I4	$t \geq \beta \leftrightarrow dt \geq d\beta$ if $d > 0$
I5	$t \geq \beta \vee t \leq \beta$
I6	$t \geq \beta \rightarrow t \geq \gamma$ if $\beta > \gamma$

Axioms for probabilities

1. $(\Pr(p) = 0) \leftrightarrow \sim p$
2. $(\Pr(p) > 0) \leftrightarrow \Diamond p$
3. $p \rightarrow (\Pr(p) = 1)$
4. $T(p) \rightarrow (p \leftrightarrow \Pr(p) = 1)$
5. *Orthocomplement*
   $(\Pr(p) = \rho) \leftrightarrow (\Pr(\sim p) = 1 - \rho)$
6. *Quantum join*
   $(p \perp q) \wedge (\Pr(p) = \rho) \wedge (\Pr(q) = \tau) \rightarrow (\Pr(p \sqcup q) = \rho + \tau)$
7. *Superposition*
   $Ep \wedge Eq \wedge (p \perp q) \rightarrow E\left[\langle p? \rangle_{=\rho} p \wedge \langle q? \rangle_{=1-\rho} q\right]$
8. $(p \leq q) \wedge \langle q? \rangle_{=\rho} (\Pr(p) = \tau) \rightarrow (\Pr(p) = \rho\tau)$

Axioms for probabilities

1. $(\Pr(p) = 0) \leftrightarrow \sim p$
2. $(\Pr(p) > 0) \leftrightarrow \Diamond p$
3. $p \rightarrow (\Pr(p) = 1)$
4. $T(p) \rightarrow (p \leftrightarrow \Pr(p) = 1)$
5. *Orthocomplement*
   $(\Pr(p) = \rho) \leftrightarrow (\Pr(\sim p) = 1 - \rho)$
6. *Quantum join*
   $(p \perp q) \wedge (\Pr(p) = \rho) \wedge (\Pr(q) = \tau) \rightarrow (\Pr(p \sqcup q) = \rho + \tau)$
7. *Superposition*
   $Ep \wedge Eq \wedge (p \perp q) \rightarrow E\left[\langle p? \rangle_{=\rho} p \wedge \langle q? \rangle_{=1-\rho} q\right]$
8. $(p \leq q) \wedge \langle q? \rangle_{=\rho} (\Pr(p) = \tau) \rightarrow (\Pr(p) = \rho\tau)$

Axioms for probabilities

1. $(\mathrm{Pr}(p) = 0) \leftrightarrow {\sim}p$
2. $(\mathrm{Pr}(p) > 0) \leftrightarrow \Diamond p$
3. $p \rightarrow (\mathrm{Pr}(p) = 1)$
4. $T(p) \rightarrow (p \leftrightarrow \mathrm{Pr}(p) = 1)$
5. *Orthocomplement*
   $(\mathrm{Pr}(p) = \rho) \leftrightarrow (\mathrm{Pr}({\sim}p) = 1 - \rho)$
6. *Quantum join*
   $(p \perp q) \wedge (\mathrm{Pr}(p) = \rho) \wedge (\mathrm{Pr}(q) = \tau) \rightarrow (\mathrm{Pr}(p \sqcup q) = \rho + \tau)$
7. *Superposition*
   $Ep \wedge Eq \wedge (p \perp q) \rightarrow E\left[\langle p? \rangle_{=\rho} p \wedge \langle q? \rangle_{=1-\rho} q\right]$
8. $(p \leq q) \wedge \langle q? \rangle_{=\rho} (\mathrm{Pr}(p) = \tau) \rightarrow (\mathrm{Pr}(p) = \rho\tau)$

Axioms for probabilities

1. $(\mathrm{Pr}(p) = 0) \leftrightarrow \sim p$
2. $(\mathrm{Pr}(p) > 0) \leftrightarrow \Diamond p$
3. $p \rightarrow (\mathrm{Pr}(p) = 1)$
4. $T(p) \rightarrow (p \leftrightarrow \mathrm{Pr}(p) = 1)$
5. *Orthocomplement*
   $(\mathrm{Pr}(p) = \rho) \leftrightarrow (\mathrm{Pr}(\sim p) = 1 - \rho)$
6. *Quantum join*
   $(p \perp q) \wedge (\mathrm{Pr}(p) = \rho) \wedge (\mathrm{Pr}(q) = \tau) \rightarrow (\mathrm{Pr}(p \sqcup q) = \rho + \tau)$
7. *Superposition*
   $Ep \wedge Eq \wedge (p \perp q) \rightarrow E\left[\langle p? \rangle_{=\rho} p \wedge \langle q? \rangle_{=1-\rho} q\right]$
8. $(p \leq q) \wedge \langle q? \rangle_{=\rho} (\mathrm{Pr}(p) = \tau) \rightarrow (\mathrm{Pr}(p) = \rho\tau)$

Axioms for probabilities

1. $(\Pr(p) = 0) \leftrightarrow \sim p$
2. $(\Pr(p) > 0) \leftrightarrow \Diamond p$
3. $p \rightarrow (\Pr(p) = 1)$
4. $T(p) \rightarrow (p \leftrightarrow \Pr(p) = 1)$
5. *Orthocomplement*
   $(\Pr(p) = \rho) \leftrightarrow (\Pr(\sim p) = 1 - \rho)$
6. *Quantum join*
   $(p \perp q) \wedge (\Pr(p) = \rho) \wedge (\Pr(q) = \tau) \rightarrow (\Pr(p \sqcup q) = \rho + \tau)$
7. *Superposition*
   $Ep \wedge Eq \wedge (p \perp q) \rightarrow E\left[\langle p? \rangle_{=\rho} p \wedge \langle q? \rangle_{=1-\rho} q\right]$
8. $(p \leq q) \wedge \langle q? \rangle_{=\rho} (\Pr(p) = \tau) \rightarrow (\Pr(p) = \rho\tau)$

Quantum leader election

Theorem

For all n and all sets of n proposition letters $\{p_1, \ldots, p_n\}$

$$\vdash \bigwedge_{i \leq n} Ep_i \wedge \bigwedge_{i<j \leq n} p_i \perp p_j \rightarrow E \bigwedge_{i \leq n} \Pr(b_i) = \frac{1}{n}$$

1. $Ep_1 \wedge Ep_2 \wedge (p_1 \perp p_2) \rightarrow E\left[(\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2})\right]$
2. $(p_1 \perp p_2) \wedge (\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}) \rightarrow (\Pr(p_1 \sqcup p_2) = 1)$
3. $T(p_1 \sqcup p_2) \rightarrow (\Pr(p_1 \sqcup p_2) = 1) \rightarrow p_1 \sqcup p_2$
4. $(p_3 \perp p_1) \wedge (p_3 \perp p_2) \rightarrow p_3 \perp p_1 \sqcup p_2$
5. $\Longrightarrow$
   $E\left[(\Pr(p_3) = \frac{1}{3}) \wedge \langle p_1 \sqcup p_2 ? \rangle_{=\frac{2}{3}}((\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}))\right]$
6. $p_1 \rightarrow p_1 \sqcup p_2$
7. $E\left[\bigwedge_{i \leq 3} \Pr(p_i) = \frac{1}{3}\right]$

Quantum leader election

Theorem

For all n and all sets of n proposition letters $\{p_1, \ldots, p_n\}$

$$\vdash \bigwedge_{i \leq n} Ep_i \wedge \bigwedge_{i<j \leq n} p_i \perp p_j \rightarrow E \bigwedge_{i \leq n} \Pr(b_i) = \frac{1}{n}$$

1. $Ep_1 \wedge Ep_2 \wedge (p_1 \perp p_2) \rightarrow E\left[(\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2})\right]$
2. $(p_1 \perp p_2) \wedge (\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}) \rightarrow (\Pr(p_1 \sqcup p_2) = 1)$
3. $T(p_1 \sqcup p_2) \rightarrow (\Pr(p_1 \sqcup p_2) = 1) \rightarrow p_1 \sqcup p_2$
4. $(p_3 \perp p_1) \wedge (p_3 \perp p_2) \rightarrow p_3 \perp p_1 \sqcup p_2$
5. $\Longrightarrow$
   $E\left[(\Pr(p_3) = \frac{1}{3}) \wedge \langle p_1 \sqcup p_2 ? \rangle_{=\frac{2}{3}} ((\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}))\right]$
6. $p_1 \rightarrow p_1 \sqcup p_2$
7. $E\left[\bigwedge_{i \leq 3} \Pr(p_i) = \frac{1}{3}\right]$

Quantum leader election

Theorem

For all n and all sets of n proposition letters $\{p_1, \ldots, p_n\}$

$$\vdash \bigwedge_{i \leq n} Ep_i \wedge \bigwedge_{i<j \leq n} p_i \perp p_j \rightarrow E \bigwedge_{i \leq n} \Pr(b_i) = \frac{1}{n}$$

1. $Ep_1 \wedge Ep_2 \wedge (p_1 \perp p_2) \rightarrow E\left[(\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2})\right]$
2. $(p_1 \perp p_2) \wedge (\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}) \rightarrow (\Pr(p_1 \sqcup p_2) = 1)$
3. $T(p_1 \sqcup p_2) \rightarrow (\Pr(p_1 \sqcup p_2) = 1) \rightarrow p_1 \sqcup p_2$
4. $(p_3 \perp p_1) \wedge (p_3 \perp p_2) \rightarrow p_3 \perp p_1 \sqcup p_2$
5. $\Longrightarrow$
   $E\left[(\Pr(p_3) = \frac{1}{3}) \wedge \langle p_1 \sqcup p_2 ? \rangle_{=\frac{2}{3}} ((\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}))\right]$
6. $p_1 \rightarrow p_1 \sqcup p_2$
7. $E\left[\bigwedge_{i \leq 3} \Pr(p_i) = \frac{1}{3}\right]$

Quantum leader election

Theorem

For all n and all sets of n proposition letters $\{p_1, \ldots, p_n\}$

$$\vdash \bigwedge_{i \leq n} Ep_i \wedge \bigwedge_{i<j \leq n} p_i \perp p_j \rightarrow E \bigwedge_{i \leq n} \Pr(b_i) = \frac{1}{n}$$

1. $Ep_1 \wedge Ep_2 \wedge (p_1 \perp p_2) \rightarrow E\left[(\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2})\right]$
2. $(p_1 \perp p_2) \wedge (\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}) \rightarrow (\Pr(p_1 \sqcup p_2) = 1)$
3. $T(p_1 \sqcup p_2) \rightarrow (\Pr(p_1 \sqcup p_2) = 1) \rightarrow p_1 \sqcup p_2$
4. $(p_3 \perp p_1) \wedge (p_3 \perp p_2) \rightarrow p_3 \perp p_1 \sqcup p_2$
5. $\Longrightarrow$
   $E\left[(\Pr(p_3) = \frac{1}{3}) \wedge \langle p_1 \sqcup p_2 ? \rangle_{=\frac{2}{3}} ((\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}))\right]$
6. $p_1 \rightarrow p_1 \sqcup p_2$
7. $E\left[\bigwedge_{i \leq 3} \Pr(p_i) = \frac{1}{3}\right]$

Quantum leader election

Theorem

For all n and all sets of n proposition letters $\{p_1, \ldots, p_n\}$

$$\vdash \bigwedge_{i \leq n} Ep_i \wedge \bigwedge_{i<j \leq n} p_i \perp p_j \rightarrow E \bigwedge_{i \leq n} \Pr(b_i) = \frac{1}{n}$$

1. $Ep_1 \wedge Ep_2 \wedge (p_1 \perp p_2) \rightarrow E\left[(\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2})\right]$
2. $(p_1 \perp p_2) \wedge (\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}) \rightarrow (\Pr(p_1 \sqcup p_2) = 1)$
3. $T(p_1 \sqcup p_2) \rightarrow (\Pr(p_1 \sqcup p_2) = 1) \rightarrow p_1 \sqcup p_2$
4. $(p_3 \perp p_1) \wedge (p_3 \perp p_2) \rightarrow p_3 \perp p_1 \sqcup p_2$
5. $\Longrightarrow$
   $E\left[(\Pr(p_3) = \frac{1}{3}) \wedge \langle p_1 \sqcup p_2 ? \rangle_{=\frac{2}{3}}((\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}))\right]$
6. $p_1 \rightarrow p_1 \sqcup p_2$
7. $E\left[\bigwedge_{i \leq 3} \Pr(p_i) = \frac{1}{3}\right]$

Quantum leader election

Theorem

For all n and all sets of n proposition letters $\{p_1, \ldots, p_n\}$

$$\vdash \bigwedge_{i \leq n} Ep_i \wedge \bigwedge_{i<j \leq n} p_i \perp p_j \rightarrow E \bigwedge_{i \leq n} \Pr(b_i) = \frac{1}{n}$$

1. $Ep_1 \wedge Ep_2 \wedge (p_1 \perp p_2) \rightarrow E\left[(\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2})\right]$
2. $(p_1 \perp p_2) \wedge (\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}) \rightarrow (\Pr(p_1 \sqcup p_2) = 1)$
3. $T(p_1 \sqcup p_2) \rightarrow (\Pr(p_1 \sqcup p_2) = 1) \rightarrow p_1 \sqcup p_2$
4. $(p_3 \perp p_1) \wedge (p_3 \perp p_2) \rightarrow p_3 \perp p_1 \sqcup p_2$
5. $\Longrightarrow$
   $E\left[(\Pr(p_3) = \frac{1}{3}) \wedge \langle p_1 \sqcup p_2 ? \rangle_{=\frac{2}{3}} ((\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}))\right]$
6. $p_1 \rightarrow p_1 \sqcup p_2$
7. $E\left[\bigwedge_{i \leq 3} \Pr(p_i) = \frac{1}{3}\right]$

Quantum leader election

Theorem

For all n and all sets of n proposition letters $\{p_1, \ldots, p_n\}$

$$\vdash \bigwedge_{i \leq n} Ep_i \wedge \bigwedge_{i<j \leq n} p_i \perp p_j \rightarrow E \bigwedge_{i \leq n} \Pr(b_i) = \frac{1}{n}$$

1. $Ep_1 \wedge Ep_2 \wedge (p_1 \perp p_2) \rightarrow E\left[(\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2})\right]$
2. $(p_1 \perp p_2) \wedge (\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}) \rightarrow (\Pr(p_1 \sqcup p_2) = 1)$
3. $T(p_1 \sqcup p_2) \rightarrow (\Pr(p_1 \sqcup p_2) = 1) \rightarrow p_1 \sqcup p_2$
4. $(p_3 \perp p_1) \wedge (p_3 \perp p_2) \rightarrow p_3 \perp p_1 \sqcup p_2$
5. $\Longrightarrow$
   $E\left[(\Pr(p_3) = \frac{1}{3}) \wedge \langle p_1 \sqcup p_2 ? \rangle_{=\frac{2}{3}} ((\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}))\right]$
6. $p_1 \rightarrow p_1 \sqcup p_2$
7. $E\left[\bigwedge_{i \leq 3} \Pr(p_i) = \frac{1}{3}\right]$

Quantum leader election

Theorem

For all n and all sets of n proposition letters $\{p_1, \ldots, p_n\}$

$$\vdash \bigwedge_{i \leq n} Ep_i \wedge \bigwedge_{i<j \leq n} p_i \perp p_j \rightarrow E \bigwedge_{i \leq n} \Pr(b_i) = \frac{1}{n}$$

1. $Ep_1 \wedge Ep_2 \wedge (p_1 \perp p_2) \rightarrow E\left[(\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2})\right]$
2. $(p_1 \perp p_2) \wedge (\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}) \rightarrow (\Pr(p_1 \sqcup p_2) = 1)$
3. $T(p_1 \sqcup p_2) \rightarrow (\Pr(p_1 \sqcup p_2) = 1) \rightarrow p_1 \sqcup p_2$
4. $(p_3 \perp p_1) \wedge (p_3 \perp p_2) \rightarrow p_3 \perp p_1 \sqcup p_2$
5. $\Longrightarrow$
   $E\left[(\Pr(p_3) = \frac{1}{3}) \wedge \langle p_1 \sqcup p_2 ? \rangle_{=\frac{2}{3}} ((\Pr(p_1) = \frac{1}{2}) \wedge (\Pr(p_2) = \frac{1}{2}))\right]$
6. $p_1 \rightarrow p_1 \sqcup p_2$
7. $E\left[\bigwedge_{i \leq 3} \Pr(p_i) = \frac{1}{3}\right]$

Axioms for multi-agent properties

$\top 1$	$[\bot?]\bot$
$\top 2$	$p \to \langle \top? \rangle p$
$\top 3$	$[\top_I](p \to q) \to ([\top_I]p \to [\top_I]q)$
$\top 4$	$[\top_I]p \to p$
$\top 5$	$[\top_I]p \to [\top_I][\top_I]p$
$\top 6$	$\neg[\top_I]p \to [\top_I]\neg[\top_I]p$
$\top 7$	$[\top_I]p \to [\top_J]p$ for all $I \subseteq J$
$\top 8$	$\top_I \leftrightarrow \top_{N \setminus I}$
$\top 9$	$\top_I \to [\top_I]\top_I \wedge [\top_{N \setminus I}]\top_I$
$\top 10$	$\top_N$
$\top 11$	$(\top_I \wedge \top_J) \to (\top_{I \cup J} \wedge \top_{I \cap J})$
$\top 12$	$T(p) \wedge I(p) \wedge I(q) \wedge (\bot \neq q) \wedge (q \leq p) \to (p = q)$ if $I \neq N$
$\top 13$	$\sim\top_I \leftrightarrow \bot$
$\top 14$	$I(\alpha) \to \langle \alpha \rangle p \leq \langle \top_I \rangle p$

Summary and future work

- An axiomatization may be useful for analyzing the correctness of other protocols. Next step: BB84?
- The existing proof system might be reducible (some axioms may be provable)
- Completeness?
- Complexity of the validity problem of the logic?

Thank you!