Multi-modal Type Theory for Trusted Distributed Knowledge

Giuseppe Primiero
work with Mariarosaria Taddeo

FWO – Reserach Foundation Flanders
Centre for Logic and Philosophy of Science, Ghent University
Information Ethics Group - Oxford

Giuseppe.Primiero@Ugent.be
http://www.philosophy.ugent.be/giuseppeprimiero/

21, September, 2010 - LRR10 – Ghent University

Outline

Trust as a second-order property

- Trust affects pre-existing relations, like purchase, negotiation and **communication**;
- The first-order relation "to inform" is represented by a message M and it ranges over two agents S and R;
- The second-order property of trust ranges over $S \rightarrow M \rightarrow R$ and affects the way it occurs.

Efffects of trust on the communication system

- Message M from S to R contains a declarative sentence p
    - R accepts p as true, without checking its truthfulness;
    - R **does not supervise** the trustee's S performance (R takes for good what the trustee communicates).

Testimony: the case of trusted communication (II)

- Minimal requirements on the message (*M*)
  - *M* must be **meaningful**: understandable by the intended receiver.
  - *M* must be **truthful**: *M* is not proved to be true, but it is at least **assumed** to be true.
  - **M is an instance of functional information.**: meaningful contents to which **truth is ascribed**, but which can **still be falsified** (possibly turn into mis-information).

Trust as Dependency

- The relation $S \to M \to R$ is a **dependency relation**: R is dependent on S in order to acquire the new epistemic content in M.
- The dependency determines a **hierarchy** among agents: S always occupies a **higher place** in the hierarchy than R.
- Trust occurs by having R **accepting as true the content in** M **even though she has not a (direct) proof for it**.

Epistemology of Trusted Communications

- *R* is in a **weak epistemic status** by holding a communicated content as true but not verified.
- *p* is represented as an hypothesis *h*, an accepted but refutable content.
- *S* is in a **strong epistemic status** regarding *h* when **she can provide a proof for it without relying on any other agent in the system**.
- Verification is **the reduction of** *h* **to an objective proof of it by** β**-reduction**.

Polymorphism and its semantics

- **Terms in formulae (as the distinct kinds of knowledge contents)**:
  - indexed term constructors $a_i, b_j, \ldots$
  - variable constructors $x_i, y_j, \ldots,$

Polymorphism and its semantics

- **Terms in formulae (as the distinct kinds of knowledge contents)**:
  - indexed term constructors $a_i, b_j, \ldots$
  - variable constructors $x_i, y_j, \ldots,$
- **Types in formulae (as the distinct realised epistemic states)**:

$$\mathcal{K} := \{(A, B, \ldots type); (A, B, \ldots type_{inf})\}$$

Polymorphism and its semantics

- **Terms in formulae (as the distinct kinds of knowledge contents)**:
  - indexed term constructors $a_i, b_j, \dots$
  - variable constructors $x_i, y_j, \dots,$

- **Types in formulae (as the distinct realised epistemic states)**:

$$\mathcal{K} := \{(A, B, \dots type); (A, B, \dots type_{inf})\}$$

- **Indices as Agents**: $i, j \in \mathcal{G}$;

Polymorphism and its semantics

- **Terms in formulae (as the distinct kinds of knowledge contents)**:
  - indexed term constructors $a_i, b_j, \ldots$
  - variable constructors $x_i, y_j, \ldots,$

- **Types in formulae (as the distinct realised epistemic states)**:

$$\mathcal{K} := \{(A, B, \ldots type); (A, B, \ldots type_{inf})\}$$

- **Indices as Agents**: $i, j \in \mathcal{G}$;

- **Basic Semantic Formulae for distinct states**:

  $a_i : A\ type$ – verification for A by $i \Rightarrow A\ true$

  $x_i : A\ type_{inf}$ – admissible claim of A by $i \Rightarrow A\ true^*$ (hypothetically)

Contexts

1. **context as a list of senders/messages**: $\Gamma = \{x_i : A, \ldots, x_n : N\}$ (distinct subjects), list of distinct assumptions depending on forecoming ones;

Contexts

1. **context as a list of senders/messages**: $\Gamma = \{x_i : A, \ldots, x_n : N\}$ (distinct subjects), list of distinct assumptions depending on forecoming ones;
2. **derivability from context as the dependency from sender(s)**: $\{x_i : A, \ldots, x_n : N\} \vdash J$ holds given $x_i/[a_i] : A$;

Contexts

1. **context as a list of senders/messages**: $\Gamma = \{x_i : A, \dots, x_n : N\}$ (distinct subjects), list of distinct assumptions depending on forecoming ones;

2. **derivability from context as the dependency from sender(s)**: $\{x_i : A, \dots, x_n : N\} \vdash J$ holds given $x_i/[a_i] : A$;

3. **extended context**: $\Delta = \{\Gamma, x_{n+1} : N + 1\}$ is equivalent to $\Delta = \{x_i : A, \dots, x_{n+1} : N + 1\}$. (for a fresh declaration $x_{n+1} : N + 1$ independent of the order in Γ, $\Gamma \mid x_{n+1} : N + 1$ is equivalent to Γ, Δ).

Rules for $\vdash type : \mathcal{K}$

$$\frac{a_i : A}{A\ type}\ \text{Type Formation} \qquad \frac{a_i : A \quad A\ true \vdash b_j : B}{a_i(b_j) : A \rightarrow B}\ I\rightarrow$$

$$\frac{a_1 : A, \ldots, a_i : A \quad [A\ true] \vdash b_j : B \quad \lambda((a_{1-i}(b_j))A, B)}{(\forall a_i : A_i)B\ type}\ I\forall$$

$$\frac{a_1 : A, \ldots, a_i : A \quad [a_i : A] \vdash b_j : B \quad (< a_i, b_j >, A, B)}{(\exists a_i : A)B\ type}\ I\exists$$

$$\frac{a_i : A}{\neg A \rightarrow \bot}\ I\bot \qquad \frac{}{\Gamma, a_i : A, \Delta \vdash A\ true.}\ \text{Premise Rule}$$

Othe standard connectives with their elimination and structural rules are validated.

Rules for $\vdash type_{inf} : \mathcal{K}$

$$\frac{\neg(A \rightarrow \bot)\ type \quad x : A}{A\ type_{inf}}\ Type_{inf}\ \text{Formation}$$

$$\frac{A\ type_{inf} \quad x_i : A \vdash b_j : B}{((x_i)b_j) : A \supset B\ type}\ \text{Functional abstraction}$$

$$\frac{A\ type_{inf} \quad x_i : A \vdash b_j : B \quad a_i : A}{(x(b_j))(a_i) = b[a/x] : B\ type[a/x]}\ \beta - conversion$$

$$\frac{}{\Gamma, x_i : A, \Delta \vdash A\ true^{*}}\ \text{Hypothesis Rule}$$

Structural rules are restricted on the external order of Γ.

Introducing Modalities via Structural Properties

- **Categorical Derivability equals Necessity**:

  if **any** Δ extending a context Γ makes A *true*, it means $\Gamma \vdash a : A$ holds and eventually $\Gamma = \emptyset$;

$$\frac{a_i : A}{\Box_i(A\ true)}\ \Box - \text{Formation}$$

Introducing Modalities via Structural Properties

- **Categorical Derivability equals Necessity**:

  if **any** Δ extending a context Γ makes *A true*, it means $\Gamma \vdash a : A$ holds and eventually $\Gamma = \emptyset$;

$$\frac{a_i : A}{\Box_i(A\ true)}\ \Box - \text{Formation}$$

- **Dependent Derivability equals Possibility**:

  if *A true* is valid under some non-empty Γ containing $type_{inf}$ expressions, only **some** Δ will keep *A true* valid;

$$\frac{x_i : A}{\Diamond_i(A\ true)}\ \Diamond - \text{Formation}$$

Generalizing Modalities to Contexts

Definition (Signed and Modal Contexts)

1. For any context $\Gamma_i = \{x_i : A, \ldots, x_i : N\}$, $\Box_i\Gamma$ is given by $\bigcup\{\Box_i(A\ true) \mid \text{ for all } A \in \Gamma\}$;

2. For any context $\Gamma_i\{x_i : A, \ldots, x_i : N\}$, $\Diamond_i\Gamma$ is given by $\bigcup\{\circ_i(A\ true) \mid \circ = \{\Box, \Diamond\}$ and $\Diamond_i(A\ true)$ for at least one $A \in \Gamma\}$.

Introduction and Elimination for $\Box$

Definition (Rules for $\Box_{\mathcal{G}}\Sigma$)

$$\frac{\Gamma_i \mid x_j : A \vdash A\ true^* \qquad \Box_i\Gamma, [x_j/a_j] : A \vdash A\ true}{\Box_{\mathcal{G}}\Sigma \vdash \Box_{\mathcal{G}}(A\ true)}\ I\Box$$

$$\frac{\Box_i\Gamma \mid a_j : A \vdash \Box_{i,j}(A\ true) \qquad \Box_{\mathcal{G}}(A\ true) \mid \Box_k\Delta \vdash \Box_{\mathcal{G}}(B\ true)}{\Gamma_i \mid a_j : A, \Delta_k \vdash B\ true}\ E\Box$$

Introduction and Elimination for $\Diamond$

Definition (Rules for $\Diamond_{\mathcal{G}}\Sigma$)

$$\frac{\Gamma_i \mid x_j : A \vdash B\ true^*}{\Diamond_{\mathcal{G}}\Sigma \vdash \Diamond_{i,j}(B\ true)}\ I\Diamond$$

$$\frac{\Box_i\Gamma \mid \Diamond_j\Delta \vdash \Diamond_{i,j}(A\ true) \qquad \Diamond_j\Delta, x_k : A \vdash \Diamond_{j,k}(B\ true)}{\Gamma_i \mid \Delta_j \vdash B\ true^*}\ E\Diamond$$

Properties of Trusted Information

We now use possibility judgements in a dependency relation to define a notion of Trusted Communication:

Properties of Trusted Information

We now use possibility judgements in a dependency relation to define a notion of Trusted Communication:

Definition (Trusted Communication)

We say that $TC = \langle \Diamond_i, \Diamond_j, J, J' \rangle$ such that $i < j \in \mathcal{G}$ and $J = (A\ true), J' = (B\ true)$, is a Trusted Communication if there are judgements $\Diamond_j(B\ true), \Diamond_i(A\ true)$ that form a communication chain and $\Diamond_j(B\ true)[\Diamond_i(A\ true)]$ and $x_i : A \vdash \Diamond_i(A\ true)$.

Properties of Trusted Information (II)

Definition (Admissible Rules)

$$\frac{x_i : A \vdash A\ true^*}{\Gamma, x_i : A, \Delta \vdash \Diamond_i(A\ true)}\ \text{Reflexivity}$$

$$\frac{x_i : A \vdash A\ true^* \quad \Diamond_j(B\ true)[\Diamond_i(A\ true)] \quad \Diamond_k(B\ true)[\Diamond_j(B\ true)]}{\Diamond_i(A\ true) \vdash \Diamond_k(B\ true)}\ \text{Transmission}$$

Symmetry for such relation is not admitted, trust being a uni-directional relation.

Bridging Properties

Definition (Admissible Rules)

$$\frac{\Box_i\Gamma, a_j : A \vdash \Box_{i,j}(B\ true) \quad x_j : A \vdash A\ true^*}{\Box_i\Gamma, \Diamond_j(A\ true) \vdash \Diamond_{i,j}(B\ true)}\ \Diamond\ \text{Import}$$

$$\frac{\Gamma_i, x_j : A \vdash B\ true^* \quad a_j : A \vdash A\ true}{\Box_i\Gamma, a_j : A \vdash \Box_{i,j}(B\ true)}\ \Box\ \text{Import}$$

$$\frac{\Box_i\Gamma, a_j : A \vdash \Box_k(B\ true) \quad x_j : A \vdash A\ true^*}{\Box_i\Gamma, \Diamond_j(A\ true) \vdash \Diamond_k(B\ true)}\ \text{Common Seriality}$$

$$\frac{\Box_i\Gamma \vdash A\ true \quad \Diamond_j(A\ true)[x_i : A]}{\Box_i\Gamma, x_i : A \vdash \Diamond_j(A\ true)}\ \text{Convergence}$$

Properties of Knowledge

Definition (Admissible Rules)

$$\frac{\Box_{\mathcal{G}}\Sigma \vdash \Box_k(A\ true) \quad \Box_{i,j}\Sigma \mid a_k : A \vdash \Box_{\mathcal{G}}(A\ true)}{\Box_{\mathcal{G}}\Sigma \vdash \Box_{i,j}(A\ true)}\ \textit{Upper Inclusion}$$

$$\frac{\Box_i\Gamma \mid \Box_j\Delta \vdash \Box_{i,j}(A\ true) \quad \Box_{i,j}\Sigma \vdash \Box_k(A\ true)}{\Box_{\mathcal{G}}\Sigma \vdash \Box_k(A\ true)}\ \textit{Lower Inclusion}$$

$$\frac{\Box_i\Gamma \mid \Box_j\Delta \vdash \Box_k(A\ true)}{\Box_{\mathcal{G}}\Sigma \vdash \Box_k(\Box_{i,j}(A\ true))}\ \textit{Ascending Iteration}$$

$$\frac{\Box_i\Gamma \mid \Box_j\Delta \vdash \Box_k(A\ true)}{\Box_{\mathcal{G}}\Sigma \vdash \Box_{i,j}(\Box_k(A\ true))}\ \textit{Descending Iteration}$$

Forms of Equivalence and Union hold as well.

Distributed and Common Knowledge

Definition ($\Diamond_{\mathcal{G}}$ as a distributed knowledge operator)

$$\Diamond_{\mathcal{G}}\Sigma \vdash \Diamond_{i,j}(A\ true) \text{ iff } \Gamma_i \mid \Gamma_j \vdash A\ true \text{ for any } (i,j) \in \bigcap \mathcal{G}$$

Distributed and Common Knowledge

Definition ($\Diamond_{\mathcal{G}}$ as a distributed knowledge operator)

$$\Diamond_{\mathcal{G}}\Sigma \vdash \Diamond_{i,j}(A\ true) \text{ iff } \Gamma_i \mid \Gamma_j \vdash A\ true \text{ for any } (i,j) \in \bigcap \mathcal{G}$$

Theorem (Trusted Communication as a bound to *CK*)

Suppose that $\Sigma = \langle \circ_i, \circ_j, J \rangle$ and $i < j$, i.e. $|\mathcal{G}| \geq 2$. Then for all judgements $J \in \Sigma$, $\Sigma \vdash \Box J$ iff $TC^j = 0$.

Distributed and Common Knowledge

Definition ($\Diamond_{\mathcal{G}}$ as a distributed knowledge operator)

$$\Diamond_{\mathcal{G}}\Sigma \vdash \Diamond_{i,j}(A\ true) \text{ iff } \Gamma_i \mid \Gamma_j \vdash A\ true \text{ for any } (i,j) \in \bigcap \mathcal{G}$$

Theorem (Trusted Communication as a bound to *CK*)

Suppose that $\Sigma = \langle \circ_i, \circ_j, J \rangle$ and $i < j$, i.e. $|\mathcal{G}| \geq 2$. Then for all judgements $J \in \Sigma$, $\Sigma \vdash \Box J$ iff $TC^j = 0$.

Definition ($\Box_{\mathcal{G}}$ as a common knowledge operator)

$$\Box_{\mathcal{G}}\Sigma \vdash \Box_{i,j}(A\ true) \text{ iff } \Gamma_i \vdash A\ true \text{ for all } i \in \mathcal{G}$$

Conclusions

1. We have presented a formal model for epistemic processes qualified by trust as a second-order relation ranging over information transmissions;
2. The embedding for DK/CK is obtained;
3. It is a flexible language that can be applied to distributed ordered computation;
4. It can be extended to the cases of communications characterized by mistrust and distrust.