Formalizing Trusted Communications

Giuseppe Primiero & Mariarosaria Taddeo

FWO - Centre for Logic and Philosophy of Science, Ghent University
University of Hertfordshire
IEG - Oxford

Giuseppe.Primiero@Ugent.be
mariarosaria.taddeo@philosophyofinformation.net

May, 2010 - Second International Workshop on the Philosophy of Information – Ankara

Outline

Trust as a second-order property

- The occurrences of trust are related to, and affect, pre-existing relations, like purchase, negotiation and communication;

  A trusts B to sell good wine.

- There is a first-order relation, purchasing, which ranges over the two agents, and there is the second-order property of trust, which ranges over the first-order relation and affects the way it occurs.

Effects of trust on the system

- Trust affects the interaction between the trustor and the trustee by minimising the trustor's effort and commitment for the achievement of a given goal.

Efffects of trust on the system

- Trust affects the interaction between the trustor and the trustee by minimising the trustor's effort and commitment for the achievement of a given goal.

It does so in two ways:

- the trustor can avoid performing the necessary action to achieve her goal herself, because she can count on the trustee to do it.
- the trustor does not supervise the trustee's performance.

Testimony: the case of trusted communication (I)

- Testimony is understood as the assertion of a declarative sentence carrying the belief of a sender to a receiver, who then accepts it as true, without checking its truthfulness.

Testimony: the case of trusted communication (I)

- Testimony is understood as the assertion of a declarative sentence carrying the belief of a sender to a receiver, who then accepts it as true, without checking its truthfulness.

  Ex.: The spy who does not understand the message she is carrying.

- In this case, S does not hold a belief about p, still R accepts p and might also know that p on the basis of S' assertion.
- Testimony does not necessarily require beliefs.
- What is the nature of the message transmitted through testimony?

Testimony: the case of trusted communication (II)

- What are the minimal requirements that the message (M) must satisfy in order for testimony to occur?

Testimony: the case of trusted communication (II)

- What are the minimal requirements that the message (M) must satisfy in order for testimony to occur?

- M must be meaningful and truthful*.

  Meaningful: M must be understandable by the intended receiver.

  Truthful*: if M is false then testimony becomes false testimony, i.e. not a genuine form of testimony at all. M is not proved to be true, but it is at least assumed to be true.

Testimony: the case of trusted communication (II)

- What are the minimal requirements that the message (M) must satisfy in order for testimony to occur?

- M must be meaningful and truthful*.

  Meaningful: M must be understandable by the intended receiver.

  Truthful*: if M is false then testimony becomes false testimony, i.e. not a genuine form of testimony at all. M is not proved to be true, but it is at least assumed to be true.

- M is an instance of functional information.

- An instance of functional information is a instance of meaningful contents to which truth is ascribed, but which can still be falsified (mis-information).

Testimony the case of trusted communication (III)

- Testimony involves the communication of (functional) information from S to R.
- The communication from S to R is a first-order relation.

Testimony the case of trusted communication (III)

- Testimony involves the communication of (functional) information from S to R.
- The communication from S to R is a first-order relation.
- Testimony is also characterised by:
  - the delegation by R to S. R delegates to S the task of communicating *p*,
  - the absence of supervision. R does not supervise S' performances.
- These aspects are peculiar to the occurrence of trust and can be explained if one considers trust as a property qualifying the communication occurring between R and S.

Testimony: from the weak to the strong epistemic status

- An epistemic agent who holds some information as true on the basis of her trust in the sender is in a weak epistemic status.
- Such information can be upgraded to knowledge if and only if the agent is able to connect the transmitted information to the conceptual network of interrelations to which it belongs.
- Floridi's Network Theory of Account (NTA) show how such a network allows the epistemic agent to achieve knowledge on the basis of the communicated information.

Trust as Dependency

- In our formal system the relation between the sender and the receiver of the message is presented as a dependency relation, i.e. the receiver of the message is dependent on the sender in order to acquire new epistemic content.

- The dependency determines a hierarchy among the agents, for this reason the agents are ordered so that the sender of the message always occupies a higher place in the hierarchy than the receiver.

Trust as Dependency

- In our formal system the relation between the sender and the receiver of the message is presented as a dependency relation, i.e. the receiver of the message is dependent on the sender in order to acquire new epistemic content.
- The dependency determines a hierarchy among the agents, for this reason the agents are ordered so that the sender of the message always occupies a higher place in the hierarchy than the receiver.
- The communications among the agents are trust-qualified relations. In the formal model the occurrence of trust is represented by having the receiver accepting as true the communicated message even though she has not a (direct) proof for it.

Distributed Knowledge

- The receiver of the message is in a weak epistemic status by holding a communicated content as true but not verified.
- We express this aspect of the analysis in our formal model by representing the epistemic content held by the receiver as a hypothesis (h), i.e. an epistemic content that might potentially be true but has not been verified yet.
- S and R together instantiate an epistemic system in which is present distributed knowledge (DK).

Common Knowledge

- An agent is said to have a strong epistemic status regarding *h* when she can account for such content without relying on any other agent in the system.
- In the formal model an agent has a strong epistemic status with respect to *h* when she can provide a proof for it without relying on any other agent in the system.
- The verification is represented in the formal model by the reduction of *h* to a proof of it by β-reduction. The proof is objective, i.e. it can be accessed from any agent's epistemic state holding *h*.
- As iteration of distinct agents' epistemic contents can be inferred (*i* knows that *A* and that *j* knows that *i* . . .), this represents the basis to formulate common knowledge (CK).

Polymorphism and its semantics

- Terms in formulae: indexed term constructors $a_i, b_j, \ldots$ and variable constructors $x_i, y_j, \ldots,$
- Types in formulae: $\mathcal{K} := \{(A, B, \ldots type); (A, B, \ldots type_{inf})\}$
- Indices: $i, j \in \mathcal{G}$ range over an enumerable set $\mathcal{G}$ of distinct sources;
- Basic Formulae:

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

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

Contexts

1. context: Γ is a finite sequence of assumptions $\{x_i : A, \ldots, x_n : N\}$ (distinct subjects), with each assumption depending on forecoming ones;
2. derivability from context: $\{x_i : A, \ldots, x_n : N\} \vdash J$ holds provided $x_i/[a_i] : A$;
3. extended context: $\Delta = \{\Gamma, x_{n+1} : N+1\}$ is equivalent to $\Delta = \{x_i : A, \ldots, x_{n+1} : N+1\}$. (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 $\vdash type : \mathcal{K}$

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

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

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

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

Standard elimination Rules and Weakening, Contraction and Exchange are validated.

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

$$\frac{\neg(A \to \bot)\ type}{A\ type_{inf}}\ Type_{inf}\ \text{Formation} \qquad \frac{A\ type_{inf} \quad x_i : A \vdash b_j : B}{((x_i)b_j) : A \supset B\ type}\ \text{Functional abstraction}$$

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

$$\frac{\lambda((a_{1-i}(b_j))A, B) \quad (b_j)[a_i := a]}{(a_i(b_j)) : A \to B\ type}\ \alpha - conversion$$

$$\frac{}{\Gamma, x_i : A, \Delta \vdash A\ true^*}\ \text{Hypothesis Rule} \qquad \frac{\Gamma \vdash B\ type_{inf} \quad x_i : A \vdash A\ type_{inf}}{\Gamma \mid x_i : A \vdash B\ type_{inf}.}\ \text{Weakening}$$

$$\frac{\Gamma \mid x_i : A, y_j : B \vdash C\ type_{inf} \quad \Gamma \vdash y_j : B}{\Gamma \mid x_i : A \vdash C\ type_{inf}}\ \text{Contraction}$$

$$\frac{\Gamma \mid x_i : A \mid y_j : B \vdash C\ type_{inf}}{\Gamma \mid y_j : B \mid x_i : A, \vdash C\ type_{inf}}\ \text{Exchange}$$

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

1. Γ_i is a context signed for i iff for any declaration in Γ the signature is i;
2. $\Box_i(A\ true)$ generated by $\Box$-Formation from $x_i[/a_i] : A$ is the declaration that A is valid for any extension of context Γ_i;
3. $\Diamond_i(A\ true)$ generated by $\Diamond$-Formation from $x_i : A$ is the declaration that A is an admissible assumption for some extension of context Γ_i;
4. Γ_i, $\Box_i\Gamma$ is given by $\bigcup\{\Box_i(A\ true) \mid$ for all $A \in \Gamma\}$;
5. $\Diamond_i\Gamma$ is given by $\bigcup\{\circ_i(A\ true) \mid \circ = \{\Box, \Diamond\}$ and $\Diamond_i(A\ true)$ for at least one $A \in \Gamma\}$.

Extension of Signed and Modal Contexts

1. $\Sigma_{i,j}$ is a context extension

$$\circ_i\Gamma \mid \circ_j\Delta = \{\circ_i(A\ true), \ldots, \circ_i(N\ true), \circ_j(O\ true)\}$$

2. $\circ_i\Gamma \mid \circ_j\Delta$ is admissible if, for any judgement $J \in \Delta$ such that $J = A\ type_{inf}$, $\Gamma \nvdash (A \rightarrow \bot)$;

3. $\Diamond_{\mathcal{G}}\Sigma \vdash J$ is obtained by $\Box_i\Gamma \mid \Diamond_j\Delta \vdash J$;

4. $\Box_{\mathcal{G}}\Sigma \vdash J$ is obtained by $\Box_i\Gamma \mid \Box_j\Delta \vdash J$.

Modal Judgements from multi-signed contexts

- Deriving Necessity Judgements from Multi-Contexts

  $\Box_k(A\ true)$ iff for all $\Gamma_j \in Context$, $\emptyset \mid \Box_j\Gamma \vdash \Box_k(A\ true)$, where $j = \bigcup\{1, \ldots, k-1\} \in \mathcal{G}$;

Modal Judgements from multi-signed contexts

- Deriving Necessity Judgements from Multi-Contexts

  $\Box_k(A\ true)$ iff for all $\Gamma_j \in Context$, $\emptyset \mid \Box_j\Gamma \vdash \Box_k(A\ true)$, where $j = \bigcup\{1, \ldots, k-1\} \in \mathcal{G}$;

- Deriving Possibility Judgements from Multi-Contexts

  $\Diamond_k(A\ true)$ iff for some $\Gamma_i, \Delta_j \in Context$, $\Box_i\Gamma \mid \Diamond_j\Delta \vdash \Diamond_k(A\ true)$, where $j = \bigcup\{1, \ldots, k-1\} \in \mathcal{G}$;

Properties of Trusted Information

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)

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

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

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

Properties of Trusted Information

Definition (Sequenced admissible communication)

If $\vdash B\ true[\Diamond_i(A\ true), \ldots, \Diamond_k(N\ true)]$ we write $\Diamond_{i,k}\Sigma \vdash \Diamond_l(B\ true)$ and say that $(B\ true)$ is reachable at l ($k \leq l \in \mathcal{G}$) from $\Diamond_{i,k}\Sigma$ if there are trusted communications $TC^1 = \langle \Diamond_i, (A\ true) \rangle$ up to $TC^k = \langle \Diamond_k, \Diamond_l, (B\ true) \rangle$ such that at TC^k agent l trusts agents k on N, at TC^{k-1} agent k trusts agents $k-1$ on $N-1$ up to TC^{1-k} where agent $i+1$ trusts agent i on A and $\Sigma_{i,k} \mid \Diamond_l\Delta$ is admissible.

Properties of Trusted Information

Definition (Sequenced admissible communication)

If $\vdash B\ true[\Diamond_i(A\ true), \ldots, \Diamond_k(N\ true)]$ we write $\Diamond_{i,k}\Sigma \vdash \Diamond_l(B\ true)$ and say that $(B\ true)$ is reachable at l ($k \leq l \in \mathcal{G}$) from $\Diamond_{i,k}\Sigma$ if there are trusted communications $TC^1 = \langle \Diamond_i, (A\ true) \rangle$ up to $TC^k = \langle \Diamond_k, \Diamond_l, (B\ true) \rangle$ such that at TC^k agent l trusts agents k on N, at TC^{k-1} agent k trusts agents $k-1$ on $N-1$ up to TC^{1-k} where agent $i+1$ trusts agent i on A and $\Sigma_{i,k} \mid \Diamond_l\Delta$ is admissible.

A lemma holds such that derivability is expressed via an ordered admissible chain of Trusted Communications.

Bridging Properties

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

Bridging Properties

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

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

Bridging Properties

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

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

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

Bridging Properties

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

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

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

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

Properties of Knowledge

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

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

Properties of Knowledge

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

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

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

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

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 $TC^j = 0$.

Reducing the need for Trusted Communications corresponds to acquiring CK.

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* $TC^j = 0$*.*

Reducing the need for Trusted Communications corresponds to acquiring CK.

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;
2. Considering trust as a second-order relation avoids the issue of formalizing it at the same level of the underlying epistemic relation;
3. Advantages of this model is the representation of multiagent interactions and the embedding in DK/CK;
4. A flexible language that can be applied to distributed ordered computation;
5. This analysis remains consistent is adapted to the cases of communications characterized by mistrust *and* distrust.

Thanks

Thanks to Hilmi Delmir & David Davenport and to you!