# 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

Primiero Type Theory f

Type Theory for Trusted Distributed Knowledge

MQ P

# Outline



#### Trust & Testimony

- Prom conceptual to formal analysis
- 3 Type theory for multiagent epistemic processes
- 4 Multi-modalities for collective knowledge
- 5 Properties of trusted communication and knowledge

### 6 Conclusions





From conceptual to formal analysis Type theory for multiagent epistemic processes Multi-modalities for collective knowledge Properties of trusted communication and knowledge Conclusions

# 1 Trust & Testimony

INIVERSIT

- From conceptual to formal analysis
- 3 Type theory for multiagent epistemic processes
- 4 Multi-modalities for collective knowledge

5 Properties of trusted communication and knowledge



From conceptual to formal analysis Type theory for multiagent epistemic processes Multi-modalities for collective knowledge Properties of trusted communication and knowledge Conclusions

## 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.





From conceptual to formal analysis Type theory for multiagent epistemic processes Multi-modalities for collective knowledge Properties of trusted communication and knowledge Conclusions

# 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).





From conceptual to formal analysis Type theory for multiagent epistemic processes Multi-modalities for collective knowledge Properties of trusted communication and knowledge Conclusions

# 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).





INIVERSIT

#### Prom conceptual to formal analysis

- 3 Type theory for multiagent epistemic processes
- 4 Multi-modalities for collective knowledge

5 Properties of trusted communication and knowledge



# Trust as Dependency

- The relation S → M → 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.

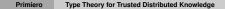




# Epistemology of Trusted Communications

- *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  $\beta$ -reduction.





### 1 Trust & Testimony

From conceptual to formal analysis

#### 3 Type theory for multiagent epistemic processes

4

NIVERSIT

Multi-modalities for collective knowledge

5 Properties of trusted communication and knowledge



# 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<sub>i</sub>, y<sub>j</sub>, ...,





# 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<sub>i</sub>*, *y<sub>j</sub>*, ...,

#### • Types in formulae (as the distinct realised epistemic states):

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



# 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<sub>i</sub>*, *y<sub>j</sub>*, ...,
- Types in formulae (as the distinct realised epistemic states):

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

• 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<sub>i</sub>*, *y<sub>j</sub>*, ...,
- Types in formulae (as the distinct realised epistemic states):

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

- 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<sub>inf</sub> – admissible claim of A by  $i \Rightarrow A$  true<sup>\*</sup> (hypothetically)





# Contexts

 context as a list of senders/messages: Γ = {x<sub>i</sub>: A,..., x<sub>n</sub>: N} (distinct subjects), list of distinct assumptions depending on forecoming ones;





# Contexts

- context as a list of senders/messages: Γ = {x<sub>i</sub>: A,..., x<sub>n</sub>: 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  $x_i/[a_i]:A$ ;

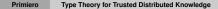




# Contexts

- context as a list of senders/messages: Γ = {x<sub>i</sub>: A,..., x<sub>n</sub>: 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  $x_i/[a_i]: A$ ;
- **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  $\Gamma$ ,  $\Gamma \mid x_{n+1} : N + 1$  is equivalent to  $\Gamma, \Delta$ ).





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

$$\begin{array}{c} \displaystyle \frac{a_i:A}{A \ type} \ \text{Type Formation} \quad \displaystyle \frac{a_i:A \ A \ true \vdash b_j:B}{a_i(b_j):A \to B} \quad I \to \\ \\ \displaystyle \frac{a_1:A,\ldots,a_i:A \ [A \ true] \vdash b_j:B \ \lambda((a_{1-i}(b_j))A,B)}{(\forall a_i:A_i)B \ type} \quad N \\ \\ \displaystyle \frac{a_1:A,\ldots,a_i:A \ [a_i:A] \vdash b_j:B \ (< a_i, b_j >, A, B)}{(\exists a_i:A)B \ type} \quad I \\ \\ \displaystyle \frac{a_i:A \ \ldots,a_i:A \ [a_i:A] \vdash b_j:B \ (< a_i, b_j >, A, B)}{(\exists a_i:A)B \ type} \quad I \\ \end{array}$$

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



Rules for  $\vdash$  *type*<sub>inf</sub> :  $\mathcal{K}$ 

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

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

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

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

$$\frac{F_i(x_i) : A \ b_i : B \ type[a/x]}{F_i(x_i) : A \ b_i : A \ true^*} \ Hypothesis \ Rule$$



Structural rules are restricted on the external order of  $\Gamma$ .



### 1 Trust & Testimony

- 2 From conceptual to formal analysis
- 3 Type theory for multiagent epistemic processes

#### 4

INIVERSIT

#### Multi-modalities for collective knowledge

Properties of trusted communication and knowledge



# Introducing Modalities via Structural Properties

#### • Categorical Derivability equals Necessity:

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

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





# Introducing Modalities via Structural Properties

#### • Categorical Derivability equals Necessity:

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

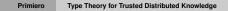
$$\frac{a_i:A}{\Box_i(A \ true)} \Box - Formation$$

#### • Dependent Derivability equals Possibility:

if *A* true is valid under some non-empty  $\Gamma$  containing type<sub>inf</sub> expressions, only **some**  $\Delta$  will keep *A* true valid;

$$\frac{x_i:A}{\diamond_i(A \ true)} \diamond - \text{Formation}$$





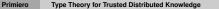


# Generalizing Modalities to Contexts

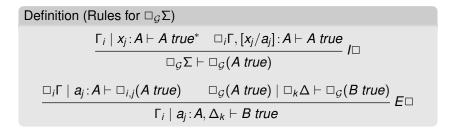
Definition (Signed and Modal Contexts)

- **①** For any context  $\Gamma_i = \{x_i : A, ..., x_i : N\}$ , □<sub>i</sub> $\Gamma$  is given by  $\bigcup \{\Box_i(A \text{ true}) \mid \text{ for all } A \in \Gamma\};$
- ② For any context  $\Gamma_i$ { $x_i$ : A, ...,  $x_i$ : N},  $\diamondsuit_i \Gamma$  is given by ∪{ $\circ_i$ (A true) |  $\circ$  = {□,  $\diamondsuit$ } and  $\diamondsuit_i$ (A true) for at least one  $A \in \Gamma$ }.



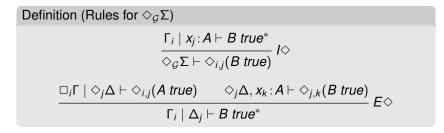


## Introduction and Elimination for $\Box$





## Introduction and Elimination for $\diamond$







### 1 Trust & Testimony

- 2 From conceptual to formal analysis
- 3 Type theory for multiagent epistemic processes
- 4

INIVERSITE

Multi-modalities for collective knowledge

#### 5 Properties of trusted communication and knowledge



# 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)

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

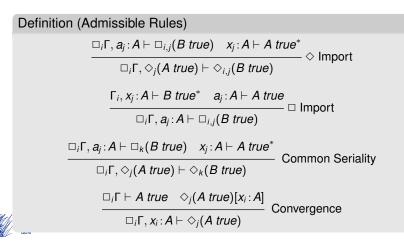
 $\frac{x_i: A \vdash A \ true^* \quad \diamondsuit_j(B \ true)[\diamondsuit_i(A \ true)] \quad \diamondsuit_k(B \ true)[\diamondsuit_j(B \ true)]}{\diamondsuit_i(A \ true) \vdash \diamondsuit_k(B \ true)} \text{ Transmission}$ 

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

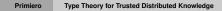




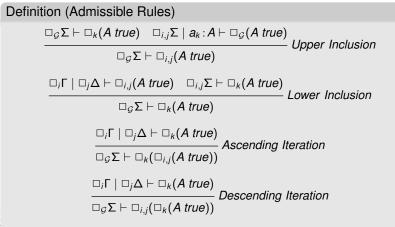
# **Bridging Properties**



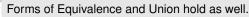




# Properties of Knowledge



Primiero





# Distributed and Common Knowledge

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

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





# Distributed and Common Knowledge

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

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

Theorem (Trusted Communication as a bound to CK)

Suppose that  $\Sigma = \langle \circ_i, \circ_j, J \rangle$  and i < j, i.e.  $|\mathcal{G}| \ge 2$ . 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)

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

Theorem (Trusted Communication as a bound to *CK*) Suppose that  $\Sigma = \langle \circ_i, \circ_j, J \rangle$  and i < j, *i.e.*  $|\mathcal{G}| \ge 2$ . Then for all judgements  $J \in \Sigma$ ,  $\Sigma \vdash \Box J$  iff  $TC^j = 0$ .

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

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



# Conclusions

- 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;
- It is a flexible language that can be applied to distributed ordered computation;
- It can be extended to the cases of communications characterized by mistrust and distrust.



