Journal of Applied Logic 10 (2012) 92–114

Contents lists available at SciVerse ScienceDirect

Journal of Applied Logic

www.elsevier.com/locate/jal

A modal type theory for formalizing trusted communications

Giuseppe Primiero[a,b,d,*], Mariarosaria Taddeo[c,d]

[a] FWO – Research Foundation Flanders, Belgium
[b] Centre for Logic and Philosophy of Science, Ghent University, Blandijnberg 2, Ghent, B-9000, Belgium
[c] University of Hertfordshire, United Kingdom
[d] Information Ethics Group, University of Oxford, United Kingdom

ARTICLE INFO

Article history:
Received 18 December 2010
Accepted 19 December 2011
Available online 23 December 2011

Keywords:
Testimony
Trust
Modal Type Theory
Epistemic Modalities
Common and Distributed Knowledge

ABSTRACT

This paper introduces a multi-modal polymorphic type theory to model epistemic processes characterized by trust, defined as a second-order relation affecting the communication process between sources and a receiver. In this language, a set of senders is expressed by a modal prioritized context, whereas the receiver is formulated in terms of a contextually derived modal judgement. Introduction and elimination rules for modalities are based on the polymorphism of terms in the language. This leads to a multi-modal non-homogeneous version of a type theory, in which we show the embedding of the modal operators into standard group knowledge operators.

1. Introduction

This paper introduces a multi-modal type-theoretic system to model trust-qualified communication processes ongoing among rational agents. The formulation of such a language and the analysis of its properties contributes to the epistemic debate on testimony and it provides a novel analysis of trust-based knowledge representation in a multi-agent system. Provided the syntactic nature of the language, the resulting semantics is easily adapted to computation within distributed networks: we focus here only on the analogy with testimony relations.

In the epistemic debate, testimony is commonly understood as the assertion of a declarative sentence carrying the message of a sender (S) to a receiver (R),[1] who then accepts it as true, without checking its truthfulness. From an epistemological point of view, true beliefs acquired through testimony are not (yet) justified, because they (still) lack any verification of their truthfulness. So it seems that testimony allows the agents in the system only to achieve a weak epistemic status, whereas a strong epistemic status can be obtained only once the receiver of the message verifies its truthfulness.

The formal model proposed in this paper rests on two conceptual pillars, the definition of trust as second-order property qualifying first-order relations [72] and the analysis of testimony proposed in [73]. Before focusing on the analysis of testimony we shall briefly recall the reader's attention on the novelty of the definition of trust as second-order property. Such definition clarifies that, contrary to what a first analysis would suggest, trust is not a relation occurring among the agents of a system. Rather it is a way in which such relations may occur. In particular, trust qualifies a relation making it more convenient for the agent who decides to trust (the trustor) another agent (the trustee), as in doing so the trustor

[*] Corresponding author at: Centre for Logic and Philosophy of Science, Ghent University, Blandijnberg 2, Ghent, B-9000, Belgium.
E-mail addresses: giuseppe.primiero@ugent.be (G. Primiero), m.taddeo@herts.ac.uk (M. Taddeo).

[1] In this paper we will refer to '*sender*' and '*receiver*' of a message rather than to 'speaker' and 'hearer' to indicate the agents involved in a testimony scenario. 'Speaker' and 'hearer', although common terms in the philosophical literature on testimony, specifically refer to verbal communication, which is only one of the possible ways in which testimony can occur, while 'sender' and 'receiver' generally refer to a case of communication among agents, without specifying the nature of the communication. For this reason the latter is more appropriate to describe testimony scenarios.

1570-8683/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.jal.2011.12.002

saves the resources (time and energy) that he would deploy to perform a given task. When considered with respect to an epistemic context, this definition of trust becomes extremely useful in understanding its role in the processes of communication of information and knowledge among the agents of a distributed system. This is particularly true when considering the occurrences of testimony. According to the analysis of testimony provided in [73] on the basis of this definition of trust, testimony is the occurrence of first-order relations of communication qualified by the second-order property of trust. This is the definition interpreted by the formal model described in this paper, which interprets communication in a multi-agent system by focusing on the distinction among agents that hold directly the relevant information and those that have to rely on others in order to possess it. In this way, we design communication chains that inherently use the notion of trust, defined as the result of linking two epistemic states by way of a message passing system.

Our language is an extension of the modal polymorphic type theory with partial term-assignment on judgements developed in [65]. The polymorphic language serves the task of formalizing the two kinds of epistemic states involved by a communication act: a standard constructive *type* preserves verification-terms on propositions and qualifies them as 'known contents'; a type with partial-terms $type_{inf}$ preserves only consistency and qualifies its contents as 'information', in the sense of communicated but not verified contents. For each of the two kinds of contents, an appropriate portion of the language is used. A side property of the system is the extension of a strongly constructive language with a fragment that accommodates a weaker epistemic notion, to use it for knowledge representation purposes. The language has also a modal extension, based on the judgemental modalities introduced in [64]: judgements $\Box/\Diamond(A\ true)$ are defined to express the reducibility of the corresponding proof constructions. Modalities are then generalized to collections of judgements used in contexts Γ, Δ, interpreted as knowledge states. Multi-modalities are used to formalize the occurrence of distinct, prioritized sources in the communication act.

We can sum up the novelties offered by the present contribution as follows:

1. We present the first type-theoretic model of trusted communications; in this way we extend the range of syntactic approaches to group knowledge and provide a novel research direction for type systems;
2. The model relies on an effective representation of different epistemic states for rational agents, thus making an effort in the direction of realistic representation of human knowledge processes;
3. The model endorses an innovative definition of trust. Rather than focusing on the traditional conceptualization of trust as a relation, it endorses a recently provided account of this phenomenon, according to which trust is a second-order property qualifying first-order relations. Such a definition not only constitutes quite an innovative approach to the analysis of trust when compared to the relevant literature, it also allows for developing a completely new analysis of trust-communications and of their role in the processes of knowledge communication in a distributed system, as described in Section 2.
4. We make use of the notion of refutable content for a type system, introduced in [65]; we consider this a crucial notion for the development of epistemic logics for defeasible reasoning and, in particular, consider it especially important in its present combination with a strong verificationist semantics, in order to combine different aspects of knowledge acquisition processes that often are difficult to highlight in a formal setting;
5. Finally, we explore the relation of this syntactic model and the thereby defined notion of trusted communications with the well-known notions of Distributed and Common Knowledge from epistemic logic; this direction of research is still very young but we provide a first interesting connection between two fields that grow largely separated from one another.

There is a growing literature on trust and the formalization of communication acts that uses modal logics; such literature is for the greatest part developed in the vein of model-theoretic, Kripke- and Dynamic semantics of modal logics, whereas little is done in the area of proof-theoretic approaches. Our work especially aims at providing the *first type-theoretic* treatment of the notion of trusted communication. The greatest advantage of such language is that it provides a syntax with embedded meanings, so that its rules immediately define corresponding semantic notions and a procedural semantics comes entirely natural, as done in [66] for a model of safe distributed programming. Moreover, we exploit the predicative structure of Dependent Types in order to mimic the behavior of communication acts. This approach is, to our knowledge, entirely new especially because it relies on a syntactic distinction between constructors that accommodate partial terms. Finally, we induce a modal extension of the language which differs both from the original formulation of the type theory in use and from the already existing contextual modal extensions.

In providing this language, we focus on the concurrent combination of the two epistemic states that we consider essentially involved in the act of trusted communication. Also in this case, we believe this is a rather novel approach. The largest part of the work done in modeling trusted communications and distrust relations comes from computer science and network analysis, where such distinction is treated in terms of authorizations. Our treatment is clearly more focused on the epistemic relations occurring among rational human agents. The formal representation of epistemic acts combining weaker and stronger attitudes represents a step forward towards more realistic approaches of human-based communications.

As mentioned above, a conceptual novelty of this paper is related to the definition of trust as a second-order property and the reference to testimony as the specific instance of trusted communications. This point is largely addressed in Section 2.

Finally, we consider both useful and important that first results in the direction of identity with the (usually semantically defined) notions of Common and Distributed Knowledge are provided, something we believe will be crucial in future directions of this research.

The paper is structured as follows. Section 2 provides the theoretical and philosophical background on which the formal model rests. Section 3 introduces the formal model, first in view of the non-modal fragment of the type-theoretic system and then via its extension to modalities and multi-modalities. Section 4 clarifies the structure of our language as a non-homogeneous multi-modal logic to express reliable communication and knowledge within the spectrum of standard modal logics. Section 5 shows how to infer appropriate definitions of Distributed and Common Knowledge from our language. Section 6 presents completeness results of the syntactic language with respect to frames of standard modal logics. Section 7 describes the debates that stand at the background of this research: a) the epistemic debate on testimony, b) the existing formal approaches to trusted communication relations in knowledge representation and information systems. Finally, Section 8 concludes the paper by pulling together the threads of our analysis and it briefly describes the content of future work.

2. Testimony: the case of trusted communications among the agents of a distributed system

In a testimony scenario, R accepts a message by S on the basis of R's trust in S. R is the trustor, who accepts S' message as true without verifying it and only on the basis of his trust in S, while S is the trustee: she is the referent of R's trust. According to this analysis, the occurrences of trust are related to, and affect, pre-existing relations, like purchasing, negotiation, delegation and, in our case, communication. Trust is not to be considered a relation itself but a property of relations, something that changes the way relations occur. As a property of relations, trust affects the way relations occur by minimizing the trustor's effort and commitment for the achievement of a given goal. It does so in two ways. First, the trustor can avoid performing the action necessary to achieve his goal himself, because he can count on the trustee to do it (or have done it). This is true even in epistemic contexts in which the trustor, e.g. a member of a jury, could not physically replace the trustee, e.g. an eyewitness. Second, the trustor can decide not to supervise the trustee's performance. This is a peculiarity of trust scenarios as shown in [72], where the trustor decides to delegate and not supervise the performance of a given task to a *trustworthy agent*.[2] It follows that trust can be defined thus:

Definition 1 *(Trust).* Assume a set of first-order relations functional to the achievement of a goal. Assume that one such relation holds between two agents, such that one of them (the trustor) has to achieve the given goal while the other (the trustee) is able to perform some tasks in order to achieve that goal. If the trustor chooses to achieve his goal through the task performed by the trustee, and if the trustor considers the trustee a trustworthy agent, then the relation has the property of being advantageous for the trustor. Such a property is a second-order property called *trust* that affects the first-order relations occurring between agents.[3]

We shall endorse this definition of trust to analyze the first-order relation of communication of epistemic contents among agents, namely what is known as testimony. In a testimony scenario, S transmits some information to R,[4] so testimony is an instance of communication, a first-order relation. This is a partial definition, because it does not take into consideration other aspects of testimony, such as the goal of R of obtaining (at least) some information by counting on the performance of S, and the absence of supervision on S' performances. We focus on the fact that R does not verify the truthfulness of S' messages, nor does she verify how S elaborated the transmitted information. Following this analysis, testimony can be defined thus:

Definition 2 *(Testimony).* Assume a first-order ternary relation of communication, where some information i is passed from a sender S to a receiver R. If the communication occurs between a receiver and a trustworthy sender, and if the receiver acquires the sender's messages without checking their truthfulness, then the communication is affected by the second-order property of trust. Such an occurrence of communication is called testimony.

[2] Trustworthiness is a measure of the probability that the trustee is able to perform a given action correctly and autonomously. The criteria for the assessment of trustworthiness vary from case to case, and may or may not be rational or objective. The level of risk undertaken by the trustor will increase in those cases in which trustworthiness is assessed on the basis of non-rational criteria. It is worth noting that the formal model we present describes communications among rational agents, hence we assume that the agents of the presented model will rationally choose the potential trustee on the basis of their reputation, but the execution of such selection is not a task of the formal model itself. This assumption avoids the problem of a possible stronger requirement on the definition of the trust relation, such as that the trustee *must be* trustworthy. An example of a general system to evaluate trustworthiness in actions such as negotiations, pacts and trading networks is given in [70]: it provides an information theoretic approach where the employed notion of trust measures the relationship between commitment and execution of contracts being given as the negative entropy of the probability distribution of possible outcomes for a given contract.

[3] See [72] for the analysis in support of this definition.

[4] For an analysis of the nature of the message transmitted in a testimony scenario, see [73] and [45].

The reader should note that, at this point, by the definition of testimony the truth value of the transmitted information is not specified. We consider the information communicated by the sender as meaningful contents to which truth is ascribed (rather than true contents), but which can still be falsified (mis-information). We call such content *functional information*.

To make things clearer, consider a case of communication. The aim of this paper is to provide a formal counterpart to the notion of testimony introduced above and to present the appropriate formal properties of the notion of communication as exemplified below.

> Over a hundred biologists are writing together an article on molecular biology. None of them knows enough to ground the overall conclusion of the paper, so none of them can be given a 'strong epistemic status' with respect to the *whole* information conveyed in the article. But, eventually, each of them provides the part of content for which she is able to support justification. In the context of their interaction various communication acts are in place: biologist a will communicate to her colleague b the content of message M, which b does not posses nor is able to test, so that b 'trusts' a about the actual truth of M. These relations are what we shall call 'trusted communications' (see Definition 17): a trusted communication is a ternary relation between the epistemic states of agents a, b and the judgement A *true* that is content of the communicated message.[5]

According to the analysis in [73], the receiver of the message is in a weak epistemic status, as she accepts the message to be true on the basis of her trust in the sender and without verifying it. The formal model expresses this aspect by representing the epistemic content held by the receiver as a *hypothesis* (h), i.e. an epistemic content that is admissibly true but has not been verified yet. The weak status resulting from possessing content via a trusted communication is what we shall formalize by terms of the $type_{inf}$-kind and express by the induced $\Diamond$-modality, see Section 3.3 and Definition 12.

The message-passing system is defined by functional expressions of the language, in terms of dependent types. For each expression B dependent on A in the language, we enforce the presence of an agent a which passes content A to an agent b which holds content B true given she accepts A. We will say that there is a hierarchical relation among a and b provided the receiver of the message is considered dependent from the sender with respect to this message. This communication becomes in turn trust-qualified, as b does not possess any means to verify A, but uses it to hold B true. The verification of the message is represented in the formal model by the reduction of h to a term via β-reduction. 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. This strong status is what we shall formalize by means of terms of the *type*-kind and express by the induced $\Box$-modality, see Section 3.2 and Definition 12. As the content justified by agent a can in turn be based on some other content obtained by a via trusted communication from agent $a-1$, we will say that there is a hierarchy of trusted communications between agents $b < a < a-1$. The hierarchical structure of our agents seems to induce a very strong acyclic message-passage system, which would ban any receiver of a given communication act to ever be the sender in any other communication act involving the same agents. This possibly problematic issue is resolved by understanding that the hierarchical relation among agents is only induced by the dependency relation of contents involved in the message-passing system: it is the dependency of content B from content A that makes agent b hierarchically dependent on agent a and thus let us say that a trust relation of b from a holds with respect to content A. The hierarchical relation might well be reversed with respect to some other content C.

Coming back to our biologists, looking at the whole interactions, their result form Distributed Knowledge (DK, Theorem 1): the content of the paper can be inferred from what each and all the biologists together know. For the content of this distributed state to become actually knowledge for each of them, it is necessary that the verification process that validates a content is checkable and admissible to any peer. In the formal system this requires a notion of verification valid over contexts, which we shall interpret in terms of canonical proof-objects. As a result, direct verification of a content by each agent formally corresponds to removal of any trust relation (Theorem 2) and, in turn, the attaining of Common Knowledge (CK, Theorem 3).[6]

Our epistemic model deals therefore with different sorts of justifications in order to represent qualitative differences among epistemic states. A strong notion of verification is used to define a 'strong epistemic state' and this naturally recalls the Platonic notion of 'justified true belief'. The very same analogy has been put forward in Justification Logic, see e.g. [2,5], in which a language based on classical propositional logic is augmented by justification assertions $t : F$ that read 't is a justification for F'. Justification Logic assumes certain justification principles originating from both mainstream epistemology and the mathematical theory of proofs and use them to analyze a definition of knowledge relying on the fact that every valid principle of modal logics of knowledge such as T, $S4$, and $S5$ has a counterpart in it. The similarity of

[5] As our formal expression always looks at the content of messaging at the Receiver state, the model formalizes a delivery system in which communications are always successful. This would suggest that our analysis focuses only on the cases of query-triggered testimony. Nevertheless, the conceptual understanding of testimony remains neutral with this respect.

[6] This latter logical requirement induces a further difficulty with respect to real-based situations: the trustor behaves as a complete ignorant with respect to the trustee's verification, which puts the relation of trusted communication among scientists from related areas on a par with the same relation between an expert and a layman. The trustor needs in both cases to show additional competences in order to be able to reconstruct the verification initially grounding the trustee's information. This may be practically difficult to attain in the case of trusted communications between an expert and a layman. Nonetheless, from a logical point of view, admissibility of a proof-object at each index is a formal requirement that guarantees proofs are canonical.

the two approaches is not surprising, as Justification Logic can be traced back to the idea of provability models of the Brouwer–Heyting–Kolmogorov semantics (see [3]), whereas the constructive version of Type Theory explicitly refers to the realizability models of the very same semantics, according to the distinction that goes back to [42]. Nonetheless, major differences can be identified between the two approaches. In the first place, Justification Logic embeds the notion of justification into a classical logic propositional framework and therefore it also exploits the characteristic semantic treatment of related epistemic notions such as common and distributed knowledge. Secondly, it entirely misses the notion of dependent construction that is typical of the predicative format of Intuitionistic Type Theory and which is here exploited to define trust relations syntactically. Finally, and precisely on the basis of the previous point, it does not allow a polymorphic language as the one we will present in the next section, which allows us to define at the same time a stronger and a weaker epistemic state, and to characterize trusted communications as a relation among the two.

In Section 7 we shall refer extensively to the large number of other formal approaches that deal with the issue of trust and we will see how the greatest part of this literature presents semantic approaches, mostly pivoted on the use of Kripke semantics for modal logics. In the following, we will introduce one syntactic approach which we believe is worth exploring on its own. As explained above, it gives a fine-grained analysis of the relation between agent and content, making it possible to distinguish among different epistemic states. In doing so, it proves well-behaving in analyzing interesting properties for communication acts. Most importantly, our language is already in predicative form, whereas other semantic treatments mostly deal with propositional languages. Finally, it presents the advantage that it can be easily interpreted into machine-language via a translation to a procedural semantics, as mentioned in Section 7. Moreover, we do not know of any other formal treatment that so explicitly connects to the literature in epistemology for the problem of testimony under the reading we are proposing, where an act of testimony is understood as a first-order relation of communication characterized by the second-order property of trust.

3. A type theory for multi-agents epistemic processes

The constructive version of type theory (CTT)[7] admits objects as constructors defining types, hence the semantics entirely relies on the syntax of the language. In this paper, the standard syntax of CTT is extended as to accommodate indices on terms and variables constructors. Sets of indexed term constructors $a_i, b_j, \ldots$ and variable constructors $x_i, y_j, \ldots$ are used, so that each is a constructor for an appropriate type $A, B, \ldots$ and $i, j \in \mathcal{G}$ range over an enumerable set $\mathcal{G}$ of distinct sources or agents. We call these indices the *signatures* of the sources. Our types are propositions and each type is justified by a source-dependent construction, i.e. a *signed construction*. A message can always be taken to be passed from an agent to herself, as she trust her own assumption to formulate a given expression. In this case the expression contains only one index, $\mathcal{G}$ reduces to a singleton and the language to the mono-modal case.

An indexed term constructor a_i for type A is intended as the verification with signature (issued by source or agent) i that makes A a justified claim. The type-theoretic formula $a_i : A$ can be understood as expressing that a type A is presented with a name a for its proof-variable signed by its issuer i. Computationally, this corresponds to a term for which usual α-conversion applies. It will be ensured later on by the modal extension of the system that proof terms are treated as canonical within a group of signatures.

An indexed variable constructor x_i for a type A is intended as the consistently admissible but unverified claim of the truth A with signature (issued by source or agent) i. The type-theoretic formula $x_i : A$ can be understood as expressing that a type A is admitted or assumed by agent i: the computational explanation of this notion of assumption is based on a proof-variable for which no appropriate substitution is executed, but admissible. As this implies that a β-redex for A is possible, then by definition we are working with formulas that are not in normal form and with non-canonical terms. Also this property will be expressible by an appropriate modal extension of the language.

A single non-atomic formula can be obtained by distinctly signed terms or variable constructors. This happens according to two distinct cases, each involving one of the atomic types of the language. Where a formula is categorical and constructed out of proof-constructors a_i, b_j, it will be possible to sign it by either i or j, or both. Where a variable x_i is involved in a dependent construction performed under signature j, the obtained formula will be signed by both signatures i, j, but not separately. To express these properties, the modal extension of the language will apply to contextual judgements as well, inducing the definition of modal contexts and leading to appropriate counterparts of Common and Distributed Knowledge.[8]

3.1. The non-modal fragment for functional information

Let us start by defining the non-modal fragment of our language and giving it a sensible interpretation. Our alphabet is built by introducing the kinding:

[7] See [49,50]; see also [59] for an introduction oriented towards computer scientists and [62] for a more logico-philosophical perspective.

[8] The formal treatment of contextual reasoning and the dynamics of contexts originating in natural deduction calculi and inherited in the stronger format of constructive logic embedded in Martin-Löf's Type Theory is further analyzed in its natural language interpretation in [67]. The multi-contextual approach underlying our model recalls well-known research in Artificial Intelligence, see [51,29,30], which eventually led to the propositional logic and first-order logic of context, see [15,14]; [68] provides a general method for designing multi-contextual logics with agents. Recently a newly formulated semantics for constructive contextual K has been given in [53].

Definition 3 *(The set of kinds).* The set $\mathcal{K}$ of kinds includes two sets:

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

where *type* is the kind of all justified knowledge claims defined by term constructors, and $type_{inf}$ is the kind of all communicable information chunks defined by variable constructors. Elements of $type_{inf}$ can be used to define elements in *type*.

The objects in $\mathcal{K}$ are next defined via the set of terms:

Definition 4 *(The set of terms).* The set of terms $\mathcal{T} = \{\mathcal{C}, \mathcal{V}\}$ is given by the set of constructors for terms

$$\mathcal{C} := \{a_i; (a_i, b_j); a_i(b_j); \lambda(a_i(b_j)); \langle a_i, b_j\rangle\};$$

and the set of variables for terms

$$\mathcal{V} := \{x_i; (x_i(b_j)); (x_i(b_j))(a_i)\}.$$

So terms can be respectively:

- a_i – an inhabitant or constructor of our basic kind *type*;
- (a_i, b_j) – a pair of constructors;
- $a_i(b_j)$ – an application of constructors;
- $\lambda(a_i(b_j))$ – an abstraction of constructors;
- $\langle a_i, b_j\rangle$ – an ordered pair of constructors;
- x_i – a constructor for our basic kind $type_{inf}$;
- $(x_i(b_j))$ – an abstraction of a variable w.r.t. a constructor;
- $(x_i(b_j))(a_i)$ – the application of an abstracted variable to a type constructor.

Two remarks are needed here: first, variables in this language are not just abstractions from term constructors, rather separate terms on their own to construct the kind of $type_{inf}$; second, as our modalities are purely judgemental, $\mathcal{T}$ does not contain modal terms, as it is the case with other systems.[9] We now look at contexts.

Definition 5 *(Contexts).* A context is the set of assumptions under which a given constructor can be formulated. We construct contexts in the following way:

1. A type-theoretic expression $x_i : A$ is an assumption with $x_i \in \mathcal{T}$ and A $type_{inf}$; an assumption is the declaration that a source or agent i assumes an admissible construction for type A, which is then declared to be true.
2. A context Γ is a finite sequence of assumptions $\{x_i : A, \ldots, x_n : N\}$, all with distinct subjects. Each assumption in Γ depends on previous assumptions in the same context, i.e. each $x_i : \alpha$ depends on the assumptions from $x_1 : \alpha$ up to $x_{i-1} : \alpha$, where α stands for a metavariable in $\mathcal{K}$.
3. If $\Gamma = \{x_i : A, \ldots, x_n : N\}$, an extended context $\Delta = \{\Gamma, x_{n+1} : N + 1\}$ corresponds to $\Delta = \{x_i : A, \ldots, x_{n+1} : N + 1\}$. When the declaration of a freshly introduced variable $x_{n+1} : N + 1$ is meant to be independent of the order of declarations in Γ, we introduce it following a separation sign as follows: $\Gamma \mid x_{n+1} : N + 1$. A judgement dependent on a context of assumptions $J[x_i : A, \ldots, x_n : N]$, means that J *type* holds given the substitution $[x_i/a_i : \alpha]$ of each x_i with a certain a_i in α.

Standardly, contexts $\Gamma = \{x_1 : A_1, \ldots, x_n : A_n\}$ are built according to the requirement that wants the list of expressions in contexts to contain all distinct subjects. The structure of contexts in our language differs in the obvious sense that expressions with variables contained in a context are now made distinct by their signature from the set $\mathcal{T}$. Hence, we cannot just ensure that all signatures are different, because one single signature might be attached to different contents in the same context. We require instead explicitly the use of distinct elements in $\mathcal{K}$ for each expression in a context.[10]

We extend now our syntax with semantic judgements, considering two distinct truth predicates induced by our kinds:

Definition 6 *(Semantic judgements for $\mathcal{K}$).* The kinding $\mathcal{K}$ induces truth definitions as follows:

$$\frac{a_i : A}{A \; true} \text{ Truth Definition} \qquad \frac{A \; type_{inf} \quad x_i : A}{A \; true^*} \text{ Hypothetical Truth Definition.}$$

[9] See e.g. the languages presented in [56,55].

[10] This in turn implies the simplification that wants redundant information to be avoided within a context.

3.2. Axioms and rules for *type*

Let us analyze the rules for this non-modal fragment of our language. Typing for the first element in $\mathcal{K}$ gives the first basic axiom of the system:

Definition 7 *(Axiom for type).* $\vdash$ *type* : $\mathcal{K}$.

We need now to explain how to construct objects within the kind *type* based on constructions by signed terms a_i, b_j. Within this kind, we have a few construction steps: what is usually functional abstraction reduces to application; generalization by ∀-introduction and specification by ∃-introduction are restricted to enumerable constructors and without abstraction; a negation introduction is admissible by type checking on the enumerable constructions. The standard start rule is reformulated as a rule to introduce a premise; usual structural rules are easily defined for this fragment.

Definition 8 *(Rules for type).* The rules for signed expressions in the kind *type* are:

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

$$\frac{a_i : A \quad A\ \mathit{true} \vdash b_j : B}{a_i(b_j) : A \to B}\ I\to$$

$$\frac{a_1 : A, \ldots, a_n : A \quad A\ \mathit{true} \vdash b_j : B \quad \lambda((a_i(b_j))A, B)}{(\forall a_i : A)B\ \mathit{type}}\ I\forall$$

$$\frac{a_1 : A, \ldots, a_n : A \quad a_i : A \vdash b_j : B \quad (\langle a_i, b_j\rangle, A, B)}{(\exists a_i : A)B\ \mathit{type}}\ I\exists$$

$$\frac{a_i : A}{\neg A \to \bot}\ I\bot$$

$$\frac{}{\Gamma, a_i : A, \Delta \vdash A\ \mathit{true}}\ \text{Premise Rule}$$

$$\frac{\Gamma \vdash B\ \mathit{type} \quad \Gamma \vdash A\ \mathit{type}}{\Gamma \mid a_i : A \vdash B\ \mathit{type}}\ \text{Weakening}$$

$$\frac{\Gamma \mid a_i : A, b_j : B \vdash C\ \mathit{type} \quad \Gamma \vdash b_j : B}{\Gamma \mid a_i : A \vdash C\ \mathit{type}}\ \text{Contraction}$$

$$\frac{\Gamma \mid a_i : A, b_j : B \vdash C\ \mathit{type}}{\Gamma \mid b_j : B, a_i : A \vdash C\ \mathit{type}}\ \text{Exchange}$$

The structural rules can be interpreted as follows, with Γ, Δ possibly empty contexts. The Premise Rule corresponds to a Global Validity Rule: if the truth of A is generated at source i by verification, its validity is global to the relevant $\mathcal{G}$ to which i belongs. This property is obviously crucial to induce the desired canonical proof-terms, and important to validate the other structural rules. Weakening says that the external addition of a premise to the context of a truth is possible (but ineffective with respect to its value). Contraction says that if a context Γ includes a premise at an external source j, then what holds for Γ and the external premise at j, holds at Γ. Exchange says that the order of external premises is not relevant (whereas it will be for assumptions in a context, under the fragment for type_{inf}). Notice that the validity of Weakening, Contraction and Exchange is restricted to external premises, i.e. for additional sources not within a context but attached to a context, for which we use the separator | after the contexts. This is because by Definition 5, assumptions in a context come with a strict order relation, such that each element depends on previous ones: this imposes that addition or exchange of premises do not interfere with such order.

3.3. Axioms and rules for type_{inf}

The new inhabitant for our kinding, namely type_{inf}, requires specific typing and formation rules, based on our notion of legal assumption. We state the ability of a user or source $i \in \mathcal{G}$ to generate a legal assumption for A whenever in the enumerable set of multi-indexed constructions available to $\mathcal{G}$, no declaration $A \to \bot$ is construed. The weak constructive nature of this principle recalls Kolmogorov's notion of pseudo-truth introduced in [43]. The admissibility rule for the type_{inf}

sort interprets the distinction between intensionality and extensionality of types, treated e.g. explicitly in [60]: expressions are treated intensionally being subject only to α-conversion; terms are treated extensionally, being additionally subject to β and η-conversion.[11]

Definition 9 *(Axiom for $type_{inf}$).* $\vdash type_{inf} : \mathcal{K}$.

Constructors for $type_{inf}$ are restricted to interpret the function formation rule. The construction for $type_{inf}$ is based on a missing refutation for the corresponding *type*, i.e. it is configured as double negation introduction, without elimination. The β-conversion rule expresses substitution of an open variable with a value constructor, i.e. it constructs an appropriate value for a non-contradicting assumption, representing the reduction to *type*. An α-conversion rule expresses substitution, by the obvious inductive definition, of an instance of value constructor for a signed variable on a finite domain of equivalent constructors, constructing a function among those defining a class of dependent types.

Definition 10 *(Rules for $type_{inf}$).* The rules for signed expressions in the kind $type_{inf}$ are:

$$\frac{\neg(A \to \bot)\ type}{A\ type_{inf}}\quad type_{inf}\ \text{Formation}$$

$$\frac{A\ type_{inf} \quad b_j : B[x_i : A]}{((x_i)b_j) : A \supset B\ true}\quad \text{Functional abstraction}$$

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

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

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

$$\frac{\Gamma \vdash B\ type_{inf} \quad x_i : A \vdash A\ type_{inf}}{\Gamma \mid x_i : A \vdash B\ type_{inf}}\quad \text{Weakening}$$

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

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

The structural rules can be interpreted as follows. The Hypothesis Rule is a Local Validity Rule: if the truth of A depends on a legal assumption at source i, its validity is bound (starred) to that point in $\mathcal{G}$, until discharged (by β-conversion). Weakening says that the addition of a legal hypothesis external to the context of a starred truth is possible (but ineffective with respect to its value). Contraction says that if a context Γ includes a legal assumption at source j, then what holds for Γ and the explicit external formulation of the assumption at j, holds at Γ. Exchange says that the order of external assumptions is not relevant. Notice that in this case, validity of the structural rules is restricted to assumptions that are not in a relation order within a context (presence of the context separator in the Exchange Rule).

3.4. *The multi-modal fragment: reasoning about collective knowledge*

The aim of the present section is to introduce modal operators in order to generalize the formulation of available judgements. From Definition 5 of context and the construction of our alphabet, modalities are defined on the basis of the different kinds. If all subformulae in a dependent expression have the same index, our language reduces to the mono-modal polymorphic type theory presented in [65]. Otherwise, the machinery for a multi-modal language needs to be developed, with the

[11] The Lax modality defined in a propositional intuitionistic logic in [23] has also similar properties: the modal formula $\circ\phi$ expresses the inhabitation of ϕ in the context of a number of assumptions holding in a stronger theory; the theory designs two distinct and dual contexts: one where the formula is true only in certain worlds where appropriate constraints hold, the other only where constraints are false. The former is the partial element lifting and the latter the exception lifting for the type formula ϕ at hand. See [23, p. 65]. Our double-negated typing might be seen as a way of admitting the first kind of constraints, up to proving that the second kind holds.

further complication of determining if the modalities involved are all definable within the same language (in other words, if the language is homogeneous or heterogeneous). With the multi-modalities, derivability in context generates different forms of collective knowledge of a judgement J under a multi-modal context Σ.

We start from considering a judgement $\Gamma \vdash J$. The validity of J depending on the (ordered) list of assumptions in Γ formalizes an assumption-based reasoning process from declarations generated by multiple agents $\{i, \ldots, n\} \in \mathcal{G}$ all occurring in Γ. Ordering the declarations in Γ expresses the fact that these are not independent typing declarations, rather there is a strict order relation among signed assumptions.[12] We are therefore describing the structure of a process in which each agent i *communicates* a message ϕ that another agent j lower in the list $(i < j)$ takes as a *reliable* message. Each such communication is expressed as the function that makes ϕ valid at j provided it is valid at i. When the communication involves more that one content ϕ or more than two agents $i < j < k$, we express the state at k dependently from the extension of a context Γ_i by a context Δ_j.[13]

Whereas in standard modal logics, operators are defined by the corresponding accessibility relations on worlds; we induce them from the (local) validity of hypotheses, simulating update on epistemic conditions from the validity of some propositional truth. The basic idea is to express the validity of a proposition within such context, and to use modalities to define the possible extension of such validity under accessibility of other contexts: necessity is explained as validity in all contexts and possibility as validity in some contexts. The role of the accessibility relation among contexts is played by a context extension function, which can be seen as a form of contextual weakening[14]:

$$\frac{\Gamma \vdash A\ \mathit{true}}{\Gamma \mid \Delta \vdash A\ \mathit{true}}\ \text{Context Extension}$$

The justification of the main judgement *A true* determines if all or some contexts Δ extending the relevant context Γ are valid, where both Γ, Δ can be taken to be empty. In the first case, if any Δ extending a context Γ preserves *A true*, it means $\Gamma \vdash a : A$ holds and eventually $\Gamma = \emptyset$. This holds provided that: (1) according to Definition 5, any declaration in Γ has its corresponding β-redex and so it is in normal form; and (2) no non-monotonic extension by a $\mathit{type}_{\mathit{inf}}$ term is possible with respect to constructors in Γ. In the second case, if *A true* is valid under some non-empty Γ containing $\mathit{type}_{\mathit{inf}}$ expressions, only some of the extensions of the latter context will keep the judgement *A true* valid. In this sense, the weakening

$$\frac{\Gamma \vdash A\ \mathit{true}^{*}}{\Gamma \mid \Delta \vdash A\ \mathit{true}}\ \text{Local Context Extension}$$

is possible iff Δ provides no redex falsifying some $(x_i : \alpha) \in \Gamma$. This means that the extension by a predicate true^{*} is not necessarily monotonic, and hence the inference holds under some but not all context extensions. This explanation gives the following definition of simple or global contextual validity under extension:

Definition 11 *(Validity under contextual extension).* A type A derivable in a context $\Gamma \mid \Delta$ holds as follows:

1. The judgement $J = A\ \mathit{true}$ is justified by $[x_i/a_i] : A$ in context Γ, i.e. its construction is in normal form in Γ and it remains valid under any extension $\Gamma \mid \Delta$; then A is said to be globally valid under $\Gamma \mid \Delta$;
2. The judgement $J = A\ \mathit{true}^{*}$ is justified by $x_i : A$ in context Γ, i.e. its construction contains all needed open variables but is not in normal form in Γ or in some extension $\Gamma \mid \Delta$; then A is said to be locally valid under $\Gamma \mid \Delta$.

The notion of global validity holds obviously for categorical judgements as special cases of contextual global validity under empty contexts: by definition with $\Gamma = \emptyset$, it holds that $\emptyset \vdash A\ \mathit{true} \Rightarrow \Gamma \vdash A\ \mathit{true}$, for any Γ. The context extension operation allows for mimicking syntactically the notion of accessibility on worlds, so that judgemental modal operators express that a proof holds somewhere or everywhere, with respect to contexts.[15]

We inherit now modal judgements from indexed constructors, to express single-agent modes of validity:

Definition 12 *(Modal judgements).* The set of modal judgements $\mathcal{M}$ for any $i \in \mathcal{G}$ is defined by the following modal formation rules:

$$\frac{a_i : A}{\Box_i(A\ \mathit{true})}\ \Box\text{-Formation} \qquad \frac{x_i : A}{\Diamond_i(A\ \mathit{true})}\ \Diamond\text{-Formation}$$

[12] The counterpart strategy amounts to collecting *distinct* and equally ordered indexed contexts (eventually singletons), when we want to express that the different sources are not prioritized. This is the strategy pursued for the mono-modal version in [65].

[13] Our model simulates a *reliable message delivery systems*, see [24], where for each agent holding a content true there is an effective communication chain towards her (but in our case not necessarily from her), meaning that for each content that is known, it is also transmitted. We shall further develop this analogy, in particular to show the holding of properties involved by the usual definitions of Common and Distributed Knowledge.

[14] In a comparison with the standard modal explanation, one would say that the validity of A is *indistinguishable* from the point of view of contexts Γ and Δ.

[15] Our distinction between terms and modal operators is technically the same distinction that it is obtained in [55] by distinguishing between variables for different kind of hypotheses and labels to refer to locations of such constructors. We can directly use modalities because we define them as judgement rather than propositional operators, hence they apply to processes rather than to specifications.

The meaning of these expressions is the following: $\Box_i(A\ \mathit{true})$ says that if A is true by a verification (constructor in normal form) generated by source i, then it will be valid with respect to any context accessible from i (i.e. under any context that extends the empty context of i); $\Diamond_i(A\ \mathit{true})$ says that if A is declared true by a legal assumption (constructor in non-normal form) generated by source i, then it will be locally valid with respect to some context accessible from i. We want now to make explicit this hidden reference to contextually accessible modal judgements:

Definition 13 *(Signed and modal contexts).* A signed modal context is construed as follows:

1. If all declarations in context Γ are signed by index i, we indicate it as $\Gamma_i = \{x_i : A, \ldots, x_i : N\}$ (where all subjects $\{A, \ldots, N\} \in \mathit{type}_{\mathit{inf}}$ are distinct);
2. Given an expression $x_i : A$ by the rule of $\Diamond$-Formation we obtain the expression $\Diamond_i(A\ \mathit{true})$, which declares that A is a type valid for some extension of context Γ_i;
3. Given a construction a_i available for the explicit substitution $[x_i/a_i] : A$ by the rule of $\Box$-Formation we obtain the expression $\Box_i(A\ \mathit{true})$, which declares that A is a type valid for any extension of context Γ_i;
4. For any context Γ_i, if there is at least one $A \in \Gamma$ such that $\Diamond_i(A\ \mathit{true})$, we infer $\Diamond_i\Gamma$;
5. For any context Γ_i, if for all $A \in \Gamma$ it holds $\Box_i(A\ \mathit{true})$, we infer $\Box_i\Gamma$.

By the first clause in this definition, a signed context Γ_i behaves like a standard context where all declarations are generated at the same source; by the second and the third clause each declaration in a context Γ_i can be transformed in the appropriate modal counterpart by the corresponding modal Formation rule; by the fourth clause a context containing all boxed assumptions becomes a boxed context; by the fifth clause the presence of a locally valid assumption makes the corresponding context a locally valid one.

3.5. Extension to multi-modalities

Now that definitions for modal contexts with a unique index have been formulated, each context can be defined further by allowing differently indexed modalities to interact with one another. This is obtained by extending a signed (modal) context $\circ\Gamma_i$ in view of a differently signed (modal) context $\circ\Delta_j$. This extension is meant to allow judgements of the form

$$(1)\quad \Diamond_{\mathcal{G}}\Gamma \vdash \Diamond_k(A\ \mathit{true})$$

$$(2)\quad \Box_{\mathcal{G}}\Gamma \vdash \Box_k(A\ \mathit{true})$$

where $\mathcal{G} = \{i, \ldots, j\}$ and $j < k$. The modal dependency defined by these formulas allows for different interpretations: formulas of the type (1) say that "A is a message accepted as true by agent k, trusting the information Γ received from agent i to agent $j \in \mathcal{G}$", where $i \leqslant j \leqslant k$ is a strict order relation; formulas of the type (2) rely on actual verification of the involved contextual formulae, resulting in an epistemic expression where the trust relation is no longer necessary. We shall consider which of the typical bridging axioms for normal multi-modal logics fit best the composition of such two interpretations.

In the first place we have to define the construction rule for $\circ_{\mathcal{G}}\Gamma$, where $\circ = \{\Box, \Diamond\}$. The role of contexts is primarily that of formalizing information communication acts and the inner order of their structure simulates the strict order relation of trust among agents. The modalities prefixing a context will dictate the nature of any epistemic state valid under such a context. A consistency constraint is intuitively satisfied as follows: it is impossible for an extension $\Box_i\Gamma \mid \circ_j\Delta$ to be such that $\Box_i(A\ \mathit{true})$ holds and the extension $x_j : A \to \bot$ being admitted; $\Diamond_i\Gamma \mid \circ_j\Delta$ allows instead any extension by definition of $\mathit{type}_{\mathit{inf}}$ present in Γ. (Here and in the following Γ, Δ are always sets, whereas Σ is always a multiset and J on the right-hand side of the derivability relation is meant to be a place holder for any derivable judgement of the form $(A\ \mathit{true})$.)

Definition 14 *(Extension of signed and modal contexts).* An extended signed modal context is construed as follows:

1. A multi-modal context $\Sigma_{i,j}$ is a context extension

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

   where $\circ = \{\Box; \Diamond\}$ and the set of signatures used in $\Sigma_{i,j}$ are abbreviated as $\Sigma_{\mathcal{G}}$;
2. A context extension $\circ_i\Gamma \mid \circ_j\Delta$ is admissible if, for any judgement $J \in \Delta$ such that $J = A\ \mathit{type}_{\mathit{inf}}$, $\Gamma \nvdash (A \to \bot)$;
3. A multi-modal context $\Sigma_{\mathcal{G}}$ is prefixed by an appropriate multi-modal operator $\Box_{\mathcal{G}}$ or $\Diamond_{\mathcal{G}}$ following appropriate counterparts of instruction items 4 and 5 of Definition 13;
4. The type-theoretic expression $\Diamond_{\mathcal{G}}\Sigma \vdash J$ is thus obtained by

   $$\Box_i\Gamma \mid \Diamond_j\Delta \vdash J$$

   and it expresses the local validity of J from source i and j by information available at source j accessed from source i; the content of J remains unverified, and hence refutable, at some further point k;

5. The type-theoretic expression $\Box_{\mathcal{G}} \Sigma \vdash J$ is thus obtained by

$$\Box_i \Gamma \mid \Box_j \Delta \vdash J$$

and it expresses the global validity of J from source i and j, in view of the information that source j makes available when accessed from source i; the content of J remains verified, hence irrefutable, at any further point k.

By this definition, a multi-modal context is the extension of mono-modal contexts (given eventually by singletons) with an accordingly modified signature. The informal reading of the formula $\circ_i \Gamma \mid \circ_j \Delta$ is that a communication process about information contained in J happens from the agent or source i to agent or source j, for $i \leqslant j \in \mathcal{G}$.

We can now define modal derivability from multi-modal contexts, i.e. where now we admit a context to include an enumerable number of distinct signatures $\mathcal{G} = \{1, \dots, n\}$[16]:

Definition 15 *(Modal judgements from multi-signed contexts).* Modal judgements are derived from multi-modal signed contexts according to the following cases:

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

Our next aim is to evaluate multi-modal contextual derivations and to explore the resulting properties. It will be shown how evaluation on information communicated under trust results in knowledge formation (common and distributed).

4. From reliable Communication to Knowledge

The interpretation of modal derivability for our type-theoretic language in terms of reliable communication and knowledge will start by considering first the properties for the epistemic operation of communication of (unverified, functional) information constrained by the hierarchy of agents. Then we shall consider how to bridge this system with the additional properties obtained by performing verification. Finally, we will see which properties survive the upgrade to knowledge.

4.1. Properties of trusted communication

The weaker epistemic state involved in the process of communication corresponds in the type-theoretic setting to the use of open (refutable) judgements $x_i : A$ in a dependent judgement. Such formula admits the inference to the $\Diamond_i$ operator by the modal formation rule in Definition 12. The informal meaning of the $\Diamond$-Formation rule is therefore that if A is admissible in the system, then someone has information about A. Notice that, being generated from the weaker *true** predicate, this rule keeps reliability separated from alethic properties, whence validity is not guaranteed. Informally, this tells us that acceptance of contents is based on the trust relation among agents, without implying global truth of the communicated messages.[17] In the case of $\mathcal{G} = \{1\}$, we have the admissibility of the formula

$$\frac{}{\Gamma, x_i : A, \Delta \vdash \Diamond_i(A\ true)}\ \text{Autonomous Hypothesis Rule}$$

This rule expresses the basic property that agents trust themselves on admissible contents.[18] This rule can be generalized under hypotheses to admit a form of *Reflexivity*:

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

With $\mathcal{G} = \{1, \dots, n\}, n > 1$, the basic requirement is that communications happen in a strictly ordered way, from higher to lower positions in the trust hierarchy. Under this proviso, a communication formula $x_i : A$ is always taken to hold in the context of information generated at Γ_{i-1}.

In the following, we shall abbreviate any formula of the form $(A\ true)$ by J, followed by indices $J', J'', \dots$ when we want to refer to distinct contents $(A, B, \dots) \in \mathcal{K}$. In turn, any modal judgement $\circ_{i \in \mathcal{G}}(A\ true) \mid \circ = \{\Box, \Diamond\}$ will be abbreviated by

[16] Indices for agents can be compared intuitively to different states in a Kripke semantics. The context extension function works as a domain inclusion assumption in relational Kripke structures: if $M = (S, \pi, k_1, \dots, k_n)$ is such a structure and $(s, t) \in k_i$, according to the domain inclusion assumption $dom(\pi(s)) \subseteq dom(\pi(t))$, i.e. one assumes that if the state t is connected from s, then the domain corresponding to s is a subset of the domain corresponding to t, cf. [24, pp. 86–87]. Under this analogy, a context extension produces a subset of the overall domain on which evaluations are performed and the formula $\circ_i \Gamma \mid \circ_j \Delta$ says that the contents in Δ are accessible from those in Γ, where the properties of such accessibility shall depend on the configuration given by $\circ_i$ and $\circ_j$.

[17] This rule goes via the inference $x_i : A \Rightarrow A\ true^* \Rightarrow \Diamond_i(A\ true)$, generating a weaker form of the 'vigilance' property suggested in [21]. As we shall see later on, the *true* predicate, on the other hand, enforces communication of true messages.

[18] This is a basic weaker counterpart of 'sincerity' than what is admitted in [21].

$\circ_i J$. In order to express the admissibility of B at signature j based on trusting A *true* at signature i and $i < j$ we shall use the abbreviated format $\Diamond_j(B\ true)[\Diamond_i(A\ true)]$, further simplified as $\Diamond_k J[\Diamond_i J']$. Whenever the content is intended to be the same, we shall of course drop the index on judgements. Now we can use this simplified notation to define our notion of Communication Chain:

Definition 16 *(Communication Chain).* For every message $\Diamond J$ and agents $\mathcal{G} = \{i < k\}$, either $\Diamond_k J[\Diamond_i J]$ and $k = j$, or there is a j such that $\mathcal{G} = \{i < j < k\}$ and $\Diamond_k J[\Diamond_j J[\Diamond_i J]]$. We call the hierarchical relation between $i, j, k \in \mathcal{G}$ a Communication Chain where $\Diamond_k J$ relies on $\Diamond_j J$, which relies on $\Diamond_i J$.

By this definition every communication is unidirectional (going top-down in the trust hierarchy) and compact (meaning that messages are communicated among all agents present in the hierarchy).[19] We can now use the notion of Communication Chain and its structure to unveil the definition of Trusted Communication, which is our formal counterpart to the definition of Testimony given in Definition 2:

Definition 17 *(Trusted Communication).* We say that a Trusted Communication is a ternary relation $TC = \langle \Diamond_i, \Diamond_j, J\rangle$, $i < j \in \mathcal{G}$, holding between the epistemic state of the sender, that we indicate by the corresponding modal attitude expressed by $\Diamond_i$, the epistemic state of the receiver, equivalently indicated by the corresponding modal attitude expressed by $\Diamond_j$, and a content J. A *TC* is then enforced by a Communication Chain of the form $\Diamond_j J[\Diamond_i J]$ and $x_i : A \vdash \Diamond_i J$.

The first and second element in the ternary relation are the epistemic states of the trustor and of the trustee towards the content of J. This third element in the relation enforced by *TC* can be of course composed by distinct judgements J, J' when $J \vdash J'$. A generalization of this definition enforcing relations among *sets of* trustors and trustees can be given by defining identity over agents, starting from equality rules of contents defined over the corresponding derivability relations: agents i and j enforce the same set of TCs with respect to another agent k and a content J iff the derivability relations indexed by i and k produce the same set of judgements as that indexed by j and k.[20]

By the definition of Communication Chain, a form of (ordered) *Transitivity* called *Transmission* is enforced:

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

It says that if Agent k trusts Agent j on J and Agent j holds J trusting Agent i on J', then Agent k will also consider Agent i trustworthy on J' (for $(i < j < k \in \mathcal{G})$). An example of this property on the trust relation can be formulated as follows: a patient (agent k) trusts her doctor (agent j) to provide correct medical information and diagnosis (J); agent j holds J because she trusts his studies (agent i) to have provided accurate information about how to formulate diagnoses; then (though indirectly) agent k trusts agent i to provide accurate information about how to formulate diagnoses.[21]

Obviously, we do not want to admit that a trusted communication be reversible in the order of the signatures, to avoid the validity of expressions of the following form: "If Agent j considers B true by trusting Agent i on the truth of A, then Agent i considers A true by trusting Agent j on the truth of B". Hence *Symmetry* for such a relation is not admitted, in other words a trusted communication is a uni-directional relation.[22] In this way, our trust relation is transitive only towards sources, but not towards receivers.

The epistemic value of functional information as admissible (but unverified) content should be preserved under locally valid modal contexts. This means that from a multi-context $\Diamond_{\mathcal{G}}\Sigma$ one infers possibility judgements. This validates the following rules:

[19] As we focus on a delivery system, i.e. on the message from the point of view of the receiver, we cannot grant that every message sent is successfully received.

[20] The restriction enforced by considering an occurrence of trust between two agents with respect to a content, perfectly endorses the definition of *trust relationship at runtime* for information systems given in [76], where also the generalization to sets of agents is presented.

[21] We model this property having in mind its semantic counterpart: the difference between Transmission and Transitivity is that whereas the former is of the form $K_a K_b p \rightarrow K_a p$, the latter takes the form $K_a p \rightarrow K_b K_a p$, with a, b in the set of Agents and p a propositional content of information. [38, Section 4.2] uses the term 'Transmissibility' to refer to such a property of communication. 'Transmission' is also used in the literature on the epistemology of testimony, for instance [45] uses "transmission of epistemic properties" as a label for several theories of testimony. Notice that the transitivity of trust only applies to identical tokens of information (in this case J'), which guarantees that – in the previous example – agent i is trusted only with respect to the communication of J' and not with respect to any other instance of information she may hold. This is a most needed property, which is formally secured by the fact that the transmissions are defined by dependencies of content generated by agents. Trust is then the property holding between agents instantiating such transmissions. This means that trust between agents i, j, k is not generalized with respect to any other information item they might possibly share. Transitivity as the basic property for generation of trust among unknown entities in information systems is studied in [40].

[22] To put it in a rough comparison with the model developed in [18], we are not considering in this formal framework any 'outputting trust' relation, that is the relation of trust relating the process of transmitting knowledge from the knowing to the accepting agent and the trust that the former has in the latter. Nonetheless, the asymmetric nature of our model can be avoided in an obvious way, by defining two distinct TC's reversing the order of the indices in the first two elements of the triple.

Definition 18 *(Rules for $\Diamond_{\mathcal{G}}\Sigma$).* The set of rules for working within a multi-modal context $\Diamond_{\mathcal{G}}\Sigma$ are of the following form:

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

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

The first rule is an instance of substitution of declarations within contexts with modal assumptions: by extending the (either global or local) Γ_i with information accessible locally at source j, the judgement ($B\ true$) is prefixed by $\Diamond_{i,j}$, meaning these sources are always to be called upon for the validity of B (i.e. B holds at their intersection). The corresponding elimination starts from a similarly derivable judgement $\Diamond_{i,j}(A\ true)$ to infer its variable constructor (which needs to be located) and to obtain a well-formed $\Diamond_{j,k}(B\ true)$, then it infers that the initial conditions $\Gamma_i \mid \Delta_j$ suffice to derive the local validity of B (without the additional location of A). The multiplicity condition means that equivalent operations need to be performed within Γ_i, Δ_j where necessary.

We can now reconnect these inference rules for $\Diamond$ with the notion of Trusted Communication as given by Definition 17 in order to relate trusted information to derivable contents:

Definition 19 *(Sequenced admissible communication).* If $\Diamond_l J[\Diamond_i J', \ldots, \Diamond_k J^n]$, we write $\Diamond_{i,k}\Sigma \vdash \Diamond_l J$ and say that

1. judgement J is reachable at l ($k \leqslant l \in \mathcal{G}$) from $\Diamond_{i,k}\Sigma$ if there are trusted communications $TC^1 = \langle \Diamond_i, J\rangle$ up to $TC^n = \langle \Diamond_k, \Diamond_l, J, J^n\rangle$ such that at TC^k agent l trusts agents k on the content of J^n to infer the content of J, at TC^{k-1} agent k trusts agents $k-1$ on the content of J^{n-1} to infer the content of J^n and so on up to TC^{1-k} where agent $i+1$ trusts agent i on the content of J' to infer the content of $J^{'+1}$, and
2. $\Sigma_{i,k} \mid \Diamond_l\Delta$ is admissible.

The first condition says that an accessible informational content in a multi-modal context needs to be reachable from a sequence of trusted communications among the ordered agents. The second condition says that the extension of the multi-modal context by the communicated information needs to be admissible. As a lemma, we obtain that trusted communication leads to admissibility:

Lemma 1 *(Admissibility via Trusted Communication). Given $\Diamond_{i,k}\Sigma \vdash \Diamond_l J$, for $\mathcal{G} = \{i < j < k\}$ and $TC = \langle \Diamond_i, \ldots, \Diamond_k, J\rangle$,*

1. *either $\Gamma_{i,k} \mid \Delta_j$ is admissible, or*
2. *there are judgements $\langle \Diamond_j J', \ldots, \Diamond_k J^n\rangle$ such that $TC^1 = \langle \Diamond_i, \Diamond_j, J_j\rangle$ up to $TC^{n-1} = \langle \Diamond_j, \Diamond_k, J_k\rangle$ and $\Diamond_l J[\Diamond_j J', \ldots, \Diamond_k J^n]$.*

Proof. The proof goes by induction on the length of the propositional contents $(A, \ldots, N) \in \Sigma$:

- $k = 1$ is satisfied by the Autonomous Hypothesis Rule, which also shows the two conditions to be not exclusive;
- where $k > 1$, there are at least $k - 1$ steps in trusted communication such that at the latter of these steps $\Diamond_l J$ becomes admissible in view of the multi-modal context $\Sigma_{j,k}$. Each such step will consist of any of the rules for $type_{inf}$ such that the construction of $\Diamond_{j,k}\Sigma$ is preserved.[23] □

4.2. Bridging properties

The β-conversion rule listed for the $type_{inf}$ kind is the syntactical rule that enforces verification of communicated information, giving the bridge from possibility to necessity contexts. Going in the other direction, a modal version of abstraction on terms expresses communication of verified information, giving the bridge from necessity to possibility contexts. This shows the basic interaction between the two forms of modal judgements that can be generated from *type* and $type_{inf}$ formulae. We list in the following the properties resulting from admitting this bridging among the two modalities.

Let us start from the latter case, obtained by the following $\Diamond$-import rule:

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

[23] Notice that Definition 19 and Lemma 1 give for our system what the definition of reachability in asynchronous message passing systems and Lemma 4.5.2 give for message transmission in [24, p. 146].

justified by an instance of the Hypothesis Rule and $\Diamond$-Formation. It says that starting from $a_i : A$, one is allowed to infer $x_i : A$, or in other words that each content derivable from an agent's state can always be formulated in the weaker informational state of the same agent.[24] If we force the order relation to work in the rule and use accessibility to a new state in the first premise, we can provide an instance of the $\Diamond$-Import rule that satisfies Common Seriality:

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

The intuitive meaning of *Common Seriality* is that each agent's knowledge (conclusion of the first premise) can be traced back to some agent's information (second premise and conclusion). Note that by Definition 16 where reflexivity holds, this does not need to imply an infinite chain. This intuitively refers to the path of trusted communications that links together the agents in the hierarchy.[25]

The modal version of β-conversion is here reformulated as $\Box$-Import:

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

obtained by an instance of the Premise Rule and $\Box$-Formation.

If we look at the modal import rules, we obtain a description of our agents as informers consistent with their knowledge and knowers consistent with their verified informations. Notice that information reduces to knowledge only provided that for every fresh variable constructor x_i of the type_{inf} on a $\Diamond$-Import Rule, a new application of the β-Conversion Rule is formulated such that the corresponding $B\ \mathit{type}_{inf}$ in its second premise is reduced to its normal form $B\ \mathit{type}$ and in the conclusion every occurrence of $\Diamond_{i,j}(B\ \mathit{true})$ is reduced to $\Box_{i,j}(B\ \mathit{true})$.

To interpret the transmission of epistemic contents among distinct agents, we enforce a rule for communication of known contents corresponding to convergence:

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

Informally, this rule says that if there is a knowledge obtained at i and j is informed about that (for the usual $i < j$ and using Common Seriality), then at i it is known that j is informed about that. Convergence satisfies Semi-Adjunction (or Seriality, for the mono-modal B) as an instance, which means that the condition expressed by Convergence is strictly stronger than Common Seriality, as it implies that knowledge is communicated and that communications are known: if something is known to be communicated, then each agent knows that those lower in the trust hierarchy are informed about it. Convergence ensures the transparency of the system, as it allows all the agents to know what content has been communicated and at what level of the hierarchy.

4.3. *Properties of knowledge*

The validity of truth from $\Box$ was already established by the *Truth Definition* in Definition 6, which implements an equivalent of (standard) Axiom T, preserving Reflexivity, saying that any verified A is valid and hence admissible in any context. In this case trust does no longer occur, as the receiving agent accepts a content A as true on the basis of its verification. Hence, in our model truth of contents is independent from the trust in the sender.

We rely on the basic property instantiated by the first item in Definition 15, according to which $\Box_k(A\ \mathit{true})$ is derivable from $\emptyset \mid \Box_j\Gamma$ and hence $\Gamma_j \mid \Delta_k$ is admissible for $\Delta = \{\Box_k(A\ \mathit{true})\}$. This definition implies the validity of $(A\ \mathit{true})$ at any point in $\mathcal{G}$, which establishes modal derivability under verification:

Definition 20 *(Rules for $\Box_\mathcal{G}\Sigma$).* The set of rules for working within a modal context $\Box_\mathcal{G}\Sigma$ are of the following form:

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

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

[24] Hence, it provides a counterpart to the model-theoretic D axiom scheme $\Box\alpha \rightarrow \Diamond\alpha$.

[25] The relation between trusting agents and the occurrence of communication analyzed in [21] implements a cooperativity axiom that forces *each* belief content to be communicated among trusting agents. From our Common Seriality Rule a much more reasonable property is obtained: where knowledge has been achieved in the context of trusting agents, communication has been performed.

The first rule is an instance of β-conversion followed by $I\Box$, which explains how to turn local validity into global validity by instantiation of all premises: in other words, we require that each term be valid at all sources accessible from within $\mathcal{G}$. This is the fundamental step towards the elaboration of CK, where all the known contents are equally accessible from any agent in the system. Notice that in the base case of $\Sigma = \{\emptyset\}$, this multi-modal rule becomes of the form $\Box_{0,1}$, verifying the Necessitation Rule. The corresponding elimination starts from a similarly derived $\Box_{\mathcal{G}}(B\ true)$ to decompose its conditions. The multiplicity condition applies as in the corresponding rule for $\Diamond\Sigma$. This explanation of knowledge makes the notion of validity of a content A known by some agent i strictly dependent on data verification that is accessible by i and equally by any other agent involved in the knowledge process, but completely independent from any trust relation among those agents.[26]

By a specific instance of derivability under $\Box_n\Sigma$, we show the admissibility of $\Box_k(A\ true)$ by any $\Gamma_i, \Delta_j \in \Box_n\Sigma$ and $i < j < k \in \mathcal{G}$, from which follows *Upper Inclusion*, that is accessibility of valid contents at any higher point in $\mathcal{G}$:

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

The intuitive meaning of Upper Inclusion is that if an agent has some verified knowledge, then every other agent higher in the trust hierarchy knows it. This is proven by relying on the assumption that locating the source of the proven content admissibility extends the initial contexts and is accessible directly from there. The converse *Lower Inclusion* expresses accessibility of valid contents at any lower admissible point in $\mathcal{G}$:

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

It establishes the same relation in the reverse order. Even though this might seem obvious in view of the definition of our $\Box$ operator, its actual explanation requires additionally that the lower point considered be in fact accessible, a requirement satisfied implicitly by the second premise in the rule. This hidden requirement is to be made explicit on the basis of the communication operation within knowledge, ensured by Common Seriality from the previous section.

Letting the Inclusion properties follow one another, validity implies admissibility at each point, which in turn says that *Equivalence* holds:

$$\frac{\Box_i\Gamma \vdash \Box_i(A\ true)}{\Box_i\Gamma \mid \Box_j\Delta \vdash \Box_{i,j}(A\ true)}\ \text{Equivalence}$$

to be read both top-down and bottom-up. If we take $|\mathcal{G}| > 2$, we can also validate a version of *Union*:

$$\frac{\Box_i\Gamma \mid \Box_j\Delta \vdash \Box_k(A\ true)}{\Box_{\mathcal{G}}\Sigma \vdash \Box_{i,j,k}(A\ true)}\ \text{Union}$$

which is again readable in both directions and holds by the required multiple substitutions of i, j for $\Box_{\mathcal{G}}\Sigma$ in the Inclusion rules and the Compactness property from Definition 16. Notice that by the multi-modal version of $\Box_{1,2}$-Formation, we can instantiate ordered iteration very easily:

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

which says that if at k it is known that A is true in the context of reliable sources i, j, then in the same context it is known at k that A being true is known at i, j (in other words, anything known at some point is known at that point to be known at higher points). This is obtained by applying Common Seriality. The counterpart

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

says that if at k it is known that A is true in the context of reliable sources i, j, then in the same context it is known at i, j that A is known to be true at k. This is easily derivable from Convergence and β-Reduction.[27]

[26] The equivalence of verification for any agent in the same group as the one actually issuing the proof-term is a necessary requirement to enforce a sensible notion of knowledge and to avoid that either trusted communications be reduced only to refutable beliefs or a solipsist turn of the underlying epistemology. This requirement is formally satisfied by α-conversion and our definition of the $\Box$ operator.

[27] The proof that the present type-theoretic language including both modalities actually correspond to a non-standard fragment of a modal Kripke semantics is possible in view of a variant of the constructive modal logic introduced in [1]. Then the fragment containing only the $\Box$ modality can be proven equivalent to $S4$ models, whereas with the $\Diamond$ operator it reduces to a contextual format of $KT_\Diamond$. This result is shown in ongoing research, see [63].

5. Distributed and Common Knowledge

The standard intuitive definition of Distributed Knowledge (*DK*) from epistemic logics says that a group has distributed knowledge of proposition A if the combined knowledge of agents in the group implies A.[28] The basic requirement is therefore that not every item in the knowledge base is accessible to every agent involved in the reasoning process and that therefore the deductive closure is performed 'outside of the box' to find what all agents together might know (the 'wise man' knowledge). In the case of knowledge processes based on a trust relation, in which the trustor justifies a given content relying on the justification of some other content accessible only to the trustee, the group formed by (at least) two agents involved by such relation can indeed be said to have distributed knowledge. In the present section we actually show that a counterpart of the standard notion of Distributed Knowledge from Epistemic Logic is correctly satisfied by our multiple $\Diamond$ introduction rule for a modal context $\Diamond_{\mathcal{G}}\Sigma$, which allows inference for the intersection of agents in $\mathcal{G}=\{1,\dots,n\}$. Once this is proven to be the case, another obvious question arises concerning the counterpart notion of Common Knowledge (see especially [34] and [24]): in particular, we shall see that the presence of relations of Trusted Communications represent an actual limitation to the acquisition of Common Knowledge and that our $\Box_{\mathcal{G}}\Sigma, \mathcal{G}=\{1,\dots,n\}$ can indeed be defined as Common Knowledge operator.

Consider two signed contexts, by now without any priority relation defined over them[29]:

$$\Diamond_i\Gamma=\{\Diamond(S\ true),\Diamond(T\ true),\Box(U\to\bot\ true)\}$$

$$\Diamond_j\Delta=\{\Diamond(S\ true),\Diamond(U\ true),\Box(T\to\bot\ true)\}$$

Distributed Knowledge of $\Sigma_{\mathcal{G}}=\{\Gamma_i\mid\Delta_j\}$ implies:

$$\Diamond_{\mathcal{G}}\Sigma\vdash\Diamond_{i,j}(S\ true)$$

obtained by eliminating in Γ_i the open variables that are no longer satisfiable when Γ_j is taken as a possible extension, and vice versa. Recalling that *DK* is obtained as an inference relation between non-reciprocally accessible epistemic states (the 'wise-man'), we use the structural properties of possibility contexts to mimic the accessibility from inside the language. Strictly speaking, the resulting content would still need to be verified (β-reduced) to turn it into proper knowledge, but up to any further contextual extension being considered, this would remain the only shared content among the involved states, hence to be considered as their 'knowledge'. This induces our next result:

Theorem 1 *($\Diamond_{\mathcal{G}}$ as a distributed knowledge operator).*

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

Proof. To show that our $\Diamond_{\mathcal{G}}$ operator corresponds indeed to the derivability under two distinct indices, and hence is a *DK* operator, it is enough to recall that $\Diamond_{\mathcal{G}}$ satisfies in some form the standard properties for *DK*: Distribution is induced by Definitions 12 and 18; Reflexivity by the corresponding rule from Section 4.1; Transitivity holds in its ordered backward format by Transmission, whereas Seriality holds only when taken in the context of communication, i.e. with its relation to our $\Box$-modality. The application of appropriate β-reductions leads the set of valid formulae to those derivable in the axiomatization that is sound and complete with respect to Reflexivity and Transitivity. The characteristic standard properties of Distributed Knowledge are easily satisfied. For *DK* in $|\mathcal{G}|=\{1\}$, *DK* in $\mathcal{G}$ is equivalent to just dependent knowledge:

$$\frac{\Diamond_i\Gamma\vdash\Diamond_i(A\ true)}{\Diamond_{\mathcal{G}=i}\Sigma\vdash\Diamond_{\mathcal{G}=i}(A\ true)}\ DK_1$$

which can be read in both top-down and bottom-up directions. For extensions of $\mathcal{G}$, the larger a $\mathcal{G}\subseteq\mathcal{G}'$ the greater the distributed knowledge of $\mathcal{G}'$:

$$\frac{\Diamond_i\Gamma\vdash\Diamond_i(A\ true)\quad \Diamond_i\Gamma\mid\Diamond_j\Delta\vdash\Diamond_{\mathcal{G}=i,j}(A\ true)}{\Diamond_{\mathcal{G}=i}\subseteq\Diamond_{\mathcal{G}=i,j}(A\ true)}\ DK_{i\subset j}$$

which is simply satisfied by the definition of admissible context extension. □

Notice that by this definition, which mimics inclusions by single step contextual extensions, the *order* of the signatures plays no role, as the pair of agents is not an ordered pair. In the general argument, where $|\mathcal{G}|>\{2\}$, each single pair of agents needs to be considered in descending order: as Transitivity works only backwards, for every $\Diamond_{i,k}(A\ true)$ and $i<j<k\in\mathcal{G}$, there must be TCs' such that $\Diamond_{i,j}(A\ true)$ and $\Diamond_{j,k}(A\ true)$.

[28] See [24].

[29] The following example is adapted accordingly from [24, p. 24].

An indirect way of proving that $\Diamond_{\mathcal{G}}$ is an operator for *DK*, is to show that no operation of *CK* obtains in the context of $\Diamond_{\mathcal{G}}$. This result corresponds to proving that under $\Diamond_{\mathcal{G}}$ at least one *TC*-relation occurs and that *CK* obtains only when the number of *TC* in the system is reduced to zero.[30]

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

Proof. The proof goes by induction on the structure of Σ.

- The base case for $J = 1, i = j$ corresponds to a Derivation with just one step by the Autonomous Hypothesis Rule and no admissible extension of the relevant context taken into account. This satisfies by definition the validity of J into all contexts, it reduces $TC^j = 0$ and by Definition 15 allows for $\Box_i J$.
- Where $J = 1, i \neq j$, we are considering a Derivation with at most one application of multiple I-$\Diamond$ rule, and the extension is admissible since by hypothesis $|\mathcal{G}| \geqslant 2$. By application of the rule and the construction from Definition 17, $TC^j = 1$ and $\Diamond_{\mathcal{G}} J$. From the conclusion of this derivation, I-$\Box$ can be applied to make the extension everywhere accessible, which is the only rule to allow inference of $\Box_{\mathcal{G}} J$ and hence of $\Box_i J$. From the latter, TC^j is reduced to zero.
- Where $J \neq 1, i \neq j$, the case is similar to the previous one, with at least one application of multiple I-$\Diamond$ rule and $TC^j = |J - 1|$. The previous procedure applies to any occurrence of such a derivation step with $|J - 1|$ applications of I-$\Box$. $\Box$

This theorem says something slightly stronger than what holds for asynchronous message passing systems where unreliable communication is used. It says that nothing becomes common knowledge unless it is also knowledge in the absence of trusted communication, i.e. common knowledge does not hold if the communication chain is not reduced to verifiability at each point. We can now formulate our final result:

Theorem 3 *($\Box_{\mathcal{G}}$ as a common knowledge operator).*

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

Proof. The standard properties of *CK* are satisfied by the definition of $\Box_{\mathcal{G}} J$ as holding iff $\emptyset \mid \Gamma_{i \in \mathcal{G}} \vdash J$, which expresses admissibility of contexts extensions within $\mathcal{G}$:

- *CK* is equivalent to its conjunction with the fact that everyone in $\mathcal{G}$ knows: use Lemma 1 on the admissibility of Trusted Communication and multiple I-$\Box$, by which every source needs to be admissible and its β-redex induces the $\Box$ operator.
- If $\Sigma_{\mathcal{G}} \vdash J$ and this implies $\Gamma_i \subseteq \Sigma \vdash (J \wedge J')$ for every $i \in \mathcal{G}$, then $\Box_{\mathcal{G}} \Sigma \vdash \Box_{\mathcal{G}} J'$, which is proven again by induction: for $|\mathcal{G}| = 1$ this requires only the admissibility of $\Gamma_i \vdash J$, this will imply by hypothesis $\Gamma_i \vdash (J \wedge J')$, and hence by definition $\Box_i \Gamma \vdash \Box_i J'$. If $|\mathcal{G}| > 1$, then there is TC^{k-1} which makes $\Gamma_i \mid \Delta_k$ admissible. As by the previous argument, if the context extension is admissible, $\Gamma_i \mid \Delta_k \vdash (J \wedge J')$ and by I-$\Box$ we have $\Box_{i,k} \Sigma \vdash \Box_{i,k} J'$. $\Box$

A comparison is due with the results for Justified Common Knowledge presented in [4]. The notion of Justified knowledge in the form a modal operator $J\phi$ (ϕ is justified) is the forgetful projection of an evidence assertion $t : \phi$ [4, p. 12]. This operator for common knowledge is defined in a language which contains multi-modalities, as for our $\Box_{\mathcal{G}}$ operator and it satisfies the Fixed-Point Axiom in each of the fragment of modal logics $T_n, S4_n, S5_n$. This represents the first basic distinction with our operator for common knowledge: as we deal with a constructive language, the iteration of operators is restricted to positive introspection, hence Axiom 5 (respectively, Symmetricity on frames) is not validated. Moreover, the validity of Reflexivity is considered in the two fragments of the language, the one that admits only $\Box_i$ operator, the other where expression with $\Diamond_i$ operators are considered; in the latter case the corresponding axiom is taken in its appropriate formulation $T^n_\Diamond$. Finally, soundness and completeness are obviously proven in different ways, as the logic of Justified Common Knowledge is presented in the first place as a modal logic, and then a Gentzen–Hilbert-style system is introduced.

6. Properties on modal frames for trusted communications and knowledge

In this section we sketch completeness results of our rules w.r.t. corresponding modal frames. In terms of Kripke structures, our modal operators $\Diamond_{\mathcal{G}}$ and $\Box_{\mathcal{G}}$ will have to be definable in terms of modal frames $\mathcal{F} : \langle \mathbb{K}, \mathbf{R} \rangle$ with a nonempty set

[30] In [24, p. 149], Theorem 4.5.4 proves the impossibility to gain or lose *CK* in an interpreted asynchronous message passing systems. Provided the appropriate identities between a run and message events with respectively a Communication Chain and the number of Trusted Communications in our system, it follows the identity of the two theorems for the acquisition of *CK*. It also follows from the definition of *CK* as knowledge of every agent in an interpreted system with more than one agent, see [34, Section 3].

of states $\mathbb{K} = \{K_1, \dots, K_n\}$, first for each $\Diamond_1, \dots, \Diamond_n$ occurring in our *TC*s and then for the states where global validity is ensured; $\mathbb{R} = \{R^1, \dots, R^n\}$ represent the set of indexed binary relations for each pair of modalities $\Diamond_i, \Diamond_j$ in a *TC* and $\Box_{i,j}$.

Let us start with a Kripke model M which valuates the primitive propositions derivable under $\Diamond/_{\mathcal{G}}\Sigma$. This will turn out to be a non-standard model sound and complete with the multi-modal version of $KT_\Diamond$[31]:

$K^n_\Diamond$	$\Box_i(A \supset B) \to (\Diamond_i A \supset \Diamond_i B)$
$T^n_\Diamond$	$A \to \Diamond_i A$
$4^{<n}$ Modus Ponens	$\Diamond_j \Diamond_i A \to \Diamond_i A$

Here all occurrences of $\Diamond_i$ operators have been substituted by a $\Box_i$, we obtain a correspondence with an $S4$-model. We show in the following how the rules satisfy corresponding properties on frames.

We start with the Reflexivity Rule:

Lemma 2 *(Reflexivity over States). For every derivation $\Gamma_{i-n} \vdash \Diamond_i(A\ true)$, $A\ true^* \Rightarrow \Diamond_i(A\ true)$ is a reflexive relation over A.*

Proof. Reflexivity in our modal models means that for every state K_i corresponding to one indexed modality, it holds $K_i R^i K_i$. This means that constructing the appropriate relation in a canonical model for $\Diamond_i(A\ true)$, if $K_i \vDash A$ then $K_i \vDash \Diamond_i A$. This corresponds to our $A\ true^* \Rightarrow \Diamond_i(A\ true)$. To prove that this holds, suppose by contradiction that given $K_i \vDash A$ then $K_i \nvDash \Diamond A$: so $K_i \vDash \neg\Diamond A$, then A becomes not admissible at i, i.e. there is no context extension $\Gamma \mid \Delta$ that validates $\Diamond_i(A\ true)$ so that $K_i \nvDash A$, contrary to the hypothesis. Hence $A\ true^* \Rightarrow \Diamond_i(A\ true)$ holds, and the rule corresponds to $K_i R^i K_i$ for states. □

Let us consider now Transmission. Its meaning is reflected by a backward ordered transitivity relation:

Lemma 3 *(Backward Ordered Transitivity over States). For every derivation $\Gamma_i \vdash \Diamond_j(A\ true)$, $\Diamond_i\Diamond_j(A\ true) \Rightarrow \Diamond_i(A\ true)$ is a (backward only) ordered transitive relation over A.*

Proof. Backward Transitivity in our modal models can be explained as follows: for every K_i, K_j, K_k if $K_k R^k K_j$ and $K_j R^j K_i$, then $K_k R^i K_i$; in other words, if $K_j \vDash \Diamond A$ and $K_i R^j K_j$, then it holds $K_i \vDash \Diamond A$. As the accessibility relation is mimicked in the derivability relation, this simulates the iteration $\Diamond_i\Diamond_j$ and it implies the reduction to the lower indexed state. This is what implemented by our $4^{<n}$ axiom. Let us show that Transitivity does not hold forward. Its validity means that for every K_i, K_j, K_k if $K_i R^i K_j$ and $K_j R^j K_k$, then $K_i R^k K_k$, or in other words, if $K_i \vDash \Diamond A$ it holds $K_j \vDash \Diamond A$ for every R^j and hence $\vDash A$. Let now M be a model based on $\mathcal{F}$ such that $K_i \vDash \Diamond A$, and which still satisfies $K_k \vDash \Diamond\neg A$. This is still possible as Symmetry fails (see step 2 in the proof of the following Lemma 4); this model still satisfies $K_i \vDash \Diamond A$. Such M is not transitive, and neither can $\mathcal{F}$ be. □

It follows that frames for $\Diamond_{\mathcal{G}}$ are (only) reflexive:

Lemma 4 *(Frames for $\Diamond_{\mathcal{G}}\Sigma$). For every judgement A true such that $\Gamma_k, \Delta_k \vdash \Diamond_i(A\ true)$ holds implementing a Communication Chain as by Definition 16, there is a model $M \vDash A$ such that for every frame $\mathcal{F} : \langle \mathbb{K}, \mathbb{R} \rangle$ on which M is based, $\mathcal{F}$ is reflexive.*

Proof. 1. Reflexivity is immediate by Lemma 2.

2. Symmetry means that if $K_j \vDash \Diamond A$, then $K_i \vDash A$. It is not difficult to show that if $K_j \vDash \Diamond A$, then $K_i \vDash \Diamond\neg A$ can still be obtained, so that symmetry fails. Suppose $K_j \vDash \Diamond A$, and $K_i R^i K_j$, i.e. there is an admissible *TC* ending with $\Diamond_j$; then there is no admissible step that implies $\vDash A$, for any *TC*, therefore it is still admissible a $TC^k = \langle \Diamond_j, \Diamond_k, \neg A \rangle$, hence $K_i \vDash \Diamond\neg A$ and $K_i \nvDash A$, contrary to the hypothesis.

3. Backward ordered transitivity is immediate by Lemma 3; by the same lemma general Transitivity fails. □

Theorem 4. *Rules for our $\Diamond_{\mathcal{G}}$ operator are sound and complete to models of $KT^n_\Diamond 4^{<n}$.*

Proof. Immediate from Lemmas 2 and 4 and standard argument of soundness and completeness of *KT*4 for reflexive frames adapted for the $T_\Diamond$ axiom and restricted over the axiom 4. □

Similarly, we sketch here the proof that establishes the models of formulas derivable under the $\Box_{\mathcal{G}}$ to be sound and complete with respect to the modal logic $S4^n$. For this we need the following:

[31] It is a fragment of the constructive contextual modal logic introduced in [1]. A full analysis of the conditions on frames for such semantics is presented in [63].

Lemma 5 *(Transitivity over States). For every derivation* $\Gamma_i, \Delta_j \vdash \Box_k J$, $\Box_{i,j} A$ *true* $\Rightarrow \Box_{i,j}\Box_k(A$ *true*$)$ *is a transitive relation over* A.

Proof. Transitivity in our modal models means that for every K_i, K_j, K_k if $K_i R^i K_j$ and $K_j R^j K_k$, then $K_i R^k K_k$, or in other words, if $K_i \vDash \Box A$ it holds $K_j \vDash \Box A$ for every R^j and hence $\vDash \Box A$. By I$\Box$ rule, $K_k \vDash \Box A$ holds as well by definition and properties of our operator. Now transitivity holds over any index and iteration is both ascending and descending. □

Lemma 6 *(Reflexive and Transitive Frames for* $\Box_{\mathcal{G}}\Sigma$*). For every judgement A true such that* $\Gamma_k, \Delta_k \vdash \Box_i(A$ *true*$)$ *holds implementing a Communication Chain as by Definition 16, there is model* $M \vDash A$ *such that for every frame* $\mathcal{F} : \langle \mathbb{K}, \mathbb{R} \rangle$ *on which M is based,* $\mathcal{F}$ *is reflexive and transitive.*

Proof. Immediate, by preservation of Reflexivity by $\Box_{\mathcal{G}}\Sigma$ and Lemma 5. □

Theorem 5. *Rules for our* $\Box_{\mathcal{G}}$ *operator are sound and complete to models of* $S4^n$.

Proof. Immediate from Lemmas 5 and 6 and standard argument of soundness and completeness of $S4$ for reflexive and transitive frames. □

7. Discussion

The debate on testimony is wide and heterogeneous, and different analyses have been provided from a variety of points of view, e.g. in the debate between reductionism and anti-reductionism or within the framework of social epistemology [6,32,33] and [27]. Many of the contributions to the debate on testimony agree in considering it linked in some way to trust, see for example [12,35,75,69,31,7] and [41]. Trust has been considered the source of epistemic justification for the receiver of the message to believe the communicated message to be true. This is a problematic thesis; even once this is accepted other problems arise, since one has not explained yet whether and how trust can provide such a justification, and what the reasons are that justify R's decision to trust S in transmitting true messages. In our approach, we explicitly distinguish between contents that are presented together with their justification and contents transmitted without.

This distinction is formally justified and it allows for implicitly endorsing a notion of trust in the language. In this paper we have analyzed the relation between testimony and trust on the basis of the definition of trust put forward in [72], where it is argued that testimony is an occurrence of a first-order relation of communication affected by the second-order property of trust, and the view is defended that an epistemic agent can acquire some knowledge, on the basis of the information communicated through testimony, if and only if the agent is able to connect the transmitted information to the conceptual network of interrelation to which it belongs.[32] In the present context, we have translated acquisition of knowledge in terms of verification processes that survive network extensions. The notion of trust as a second-order property remains the crucial theoretical feature on which the calculus is constructed, something that clearly differs from most well-known formal treatment of trust as in [19].

The notion of communication as presented in the context of processes of group knowledge has found its formal explanation mostly in multi-agent epistemic logics, see [24,54], and their various modal and dynamic translations, see [8,22]. These systems have recently been extended to accommodate various interpretations of the notions of trust and testimony. The current approaches privilege the interpretation of trust as a modal operator ranging over agents ("Agent *a* trusts agent *b*"), and the corresponding informal explanation can vary. The formal treatment is mostly model-theoretic. In [9], trust relations are modeled in terms of graphs designed over the plausibility models for belief revision: this has led to a different task, namely a dynamic definition of doxastic merging states by sharing information via acts of sincere communication in [10], stressing the property of reliable communication. The notion of sincerity of a communication act is defined as sharing of information that was already accepted by the speaker; reliability is defined in terms of the notion of (common) knowledge. Notice here the crucial distinction with our system: in our language both sincerity and reliability are informal properties that can only be induced in terms of entirely well-defined syntactical procedures of verification, and the notion of common knowledge is derived.

A variant of this model-theoretic approach is presented in [39], where a dynamic testimonial logic combines a conditional doxastic logic and a dynamic logic of belief upgrade, enriched with a belief suspension operator: in this setting so-called "authority graphs" are designed to capture agents' epistemic trust in other agents' testimony. The latter property is embedded in the derivability relation of our language, which presents a more rigid notion of hierarchy for authorities, but which comes for free with the structure of our contexts.

Another propositional dynamic logic approach to trust and commitment is presented in [13], in which the violation of stronger commitments results in higher loss of trustworthiness than the violation of weaker ones, hence describing an agent that proposes and accepts engagements in commitments, and violates them by performing actions other than the

[32] Such a thesis is supported by Floridi's Network Theory of Account (NTA), see [25] and [26, Chapter 12].

ones committed to. Such a dynamics can be easily mimicked in terms of an appropriate interpretation of the contextual dynamics proper of Martin-Löf's Type Theory.

Another recent modal approach that combines the analysis of belief states with the reliability of information sources is presented in [47]. In this framework, agents are allowed to keep track of the information sources via a signature system that recalls ours, but the hierarchical structure these sources form is entirely different, as it orders sources from the more to the less reliable and in this way allows agents to select information and to adapts her own belief state on that basis. This is certainly a very interesting dynamic to explore on the representation of sources and it would be a step forward in adding conceptual complexity to our model.

What all these models are characterized by is the usual intuition that belief states are basically not different from knowledge states, so that their epistemic notions are indistinguishable, contrary to what we aim at in our model. Another approach in the same direction as ours is represented by the debate on trust for theories of defeasible knowledge (see e.g. [11]).

The notion of trust has received attention especially in the study of information systems and distributed computing. We have already mentioned that our system can be easily transformed in an operational semantics, using the underlying Curry–Howard isomorphism which establishes the proofs-as-programs and propositions- or formulae-as-types interpretation (see [71] for a complete presentation). Let us in the following compare with some of the systems present in the literature.

The task in [44] is to provide computational declarative definitions for trust relations between interacting agents as first-order predicates, where the group of mutually trusting agents form the trust domain in a distributed system, and to obtain computational complexity results for deciding trust relationships. Informally the relation of trust is given as belief or knowledge of behavior's predictability. From the computational point of view, this task is specified in the context of web-based applications and computer-communication networks. Our contribution aims at providing a more general definition to the epistemic notion of trust. Defining it as a second-order relation we implicitly maintain that using a set of atomic propositions to refer to agent's correctness as the object of trust implies the impossibility of making a distinction between different properties such that the same agent is correct about one, and incorrect about the other. One can still avoid such a problem by naming explicitly the object of trust, as it is indeed done in [44] by adding naming in the form *correctPKI correctWebOfTrust*, but this seems a complication from a theoretical viewpoint and the solution we propose seems more elegant. Moreover, according to the latter system, the distinction among the agents' epistemic states involved in the trust relation is completely irrelevant: by means of a trust relation, knowledge of P holding for agent a induces knowledge of P in agent b, so that trust is just a function for selecting communicating agents. Our language uses a dependency relation to characterize trustworthy communications of contents between agents, whereas in the semantic approaches mentioned, the communication is usually taken meta-theoretically, or can be added via an additional predicate that would take the form $(comm(b, P, a))$, hence requiring the second-order level if that has to be given the property of trust (namely via an additional predicate of the form $Trust(comm(b, P, a)))$.

A procedural notion of trust, loosely based on the general analysis given in [52], is presented in [16]: it gives an agent-based, degree-oriented notion of trust that allows interaction among entities and enforces transmission of such a property, but it lacks both a restriction over the object of trust – because it is given as a function over agents – and the epistemic analysis of the agents' states that we include as central to our definition.

A recent approach is the generalization of the interpretation from [21] of trust based on mental attitudes given in the already mentioned [19], where it is stated: "*only a cognitive agent can trust another agent*; *only an agent endowed with goals and belief*" (p. 38). The latter is then combined with the degree-based quantitative approach, see [19, Chapter 3]. The same conceptual qualitative tools used in this latter approach to analyze trust and reputation, namely goal, capability, power, and willingness, have been used in a multi-agent setting to evaluate agents' behavior in the scope of collective beliefs, see [36]. This approach is refined in [37], using a logic of time, action, beliefs and choices and by distinguishing occurrent trust from dispositional trust.

Another model of formalization of trust relations based on modal logics is given in [46], where the relationship among belief, information acquisition and trust is both semantically and axiomatically characterized so that belief and information acquisition operators are respectively represented by $KD45$ and KD normal modalities, whereas trust is denoted by a modal operator with minimal semantics. This framework is further extended in [20] to include the derivation of trust from other notions. To do so, extensions with respect to relevance of topics and questions are introduced.

In [74], trust is a function defined between a host and a client over a set of actions and a set of effects of such actions, and such that it holds if the expectations of the host about the effects of the actions of the client are positive. This might be seen as a notion similar to ours, where we focus especially on positive epistemic actions, but its structure appears less informative from the point of view of epistemic states (it misses the doxastic representation).

A different approach to trust for distributed systems is presented in [76], based on set-theoretic operations defined over a quadruple composed by the set of trustors, the one of trustees, one of conditions and one of properties. The intended meaning is that under a given set of circumstances (conditions), the set of trustors trust the set of trustees about a given set of properties, the latter partitioned in a set of actions and a set of attributes. This strategy seems similar to our definition of trust as a second-order property, but the main difference is that their notion of trust is a primitive and ours is restricted to the declarative assertion of holding of a given property, hence focusing in the first place on a message-passing system.

A formal semantics for ontologies that focuses in particular on transitivity of trust relations is given in the already mentioned [40].

Along with the powerful model-theoretic treatments, different proof-theories have been adapted recently to an appropriate multi-agent setting to define group-based notions of knowledge: a natural deduction non-epistemic language in [28], a Gentzen's style sequent calculus in [58] and, at least for the syntactic intuition behind it, the already largely mentioned Artemov's logic of proofs. We are moreover aware of some yet unpublished work on the formalization of group knowledge via hypersequent systems. The added value of these systems is given by their ability to represent different knowledge modalities to sort among the contents and to make explicit the formulation of the information sources. Among these syntactic approaches, our formal system provides an original treatment of trusted communications, to our knowledge the first doing so explicitly for human-like messaging systems that adopts a type-theoretic interpretation. The multi-modal extension of our type-theory is derived from the mono-modal case formulated in [65] and motivated by problems similar to those inspiring other formulations of modal type theories, such as in [61] and [57]. They all have different applications, especially to Distributed and Staged Computation, see [56,55,66]. Among other calculi that treats explicitly the notion of trust for computing, let us here just remember: a process calculus for trust management in [17]; the machinery used for the formal verification of security protocols applied to security and trust processes in [48].

The body of further work that converges on this topic from philosophy, (formal) epistemology and computer science is impressive and we have given reference only to those works that most directly relate to this contribution.

8. Conclusions

In this paper, we have presented a formal model for epistemic processes qualified by trust. It relies on two basic novelties, strictly related to each other: the first is that we consider trust as a second-order property that characterizes relations of communications; the second is that so qualified relations are presented in a type-theoretic system that fully allows for their formalization. By considering trust as a second-order relation, we avoid formalizing it at the same level of the underlying epistemic relation: in the present formulation, trust has been formally defined as a function over epistemic states and affecting a propositional content. An obvious advantage of the here introduced language is that it makes possible the representation of multi-agent interactions and it is embedded into the syntactical equivalent of a non-homogeneous language for modal operators, allowing the representation of the central notions of Common and Distributed Knowledge. A further step in this research will be represented by a consistent extension of this analysis to the cases of communications characterized by mistrust and distrust.

Acknowledgements

A first version of this paper was presented at the *Second Workshop in the Philosophy of Information*, Bilkent University, Ankara, Turkey, May 20–21, 2010. The authors wish to thank all participants for insightful comments. The first author acknowledges in particular discussions with Luciano Floridi, Patrick Allo and Sonja Smets on issues of epistemic logic and with Laszlo Kosolosky for comments on trust-based relations that generated the example in Section 2. Both authors wish to acknowledge helpful comments by two anonymous referees.

References

[1] N. Alechina, M. Mendler, V. de Paiva, E. Ritter, Categorical and Kripke semantics for constructive S4 modal logic, in: Proceedings 15th Int. Workshop on Computer Science Logic, CSL'01, Paris, France, 10–13 Sept. 2001, Springer-Verlag, 2001, pp. 292–307.

[2] S. Artemov, Logic of proofs, Annals of Pure and Applied Logic 67 (2) (1994) 29–59.

[3] S. Artemov, Explicit provability and constructive semantics, Bulletin of Symbolic Logic 7 (1) (2001) 1–36.

[4] S. Artemov, Justified common knowledge, Theoretical Computer Science 357 (1) (2006) 4–22.

[5] S. Artemov, E. Nogina, Introducing justification to epistemic logic, Journal of Logic and Computation 15 (6) (2005) 1059–1073.

[6] R. Audi, The place of testimony in the fabric of justification and knowledge, American Philosophical Quarterly 34 (1997) 405–422.

[7] A. Baier, Sustaining trust, in: A. Baier (Ed.), Moral Prejudices, Harvard University Press, Cambridge, MA, 1994.

[8] A. Baltag, L.S. Moss, S. Solecki, The logic of public announcements, common knowledge and private suspicions, in: Proceedings of TARK'98, Seventh Conference on Theoretical Aspects of Rationality and Knowledge, Morgan Kaufmann Publishers, 1998, pp. 43–56.

[9] A. Baltag, S. Smets, A qualitative theory of dynamic interactive belief revision, in: G. Bonanno, W. van der Hoek, M. Wooldridge (Eds.), Logic and the Foundations of Game and Decision Theory, in: Texts in Logic and Games, vol. 3, Amsterdam University Press, 2008, pp. 9–58.

[10] A. Baltag, S. Smets, Talking Your Way into Agreement: Belief Merge by Persuasive Communication, in: CEUR Workshop Proceedings, vol. 494, Proceedings of the Second Multi-Agent Logics, Languages, and Organisations Federated Workshops, Turin, Italy, September 7–10, 2009, 2009, pp. 129–141.

[11] A. Bikakis, G. Antoniou, Distributed defeasible contextual reasoning in ambient computing, in: E. Aarts, J.L. Crowley, B. DeRuyter, H. Gerhauser, A. Pflaum, J. Schmidt, R. Wichert (Eds.), Ambient Intelligence, in: Lecture Notes in Computer Science, vol. 5355, Springer, Berlin/Heidelberg, 2008, pp. 308–325.

[12] M.J. Blais, Epistemic tit for tat, Journal of Philosophy 84 (1987) 363–375.

[13] J. Broersen, M. Dastani, Z. Huang, L.W.N. van der Torre, Trust and commitment in dynamic logic, in: Proceedings of the First EurAsian Conference on Information and Communication Technology, October 29–31, 2002, pp. 677–684.

[14] S. Buvač, Quantificational logic of context, in: Proceedings of the Thirteenth National Conference on Artificial Intelligence, 1996, pp. 600–606.

[15] S. Buvač, V. Buvač, I. Mason, Metamathematics of contexts, Fundamenta Informaticae 23 (3) (1995) 412–419.

[16] M. Carbone, M. Nielsen, V. Sassone, A formal model for trust in dynamic networks, in: Proc. of IEEE International Conference on Software Engineering and Formal Methods (SEFM'03), 2003.

[17] M. Carbone, M. Nielsen, V. Sassone, A calculus of trust management, in: Proceedings from Foundations of Software Technology and Theoretical Computer Science, 24th International Conference (FSTTCS'04), 2004.

[18] C. Castelfranchi, Trust Mediation in Knowledge Management and Sharing, Lecture Notes in Computer Science, vol. 2995, Springer Verlag, 2004, pp. 304–318.
[19] C. Castelfranchi, R. Falcone, Trust Theory. A Socio-Cognitive and Computational Model, Wiley, 2010.
[20] M. Dastani, A. Herzig, J. Hulstijn, L. Van Der Torre, Inferring trust, in: Procs. of Fifth Workshop on Computational Logic in Multi-Agent Systems (CLIMA V), in: LNAI, vol. 3487, 2004, pp. 144–160.
[21] R. Demolombe, Reasoning about Trust: A Formal Logic Framework, Lecture Notes in Computer Science, vol. 2995, Springer Verlag, 2004, pp. 291–303.
[22] H. van Ditmarsch, W. van der Hoek, B. Kooi, Dynamic Epistemic Logic, Synthese Library, vol. 337, Springer, 2006.
[23] M. Fairtlough, M. Mendler, On the logical content of computational type theory: A solution to Curry's problem, in: P. Callaghan, Z. Luo, J. McKinna (Eds.), Types for Proofs and Programs, in: Lecture Notes in Computer Science, vol. 2277, Springer Verlag, 2002, pp. 63–78.
[24] R. Fagin, J.Y. Halpern, Y. Moses, M.Y. Vardi, Reasoning about Knowledge, MIT Press, 1995.
[25] L. Floridi, semantic information and the network theory of account, Synthese, forthcoming, doi:10.1007/s11229-010-9821-4.
[26] L. Floridi, The Philosophy of Information, Oxford University Press, Oxford.
[27] E. Fricker, Telling and trusting: reductionism and anti-reductionism in the epistemology of testimony, Mind and Society 104 (1995) 393–411.
[28] C. Ghidini, L. Serafini, A context-based logic for distributed knowledge representation and reasoning, Lecture Notes in Artificial Intelligence 1688 (1999) 159–172.
[29] F. Giunchiglia, L. Serafini, E. Giunchiglia, M. Frixione, Non-omniscient belief as context-based reasoning, in: International Joint Conferences in Artificial Intelligence, 1993, pp. 548–554.
[30] F. Giunchiglia, C. Ghidini, Local models semantics, or contextual reasoning = locality + compatibility, Artificial Intelligence 127 (1997).
[31] A.I. Goldman, Knowledge in a Social World, Oxford University Press, Oxford, 1999.
[32] P.J. Graham, What is testimony? Philosophical Quarterly 47 (1997) 227–232.
[33] P.J. Graham, Transferring knowledge, Nous 34 (1) (2000) 131–152.
[34] J.Y. Halpern, Y. Moses, Knowledge and common knowledge in a distributed environment, Journal of the ACM 37 (3) (1990) 549–587.
[35] J. Hardwig, The role of trust in knowledge, The Journal of Philosophy 88 (1991) 693–708.
[36] A. Herzig, E. Lorini, J.F. Hübner, J. Ben-Naim, O. Boissier, C. Castelfranchi, R. Demolombe, D. Longin, L. Perrussel, L. Vercouter, Prolegomena for a logic of trust and reputation, in: G. Boella, G. Pigozzi, M.P. Singh, H. Verhagen (Eds.), NorMAS 2008, University of Luxembourg Press, Luxembourg, 2008, pp. 143–157.
[37] A. Herzig, E. Lorini, J.F. Hübner, L. Vercouter, A logic of trust and reputation, in: Normative Multiagent Systems, Logic Journal of the IGPL 18 (1) (2010) 214–244.
[38] J. Hintikka, Knowledge, Belief, An Introduction to the Logic of the Notions, Cornell University Press, Ithaca, 1962.
[39] W.H. Holliday, Dynamic testimonial logic, in: LORI'09: Proceedings of the 2nd International Conference on Logic, Rationality and Interaction, in: Lecture Notes in Computer Science, vol. 5834, Springer-Verlag, 2009, pp. 161–179.
[40] J. Huang, M.S. Fox, An ontology of trust. Formal semantics and transitivity, in: Proceedings of the 8th International Conference on Electronic Commerce, in: ACM International Conference Proceedings Series, vol. 156, ACM, New York, NY, USA, 2006, pp. 259–270.
[41] K. Jones, Second-hand moral knowledge, The Journal of Philosophy 96 (1999) 55–78.
[42] S.C. Kleene, On the interpretation of intuitionistic number theory, Journal of Symbolic Logic 10 (4) (1945).
[43] A. Kolmogorov, On the principle of excluded middle, in: J. Van Heijenoort (Ed.), From Frege to Gödel: A Source Book in Mathematical Logic 1879–1931, Harvard University Press, 1967, pp. 414–437.
[44] S. Kramer, R. Goré, E. Okamoto, Formal definitions and complexity results for trust relations and trust domains fit for TTPs, the web of trust, PKIs, and ID-based cryptography, ACM SIGACT News 41 (1) (2010) 75–98.
[45] J. Lackey, Learning from Words. Testimony as a Source of Knowledge, Oxford University Press, 2008.
[46] C.-J. Liau, Belief, information acquisition, and trust in multi-agent systems – A modal logic formulation, Artificial Intelligence 149 (1) (2003) 31–60.
[47] E. Lorini, L. Perrussel, J.M. Thévenin, A modal framework for relating belief and signed information, in: Proceedings of the 12th International Workshop on Computational Logic in Multi-Agent Systems (CLIMA XII), in: Lecture Notes in Artificial Intelligence, vol. 6814, 2011, pp. 58–73.
[48] F. Martinelli, M. Petrocchi, A uniform framework for security and trust modeling and analysis with crypto-CCS, Electronic Notes in Theoretical Computer Science 186 (2007) 85–99.
[49] P. Martin-Löf, Intuitionistic Type Theory, Bibliopolis, Naples, 1984.
[50] P. Martin-Löf, An intuitionistic theory of types, in: G. Sambin, J. Smith (Eds.), Twenty-five Years of Constructive Type Theory, Oxford University Press, 1998, pp. 127–172.
[51] J. McCarthy, Notes on formalizing context, in: Proceedings of the 13th Joint Conference on Artificial Intelligence (IJCAI-93), 1993.
[52] D.H. McKnight, N.L. Chervany, The meanings of trust, in: Trust in Cyber-Societies, in: Lecture Notes in Artificial Intelligence, vol. 2246, 2001, pp. 27–54.
[53] M. Mendler, V. de Paiva, Constructive *CK* for contexts, in: Proceedings of the First Workshop on Context Representation and Reasoning – CONTEXT05, Stanford, 2005.
[54] J.-J.Ch. Meyer, v.d.W. Hoek, Epistemic Logic for AI and Computer Science, Cambridge University Press, 1995.
[55] T. Murphy, Modal types for mobile code, PhD thesis, CMU-CS-08-126, School of Computer Science, Carnegie-Mellon University, Pittsburgh, PA, 2008.
[56] T. Murphy, K. Crary, R. Harper, F. Pfenning, A symmetric modal lambda calculus for distributed computing, in: H. Ganzinger (Ed.), Proceedings of the 19th Annual Symposium on Logic in Computer Science (LICS'04), IEEE Computer Society Press, 2004, pp. 286–295.
[57] A. Nanevski, F. Pfenning, B. Pientka, Contextual modal type theory, ACM Transactions on Computational Logic 9 (3) (2008) 1–48.
[58] S. Negri, R. Hakli, Proof theory for distributed knowledge, Lecture Notes in Artificial Intelligence 5056 (2008) 100–116.
[59] B. Nordström, K. Petersson, J. Smith, Programming in Martin-Löf Type Theory. An Introduction, The International Series of Monograph in Computer Science, vol. 7, Clarendon Press, Oxford University Press, 1990.
[60] F. Pfenning, Intensionality, extensionality, and proof irrelevance in modal type theory, in: J.Y. Halpern (Ed.), Proceedings of the 16th Annual IEEE Symposium on Logic in Computer Science, IEEE Computer Society Press, 2001, pp. 221–230.
[61] F. Pfenning, R. Davies, A judgemental reconstruction of modal logic, Mathematical Structures in Computer Science 11 (2001) 511–540.
[62] G. Primiero, Information and Knowledge, Logic and the Unity of Science, vol. 10, Springer, 2008.
[63] G. Primiero, A constructive modal semantics for contextual verification, in: A. Mileo, J. Delgrande (Eds.), Proceedings of the First International Workshop on Logic-Based Interpretation of Context: Modelling and Applications, in: CEUR Workshop Proceedings, vol. 550, CEUR-WS.org, 2009, pp. 33–35.
[64] G. Primiero, Epistemic modalities, in: G. Primiero, S. Rahman (Eds.), Acts of Knowledge: History, Philosophy and Logic, in: Tributes, vol. 9, College Publications, 2009, pp. 207–232.
[65] G. Primiero, A contextual type theory with judgemental modalities for reasoning from open assumptions, Logique & Analyse 220 (2012), forthcoming.
[66] G. Primiero, A multi-modal type-theory and its procedural semantics for safe distributed programming, Paper presented at Intuitionistic Modal Logic and Applications Workshop, CLMPS Affiliated, Nancy, 2011, Manuscript.
[67] A. Ranta, Type-Theoretical Grammar, Clarendon Press, Oxford University Press, 1994.
[68] J. Sabater, C. Sierra, S. Parsons, N.R. Jennings, Engineering executable agents using multi-context systems, Journal of Logic and Computation 12 (3) (2002) 413–442.

[69] F. Schmitt, Justification, autonomy, sociality, Synthese 73 (1987) 43–85.

[70] C. Sierra, J. Debenham, An information-based model for trust, in: Proceedings of the Fourth International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS 2005, ACM, New York, NY, USA, pp. 497–504.

[71] M.H. Sørensen, P. Urzyczyn, Lectures on the Curry–Howard Isomorphism, Studies in Logic and the Foundations of Mathematics, vol. 149, Elsevier, 2006.

[72] R. Taddeo, Modelling trust in artificial agents, a first step toward the analysis of e-trust, Minds and Machines 20 (2) (2010) 243–257.

[73] R. Taddeo, An information-based solution for the puzzle of testimony and trust, Social Epistemology 24 (4) (2010) 285–299.

[74] D. Xiu, Z. Liu, A formal definition for trust in distributed systems, in: Proceedings of the Information Security Conference, in: Lecture Notes in Computer Science, vol. 3650, Springer, 2005, pp. 482–489.

[75] M. Welbourne, The Community of Knowledge, Humanities Press, Atlantic Highlands, 1993.

[76] W. Zhao, V. Varadharajan, G. Bryan, General methodology for analysis and modeling of trust relationships in distributed computing, Journal of Computers 1 (2) (2006) 42–53.