UNIVERSITÉ DU QUÉBEC À MONTRÉAL

ACTIONS AND RESOURCES IN EPISTEMIC LOGIC

THÈSE PRÉSENTÉE COMME EXIGENCE PARTIELLE
DU DOCTORAT EN PHILOSOPHIE

PAR

MEHRNOOSH SADRZADEH

SEPTEMBER 2006

Contents

Acknowledgments

I would like to thank my supervisor Mathieu Marion for giving me the opportunity and helping me all along to do the thesis in distance, my co-supervisor Alexandru Baltag for his generosity in his time and speech. This thesis was partly done during my two year academic visitorship in Oxford University Computing Laboratory, I would like to thank for their very kind hospitality and academic support, specifically Samson Abramsky and the Foundations of Computing group. Special thanks to my parents and Bob Coecke for material and mental support, also to Phil Scott, Amy Felty, and the Ottawa Logic group, Dusko Pavlovic, Vincent Danos, Prakash Panagaden, Roy Dyckhoff, Isar Stubbe for valuable guidance and discussions.

Abstract

Reasoning about knowledge has been a central issue in epistemology since Plato defined knowledge as justified true belief. In the twentieth century, the discussion was renewed by the use of formal logic and modal operators in Hintikka's epistemic logic. This logic has found applications in computer science and economics, but has defects: it is mono-modal, static and has no sense of resources. In this thesis we present a logic to reason about knowledge and the change induced to it as a result of communication actions between agents in a multi-agent systems. The semantics of this logic is an algebra of propositions paired with an algebra of actions. Both have structure preserving appearance maps whose adjoints stand for knowledge of agents. The algebra of actions is a quantale, thus actions are treated as the qualitative resources of Linear Logic: they are not accessible to all agents to acquire new information. Agents themselves act as qualitative resources to other agents: their nested appearances of a context has an effect in the reasoning of other agents. We also present a sequent calculus for our semantics, in the style of Lambek Calculus and Non-commutative Intuitionistic Linear Logic. We prove the soundness and completeness of this sequent calculus with regard to the algebra and apply the setting to reason about safety of security protocols. We connect our approach to the existing literature by showing that models of dynamic epistemic logic of Baltag-Moss-Solecki are instances of our logic.

Key Words. Actions, Resources, Knowledge, Logic, Security Protocols

UNIVERSITÉ DU QUÉBEC À MONTRÉAL

LES ACTIONS ET LES RESSOURCES DANS LA LOGIQUE ÉPISTÉMIQUE

THÈSE PRÉSENTÉE COMME EXIGENCE PARTIELLE

DU DOCTORAT EN PHILOSOPHIE

PAR

MEHRNOOSH SADRZADEH

SEPTEMBRE 2006

Résumé

La logique épistémique est une logique modale qui est utilisée pour l'étude du raisonnement sur les croyances et la connaissance. Depuis ses débuts dans les années soixante par Hintikka, elle a été appliquée entre autres en informatique. Ces applications ont révélé certains défauts: elle est mono-modale, statique, et ne tient pas compte des ressources. Ces applications requièrent une logique où l'on peut étudier le raisonnement à propos des croyances et des connaissances des agents avec des ressources limitées dans un système multi-agents, où ceux-ci communiquent entre eux et où il en résulte que les agents changent leurs connaissances; en d'autres mots, il faut une approche dynamique du raisonnement sur les connaissances. Dans ma thèse, je vais développer une logique multi-agents pour la connaissance, la croyance, et le changement, et qui est aussi sensible à la question de l'usage des ressources. Cette logique, appelée IDEAL, est une logique algébrique avec un système de preuve dans le style de Gentzen. J' applique ce système IDEAL à la résolution de problèmes réels tels que celui de la sécurité des protocoles de transaction en-ligne. Ces protocoles ont un cadre multi-agents interactif, où les connaissances des agents est importante: on ne veut pas que notre information soit connue par un tiers parti. Finalement, j'examine les liens avec les autres travaux dans la même domaine, en démontrant comment la logique dynamique épistémique de Baltag-Moss-Solecki, est un cas particulier de mon système IDEAL.

Mot clés. Actions, Ressources, Connaissance, Logique, Protocoles de sécurité,

Chapter 1

Introduction

Reasoning about knowledge has been a central issue in epistemology since Plato defined knowledge as justified true belief. In the twentieth century, the discussion was renewed by the use of formal logic and modal operators to account for propositional attitudes such as 'I know that ' or 'I believe that '. Thus one could use the tools of modern logic to reason about knowledge and belief of agents. This new branch of logic, called epistemic logic, has found applications in computer science and economics [65] since its inception by Hintikka [46] in the 1960's. These applications have broadened the applicability of epistemic logic, but at the same time shed light on some defects. The epistemic logic developed by Hintikka is mono-modal, static and has no sense of resources. It being mono-modal means that it can only reason about knowledge of one agent and misses on inter-subjective and higher order reflections between agents. This is a grave limitation since most of the applications are based on a multi-agent setting, where we need to reason about what each agent knows about knowledge of other agents. For example in modeling knowledge of buyers in a stock market, what each agent knows about the knowledge of other agents and in particular knowledge of agents about his own knowledge, plays an important role in his decision. The second major defect is that it does not formalize communication actions between agents and the change induced by these actions on the knowledge of agents. From this account, epistemic logic of Hintikka is *static* and can only formalize knowledge of agents at the time of modeling. The *dynamics* and effect of actions on the knowledge of agents are mostly dealt with informally and by explanations in natural language rather then in the logical formalism. This is another limitation for epistemic logic, especially in *dynamic* multi-agent applications, where modeling communication and its effects on knowledge is as important as modeling the knowledge itself. For example the communication between bidding agents in an auction and its effects on the knowledge of agents is a crucial factor in modeling the auction, and one cannot provide a full formal analysis of the setting by informally dealing with actions. Finally, this logic has no account of resources, that is, it assumes its agents have access to the same resources and thus reason in the same way about their knowledge. Moreover, these resources are unlimited, so all the agents are uniformly perfect reasoners. As a result agents modeled by these logics are *logically omniscient* [39], which means they know all the consequences of what they know; this is not the case in the real life applications.

The goal of this thesis is to develop an epistemic logic that does not have these defects. That is, developing a general logical approach to multi-agent information flow that models 'dynamics' of reasoning about knowledge and that also has a sense of agents' resources. In this approach, knowledge of agents would be subject to change as a result of communications actions that happen between the agents, and the logic formalizes communication actions, as well as their effects. Since different agents have access to different communication actions, their knowledge changes in different ways. So these actions can be seen as resources. In the same line, each agent has different agent surroundings, so not every agent can communicate with other agents. This makes agents serve as resources to other agents. We refer to this logic as IDEAL, for Intuitionistic Dynamic Epistemic Action Logic. The features of this logic make it a proper tool to study dynamics of knowledge in social settings and at the same time makes it easier to applications in computer science and economics.

In order to put this work in perspective with the body of work on epistemic logic, note that later developments of epistemic logic discussed in detail in [39] have overcome the problem of mono-modality. They have done so by adding a family of modalities, one for each agent and asking for appropriate axioms to relate them in a $S4$ or $S5$ logic. Attempts to formalize dynamics of knowledge are more recent; the first logic to formalize the effect of actions on knowledge is the logic of public announcements of Gerbrandy and Groenveld [41, 42], and also Plaza in [72]. These systems only consider the effects of one special sort of action: public announcement of a proposition. A complete formalization of public and private announcements and their effects has been introduced by Baltag, Moss, and Solecki in [9, 10] and often referred to as Dynamic Epistemic Logic or DEL for short. DEL pioneers reasoning about dynamics of knowledge via its *update* product of Kripke structures.

The novelty of our work, based on the joint work of the author with Baltag and Coecke in [7, 8], is its algebraic semantics and corresponding sequent calculus. IDEAL uses algebraic ordered structures as its semantics rather than plain sets and relations as in [39, 9, 10], which are the usual possible worlds or Kripke semantics of epistemic logic. Moreover, IDEAL is a non-classical constructive logic as opposed to the above mentioned non-constructive classical logics. It treats actions of communication between agents and the consequent changes on their knowledge as main concepts of the logic. The main reasoning power of IDEAL comes from adjunction techniques developed in category theory [61]. These methods, first logically used in Intuitionistic logic and extended to Temporal logic by Von Karger [89], enable IDEAL to replace the usual *reasoning by negation* of epistemic logics with *reasoning by adjunction*. Moreover, they represent not the usual full modalities, but *factorizations* of the co-closure modalities of $S4$ and $S5$ and also exponential of Linear Logic [44]. The fluency and fun of reasoning by adjunction make IDEAL's proofs of challenging epistemic puzzles, which involve higher order reflections, such as 'muddy children' [39], much easier than other approach, e.g. in [39, 9, 10]. IDEAL can also easily deal with more interesting and closer to real life versions of these puzzles where children perform secret actions such as cheating and lying. Encoding these misinformation actions is a consequence of following [10] and assuming epistemic structure on actions. But we go further than [10] and introduce epistemic modalities for actions, so we can also reason about knowledge of agents about ac-

tions. IDEAL has a special sense of resource-sensitivity: it treats communication actions between the agents and the agents themselves as resources to other agents. Where the former is the usual quantitative resource of Linear Logic [44], the latter is a new quantitative-like resource. It encodes the fact that not every agent can communicate with all other agents and obtain new information: different agents have access to different information. This feature is specifically reflected in the sequent calculus where agents are themselves formulae of the logic and their contexts are encoded by different roles of comma between them and other formulae, e.g. propositions and actions. Our sequent system is the first one of its kind for a dynamic and epistemic logic, since the proof system of DEL is a Hilbert-style axiomatics. It shares techniques of, and adds novel features to Intuitionistic Non-commutative Linear Logic [94] and also Labeled Deductive systems of [12]. The constructive nature of IDEAL also makes it a suitable dynamic logic for partial information contexts, for example for belief revision [40], that is revising prior beliefs of agents when contradicted by some new information. These application have been dealt with in a recent joint work of the author with Baltag in [11]. Another application is to encode and reason about safety of internet security protocols [80], this application will be dealt with in this thesis.

The chapters of this thesis are organized as follows:

In chapter two we go through the algebraic semantics of IDEAL. The theoretical starting point of our algebraic semantics is the algebraic logic of Tarski [86], where elements of an order structure represent logical propositions. The operations of the structure stand for propositional connectives such as conjunction and disjunction. We then move on to the algebraic logic of Lambek [56], introduced to reason about sentence structure in linguistics. The elements of this logic are not propositions but linguistic types. Lambek's logic is resource-sensitive and forms the basis of various dynamic logics [45], for example quantales [2, 74, 77] and Linear Logic [44]. If elements of Lambek's logic are thought of as actions, then resource-sensitivity means that doing an action twice has a different effect than doing it once. This is very different from Tarski's logic of propositions where for example stating a proposition two times is the same as stating it once. IDEAL models both actions and the change induced by them on propositions, so its semantics is a join of Tarski and Lambek-style logics. This is a well-known method for logics used in computer science: programs are actions and propositions encode properties of the system that are changed after running a program on the system [45, 47]. The effect of programs on propositions gives rise to a dynamic modality, which is the Galois right adjoint of the connective that joins together these two logic, that is *update*. Interestingly, this dynamic modality is the *weakest precondition* of Hoare logic [47]. So we can reason about the effect of actions on proposition by adjunction. The novelty of the approach of this thesis is that these two logics should be equipped with structure preserving epistemic operators to stand for information of each agent. Another interesting point is that the Galois right adjoint to these maps will stand for knowledge of agents. This provides us with a reasoning by adjunction technique also for epistemic modalities. These structure preserving maps cannot be freely copied and deleted since they are not in general idempotent, a point that enables us to consider these maps, thought of as agents, as resources. A last point is the non-distributivity of our

setting: it is amazing that distributivity of the algebra is not a crucial property in dealing with epistemic scenarios.

In order to verify that the algebra does what it promises, we apply it to encode and solve the famous epistemic puzzle of *muddy children*, discussed in detail in [39]. We show how epistemic and dynamic features of IDEAL and its sense of resources, enable us to prove the puzzle in a very elegant equational manner. As a result, the proof of this puzzle in our logic is much easier and shorter than other approaches, for example the standard epistemic logic solution of [39] and also the solution of Dynamic Epistemic Logic, mentioned in [9]. We also present two different versions of the original puzzle, in these versions children are not honest and they take part in secret communication actions, that is they cheat and lie. As a result the honest children, since they do not have access to the secret communication actions of cheating and lying, get confused and will believe in wrong information. We encode and prove these misinformation versions and show how our sense of resources that can deal with different ways different agents reason about knowledge, plays a crucial role in our solution.

In chapter three we provide an informal presentation of the logical syntax for IDEAL. The reader only interested in technical details can skip this chapter and proceed directly to chapter four. The two common logical formalisms for modern logics are Hilbert-style axiomatic and Gentzen-style sequent calculus. The Hilbert-style logical systems for propositional logic consist of many axioms about logical connectives and only one rule, namely modus ponens. Thus one can say that the focus of these systems is on *what* are the properties of logical connectives in terms of the axioms they satisfy. The Gentzen-style sequent calculi offer an opposite approach: these systems consist of many rules and only one axiom, that is the identity axiom. The focus of these rule-based systems is thus on *how* the connectives are used rather than their properties. This feature has shown to be useful in applications in Computer Science, in investigating properties of *logical proofs*, and has led to the field of proof theory [87]. While Hilbert-style axiomatics are closer in nature to the logical semantics presented in chapter one, in the sense that they both have an equational and axiomatic approach, sequent calculi lie on a different wave length and reveal a different view on the nature of logical connectives. On the other hand, developing a sequent calculus from an algebraic semantics, with regard to which the calculus is sound and complete, is a hard and delicate task for which there exists no general method. But once developed, the sequent calculus can be used, much easier than a Hilbert-style logic, to study applicability of the formalism and also be implemented in automatic proof search tools, such as theorem provers and proof assistants, in order to mechanize the reasoning.

The logical system presented in chapter three is a Gentzen-style sequent calculus and is the first sequent calculus for dynamic epistemic logic. The sequent calculus consists of two intuitionistic systems: one for the propositions and one for the actions. These two systems are connected via the mixed rules of the propositional system. We present the syntax of each of these systems and explain what each operation means in informal terms. We also provide an intuitive way of reading the sequences of each system and use this reading to explain the rules of each system. In a nutshell, a propositional sequence is a list that can have propositions, actions, and also agents in it, for example (m, q, A) is a sequence

in which m is a proposition, q is an action, and A is an agent. In intuitive terms it encodes agent A's information about the effect of action q on proposition m. If we use this sequence in a propositional sequent denoted by $\vdash_M$, for example $m, q, A \vdash_M m'$, it means that after doing action q on proposition m, agent A knows that proposition m' holds. An action sequence is a list of actions and agents, for example (q, A) encodes agent A's information about the action q. If we use this sequence in an action sequent denoted by $\vdash_Q$, for example $q, A \vdash_Q q'$, it means while action q is happening, agent A has wrong information about it since he thinks that action q' is happening. Our sense of resource-sensitivity is well reflected in the sequent calculus. For example after a communication action q, an agent might not be able to conclude that a certain proposition holds, that is

$$m, q, A \nvdash_M m'$$

but if he does the same action twice, or performs another communication action q', he will be able to derive the desired conclusion, that is

$$m, q, q, A \vdash_M m' \qquad \text{or} \qquad m, q, q', A \vdash_M m'$$

So repetition of actions matters in validity of sequents and in agents' knowledge. Another important issue in deriving conclusions is presence of agents. A certain derivation might not hold in reality, for example

$$m, q \nvdash_M m'$$

but if an agent is present in the context, he might think that the conclusion holds, that is

$$m, q, A \vdash_M m'$$

This way of explicitly encoding agents in sequents is a novel feature of our the sequent system and resembles the labeled deductive logic of [12]. Other features of our sequent calculus is having an epistemic structure for actions, an idea not presented in the Hilbert-style logic of [9], and the non-boolean nature of both proposition and action systems. Our system recaps its reasoning power by using the properties of composition of adjoints to develop rules for epistemic and dynamic modalities.

After developing our sequent calculus from the algebraic semantics, we have to show that our development is consistent, in the sense that it does not lead to contradictory conclusions, this is referred to as the soundness theorem. We also have to show that the reasoning power of the sequent calculus is at least the same as the algebra, that is every property that holds in the algebra is derivable form the calculus, this is referred to as the completeness theorem. Thus in chapter four we prove that our sequent calculus is sound and complete with regard to our algebra. Although distributivity is not needed in algebraic verification of properties of epistemic scenarios, it comes handy in the syntax of our single-succedent sequent calculus. It is also the necessary outcome of our ideal construction, a technique

we use to build infinite semantics from finite syntax. We first formalize the meaning of sequents, presented informally in chapter three, and then show how each sequent system can be modeled by its corresponding algebra presented in chapter two: propositional sequents with the Tarski-style algebra and action sequents with the Lambek-style algebra. This makes our sequent rules different from the usual intuitionistic sequent calculi, which have internalized implication. On the action side, we use the same algebraic approach as in Lambek Calculus [56] with lattice operations (and empty sequence on the left) or more precisely Intuitionsitic Non-Commutative Linear Logic [44]. The novelty of our approach is that we have agent contexts in our sequents to encode epistemic modalities. Non-commutativity is a crucial and necessary property of our system, this is because communication actions cannot be permuted freely since they may cause different effects once applied in different orders.

The proofs of soundness and completeness are done as usual [17] with the difference that we have to prove these theorems for two systems, both of them being non-boolean and epistemic. These properties make our proofs more tedious and longer than usual soundness and completeness proofs. Another difference is that because our semantics are both based on sup-lattices, we have infinite meets and joins. So the completeness proofs have to be done in two steps: first for the finite case via building models out of syntax of logic, and then extended by ideal construction to the infinite case.

In chapter five we present a a serious domain of applications for IDEAL: reasoning about security protocols. The typical scenario in the setting of security protocols is that two agents want to share a secret via message passing. The problem is that the communication channel is not safe and there is always a chance that a malicious intruder will intercept the messages. So agents have to come up with communication protocols that guarantee safe communication of their secret. An example is an online transaction between a client and his bank, the secret is for example a credit card number that should be communicated on the Internet (while where we are all aware that internet is not a safe communication channel). This is one reason the field of security has been created, to design communication protocols along which secrets can be safely shared. These protocols use different methods for ensuring safety, such as digital signatures, hashes, keys, and encryption. But there is always a chance that the intruder can decode the hashes, forge signatures, guess the keys etc. So once the protocol has been designed, the goal is to ensure its safety in presence of such powerful intruders. One way to achieve this goal is to formalize the protocol in an epistemic logic and then prove its safety. Different epistemic logics have been specifically developed for this purpose, the most famous of these was the BAN logic [22]. The problem with the logical approach is that often protocols were proved to be safe, but flaws were discovered on them later. For example the Needham-Schroeder protocol [68] was a protocol that was proven to be safe in BAN logic, until 15 years after the proof when a flaw was discovered on it by Lowe [59] that showed the protocol was not safe. Another approach to the safety of protocols is to build the state space of the protocol and then use model-checking techniques to verify the safety. The problem with this approach is that one can only verify that after a certain amount of time and in a certain context, the protocol is safe and a general proof cannot be provided. So the field of security is now focused on more powerful logical tools and model-checking techniques. From this perspective

IDEAL can be a very good candidate for the logical approach since its reasoning powers are much more efficient than a usual epistemic logic. It can deal with properties and communication actions, but also with knowledge of agents about properties and more importantly about actions. A security protocols is nothing but a series of communication actions, about which agents do not have certain knowledge. For example when A sends a message to B, he is not sure about the receive action by B. The ability of IDEAL in formalizing knowledge of actions and connecting it with knowledge of properties provides it with a unique reasoning power about security protocols. Moreover, IDEAL has a sense of model checking too, in order to encode a protocol, it first builds the state and action space and then reasons about them using its epistemic and dynamic modalities. But since it does so in an algebraic manner, the proofs are done equationally and are easier and more efficient than usual Kripke semantics based settings. Another important issue in IDEAL is its compositionality: it builds a protocol by composing basic communication actions and then reasons about them compositionally. In chapter five we show how all these features can be used to encode security protocols and prevent agents from falsely believing that the protocol is safe when it is not. This chapter is meant to show the ability of our IDEAL in dealing with applications, further improvements and developments, for example adding encryption and automizing the reasoning constitute future work.

In chapter six we study the connection between IDEAL and the Dynamic Epistemic Logic of [9, 10]. The differences between IDEAL and DEL, in their semantics and proof systems, has been mentioned above. In this chapter we show that relational models of DEL are instances of algebraic models of IDEAL. We start by introducing the Kripke semantics of DEL: its usual state models and its new actions models. We then define the *update product* of the two, the sequential composition and choice of action models, and provide examples. Next we repackage the accessibility relations to functions and show how powerset of the states of a state model is a module and powerset of the free monoid of states of the action model is a quantale. The update inequality is obtained from the repackaged definition of update and by forcing conditions on the module and quantale, basically making them *atomistic* from atomic. It then follows that this powerset model of DEL, called a *concrete epistemic system*, is a *strong atomistic epistemic system* , a special case of the sup lattice models of IDEAL. Before finishing this last chapter, we show that asking for further conditions on the module and on the appearance maps provides us with other types of epistemic modalities, for example one that satisfies axiom 4 of $S4$. The interesting point is that only in our concrete setting of Boolean Algebras, we can define the belief diamond modality by taking the De Morgan dual of the *linear adjoint* of the appearance map.

Finally in the appendix we show how the algebraic setting of IDEAL can be expressed in the context of sup-enriched categories. The idea is that our logic of actions, that is quantales, can be seen as a one object sup-enriched category [20, 58, 85]. Our logic of propositions is also a sup-lattice and thus an object of the category Sup, which is monoidal closed and thus also sup-enriched. We encode the effect of the actions on propositions as sup-enriched functors in this category. Rather than considering only one functor for all agents, as we did in the algebra, here we have different functors for

different agents. This enables us to have a different update schema for each agent and thus relativize the notion of epistemic update: each agents updates his knowledge in his specific way. In this setting the epistemic modalities arise as lax sup-enriched natural transformations between the update functors. The setting of sup-enriched categories provides IDEAL with a structured way to deal with relativized update. Applications to philosophical and Computer Science problems, for example to the problem of Logical Omniscience constitutes future work.

The following are possible future extensions of this thesis:

Strengthening the Logic. Two important properties of a logical system are the decidability of its semantics and elimination of cuts in its logical syntax. These two properties play a crucial role in the efficiency of the modeling and reasoning powers of the logic and thus directly affect the domain of applicability of a logical system. Classical Propositional logic and Lambek Calculus are both decidable and cut is eliminable for them. However, adding epistemic operators to them and joining them together does not guarantee that the system remains decidable and cut-free. This is a possible future project: to develop a decidable and cut-free version of the IDEAL logic of this thesis, so that it can reason efficiently and structurally about knowledge resources and change. The cut-elimination problem of our logic arises from the interaction between the epistemic modalities, mainly appearance maps, and resource-sensitive multiplication and update, which need caring for context splitting and sharing at the same time. In a more technical note, the left rule for multiplication in the action logic and the left rule for update in the propositional logic, split the action and propositional context (respectively), but share the agent context. This causes problem for eliminating cut with a formula that contains appearance of update in the propositional setting and appearance of multiplication in the action setting. Solving this problem makes an interesting future project.

In the same lines, computing the complexity of IDEAL is another future project. Complexity of different systems of epistemic and dynamic logic have been studied, for example in [39, 45]. But epistemic logics with dynamics are new and their complexity is yet an open problem, recently complexity of public announcement logic has been studied in [60]. It would be interesting to extend this result to the version of dynamic epistemic logic with both public and private announcements. We believe that the algebraic semantics of this thesis provides a less complex logic and that computing its complexity is easier than doing the same for DEL.

Connections with Linear Logic Quantales without lattice operations (ordered monoids) model Lambek Calculus [56]; full quantales (with more structure) are models of non-commutative Intuitionistic Linear Logic [94]. Quantale models for commutative versions of Linear Logic has also been studied, see for example [57, 76]. However, in all these approaches, the modalities of Linear Logic, that is exponentials, are modeled by co-closure and closure operators on the quantale. The action part of IDEAL can also be seen as a model of non-commutative Intuitionistic Linear Logic, with the difference that

our modalities are not exponentials of Linear Logic, but their composition is. So our epistemic modalities can be seen as a factorization of Linear Logic exponentials. Making this connection more precise may lead to development of an epistemic action model for Linear Logic, which would perhaps help in assigning another meaning to exponentials.

Coalgebras and probability. In the Computer Science literature, three different formalisms have been used to formalize modalities, the relational semantics of Kripke structure [39], Coalgebraic systems [66, 78], and finally algebraically in [51, 50, 17]. The Kripke semantics approach is the traditional one and the coalgebraic approach has been developed recently. In a way, the coalgebraic way of doing modal logic, is half way through the relational and the sup lattice approach of this thesis. In a nutshell, in the relational semantics the knowledge modality is defined in terms of the accessibility relation on a set of states S, that is we have one such relation for each agent $R_A \subseteq S \times S$. In coalgebras, this relation is lifted one level to the functions on set of states and its power set, that is $g_A : S \to \mathcal{P}(S)$. This map is in bijections with a sup-map from the power set to the power set, that is $f_A : \mathcal{P}(S) \to \mathcal{P}(S)$ where we lift our Coalgebras to the level of sup-lattices. In general modeling probabilities order theoretically is not easy, some attempts have been done in [23]. However, probabilities are nicely formalized using coalgebraic methods [30]. A nice project would be to combine the algebraic method with the coalgebraic ones to benefit from the bonuses of both and to develop a probabilistic model of reasoning about dynamics of knowledge. This probabilistic model of knowledge can have applications in deriving secrecy of security protocols and also reasoning about Quantum security protocols, discussed below.

Applications. In the application chapter we have provided a setting in which security protocols can be encoded via the suspicions they raise in the agents. However, we have only considered clear text messages where no encryption is applied. A possible and necessary extension of this setting, would be to encode encrypted messages and reason about secrecy of them. So a wider range of protocols can be reasoned about in IDEAL and perhaps a non-discovered attack might be discovered in a protocol. However, in order to do so one needs to first implement IDEAL in a theorem prover and automate its reasoning. Another possible extension would be trying to encode Quantum protocols and perhaps to use setting to encode combinations of classical and Quantum reasoning techniques will help in design of mixed protocols. In this setting, one can think of propositions as results of measurements on Quantum systems and actions will stand for Quantum actions such as sharing a Bell pair and measurements in the style of one-way model [73] and measurement calculus [26]. We can then use the dynamic modality to express how each measurement connects to its result and the epistemic modality to reason about the knowledge of agents about these measurements. The non-deterministic choice on the quantale helps us encode possible measurements on different basis, and the disjunction on proposition will encode the choice of the result of these measurement. The interesting part would be the dynamic axiomatization of *sharing a Bell pair*, which is one of the distinctive features of Quantum protocols, and then use it to reason about knowledge of agents after sharing a Bell pair and performing measurements. In order to

give a full analysis of protocols such as BB'84 [15], B'91 [13], and BBM [14], one needs probabilities. So as mentioned above, coalgebraic settings seem a nice option. In particular it would be useful to encode the bit-commitment protocols such as the ones mentioned in [21] and see if the setting of this thesis will discover the attack discovered by Mayers in [63].

Philosophical Extensions. Resource-sensitivity sheds new light on the problem of omniscience, but is not addressed in the existing solutions in standard treatment of epistemic logic from Hintikka's [46] to the more recent textbook by Fagin et al. [39]. The idea of using a resource-sensitive logic to avoid the problem of logical omniscience has been introduced by Dubucs in [34] and its relations with antirealism has been investigated by Marion and Dubucs in [35]. Based on these ideas, Marion together with the author have argued in favor of the feasibility of an epistemic resource-sensitive logic, namely Linear Logic, to reason about knowledge in [62]. The feasibility argument is partly based on the implementation of this logic by the author [81] and using it to solve an epistemic puzzle. One very interesting philosophical extension of this thesis would be to continue the same line of argument and to study how the dynamic logical approach of IDEAL can tackle the problem of Logical Omniscience. For example how availability of different resources to different agents relativizes change of knowledge, and how would this impact omniscience, and what would be the philosophical significance of a relative omniscience. All of these can be extended to the sup-enriched setting where we have relativized update and see how this will effect the omniscience. It is worth noting that our knowledge modality is monotone, which will imply that each agent knows all the consequences of what he knows. So if an agent knows P, he knows all the consequences of P. Our aim is not to cure the second part of the argument, that is knowing all the consequences of P, but to relativize the first part, that is knowing P. We want to make our agents know the P's with regard to the communication actions that they can perform and their capability in updating their knowledge as a result of these communication actions. But once they know the P, they will know all its consequences nonetheless.

Another important philosophical issue is the very definition of knowledge as justified true belief that harks back to Plato. This definition has been dominant in the literature, but a recent philosopher of knowledge, Williamson [92], has defended the opposite view that knowledge is sui generis and cannot be defined in terms of belief. Another possible philosophical extension of this thesis would be to study the notion of knowledge through a review of the basic philosophical distinctions and definitions that underlie the development of epistemic logic in 20th century, from C.I. Lewis to Hintikka today. One should then try and see what do epistemic axioms of IDEAL that are based on adjunction rather than de Morgan dualities tell us about the nature of knowledge and its change.

Dualities and Relational semantics. One of the beauties of the field of algebraic logic is the dualities it provides for the same logics with relational semantics. The first of these dualities was developed by Tarski, together with Jonsson in [51, 50] . This duality says that the classical modal logic with its relational Kripke semantics is equivalent to a boolean algebraic logic with operators. The duality

theorem provides a way to build one given the other. The second duality was done by Stone [84] for relational and topological models of logics, where same as in Jonsson-Tarski duality, the algebraic logic part was based on a boolean lattice and dually to a power set relational structure. It was Priestely [3] who for the first time extended these dualities to other lattices, she considered distributive lattices. Recently, partly by development of substructural logics [75] such as Relevance logics, the need to extend these dualities to other lattices was raised. Different relational models were developed for different substructural logics, for example relational models for a class of substructural logics were studied in [36]. However, there was no general duality theorem for these logics and their relational models until the recent work of [37] that proves a duality for non-distributive lattices. The algebra of this thesis is non-distributive, for the module we did not assume it since we did not need it to prove epistemic scenarios. But a quantale is by definition non-distributive, we have moreover, a quantale with operators, which makes a very good case of the application of this recent duality theorem together with insights from Abramsky's duality [1] for Domain Theoretic semantics of programs. So we can build a relational model for our quantale and study its relational properties. It should be noted that in our theorem, we show how a completely atomistic boolean algebra is a relational model of DEL, but most of this extra structure, that is the power set structure, is redundant for epistemic action, what would for example the negation of a communication action mean? Developing a relational semantics for the quantale of actions would be much more helpful in investigating the properties of these actions, which are similar to the properties of programs discussed in [1], rather than imposing some properties on them and forcing them to act in a power set. In the same lines and by using the duality for non-distributive lattice, it would be interesting to build a multi-succedent sequent calculus that is complete with regard to a non-distributive epistemic system.

Domain theory. In order to build our theorem mentioned above, we form the power set of states $\mathcal{P}(S)$ and actions $\mathcal{P}(\Sigma)$ of the Kripke semantics of DEL and then lift the powerset operators to sup-maps. But before taking the power sets, we have to close our actions under sequential composition $\Sigma \bullet \Sigma \subseteq \Sigma$, and also close our states and actions under the update product, denoted in the setting of DEL by $\otimes$, that is we have to assume $S \otimes \Sigma \subseteq S$. It is only now that we can take the power set of S and Σ and make our passage to the setting of sup-lattices. This is a non-constructive step and disagrees with the beauty of the sup-lifting. One possible way would be to use Domain Theory and least fixed points to encode these closures. In a domain-theoretic setting, our operators that were sup-maps, will become continuous maps. Since these closures will also be continuous maps, we will have a uniform passage to the algebraic setting.

Belief Revision. The non-boolean algebra of this thesis has applications in partial information settings such as Belief Revision [40, 4]. The algebraic semantics presented in chapter two can be refined to incorporate a mechanism for dynamic belief revision in a multi-agent setting. This mechanism developed in [11] has a number of novel features, when compared with traditional belief revision systems

such as AGM [4]. In our approach we encode revision as a particular form of epistemic update, as a result of which we can revise with epistemic propositions as well as facts, we can also revise theories about actions as well as about states of the worlds, and we can do multi-agent belief revision. The traditional belief revision formalisms are static, only revise theories with facts, and cannot deal with multi-agent revision. In [11] we show the application of our multi-agent dynamic setting to a cheating version of the muddy children puzzle where by using this logic, after the cheating happens, honest children will not get contradictory beliefs. A possible future work in this direction would be to extend the sequent calculus of this thesis to a sequent calculus for dynamic belief revision.

Chapter 2

Algebraic Semantics

In this chapter we will present an *algebraic semantics* to formalize the knowledge of agents in a multi-agent setting, the communications between the agents, as well as the changes that are induced to their knowledge due to communication. First we briefly explain the basics of the theory on which our algebra is based, that is order theory. Then we present our algebra and next, in the interpretation section, explain the significance of these mathematical notions in the context of knowledge, communication and change. Finally we apply our algebra to the famous epistemic puzzle of muddy children and show how our algebra can solve the puzzle as well as a cheating and lying version of it.

2.1 A Brief Look at Order Theory

We start the presentation of our algebra by explaining, both in formal and intuitive terms, some key mathematical notions necessary for the understanding of algebraic logic. We start with sets and ordered sets, and proceed to lattices, sup-lattices and partially ordered monoids or quantales. We will also define the notion of structure-preserving maps or *homomorphism* for sup-lattices and quantales. The main mathematical object of our semantics is a pair of a sup-lattice and a quantale together with a family of homomorphisms of each. Choosing the appropriate notion of homomorphism of this pair helps us to come up with an elegant choice of modalities.

2.1.1 Sets and Lattices

Plain Sets. Sets are the basic object of mathematical modeling, to model a property ϕ representing, for example, even natural numbers, we build a set of numbers that satisfy the property ϕ. That is we build a set of even numbers $Even := \{x \in N \mid \phi(x)\}$. Sets are flat objects in the sense that they do not reflect any structure between their elements. For example, all the elements of our set $Even$ are treated in the same way: by being even. There is no structure on the set $Even$ to reflect the connection between these even numbers. This points to a defect of only considering plain sets for modeling properties, especially

in cases when the elements of these sets do have a structure, e.g. each even number $x \in Even$ is smaller than its successor even number $x \leq x + 2$, a relation not reflected by the set $Even$.

Ordered Sets. In order to over come this defect, one can move from plain sets to sets with structure, starting from *ordered sets* that reflect the order $\leq$ (less-than or equal to) relation between the elements of the set, and are denoted as pairs $(X, \leq)$. For example $(Even, \leq)$ is an ordered set with the order being the order of natural numbers $1 \leq 2 \leq 3 \leq \ldots$. The order relation can have different properties, for example reflexivity, symmetry or anti-symmetry, and transitivity.

- **Reflexivity** says that each element is less than or equal itself $x \leq x$.
- **Symmetry** says if an element is less than or equal another one, then the other one is also less than or equal the first one $x \leq y \rightarrow y \leq x$. While symmetry is not a very common property of ordered sets ($1 \leq 2$ but $2 \not\leq 1$), our next property is.
- **Anti-symmetry** says if there is a symmetric order relation between two elements $x \leq y$ and $y \leq x$ then they should be equal $x = y$. This is a very common property for example it is true about natural numbers.
- **Transitivity** is another important property, it says if $x \leq y$ and $y \leq z$ then $x \leq z$. The order on natural numbers satisfies transitivity, e.g. $1 \leq 2$ and $2 \leq 3$ implies that $1 \leq 3$.

The ordered sets that their order relation is reflexive, antisymmetric and transitive are called *Partially ordered sets* or *posets*. Their order is called a *partial order*. For example the set of natural numbers is a poset.

Upper and Lower Bounds. The order on a set not only represents the structure of the elements of the set, but also acts on the subsets of the set in two ways, thus give rise to two operations on the ordered set. These two ways determine the *upper bound* and the *lower bound* of the subsets, that is their greatest and least elements. Upper and lower bounds are defined for the subsets $X_1 \subseteq X$ of an ordered set $(X, \leq)$ in the following way:

- $ub \in X$ is an upper bound if for all $x \in X_1$, $x \leq ub$.
- $lb \in X$ is a lower bound if for all $x \in X_1$, $lb \leq x$.

Least Upper Bounds and Greatest Lower Bounds. The ub and lb operations are not unique, that is each subset can have more than one upper or lower bound. But one can strengthen the ub and lb operations and thus get two other (stronger) operations on the subsets. These two operations are the *greatest lower bound* and the *least upper bound*. Where each subset of X might have more than one lower or upper bound, the greatest lower bound and the least upper bound are unique by their definition below

- $lub \in X$ is a least upper bound or a *sup* if it is an upper bound and all other upper bounds $ub \in X$ are bigger than it $lub \leq ub$.

- $glb \in X$ is a greatest lower bound or an *inf* if it is a lower bound and all other lower bounds $lb \in X$ are smaller than it $lb \leq glb$.

Note that these four operations are not always defined for a subset of an ordered set. In other words, not every subset of an ordered set has an upper bound or a lower bound and similarly for greatest and least ones. This is because the elements of the subset might not even have an order relation with each other to start with. So they cannot be compared to each other. Also if a subset has upper bounds or lower bounds, it might not always have a sup or inf. This is again because there might not be an order relation defined between the upper or lower bounds of that subset. For a pictorial example and a detailed discussion see [28]. A simple example is the set of natural numbers N. In this case there is an order between all the elements, however a subset of natural numbers has upper bounds and a sup only if it is finite, but any such subset has a lower bound and also an inf.

Top and Bottom. For an ordered set $(X, \leq)$, if the sups of X exists (X being a subset of itself), we denote it as $\top$ and call it *the top of* X . Similarly, if the inf of X exists, we denote it as $\bot$ and call it *the bottom of* X . Note that since X is the greatest subset of itself $X \subseteq X$, its sup and inf $\top$ and $\bot$ are the largest and least elements of any member of X. A finite subset of natural numbers that starts with number 1, (a chain of N) and ends with number $n \in N$ has thus the bottom element $\bot = 1$ and the top element $\top = n$.

Binary and Arbitrary. When talking about sups and infs, we should distinguish between the sup (similarly for infs) of two elements in a set $x, y \in X$ denoted as $sup\{x, y\}$ and the sup of an infinite set of elements X denoted as $sup\ X$. These are also referred to as binary and arbitrary sups respectively (similarly for infs). For an infinite set the existence of binary sups of its every two element does not imply the existence of its arbitrary (including infinite)sups. But the existence of arbitrary sups implies that binary sups also exist. In the finite case, the existence of all binary sups of a set would imply the existence of the sup of the set and also the other way around.

We adopt the notation of Davey and Priestley in [28] for binary and arbitrary sups. For binary sups and infs we write

$$x \vee y$$

which reads as 'x join y' in place of $sup\{x, y\}$ when it exists, and

$$x \wedge y$$

and read it as 'x meet y' in place of $inf\{x, y\}$. Similarly we write $\bigvee X$ and $\bigwedge X$ for arbitrary joins and meets instead of $supX$ and $infX$.

Lattices and Complete Lattices. Given an ordered set $(L, \leq)$, we define:

- For all $x, y \in L$, if binary joins $x \vee y$ and binary meets $x \wedge y$ exist then L is called a *lattice*.
- For all $M \subseteq L$, if arbitrary joins $\bigvee M$ and arbitrary meets $\bigwedge M$ exist then L is called a *complete lattice*.

An example of a complete lattice is the powerset (set of all subsets of X) denoted as $\mathcal{P}(X)$. The order between its elements $X_i \in \mathcal{P}(X)$, where each X_i is a subset of X, is inclusion (the subset relation) $X_1 \subseteq X_2$. The arbitrary join (similarly for meets) of elements is their union (intersection for meets), which is again a subset of X and thus an element of $\mathcal{P}(X)$. Formally we have:

$$\begin{aligned} \bigvee_i X_i &= \bigcup_i X_i \\ \bigwedge_i X_i &= \bigcap_i X_i \end{aligned}$$

Meets in terms of Joins. Although being a complete lattice means having both arbitrary joins and meets, but if a lattice L has only one of them, for example arbitrary joins, it also has the other, that is arbitrary meets. This is because arbitrary meets can be defined in terms of arbitrary joins (and the other way around) by the following equation:

$$\bigwedge_i a_i = \bigvee \{b \in L \mid \forall i, b \leq a_i\}$$

where L is a lattice with arbitrary joins and $\forall i \in N, a_i, b \in L$. This definition says that the arbitrary meet of elements a_i of a lattice is the arbitrary join of all the elements that are below each a_i.

Sup-Lattices. Thus a lattice L that has arbitrary joins (or meets) is a complete lattice. The main object of our semantics is a special case of a complete lattice with focus on its arbitrary sups, that is why it is called a *sup-lattice*. By *focus on sups* we mean that the structure preserving maps on the lattice L, for example $f : L \to L$, called *homomorphisms* (defined below), preserve arbitrary joins, that is

$$f(\bigvee_i a_i) = \bigvee_i f(a_i)$$

Homomorphisms. A homomorphisms is a map between two mathematical objects that respects the structure of them. For example a homomorphisms on an ordered set should yield an ordered set, that is

$$h : (X, \leq) \to Y$$

then Y should be an ordered set itself $(Y, \leq')$, and not just any ordered set, its order should correspond to the order in $(X, \leq)$ in the following way:

$$\text{If for } x_1, x_2 \in X \quad x_1 \leq x_2 \quad \text{then} \quad h(x_1) \leq' h(x_2)$$

Similarly if we have a homomorphism on a complete lattice, it should yield another complete lattice, by preserving the arbitrary joins and meets. Thus if we have a sup-lattice, we ask the homomorphism to preserves arbitrary joins.

The formal definition for a sup-lattice is:

Definition 2.1.1 A *sup-lattice* L is a complete lattice for which we take as homomorphisms the maps that preserve arbitrary joins.

Algebraic Logic in Complete Lattices. We can use the mathematical structures introduced above to do logic, that is to talk about truth and falsity of properties. In a plain set X, we can say if an element is in the set or not

$$x \in X \quad \text{or} \quad x \notin X$$

In an ordered set $(X, \leq)$, we can say whether an element $x \in X$ is in order relation with another element $y \in X$ or not

$$x \leq y \quad \text{or} \quad x \not\leq y$$

In a lattice $(L, \leq)$ we can say much more: we can express that if two elements are in order relation with each other, then so are their meets and joins with any other element, for example for $a, b, c \in L$ we have

$$a \leq b \quad \text{implies} \quad a \leq (b \vee c) \quad \text{and} \quad (a \wedge c) \leq b$$

We can also say that each element is less than its join with any other element

$$(1)\, a \leq (a \vee b) \qquad \text{and} \qquad (2)\, b \leq (a \vee b)$$

and that the meet of any two elements is less than each of them

$$(3)\, (a \wedge b) \leq a \qquad \text{and} \qquad (4)\, (a \wedge b) \leq b$$

and many other nice properties derived from those, discussed in detail in books on order theory for example in [28, 49, 16].

One can think of elements of a lattice $a, b \in L$ as logical propositions and look at the order relation $\leq$ as the logical entailment, so $a \leq b$ reads as 'proposition a entails proposition b'. Consequently, meets of the lattice stand for conjunction and joins for disjunction. Also the top of the lattice becomes the always true proposition, that is a tautology, and the bottom of the lattice becomes the Falsum or contradictory proposition. The above statements, that are true in any lattice, stand for axioms of a logical system. The first and second cases above express the property of disjunction: if a proposition is true, so is its disjunction. The third and fourth cases above are properties of conjunction: if a conjunction of two propositions is true, so are both of its conjuncts. So a lattice can model logical reasoning, although in a minimal logical system with only two connectives disjunction and conjunction

and two constants: $\top$ and $\bot$. Note that these connectives, disjunction and conjunction, do not distribute over each other but are connected since one can be defined in terms of the other. However, this minimal system serves as a base logic and can be extended, by adding other connectives such as implication and negation, to more expressive logics: the familiar intuitionistic (the lattice being a Heyting algebra) and classical logics (for a Boolean algebra). But there are other ways to go more expressive, for example by asking our base lattice to be a complete lattice, and this is the way we are going to follow in the logic of this thesis.

In a complete lattice we are more expressive since we can talk about arbitrary joins and meets, and this gives rise to other very interesting properties. We can still talk about logical axioms for binary meets and joins, and we can extend them to arbitrary ones. For example for $i \in N$ and a, b, c_i in a complete lattice $(L, \leq)$, we have

$$a \leq b \quad \text{implies} \quad a \leq (b \vee (\bigvee_i c_i))$$

and also arbitrary join and meet versions of properties 1 to 4 above, for instance:

$$a \vee (\bigvee_i b_i) \leq a \qquad \text{and} \qquad a \vee (\bigvee_i b_i) \leq \bigvee_i b_i$$

These arbitrary meets and joins, can be seen as a way to reason about properties of infinite sets via the arbitrary join or meet of their elements. Another piece of extra expressiveness of a complete lattice comes from the concept of *Galois Adjunction*.

2.1.2 Galois Adjoints

In a sup-lattice (or a meet-lattice) we have an extra structure called a *Galois adjoint* that provides us with unary operations that raise the reasoning power of the logic. They are defined as follows:

Definition 2.1.2 Every sup-homomorphism $f : L \to M$ preserving arbitrary joins has a right Galois adjoint $g : M \to L$ defined as

$$f(a) \leq b \quad \Leftrightarrow \quad a \leq g(b)\,,$$

which preserves arbitrary meets. We denote such an adjoint pair as follows

$$f \dashv g\,.$$

The significance of having Galois adjoints is that only by asking for the existence of arbitrary joins and a join-preserving operation f, we get another operation g that preserves the order and arbitrary meets on the lattice and moreover it is connected to the first operation f through the adjunction relation. In other words, this structure provides us with two unary operators such that we have the result of one operation, we can calculate the result of the other and vise-versa. For example given f, its adjoint g

can be calculated as follows

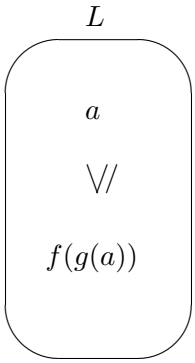
$$g(b) = \bigvee \{c \in L \mid f(c) \leq b\}\,.$$

The adjoint pair (f, g) can be seen as two unary logical connectives. The adjunction connection is a way of relating logical connectives to each other and increases the reasoning power in logics based on it. In classical logic these connections are mostly defined in terms of negation and de Morgan dualities.

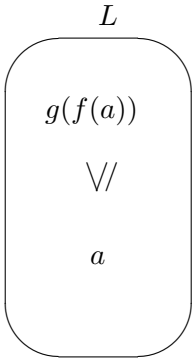
The adjunction equation helps us prove other correlations between these connectives, correlations that represent patterns of logical reasoning. For instance we have the following *composition corollaries*:

$$\begin{aligned} (f \circ g)(a) &\leq a \\ a &\leq (g \circ f)(a) \end{aligned}$$

The first equation says that if you first do the right adjoint of an operation $g(a)$ and then the operation itself $f(g(a))$, will stay less than the element you started with:



The second equation says that if you change the order, that is first the operation $f(a)$ and then its adjoint $g(f(a))$, will stay greater. This relation is depicted as follows



In logical terms, applying the sequence of two unary operators on a proposition either implies or is implied by the proposition (depending on the order). Adjunction methods were first developed and named in *category theory*. Then it was realized that Galois also used them, but did not make them explicit or name them as such. In computational terms, the right Galois adjoint g is *weakest preconditions* of the program f and is commonly used to prove correctness of programs in program logics [45, 47, 79], more on this in the next chapter.

2.1.3 Monoids, Quantales, Resources

So far we have two binary connectives $\vee, \wedge$ and two unary ones f, g. If we want to have more expressive power, one way would be to equip our base complete lattice with an extra structure: the structure of a monoid. Monoids are structures on their own and need not necessarily be based on a lattice or a complete lattice, but once based on any of those, the whole structure will become very expressive. We first define a general monoid: a monoid $\mathcal{M}$ is a set M with a binary operation

$$- \bullet - : M \times M \to M$$

that has a unit 1 such that $\forall m \in M$ we have

$$m \bullet 1 = m$$

Monoids are denoted with triples $\mathcal{M} = (M, \bullet, 1)$. An example of a monoid is set of natural numbers with multiplication operation and number 1 as the unit of multiplication

$$\mathcal{N} = (N, \times, 1)$$

If our set M is moreover a lattice, we have an order relation and three connectives (we shall return to the unary operators soon), namely the binary join $\vee$ and meet $\wedge$ and the monoid multiplication $\bullet$. There is also a connection between the multiplication of monoid and the order of lattice

$$a \leq b \quad \text{implies} \quad a \bullet c \leq b \bullet c\,,$$

that is the monoid multiplication preserves the order of lattice. If the base of a monoid is a complete lattice, we will have arbitrary joins and meets, but moreover some Galois adjoints.

Quantales. If we require that the underlying set of the monoid to be a complete lattice, we get a *quantale*. As explained before, a complete lattice has both arbitrary joins and arbitrary meets. But if we have one of them, for example arbitrary joins, we get the other one, that is arbitrary meets, for free. In the quantales, the focus is on joins and thus the base complete lattice is a sup-lattice. As a result the monoid multiplication is asked to preserves both the order of the lattice and these arbitrary joins. Preserving arbitrary joins implies preservation of order but not arbitrary meets. Quantales have

applications in different fields. They were first mathematically introduced by Dilworth and Ward by the name of Dilworth-Ward algebras [33] to analyze rings of real numbers. Subsequently, it was used by J. Lambek [56] to analyze the sentence structure in linguistics but he did not use the name quantale. The name was first introduced by Mulvey [67] for more sophisticated structures of real numbers such as non-commutative C*-Algebras and their application to quantum mechanics. The name quantale is a combination of words 'Quantum' and 'Locale' (that is a complete HA). More recently it has been used in computer science by Abramsky and Vickers [2] to model concurrent processes in a distributed system and by Coecke et al [24] to analyze quantum processes. It is formally defined as

Definition 2.1.3 A *quantale* is a sup-lattice Q equipped with a monoid structure $(Q, \bullet, 1)$ which is such that for all $a \in Q$ the maps

$$a \bullet - : Q \to Q \quad \text{and} \quad - \bullet a : Q \to Q$$

preserve arbitrary joins.

Since the multiplication preserves arbitrary joins on both arguments, i.e.

$$(\bigvee_i a_i) \bullet b = \bigvee_i (a_i \bullet b) \qquad \text{and} \qquad a \bullet (\bigvee_i b_i) = \bigvee_i (a \bullet b_i)\,,$$

it has two right Galois adjoints that can be seen as two implications and are referred to as *residuals* in [56]. They are denoted as

$$a \bullet - \dashv a \setminus - \qquad \text{and} \qquad - \bullet a \dashv -/a\,.$$

These residuals are explicitly defined in terms of multiplication as the following

$$a \setminus b := \bigvee \{c \in Q \mid a \bullet c \leq b\} \qquad \text{and} \qquad b/a := \bigvee \{c \in Q \mid c \bullet a \leq b\}.$$

Quantale Homomorphisms. Since a quantale, lattice-wise, is a sup-lattice, its homomorphisms are sup-homomorphisms, that is they preserve all joins of the underlying sup-lattice. For example $f : Q \to Q$ is a quantale homomorphism if we have

$$f(\bigvee_i b_i) = \bigvee_i f(b_i)$$

This is the minimum property that a quantale homomorphism should have. It can also satisfy some properties with regard to the monoid multiplication, as long as it remains join-preserving. In what follows we are going to ask our quantale homomorphism to satisfy the following inequality

$$f(a \bullet b) \leq f(a) \bullet f(b)$$

We shall explain our reasons in the interpretation section when we discuss how these structures help us achieve our goal, which was reasoning about knowledge and communication.

Examples of Quantales. A good example of a quantales is $\mathcal{P}(X \times X)$, which is the set of all relations $\mathcal{R}$ from a set X to itself $\mathcal{R} \subseteq X \times X$, ordered by pointwise inclusion:

$$R_1, R_2 \in \mathcal{R},\ R_1 \leq R_2 \quad \text{iff} \quad R_1 \subseteq R_2, \text{ that is } (a,b) \in R_1 \Rightarrow (a,b) \in R_2$$

Joins are relational unions

$$\bigvee_i R_i := \bigcup_i R_i$$

The monoid multiplication is the relational composition

$$R_1 \bullet R_2 \ := \ R_1; R_2 \ = \{(a,c) \mid (a,b) \in R_1 \text{ and } (b,c) \in R_2\}$$

The unit of multiplication is identity relation Id, that is

$$R_1 \bullet Id = \{(a,b) \mid (a,b) \in R_1 \text{ and } (b,b) \in Id\} = R_1$$

It is easy to see that $\bullet$ preserves all joins (or distributes over them), that is

$$R \bullet (\bigvee_i R_i) = \bigvee_i (R \bullet R_i)$$

since we have that relational composition preserves union of relations

$$R; (\bigcup_i R_i) = \bigcup_i (R; R_i)$$

These properties are the base of the relational calculus used as a logic for programs by Hoare in [47], where relations are interpreted as programs.

Another example, which is isomorphic to the first one, is $\mathcal{P}(M, ., 1)$; the powerset of any monoid with joins being union of subsets

$$\text{for } M_i \subseteq M, \qquad \bigvee_i M_i := \bigcup_i M_i$$

and composition extended to subsets point wise:

$$M_1 \bullet M_2 := \{m_1.m_2 \mid m_1 \in M_1 \text{ and } m_2 \in M_2\}$$

It is easy to see that composition preserves arbitrary joins (for $N \subseteq M$) since

$$N \bullet \bigvee_i M_i \;= \{n.m_i \mid n \in M \text{ and } m_i \in \bigcup_i M_i\}$$

which is equal to $\bigvee_i (N \bullet M_i)$ since

$$\{n.m_i \mid n \in N \text{ and } m_i \in \bigcup_i M_i\} = \bigcup_i \{n.m_i \mid n \in N \text{ and } m_i \in M_i\}$$

and

$$\bigcup_i \{n.m_i \mid n \in N \text{ and } m_i \in M_i\} \;=\; \bigvee_i (N \bullet M_i)$$

Resource-Sensitivity in a Quantale. A quantale is resource-sensitive with regard to its multiplication. That is, for example, we cannot freely multiply an element of the quantale with itself:

$$a \not\leq a \bullet a\,, \qquad a \bullet a \not\leq a \qquad \text{so} \quad a \neq a \bullet a$$

as opposed to, for example with regard to joins where, we can freely take the join of an element with itself:

$$a \leq a \vee a\,, \qquad a \vee a \leq a \qquad \text{and thus} \quad a = a \vee a$$

So by enriching our complete lattice with the monoid structure, not only we get an extra connective and thus more expressiveness, but also we can talk about the concept of a *resource*: applying the monoid operation twice is not the same as applying it once.

In logical terms, this corresponds to lack of structural rules of weakening and contraction (in a sequent style proof system) on the multiplication on a quantale. Contraction says if the multiplication of a with itself is less than b, then a alone should also be less than b, that is

$$a \bullet a \leq b \qquad \text{implies} \qquad a \leq b$$

for which we need to have the following property, that is copying

$$a \leq a \bullet a$$

Weakening says if $a \leq c$ then one can safely multiply a with any other b and keep the inequality $a \bullet b \leq c$, that is

$$a \leq c \qquad \text{implies} \qquad a \bullet b \leq c$$

and this is because we have the following property, that is deleting

$$a \bullet b \leq a$$

None of which we have in a quantale. Moreover, the multiplication in a quantale is non-commutative, that is

$$a \bullet b \not\leq b \bullet a \qquad \text{and} \qquad b \bullet a \not\leq a \bullet b\,.$$

This means that we also do not have the exchange structural rule in a quantale.

In a categorical setting, as first noticed by Lambek, quantales are monoidal closed categories [20] where objects are elements of the quantale and there is a morphism between two objects $a \rightarrow b$ iff one is less than or equal to the other $a \leq b$. The compositionality of morphisms follows by transitivity of order. Monoidal closed categories provide semantics for *Multiplicative Linear Logic* [2]. In these categories, linearity of tensor follows by the *absence* of natural morphisms $\Delta_A : A \rightarrow A \otimes A$ and left and right projections

$$p_1 : A \otimes B \rightarrow A \qquad \text{and} \qquad p_2 : B \otimes A \rightarrow A\,.$$

Thus we do not have $a \otimes b \rightarrow a$ and $a \otimes b \rightarrow b$. This feature makes quantales candidates for models of Linear Logic with tensor as multiplication.

2.1.4 Modules

Another nice property of a quantale is that it can be paired with an object of the same nature as its underlying lattice, that is a sup-lattice, and form a couple! A quantale Q and a sup-lattices M form a pair (M, Q), where the sup-lattice M is referred to as a Q-right module. Because both M and Q are sup-lattices, structure-preserving operations can be defined on the pair of the two. In other words, elements of the quantale, can *act* on the elements of the module through an operation whose result will still be an element of the module. This feature enables us to encode *dynamics*. On the first sight this pairing provides us with a dynamic, two-level (one level for the quantale, one for the module) logic of 6 connectives: $\vee$ and $\wedge$ on the module and $\vee$, $\wedge$, and $\bullet$ on the quantale (for the time ignoring the residuals), plus the action of the quantale on the module. But we get more, since the action operation is join-preserving and has a Galois right adjoint. In formal terms:

Definition 2.1.4 A *Q-right module* for a quantale Q is a sup-lattice M with a *module action* $-.-$: $M \times Q \rightarrow M$ that satisfies the following properties

1. Preserves arbitrary joins in both arguments, that is $\forall m, m_i \in M$ and $\forall q, q_i \in Q$

$$(\bigvee_i m_i)\,.\,q = \bigvee_i (m_i\,.\,q) \quad \text{and} \quad m\,.\,(\bigvee_i q_i) = \bigvee_i (m\,.\,q_i)\,.$$

2. Preserves the unit of quantale, that is $\forall m \in M$

$$m\,.\,1 = m$$

3. It is associative over the quantale multiplication, that is $\forall m \in M, q_1, q_2 \in Q$

$$m \,.\, (q_1 \bullet q_2) = (m \,.\, q_1) \,.\, q_2$$

The first axiom is the usual join-preservation requirement for sup-morphisms. It asks the action of quantale to preserve both the join-structure of the module and quantale. So the action is consistent with the sup-structure of both elements of the pair (M, Q). The second axioms says that if the quantales acts on the module with the unit of multiplication, then it is as if it has not acted on the module. This reflects the neutral nature of the unit 1, and says the actions preserves this neutral character. The thirds axiom connects the multiplication of the quantale with its action on the module, it says that if we act on the module with the multiplication of two elements of quantale, then we get the same effect as when we first act on the module with the first one and then with the second one.

The action has adjoints since it preserves arbitrary joins of module and quantale (axiom 1 above). More explicitly the action can be factorized to two unary operations

$$- \,.\, q : M \to M$$

which preserves the joins on the module, and

$$m \,.\, - : Q \to Q$$

which preserves the joins on the quantale. Each of these factorized operator s have an adjoint. These two adjoints are denoted as $[q]-$ and $\{m\}-$, and we have

$$- \,.\, q \dashv [q] - \qquad \text{and} \qquad m \,.\, - \dashv \{m\} -$$

They are explicitly defined as follows

$$[q]m := \bigvee \{m' \in M \mid m' \,.\, q \leq m\} \qquad\qquad \{m\}m' := \bigvee \{q \in Q \mid m \,.\, q \leq m'\}.$$

The first right adjoint $[q]m$ is what will be focused on in our setting. $[q]m$ is, by definition, the join of all elements of the module on which the quantale can act with q and the result will be less than m. Since $[q]m$ returns the join of all such elements, it is said that it returns the *weakest* such element: the weakest element on which q acts and the result implies m. It is the weakest because any element of a join is less than the join

$$m' \leq \bigvee \{m' \in M \mid m' \,.\, q \leq m\}$$

This operation is referred to as *weakest precondition* or *dynamic modality* in the literature [47, 45] and we will return to it in detail later.

Examples of Modules. Consider the example quantale of the set of all relations on a set X, that is $\mathcal{P}(X \times X)$ discussed before. It is easily seen that the powerset of a set $\mathcal{P}(X)$ is a complete lattice and it is the right module for $\mathcal{P}(X \times X)$. The action of this quantale on its module is defined as follows

$$\begin{aligned} - \,.\, - \quad &: \quad \mathcal{P}(X) \times \mathcal{P}(X \times X) \to \mathcal{P}(X) \\ &:: \quad (T, R) \mapsto T \,.\, R := \{x \in X \mid \exists t \in T, tRx\}. \end{aligned}$$

This says that any relation R on the set X, can be seen as an operation: it takes a subset of X as input, that is T and returns the elements of X with which the elements of T are related to via the relation R. In other words $T \,.\, R$ inputs a subset of X and outputs the image of the relation R with regard to elements of T.

A good reference on quantales is [77], another good reference that discusses the theory of modules is [53]. For applications of quantales in computing, linguistics and physics see [2, 24, 47, 56, 67, 74].

Systems. A quantale and its right module are usually considered together in a pair called a *system* [2, 74]:

Definition 2.1.5 A *system* is a pair (M, Q) with Q a quantale and M a Q-right module.

From a logical point of view, a system (M, Q) provides us with a two-sorted dynamic logic: the module constitutes a logic with two connectives $\vee$ and $\wedge$. The elements of the quantale are part of another logic with three connectives (ignoring residuals): $\vee$, $\wedge$, and $\bullet$, which is moreover resource-sensitive with regard to $\bullet$. But we have more: these two logics are not disconnected: one acts on the other one. So apart from the specialized connectives of each logic, we have the two adjoint connectives $m \,.\, q$ and $[q]m$. The system, thus, can be seen as a two-sorted logic with seven operators (to be precise 9 with residuals). This is the starting point of our logic (logic developed in this thesis). But first we have to enrich the system with our unary maps, discussed before, and their adjoints.

2.1.5 Epistemic Systems

We will enrich our system (M, Q) with unary operations that are homomorphisms of the system. We consider a special homomorphism from the system to itself $f : (M, Q) \to (M, Q)$, referred to as an *endomorphism*. A system has two parts and thus these endomorphisms also have two parts, or they are a pair of endomorphisms: one the module and one on the quantale, satisfying some more conditions to be given below.

Definition 2.1.6 *A* system-endomorphism $(M, Q) \xrightarrow{f} (M, Q)$ *is a pair* $\left(f^M : M \to M \,,\, f^Q : Q \to Q\right)$ *where* f^M *is a sup-endomorphism on the module,* f^Q *is a sup endomorphism on the quantale satisfying the following inequalities for* $q_1, q_2 \in Q$ *and for all* $m \in M$ *and* $q \in Q$

$$1 \leq f^Q(1) \tag{2.1}$$

$$f^Q(q_1 \bullet q_2) \leq f^Q(q_1) \bullet f^Q(q_2) \tag{2.2}$$

$$f^M(m \cdot q) \leq f^M(m) \cdot f^Q(q). \tag{2.3}$$

The first two inequalities, referred to as *unit* and *multiplication* respectively, make f^Q a lax quantale homorphisms, preserving the quantale structure, that is joins, multiplication, and unit. The reason for laxity of f^Q (rather than full functoriality) has to do with our epistemic interpretation. The last inequality connects the quantale endomorphism to the module endomorphisms through the action of the quantale on the module. The reason for it being an inequality rather than an equality, again has to do with our knowledge applications and will be discussed in the next section on interpretation.

This notion of system homomorphism differs from the one in the literature since we do not fix the quantale Q. This means that our endomorphisms are not the same as *system homomorphisms* $f : (M, Q) \to (M', Q')$ defined in Joyal and Tierney [53] as follows

$$f(m \cdot q) = f(m) \cdot q\,.$$

Our endomorphisms are different since we have a pair of maps (f^Q_A, f^M_A), one on the module and one on the quantale as homomorphisms and connect them through the update inequality $f^M_A(m \cdot q) \leq f^M_A(m) \cdot f^Q_A(q)$.

We call a system endowed with such endomorphisms an *epistemic system* defines as:

Definition 2.1.7 An *epistemic system* is a tuple $(M, Q, \{f_A\}_{A\in\mathcal{A}})$ where (M, Q) is a system and $\{f_A\}_{A\in\mathcal{A}}$ are system-endomorphisms.

We define an *atomistic epistemic system*, which will be used in building concrete models as semantics of Dynamic Epistemic Logic [10] in chapter six.

Definition 2.1.8 An atomistic system is a system where both the module M and the quantale Q are atomic with their atoms denoted respectively as $Atm(M)$ and $Atm(Q)$, and moreover we have the following conditions

$$\text{If } m \in Atm(M) \text{ and } q \in Atm(Q) \quad \text{then} \quad m\,.\,q \in Atm(M)$$

and also

$$\text{If } q, q' \in Atm(Q) \quad \text{then} \quad q \bullet q' \in Atm(Q)$$

Definition 2.1.9 An atomistic epistemic system is an epistemic system whose underlying system is atomistic.

Although distributivity of the module is not needed for algebraic verification of properties of multi-agent systems such as the muddy children puzzle (see section 2.3 below), it will come handy in the

build of a complete single-succedent sequent calculus [1]. We define a *distributive epistemic system*, which will be used in proving completeness of our sequent calculus in chapter four.

Definition 2.1.10 A distributive epistemic system is an epistemic system whose module is distributive.

We have now defined all the mathematical objects we need for our logic, all summarized in the notion of an Epistemic systems. Next, we will interpret these notions in terms of knowledge and communication between agents.

[1] An alternative solution would be to work with multi-succedent sequent calculi instead.

2.2 Interpretation

In this section we explain how elements of an epistemic system are interpreted in a multi-agent context and are used to reason about knowledge of agents that changes due to the communications between the agents. We first interpret the elements of the module and the connectives on them, then the elements of quantale and their connectives, and then the mixed connectives, that is the action of the quantale on the module and its adjoint. In the second part, we use these interpretations to explain how the axioms of the epistemic system make sense in our multi-agent epistemic setting.

2.2.1 Epistemic Propositions

Elements of the module $m \in M$ stand for *epistemic propositions*. By this we mean they are the usual logical propositions with the join as disjunction, the meet as conjunction, and the order as logical entailment, but can also stand for epistemic attitudes.

$m_1 \leq m_2$ means m_1 entails m_2

$m_1 \vee m_2$ means m_1 or m_2

$m_1 \wedge m_2$ means m_1 and m_2

Appearance. The epistemic part of the propositions is encoded in the unary operation f_A^M. We call this operator $f_A^M(m)$, *appearance* of an agent A about a proposition m. It takes an element of the module m and returns the agent's appearance about it. This appearance consists of the disjunction of all the propositions that an agent conceives as possible, if proposition m holds (or is true) in the real world. Two extreme cases of this operator are

- If $f_A^M(m) = \top$ then it stands for absence of information. The appearance is equal to the top of the lattice or the Truth proposition, since m holds in the real worlds, but it appears to agent A that any other proposition, no matter which one, holds. This is because $\top$ signifies the join of all the elements of the module, that is the disjunction of all the propositions. In other words it corresponds to absence of any information: agent A has no knowledge (to be defined below).

- If $f_A(m) = m$ then it stands for certain information, since proposition m holds both in the real world and in agent A's appearance of the world. That is agent A's appearance is consistent with reality: m is true in reality and agent A knows it.

Using the order of the module, we can compare information of an agent about different propositions:

- If $f_A^M(m) < f_A^M(m')$ then agent A has strictly more information of proposition m than of proposition m'. In terms of appearance, this says that the appearance of agent A about m entails his appearance of m', and so is stronger than it. That is why A has more information about m than about m'.

We can also compare information of different agents about one proposition:

- If $f_A^M(m) < f_B^M(m)$ then agent A has strictly more information than agent B of proposition m, this is because A's appearance about m implies (and is thus stronger than) B's appearance of it.

Since the only property that appearance map satisfies is join-preservation, there can be no relation between the appearance of reality to an agent and the reality itself. In other words, an agent can have *wrong* information:

- If $m \not\leq m'$ but $f_A^M(m) \leq m'$ then agent A has been deluded since in reality m does not imply m', but it appears to agent A that it does. So agent A has *incorrect information* for example due to being deceived by another agent, a malfunctioning communication channel or corrupted data.

Since M is a sup-lattice and appearance preserves arbitrary joins, it should also preserve the empty join, or the join of the Falsum. This means $f_A^M(\bot) = \bot$. What it means in an epistemic setting:

- If $f_A^M(\bot) = \bot$ then if the Falsum holds in the real world, that is if there is a contradiction in the real worlds, it appears as it is to all the agents: they all have contradictory information.

Note that although preserving the false proposition, appearance has no relation with the True proposition, or the top of the module, in particular we do not have the following in general

$$f_A^M(\top) \neq \top$$

The appearance maps are our first and basic epistemic modality, however they are not the *knowledge* modality, since all normal knowledge modalities preserve conjunction and appearance preserves disjunction. But appearance has a Galois right adjoint that preserves conjunction explained belows.

Knowledge. We interpreted the f_A^M maps as appearances of agents and showed how it relates to the information content of agents about reality. Now we show that its adjoint, the meet preserving endomorphism on the module, stands for knowledge of agents about reality. For each agent $A \in \mathcal{A}$ we introduce our knowledge modality $\Box_A^M$ standing for *agent A's knowledge* as the adjoint to the appearance map, i.e.

$$f_A^M \dashv \Box_A^M .$$

By adjunction we have

$$f_A^M(m) \leq m' \quad \text{iff} \quad m \leq \Box_A^M m' ,$$

which says if the appearance of an agent about m implies m' then if m holds, the agent knows that m' and also the other way around. In other words, if all the propositions that appear to be true to agent A when m holds, imply m', then whenever m holds, agent A knows m'. Using this inequality, the extreme cases of appearance will read as follows

- $f_A^M(m) = \top$ is equivalent to $m \leq \Box_A^M \top$, which means whenever m holds in reality, agent A has no knowledge.

- $f_A^M(m) = m$ is equivalent to $m \leq \Box_A^M m$, which means whenever m holds in reality, agent A knows it.

The wrong appearance or incorrect information will read as *wrong knowledge*:

- $m \not\leq m'$ but $f_A^M(m) \leq m'$ is equivalent to $m \not\leq m'$ but $m \leq \Box_A^M m'$, which means if m is true m' is not, but if m holds, agent A knows that m', which means he has wrong knowledge or belief about m', since m' is not true.

We can define our knowledge modality in terms of appearances as

$$\Box_A^M m' = \bigvee \{m \mid f_A^M(m) \leq m'\}$$

that is as the weakest proposition whose appearance implies m'.

Properties of knowledge. Some basic properties of $\Box_A^M$ is its preservations of arbitrary meets:

$$\Box_A^M(\bigwedge_i m_i) = \bigwedge_i \Box_A^M m_i \,.$$

Hence it preserves the empty meet and binary meets, that is

$$\Box_A^M \top = \top \qquad\qquad \Box_A^M(m \wedge m') = \Box_A^M m \wedge \Box_A^M m' \,,$$

This implies that it is also order-preserving or monotone, that is

$$\text{if} \quad m \leq m' \quad \text{then} \quad \Box_A^M m \leq \Box_A^M m' \,.$$

These are the properties of the *normal modality* or axiom K in modal logics. The connection to other axioms such as $T, 4, 5$ will be discussed in more detail in the next section. This modality covers both knowledge and belief. In contexts where no wrong belief is allowed, it can be read as knowledge, i.e. *justified true belief* . Otherwise, it stands for justified belief.

Example. Consider a simple scenario with two players A, B and a referee C. In front of everybody, the referee throws a fair coin, catches it in his palm and fully covers it, before anybody (including himself) can see on which side the coin has landed. The players and the referee do not know on which side the coin has landed: each of them think it might have landed heads up or tails up. We denote the proposition that says 'coin has landed heads up' by H, and the proposition that says 'coin has landed tails up' by T. The appearance maps for each agent, in case the coin has landed heads, are

$$f_A^M(H) = f_B^M(H) = f_C^M(H) = H \vee T$$

, which means all the agents are uncertain about the face of the coin. Similarly in case the coin has landed tails:

$$f_A^M(T) = f_B^M(T) = f_C^M(T) = H \vee T$$

We can now calculate the knowledge of agents in each case:

$$H \leq \Box_A^M(H \vee T) \quad \text{and} \quad T \leq \Box_A^M(H \vee T)$$

and similarly for B and C, which means each agent is uncertain about the face of the coin.

2.2.2 Epistemic Actions

Elements of the quantale $q \in Q$ are interpreted as epistemic programs or epistemic actions. That is, actions that change the information state of agents. The order of the quantale is the order of non-determinism of these actions

$$q_1 \leq q_2 \quad \text{means} \quad \text{action } q_1 \text{ is more deterministic than action } q_2$$

This is for example because q_2 is obtained from q_1 by making it depend on the outcome of a coin-toss. Accordingly, the join of quantale is interpreted as non-deterministic choice of actions

$$q_1 \vee q_2 \quad \text{means} \quad \text{either action } q_1 \text{ or action } q_2 \text{ is happening}$$

The multiplication of the quantale is interpreted as sequential composition of actions:

$$q_1 \bullet q_2 \quad \text{means} \quad \text{first action } q_1 \text{ happens then action } q_2$$

The multiplicative unit 1 of Q is the void epistemic action, that is the action that does nothing and is referred to as *skip* in literature.

Appearance. Similar to the module, the appearance maps $f_A^Q : Q \to Q$ encode how agents perceive actions. $f_A^Q(q)$ interprets as all the actions that appear to agent A as happening where in reality action q is happening. The two extreme cases are interpreted the same as in the module

- $f_A^Q(q) = \top$: means agent A has no information about what action is happening, every action seem possible to him.
- $f_A^Q(q) = q$: means agent A has certain information about what action is happening: action q is happening and agent A is aware of it.

The appearances might provide *wrong* information for the agent, since they are not truth preserving:

- $q < f_A^Q(q)$: means that in reality action q is happening, but agent A thinks a more non-deterministic action, namely $f_A(q)$ is taking place. In other words, action q is being hidden from A, he views it possibly as a choice of actions.

- $q \not\leq f_A^Q(q)$: means action q is happening but something totally different and irrelevant appears to A. There is no relation between q and its appearance to agent A, as a result of being lied to or cheated on. This is used to represent misinformation *actions such as lying and cheating.*

Since f_A preserves all joins including the empty join, we have that $f_A^Q(\bot) = \bot$. The bottom action stands for the most deterministic action or the impossible action. Thus this equality says that if the contradictory action is happening in reality, everybody will be aware of it.

Knowledge. The right adjoint to f_A^Q maps are our knowledge modality on the quantale. They are denoted as $\Box_A^Q$ and stand for *agent A's knowledge of actions*. By adjunction we have

$$q \leq \Box_A^Q q' \quad \text{iff} \quad f_A^Q(q) \leq q' \,,$$

These modalities $\Box_A^Q$ satisfy the same properties as $\Box_A^M$.

Example. Consider our coin toss scenario, and that after the referee C catches the coin, he announces the result publicly so that everybody hears it. Now all the three agents know the face of the coin. Suppose the coins is heads, we denote the action of announcement as σ, since it is a public action, it appears to every body as it is

$$f_A^Q(\sigma) = f_B^Q(\sigma) = f_C^Q(\sigma) = \sigma$$

All of them know what is the real action:

$$\sigma \leq \Box_A^Q \sigma$$

and similarly for B and C.

Consider now the same coin-toss, but this time with the difference that while agents A and B think no one knows the face of the coin, the referee *cheats* by taking a peek before covering the coin and that others did not notice this action. We denote the action of *taking a peek*, that is the real action, by γ, since agents A and B are not aware of it we have for their appearances

$$f_A^Q(\gamma) = f_B^Q(\gamma) = 1$$

which is equal to, in terms of knowledge

$$\text{and} \quad \gamma \leq \Box_B^Q 1$$

that is they think nothing has happened and thus are deceived. But the referee is aware of his own actions so

$$f_A^Q(\gamma) = \gamma \quad \text{and thus} \quad \gamma \leq \Box_C^Q \gamma$$

This is an example of a misinformation action, that is cheating.

2.2.3 Epistemic Update

The action of the quantale on the module

$$- \,.\, - : M \times Q \to M$$

encodes our notion of *epistemic updating*. We read $m \,.\, q$ as performing an epistemic action $q \in Q$ on an epistemic proposition $m \in M$, the result of which will be a new epistemic proposition, possibly with a new truth value. We use epistemic updating to encode the change of knowledge of an agent as a result of an action, for example communicating with other agents. For example when proposition m holds in the real world, agent A does not know m'

$$m \not\leq \Box_A^M m'$$

But after the communication action q happens, he does:

$$m \,.\, q \leq \Box_A^M m'$$

Using the adjunction between appearance and knowledge, we see that the above are equivalent to the following

$$f_A^M(m) \not\leq m' \quad \text{but} \quad f_A^M(m \,.\, q) \leq m'$$

In order to understand how this equation works, we need to know how $f_A^M(m \,.\, q)$ relates to $f_A^M(m)$, which is going to be explained in the axiom section below.

We can also have the other direction, if m holds in the real world, agent A know that m', but after communicating with other agents in action q, he changes his mind:

$$m \leq \Box_A^M m' \quad \text{but} \quad m \,.\, q \not\leq \Box_A^M m'$$

that is equivalent to the following in terms of appearances

$$f_A^M(m) \leq m' \quad \text{but} \quad f_A^M(m \,.\, q) \not\leq m'$$

and we will see later why this is possible.

Since update preserves all joins, it also preserves the empty join on both arguments, that is we have

$$m \,.\, \bot = \bot \quad \text{and} \quad \bot \,.\, q = \bot$$

The first one says that update with an impossible action results to a contradiction. The second one says that no action can change the Falsum, that is if a contradiction holds in the real worlds, no action can save us from it.

Example. Now we can express that in the coin toss scenario (without cheating), the agents get to know the face of the coin, after the announcement of for example heads. Recall that before the announcement we have

$$H \leq \Box_A^M (H \vee T) \quad \text{which means} \quad H \not\leq \Box_A^M H$$

and similarly for B and C. But after the announcement action σ we have

$$H \,.\, \sigma \leq \Box_A^M H$$

similarly for B and C. We will show how to prove expressions like that at the end of this chapter.

Dynamic modality. Since epistemic update $- \,.\, -$ preserves joins in both arguments, it has two Galois right adjoints. The following one

$$- \,.\, q \dashv [q] -$$

is the *dynamic modality* used in dynamic logic [45], also referred to as *weakest preconditions* in [47]. It reads as

$$[q]m : \quad \text{after action } q \text{ proposition } m \text{ holds.}$$

The definition of adjunction says the following

$$m \,.\, q \leq m' \quad \text{iff} \quad m \leq [q]m'$$

which means if doing q on m implies the truth of m' then m implies that after doing q proposition m' holds and vises versa. In other words, $[q]m$ is the weakest proposition that should be true before doing q, so that after performing q on it, proposition m will become true.

Using this modality we can express what happens to the knowledge of agents after an action happens:

$$m \not\leq \Box_A^M m' \quad \text{but} \quad m \leq [q]\Box_A^M m'$$

which is by adjunction equal to the expression of previous page:

$$m \leq [q]\Box_A^M m' \quad \text{iff} \quad m \,.\, q \leq \Box_A^M m'$$

Example. In the coin-toss scenario, we an equivalent expression to the one explained above:

$$H \,.\, \sigma \leq \Box_A^M H \quad \text{equivalent to} \quad H \leq [\sigma]\Box_A^M H$$

2.2.4 Axioms

In this section, we use the above interpretations to explain the axioms of the epistemic system. We start with the axioms of the action of the quantale on the module.

Action of Quantale on the Module. The first requirement is join preservation on both arguments:

$$(\bigvee_i m_i) \,.\, q = \bigvee_i (m_i \,.\, q)$$

says that updating the disjunction of proposition is equal to the disjunction of updates. In other words the disjunction of propositions is consistent with the disjunction of propositions updated with an action. Similarly on the other argument we have

$$m \,.\, (\bigvee_i q_i) = \bigvee_i (m \,.\, q_i)$$

which means update with choice of actions is equal to the disjunction of update with each of the actions. In this case we are asking the disjunction of propositions to be consistent with update with non deterministic choice of actions.

The second axiom is

$$m.1 = m$$

which says update with the unit of quantale, has no effect. In other words, the unit of quantale is consistent with the update operation: it keeps its neutrality.

The third axioms is the associativity of update over sequential composition

$$m \,.\, (q \bullet q') = (m \,.\, q) \,.\, q'$$

This says if we update a proposition with the sequential composition of two actions, it has the same effect as first updating with the first one and then updating with the second one. This axioms is asking for the consistency of sequential composition of the quantale with update.

Preconditions. Before explaining the axioms that deal with appearance, update, and the sequential composition, we have to introduce a new notion, that of the precondition of an action. Epistemic actions are partial in the sense that not every action can happen on every proposition. Some actions are *incompatible* with some propositions: actions can only happen if certain propositions hold. This is equal to say that if an action runs on one of its incompatible propositions, it will result in a contradiction $\bot$. That is if $m \,.\, q = \bot$ then the epistemic action q cannot be applied to the proposition m. To represent these incompatible propositions, we define a *kernel* for each action as follows

$$Ker(q) := \{m \in M \mid m \,.\, q = \bot\}$$

Note that $ker(q) = [q]\bot$ we have that $ker(q) = \downarrow(\bigvee Ker(q))$ and thus the kernel of each action exists as a proposition in M for all $q \in Q$. The kernel comprises the *precondition* of q, which is not in general a proposition in M. The action that does nothing, that is 1, can be applied on every proposition, thus

its kernel is the falsum

$$ker(1) = \downarrow\bot = \bot$$

Example. In our coin-toss scenario our σ action, that is the announcement of heads, can only apply to propositions that imply the proposition H. In other words, it cannot happen in situations where the coin has actually landed tails, so we have

$$ker(\sigma) = \downarrow T$$

Update Inequality. This inequality states the relations between the appearance maps and epistemic update:

$$f_A^M(m \,.\, q) \leq f_A^M(m) \,.\, f_A^Q(q)$$

Since each agent updates his knowledge according to how he perceives the epistemic action, it is clear that $f_A^M(m \,.\, q)$ should relate to $f_A^M(m) \,.\, f_A^Q(q)$ so that we can reason about or calculate $f_A^M(m \,.\, q)$ using its simpler parts, that is m and q and their appearances. This is an important condition and provides the core of our reasoning about knowledge with regard to actions that change it. One can view it as a consistency or rationality requirement that connects the appearance of the update proposition to the update of the initial appearances with the initial action. The fact that they relate through an inequality, rather than an equality, expresses the fact that the appearance of an updated proposition by an action, that is $f_A^M(m \,.\, q)$ is stronger than the update of appearances $f_A^M(m) \,.\, f_A^Q(q)$, since the former implies the latter. The reason is that if in reality proposition m is in the kernel of action q then the update will become $\bot$:

$$m \in ker(q) \quad \text{implies} \quad m \,.\, q = \bot$$

and we have that the appearance of $\bot$ is $\bot$:

$$f_A(\bot) = \bot \,.$$

But there is no reason for the appearance of the proposition $f_A(m)$ to be in the kernel of the appearance of the action $f_A(q)$, that is

$$m \in ker(q) \quad \not\Rightarrow \quad f_A(m) \in ker(f_A(q))$$

and we can have that

$$m \,.\, q = \bot \quad \text{but} \quad f_A(m) \,.\, f_A(q) \neq \bot$$

So the equality does not hold, where as the inequality does. Thus the inequality is more general and that is why we posed it as a condition on our setting.

Example. As an example to the inequality explained above, recall our coin-toss scenario with the cheating action γ. Assume that when the referee C cheated, he saw that the coin was heads and thus

the kernel of γ is the down set of proposition corresponding to tails:

$$ker(\gamma) = \downarrow T$$

and we have the following

$$T \,.\, \gamma = \bot \quad \text{and thus} \quad f_A(T \,.\, \gamma) = \bot$$

but recall that agents A and B did not know on which side the coin landed and also did not notice the cheating, that is

$$f_A^M(T) = H \vee T \quad \text{and} \quad f_A^Q(\gamma) = 1$$

As explained above, the kernel of 1 is only the bottom of the lattice so

$$H \vee T \notin ker(1)$$

which means

$$f_A^M(T) \,.\, f_A^Q(\gamma) = (H \vee T) \,.\, 1 \neq \bot$$

Unit and Multiplication Inequalities. Similar to the update inequality, we need to relate the appearance of sequential composition of actions $f_A^Q(q \bullet q')$ to the sequential composition of appearances of each action $f_A^Q(q) \bullet f_A^Q(q')$, and also the unit 1 to its appearance $f_A^Q(1)$. The unit and its appearance satisfy an inequality

$$1 \leq f_A^Q(1)$$

which says that the appearance of unit is more deterministic than the unit. So when nothing is happening an agent might thing either something is happening or nothing is happening, and this accommodates suspicions of agents about actions. On the other hand, posing this inequality says that when nothing is happening, the agent considers it as an option and so has a consistent appearance with the event, in this case 'skip'. This inequality leads to inequality between appearance of composition and composition of appearances

$$f_A^Q(q \bullet 1) = f_A^Q(q) = f_A^Q(q) \bullet 1 \leq f_A^Q(q) \bullet f_A^Q(1) \,.$$

which says $f_A^Q(q \bullet q')$ is more deterministic than $f_A^Q(q) \bullet f_A^Q(q')$. The informal reason is similar to the update inequality: the left hand side might become $\bot$ where as the right hand side stays non-bottom, thus the relation cannot be an equality. We explain why that could happen. A sequential composition of actions is bottom if either one of them is the bottom action, or that the kernel of the first action is true so the first action results to $\bot$, or that after performing the first action, the kernel of the second one becomes true:

$$q \bullet q' = \bot \quad \text{iff} \quad \begin{cases} q = \bot \text{ or } q' = \bot \\ \\ ker(q) \vee [q]\, ker(q') \end{cases}$$

If the first condition holds, that is if q or q' are $\bot$, then we also have that $f^Q_A(q)$ or $f^Q_A(q')$ are $\bot$ and we will have the equality between $f^Q_A(q \bullet q')$ and $f^Q_A(q) \bullet f^Q_A(q')$. But if the second condition is the case, we can have $q \bullet q' = \bot$ but not that $f^Q_A(q) \bullet f^Q_A(q') = \bot$. This is because

$$ker(q) \vee [q]\, ker(q') \quad \not\Rightarrow \quad ker(f^Q_A(q)) \vee [f^Q_A(q)]\, ker(f^Q_A(q'))$$

So

$$f^Q_A(q \bullet q') = \bot \quad \not\Rightarrow \quad f^Q_A(q) \bullet f^Q_A(q') = \bot$$

But in this case the left hand side being bottom implies any right hand side and thus the inequality between the two holds. The unit inequality is consistent with and in the same lines as the multiplication inequality. It says that the skip action, in which nothing happens, is more deterministic than its appearance. So if nothing is happening, all the agents consider it as an option; their appearance include it.

Example. As an example consider again our coin-toss scenario with the cheating action when the coin has landed heads up. Consider action σ' as the public announcement of the tails, so we have

$$ker(\sigma') = \downarrow H \quad \text{and} \quad f_A(\sigma') = f_B(\sigma') = f_C(\sigma') = \sigma'$$

The announcement of tails cannot be followed by a cheating action where the coin has landed heads

$$\sigma' \bullet \gamma = \bot$$

this is since whenever we can perform action σ', that is whenever we announce T, it means that proposition T should have been true, and announcing T will not make it false (explained in the fact section below). But we have that proposition T is in the kernel of the cheating action, since the coin has landed heads, that is $T \in ker(\gamma)$, as a result we have

$$[\sigma']T \leq [\sigma']ker(\gamma)$$

But note that we can do the following sequential composition without any difficulty

$$f^Q_A(\sigma') \bullet f^Q_A(\gamma) = \sigma' \bullet 1 = \sigma' \neq \bot$$

because 1 can be applied everywhere.

Stable facts. Every epistemic system has a non-epistemic or objective part. This objective part contains propositions that cannot be altered by any epistemic action. We call these *"facts"*. They can be

formally defined as the *stabilizer* of Q:

$$Stab(Q) := \{\phi \in M \mid \forall q \in Q, \phi \,.\, q \leq \phi\}$$

that is those epistemic propositions which are stable under the epistemic programs: $\phi \,.\, q \leq \phi$. In terms of dynamic modality that is $\phi \leq [q]\phi$, which says t that the weakest precondition for ϕ with respect to action q entails ϕ. In other words, validity of ϕ cannot be created by epistemic actions, if it is true before, it will stay true after running any program on it. Conclusively, elements of module both encode actual facts and the knowledge of each agent, that is, both factual and epistemic content.

Example. In our coin-toss scenario the propositions H and T are facts, but $\Box_A^M H$ and $\Box_A^M T$ are the epistemic ones.

2.3 The Muddy Children Puzzle

In this section we show how our algebra can be used to encode and solve an epistemic puzzle: the muddy children puzzle. This puzzle has a dynamic nature, communication between the children and the information passed via these communications are the core of solving it. However, the usual epistemic logic solutions, for example in the standard text book on epistemic logic by Fagin et al. [39], do not formalize the dynamics and deal with it on the side using natural language. The dynamic epistemic logic of Baltag et al. [10] formalizes both dynamics and epistemics and provides a dynamic solution to the puzzle in a Kripke state-based model. The logic of this thesis is the first algebraic encoding of this puzzle, that assumes much less than any of the other attempts about the connectives of the logic. We show how our minimal non-boolean propositional setting with only disjunction and conjunction and no distributivity, solves the puzzle in an elegant way. Moreover, our equational setting and our adjoint epistemic and dynamic modalities even simplify the solution to a great extent. We also show how the possibility of having wrong information in our setting (same as in Baltag et. al.), helps us to define more interesting versions of this puzzle with cheating and lying actions of children.

2.3.1 The Original Version

The puzzle goes like this: n children are playing in the mud and k of them have dirty foreheads. Each child can see all the other foreheads except for his own. Their father appears at the door and tells them that at least one of them has a dirty forehead. Then he asks if any one knows that it is him that has a dirty forehead, the children think and they all, simultaneously, answer no. Then having heard all the no answers of other children, they think again and again answer no. The question is after how many rounds of no answers, each dirty child will come to know that he is dirty? We will prove in this section, that the answer is $k - 1$, that is after $k - 1$ rounds of no answers, all the dirty children will know that they are dirty.

We encode the puzzle in an epistemic system $(M, Q, \{f_A\}_{A\in\mathcal{A}})$. The set of agents $\mathcal{A}$ includes the children, that is

$$\{C_1, \cdots, C_n\} \subseteq \mathcal{A}$$

We assume that the first k children $C_1, \cdots, C_k$ for $1 \leq k \leq n$ are the dirty ones. The module M includes all possible initial propositions about which child is dirty. So we have a proposition that says no child is dirty, and thus corresponds to the situation where no child is dirty. We denote this proposition as $s_\emptyset$. Similarly we have a proposition that says only child one is dirty, denoted as $s_{\{C_1\}}$, which corresponds to the situation where only child one is dirty and so on for all the children. So we have 2^n possible propositions, denoted as s_β where the subscript β is the set of those children that have mud on their forehead, that is

$$\beta \subseteq \mathcal{A}$$

For example the proposition $s_{\{C_1,\ldots,C_n\}}$ says that all the children are dirty. So among our propositions are the two extreme proposition: $s_\emptyset$ and $s_{\{C_1,\ldots,C_n\}}$, but the proposition that is true in the real case is $s_{\{C_1,\ldots,C_k\}}$, that stand for our assumption that children 1 to k are dirty.

We have to set the appearance maps for each child about all this proposition. That is we have to see how does each proposition appear to each child. Since the children cannot see their own foreheads (which might either be dirty or not), in each proposition, they think they might be dirty or not. In other words, in each proposition they think they might be in the set of dirty children or not. This is encoded as

$$f^M_{C_i}(s_\beta) = s_{\beta\setminus\{C_i\}} \vee s_{\beta\cup\{C_i\}}$$

where $s_{\beta\setminus\{C_i\}}$ is where the child C_i is not dirty and $s_{\beta\cup\{C_i\}}$ is where he is dirty. Each of our propositions correspond to an epistemic situation, but they also satisfy some facts, that is the facts that correspond to the situation described by the proposition. For example proposition $s_\emptyset$ corresponds the fact that 'no child is dirty'. We denote this fact by $D_\emptyset$ and set an order between the proposition and its corresponding fact, that is

$$s_\emptyset \leq D_\emptyset$$

Similarly for the other propositions, we assume D_i denotes the fact that the i'th child has a dirty forehead, hence we have

$$s_\beta \leq D_i \quad \text{for all } C_i \in \beta$$

and the set of our facts will be

$$\{D_\emptyset\} \cup \{D_i \in M \mid C_i \in \mathcal{A}\} \subseteq Stab(Q)$$

which is a subset of the set of all facts of our epistemic system, that is the stabilizer of Q.

Now we start to encode the dynamic part of the puzzle, that is the communication actions that happen between the father and the children. The first of these happens when the father tells the children

that at least one child is dirty. We denote this action by q_0 and assume that it is an element of the quantale

$$q_0 \in Q$$

Since this is a public action, all the children hear it, so it appears as it is to all the children:

$$f^Q_{C_i}(q_0) = q_0 \quad \text{for all } 1 \leq i \leq n$$

The kernel of this action, is the set of all propositions (epistemic or fact) that it cannot be applied to, that is the proposition that says no child is dirty $D_\emptyset$, and everything that implies it:

$$ker(q_0) = {\downarrow}D_\emptyset$$

Note that the proposition $s_\emptyset$ is included in the kernel since $s_\emptyset \leq D_\emptyset$.

Each round of no answers of children is also a communication action between the children. Since they all announce the same proposition, that is the no answer, we denote them all equally as the action q in our quantale

$$q \in Q$$

Since these answers are told to every one, and each child hears them, they appear as they are to each child, that is

$$f^Q_{C_i}(q) = q \quad \text{for all } 1 \leq i \leq n$$

The kernel of this action, that is the kernel of each round of no answers, is the set of all propositions in which some child knows that he is dirty. The set contains all the propositions that say for example child one knows that he is dirty, child two knows that he is dirty and so on, that is $\bigvee_{i=1}^{i=n} \Box_{C_i} D_i$. So the kernel of each q will be

$$ker(q) = {\downarrow} \bigvee_{i=1}^{i=n} \Box_{C_i} D_i$$

We are done with our encoding: we have encoded the assumptions of the puzzle in the propositions and their appearances in the module, we have also encoded the dynamic assumptions in the actions of the quantale, and their appearances. The kernel of each action connects the action to the proposition that it contains, that is the communicated proposition, it can be seen as the propositional representative of the action in the module.

We now claim that after $k-1$ rounds of no answers of children, all the dirty children know that they are dirty. This claim is formalized using the dynamic and epistemic modalities as follows:

Proposition 2.3.1 *After the $k-1$'s rounds of answers, dirty child j for $1 \leq j \leq k$ knows that he is dirty i.e.*

$$s_{\{C_1,\cdots,C_k\}} \leq [q_0 \, (\bullet q)^{(k-1)}] \Box_{C_j} D_j \, .$$

where $(\bullet q)^{(k-1)}$ *denotes* $(k-1)$ *times sequential composition of no answers* $q \bullet \cdots \bullet q$.

Proof. The proof goes by induction on the number of dirty children k.
Base Case. For the base case we prove the proposition for $k = 1$, that is

$$s_{C_1} \leq [q_0]\Box_{C_1} D_1$$

By adjunction between dynamic modality and update this is equivalent to

$$s_{C_1} \cdot q_0 \leq \Box_{C_1} D_1$$

and by adjunction between epistemic modality and appearance this is equivalent to

$$f_{C_1}(s_{C_1} \cdot q_0) \leq D_1$$

By the update inequality, to prove the above inequality it is enough to prove the following

$$f_{C_1}(s_{C_1}) \cdot f_{C_1}(q_0) \leq D_1$$

which is by the initial assumptions of the puzzle on f_{C_1} of propositions and actions equal to

$$(s_{C_1} \vee s_\emptyset) \cdot q_0 \leq D_1 \,.$$

By distributivity of update over joins of module, we have to show two cases

$$\begin{cases} s_{C_1} \cdot q_0 \leq D_1 & , \\ s_\emptyset \cdot q_0 \leq D_1 & . \end{cases}$$

For the first case, by the initial assumption for the states satisfying their corresponding facts we have $s_{C_1} \leq D_1$, now since update is order preserving, we update both sides by q_0 and get $s_{C_1} \cdot q_0 \leq D_1 \cdot q_0$. But D_1 is a fact and stable under any update so $D_1 \cdot q_0 \leq D_1$ and by transitivity we obtain $s_{C_1} \cdot q_0 \leq D_1$.

For the second case, by our initial assumptions about the kernel of the actions we have that $s_\emptyset \in ker(q_0)$, and thus by definition of kernel $s_\emptyset \cdot q_0 = \bot$, which is less than any proposition, and again by transitivity we get $\bot = s_\emptyset \cdot q_0 \leq D_1$.
Induction Hypothesis. We assume that the above proposition holds for $k-1$ dirty children and $1 \leq l \leq k-1$

$$s_{\{C_1,\cdots,C_{k-1}\}} \leq [q_0\,(\bullet q)^{(k-2)}]\Box_{C_l} D_l \,.$$

By the dynamic adjunction, this is equivalent to

$$s_{\{C_1,\cdots,C_{k-1}\}} \cdot (q_0\,(\bullet q)^{(k-2)}) \leq \Box_{C_l} D_l$$

and by the module equation for associativity of update over sequential composition this is equivalent to

$$s_{\{C_1,\cdots,C_{k-1}\}} \cdot q_0 \, (\cdot q)^{(k-2)} \leq \Box_{C_l} D_l$$

Now since $\Box_{C_l} D_l \leq \bigvee_i \Box_{C_i} D_i$ and by the initial kernel assumptions we have $\bigvee_i \Box_{C_i} D_i \in ker(q)$, we get

$$s_{\{C_1,\cdots,C_{k-1}\}} \cdot q_0 \, (\cdot q)^{(k-2)} \in ker(q)$$

We will use this in the proof of our induction step below.

Induction Step. Finally we have to show the proposition for k dirty children

$$s_{\{C_1,\cdots,C_k\}} \leq [q_0 \, (\bullet q)^{(k-1)}] \Box_{C_j} D_j \, .$$

We apply the dynamic and epistemic modalities and obtain the following equivalent form

$$f_{C_j}(s_{\{C_1,\cdots,C_k\}} \cdot (q_0 \, (\bullet q)^{(k-1)})) \leq \Box_{C_j} D_j$$

For which by the update and multiplication inequality and initial assumptions on the appearance of actions, it is enough to show the following

$$f_{C_j}(s_{\{C_1,\cdots,C_k\}}) \cdot (q_0 \, (\cdot q)^{(k-1)})) \leq D_j$$

Now we use the assumptions on the appearance of propositions and have to show the following two cases

$$\begin{cases} s_{\{C_1,\cdots,C_k\}} \cdot (q_0 \, (\cdot q)^{(k-1)})) \leq D_j & , \\ s_{\{C_1,\cdots,C_k\} \setminus \{C_j\}} \cdot (q_0 \, (\cdot q)^{(k-1)})) \leq D_j & . \end{cases}$$

Similar to the base case, the first case follows by the initial assumption on facts $s_{\{C_1,\cdots,C_k\}} \leq D_j$ and stability of D_j under updates. The second case follows from the induction hypothesis, where we obtained

$$s_{\{C_1,\cdots,C_{k-1}\}} \cdot q_0 \, (\cdot q)^{(k-2)} \in ker(q)$$

and since dirty children are the first k ones, we get $s_{\{C_1,\cdots,C_k\} \setminus C_j} \cdot q_0 \, (\cdot q)^{(k-2)} \in ker(q)$. By definition of kernel

$$s_{\{C_1,\cdots,C_k\} \setminus \{C_j\}} \cdot q_0 \, (\cdot q)^{(k-2)} \cdot q = \bot$$

and we are done since $\bot \leq D_j$. □

2.3.2 Algebraic Features of the Proof

The muddy children puzzle is based on the new information that each child acquires after hearing the no answers of other children, that is by knowing that others do not know. This is reflected in our

setting by the systematic update of the children's knowledge after each round of answers. In particular, in the inductive step we show that $s_{\{C_1,\cdots,C_k\}} \cdot q_0 \, (\, . \, q)^{(k-1)}$ is included in the kernel of the action q, which means after each round of no answers the propositions in which children know that they are dirty form part of the kernel of the next round of answers, that is it becomes impossible for the next round of no answers to take place. These impossible propositions accumulate and at some point, at round $k-1$, they all become impossible and thus the update results in $\bot$, and that is when we get our conclusion. This corresponds to eliminating possibilities in the usual Kripke model solutions of this puzzle. In this approach [39], first one draws an initial model for all the possible states, corresponding to the propositions of our module, each state has a valuation that corresponds to our propositions satisfying facts. Also in each state, the children access other states that are considered possible for them, these correspond to our appearance maps. There is no account of any action whatsoever, and the announcements and the information that they contain are dealt with informally. Thus after drawing this initial model, that can only be drawn for small numbers for example 3 children 2 of them dirty, the solution is very informal and done in natural language. It is stated on the side that after each announcement (father's and then children's no answers) some of the states become non-accessible for the children, for example after father's announcement, the state that corresponds to no dirty child, becomes inaccessible for all the children. Then the model is trimmed by deleting the corresponding accessibility relations of this state, and consequently eliminating the state. This process is repeated for each round of no answers, at the end only the states remain, in which all the children know that they are dirty. Because the elimination is also done informally on the side. The dynamics of the puzzle is not formalized in the usual proofs, there is no notion of action or update. By contrast in our setting, this constitutes the core of the proof.

Common Knowledge. It is worth mentioning that in the usual approaches to this puzzle, the Kripke method described above is the model theoretic solution and the formal proof is given in an epistemic logic proof system. These proof systems are usually Hilbert-style [39], and use the *common knowledge* operator. This operator has an infinite nature and encodes the fact that for example after father's announcement, all the children know that at least one child is dirty, and they know that all the children know that. This operator compensates for the lack of dynamics: after each round of no answers, it is the common knowledge of children that changes. As shown above, we do not need an operator of this kind to formalize the proof, the algebraic axiomatic uses the updates instead. But it is worth noting that the common knowledge operator can easily be defined in our setting in the form of a greatest fixed point that arises as the right adjoint to the least fixed point operator defined over appearances. In fact, the common knowledge is the right notion of knowledge obtained after a public announcement. Defining these notions and proving their properties constitutes future work.

Resource-Sensitivity. Another important feature of this puzzle is the repetition of actions and the different effects that they induce after each repetition, that is the action of saying no, and its repetition in each round. After the first round, the dirty children do not know that they are dirty, after the second

round they still do not know, it is only after the $k-1$ round that they get to know. This is reflected in our setting in the resource-sensitivity of the quantale with regard to sequential composition of actions, that two times doing an action is not equal to doing it once

$$q \bullet q \neq q$$

this also effects the update, and update also becomes resource-sensitive, that is update with sequential composition of one action with itself, is not equal to update once with that action

$$m \,.\, (q \bullet q) \neq m \,.\, q$$

This features of our algebra is a desirable one in solving the muddy children puzzle and other similar epistemic and dynamic scenarios. In the dynamic approaches to to this puzzle in Dynamic Epistemic Logic [9, 10], the actions and the updates are part of the formalism, but there is no account of resource, and moreover, there is no structure on the actions.

2.3.3 Muddy Children with Cheating and Lying.

Although the muddy children is a challenging puzzle and not obvious to solve, but the actions that happen in it, are very simple. They are all trivial actions that appear the same to all the agents. More sophisticated cases would be when some action is happening, but that not all the agents know about it, or some think that some other action is happening. These can be for example when some of the children are not honest and when they still do not know that they are dirty, they will answer otherwise, that is they will lie. But the honest children do not know that and they think they are telling the truth. Another example would be when some children secretly communicate with each other and tell each other than they are dirty, where as other children, outsiders to this action think the cheating has not happened. We have means in our algebraic setting to deal with these *misinformation* actions. These actions are going to lead to *wrong information* and possibly confusion of some of the children. By confusion we mean having contradictory knowledge $\Box_A^M \bot$. Since we allowed for wrong knowledge in our setting, we are able to encode all these interesting cases.

We are going to introduce a version of the puzzle where some of the children are not honest and they may *lie*, or otherwise *cheat* by engaging in secret communication. These misinformation examples were first discussed by Baltag in [6], the cheating example was partly solved in a course taught by him, where as the lying example is new.

Lying Muddy Children. Assume that the same n children are playing in the mud and this time only one of them, child number one C_1 for simplicity, has a dirty forehead. Their father does the announcement exactly as in the classical Muddy Children Puzzle, and then asks the same question. Now before the first round of answers, the dirty child who is a perfect reasoner, follows the proof

presented above and by looking around and seeing no other dirty child, concludes that he is dirty $\Box_{C_1} D_1$. But instead of announcing the truth in the first round, he lies by saying that he does not know that he is dirty. This version is encoded using the same epistemic system as muddy children above with the difference that this time we set $k = 1$. Let $\bar{D}_1$ denote the fact that child one is not dirty. This fact is being satisfied in all the propositions where child one is not dirty, that is

$$s_\beta \leq \bar{D}_1 \quad \text{where } C_1 \notin \beta$$

an example of such a proposition is

$$s_{\{C_1\}} \leq \bar{D}_2$$

Denote by $\bar{q}$ the first round of answers that includes child one's lying and others' "No!" replies. The appearance of this action to child one is identity since he knows that he is lying

$$f_{C_1}(\bar{q}) = \bar{q}$$

whereas other children who do not know that C_1 is lying think that the action q in classical muddy children (truthful public refutation) is happening, that is we have

$$\text{for } 1 < i \leq n \quad f_{C_i}(\bar{q}) = q$$

The kernel of $\bar{q}$ is the down set of the proposition in which C_1 knows he is not dirty and others know that they are dirty

$$ker(\bar{q}) = \downarrow (\Box_{C_1} \bar{D}_1 \vee \bigvee_{i=2}^{n} \Box_{C_i} D_i)$$

Proposition 2.3.2 *After the first child's lying and the others' negative answers in the first round, every clean child j (with $k < j$) thinks (wrongly) that he is dirty i.e.*

$$s_{\{C_1\}} \leq [q_0 \bullet \bar{q}] \Box_{C_j} D_j \,.$$

Proof. We proceed in the same way as the classical muddy children above, by moving the dynamic and epistemic modalities to the left and applying the update inequality we obtain

$$f_{C_j}(s_{\{C_1\}}) \,.\, f_{C_j}(q_0) \,.\, f_{C_j}(\bar{q}) \leq D_j \,.$$

By replacing the f_{C_j}'s with their values we get

$$(s_{\{C_1\}} \vee s_{\{C_1, C_j\}}) \,.\, q_0 \,.\, q \leq D_j$$

and by distributivity we have to show the following two cases (same as in the classical version above)

$$s_{\{C_1\}} \cdot q_0 \cdot q \leq D_j$$

and

$$s_{\{C_1,C_j\}} \cdot q_0 \cdot q \leq D_j$$

The second case is trivial for the same reasons as classical muddy children. For the first case we use the

$$s_{\{C_1,\cdots,C_k\}\setminus\{C_j\}} \cdot q_0 \, (.q)^{(k-2)} \in ker(q)$$

proved in the muddy children above, and get

$$s_{\{C_1\}} \cdot q_0 \in ker(q)$$

and hence

$$\bot = s_{\{C_1\}} \cdot q_0 \cdot q \leq D_j$$

□

Cheating Muddy Children. As another example, consider the original n and k version but in which, just before the $k-1$'th round, all but one of the dirty children (say, all except C_1), "cheat" by secretly telling each other that they are in fact dirty. We denote this cheating action by $\pi \in Q$, it appears to the cheating children, who are the dirty children 2 to k, as it is

$$f_{C_2} = f_{C_3} = \cdots = f_{C_k}(\pi) = \pi$$

but the first dirty child C_1 and the clean ones, that is from $(k+1)$ to n, are not aware of it:

$$f_{C_1}(\pi) = f_{C_{k+1}}(\pi) = \cdots = f_{C_n}(\pi) = 1$$

In the cheating action each child tells the others that he is dirty, that is $D_2 \wedge \cdots \wedge D_k$. Thus the kernel of the cheating action is the proposition that says the opposite

$$ker(\pi) = \downarrow \bigwedge_{i=2}^{i=k} \overline{D_i}$$

where as in the lying case $\overline{D_i}$ is the fact that says child i is clean, and is implied by all the propositions that correspond to it, for example the proposition that says children 2 to k are dirty satisfies $\overline{D_1}$

$$s_{\{C_2,\ldots,C_k\}} \leq \overline{D_1}$$

In the $k-1$'th round, all these dirty cheating children will answer yes, we know we are dirty, and at the same time child one and the clean children answer no. We denote this action with $\overline{q}$, it appears as it is to every one:

$$f_{C_i}(\overline{q}) = \overline{q}$$

and its kernel is the disjunction of proposition that says children 2 to k do not know that they are dirty and the propositions that says the rest of children know that they are dirty:

$$ker(\overline{q}) = \downarrow((\bigvee_{i=2}^{i=k} \Box_{C_i}^M \overline{D_i}) \vee (\bigvee_{j=1,k+1}^{j=n} \Box_{C_j}^M D_j))$$

We claim that in the k'th round the only non-cheating child C_1 will wrongly conclude that he is clean:

Proposition 2.3.3 *After $k-2$ rounds of no answer, and the cheating of dirty children 2 to k, and the yes answers of them at round $(k-1)$, the dirty child one will wrongly conclude that he is clean:*

$$s_{\{C_1,\ldots,C_k\}} \leq [q_0(\bullet q)^{k-2} \bullet \pi \bullet \overline{q}]\Box_{C_1}^M \overline{D_1}$$

Proof. The proof is similar to that of the original muddy children, it goes by induction on k. □

2.4 Variations on Epistemic Modalities

The epistemic modality of our setting is the right adjoint to appearance and satisfies the *normal* properties of an epistemic modality, that is monotonicity and preservation of conjunction. However, we can have more properties by posing conditions on our appearance maps, or by asking our underlying suplattice to be a Boolean Algebra where presence of classical negation helps us to define more modalities. Also the composition of our appearance-knowledge adjoint pair provides us with two more modalities, both monotone.

2.4.1 Properties of Appearance

In the usual relational models of epistemic logic, that is Kripke semantics, different modalities are obtained by asking the accessibility relation to satisfy relational properties such as reflexivity, transitivity, and anti-symmetry. We have an order-theoretic semantics and thus in order to have different knowledge modalities, our appearance maps should satisfy order properties, such as increasing, decreasing, idempotence and so on. These properties are put together to define the notions of closure and co-closure:

Closure. The f_A map is a closure if it satisfies the following properties

$$m \leq f_A(m)\,, \qquad f_A(f_A(m)) = f_A(m)\,, \quad \text{and} \quad m \leq m' \Rightarrow f_A(m) \leq f_A(m')\,.$$

The first property is called the *increasing* property, the second one is *idempotence*, and the last one monotonicity. Co-closure is defined similarly to closure except that the increasing property becomes *decreasing*, that is $f_A(m) \leq m$. We show below how by playing with these properties, we can get different epistemic modalities:

Proposition 2.4.1 If f_A is idempotent, i.e. $f_A(f_A(m)) = f_A(m)$, then the epistemic modality is positively introspective, i.e. $\Box_A m \leq \Box_A \Box_A m$.

Proof.

$$\begin{array}{rcll} f_A & \dashv & \Box_A & \\ f_A(\Box_A m) & \leq & m & \text{property of adjunction} \\ f_A(f_A(\Box_A m)) & \leq & m & \text{idempotence of } f_A \\ \Box_A m & \leq & \Box_A \Box_A m & \text{two times adjunction} \end{array}$$

Note that in this proof we only use the weaker (one direction) idempotence of f_A, that is $f_A(f_A(m)) \leq m$. The epistemic modality $\Box_A$ can also have order properties, for example if f_A is decreasing $f_A(m) \leq m$, then by adjunction the box modality becomes increasing $m \leq \Box_A m$. As a conclusion if f_A is a co-closure (decreasing and idempotent) then $\Box_A$ becomes increasing and positively introspective. The increasing property resembles the *necessitation* rule of epistemic logics and the positive introspection is the 4 axiom of the $S4$ modality. Mixing the order properties of f_A and $\Box_A$ provides us with different epistemic logics. For example we have:

Proposition 2.4.2 If f_A is idempotent and $\Box_A$ is decreasing, i.e. $\Box_A m \leq m$ then our epistemic system is an $S4$ system.

Proof. We have to show that $\Box_A$ satisfies the axioms of $S4$ modality, i.e. T and 4. Axiom T is the same as the decreasing property and axiom 4 or positive introspection is proved above by idempotence of f_A.

2.4.2 Properties of Module

If our module is a Boolean Algebra (BA), our knowledge-appearance adjunction results to two more modalities, one of them is the diamond modality of Kripke semantics. When M is a BA, it has a negation operator $\neg(-) : M \to M$ that is order reversing, i.e. $m \leq m' \Leftrightarrow \neg m' \leq \neg m$, satisfies $\neg\neg m = m$, and also $\neg(m \vee m') = \neg m \wedge \neg m'$. This negation helps us to define new modalities that also constitute an adjoint pair. In this section we go through these definitions algebraically, the definitions in terms of Kripke models are discussed in the Representation chapter.

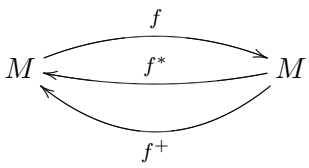
Theorem 2.4.3 In a Boolean Algebra, every pair of maps $f, g : M \to M$ that form an adjunction $f \dashv g$ gives rise to another pair of adjoint maps $f^+ \dashv g^+$ where $f^+(m) = \neg g(\neg m)$ and $g^+(m) = \neg f(\neg m)$.

Proof. For $m, m' \in M$:

$$\begin{array}{rcl} f & \dashv & g \\ f(\neg m) \leq \neg m' & \Leftrightarrow & \neg m \leq g(\neg m') \\ \neg\neg m' \leq \neg f(\neg m) & \Leftrightarrow & \neg g(\neg m') \leq \neg\neg m \\ m' \leq \neg f(\neg m) & \Leftrightarrow & \neg g(\neg m') \leq m \\ m' \leq g^+(m) & \Leftrightarrow & f^+(m') \leq m \\ f^+ & \dashv & g^+ \end{array}$$

□

These new adjoint maps are called *linear adjoints*, that is f^+ is the linear adjoint of f and g^+ is the linear adjoint of g. Thus the linear adjoint f^+ of a map f is the De Morgan dual of its categorical (Galois) adjoint f^*. Pictorially we have



where

$$f \dashv f^* \quad \text{and} \quad f^+(m) = \neg f^*(\neg m)\,.$$

In the case of our adjunction $f_A \dashv \Box_A$, we get two linear adjoints f_A^+ and $\Box_A^+$ that are also Galois adjoints $f_A^+ \dashv \Box_A^+$. We can now define the De Morgan dual of the box modality as the linear adjoint to appearance $f_A^+(m) = \neg\Box_A m$. This De Morgan dual has been referred to as the Diamond modality in epistemic logic contexts. In our setting it is the linear adjoint to appearance $f_A^+ = \Diamond_A$. The linear adjoint to $\Box_A^+ m = \neg f_A \neg m)$ stands for all the propositions that an agent A does not consider true if m does not hold in the real world.

2.4.3 Composition of Adjoints

Any pair of adjoint maps $f \dashv g$ gives rise to a closure and a co-closure, this corollary of adjunction has been discussed in books on order theory for example [28] and also books on category theory, for example [61]. The closure map is the result of the composition $f \circ g$ and the co-closure is the other direction $g \circ f$. Each of these maps can be seen as a new modality. For instance using our appearance-knowledge adjunction $f_A \dashv \Box_A$, we define a new family of modalities for each agent

$$\bigcirc_A^M : M \to M \quad \text{where} \quad \bigcirc_A^M = f_A^M \circ \Box_A^M$$

These are closure modalities, that is they are monotone and increasing. Similarly with the other direction we get a family of co-closure modalities:

$$\bigcirc_A'^M : M \to M \quad \text{where} \quad \bigcirc_A'^M = \Box_A^M \circ f_A^M$$

These new modalities are both monotone, but non are join or meet preserving. So they stand for non-standard modalities. Both of these modalities are also idempotent, that is for instance $\bigcirc_A(\bigcirc_A m) = \bigcirc_A m$ and similarly for $\bigcirc'_A$. If we consider these new modalities as knowledge modalities, then idempotence stands for positive introspection. The increasing property of closure, that is $m \leq \bigcirc'_A m$ is an instance of the generalization or necessitation rule that says if a proposition is true then everybody knows it. The decreasing property, that is $\bigcirc_A m \leq m$ is the truth property or axiom T that says if an agent knows a proposition, then it is true. In other words, wrong-knowledge is not possible. Thus in the co-closure case we get a knowledge-like modality for $S4$ that does not preserve the conjunction. All these equally hold for the quantale.

Chapter 3

Logical Syntax

In this section we present a sequent calculus proof system for the algebraic semantics of Epistemic systems presented in the previous chapter. Our system is the first sequent calculus of its kind for a dynamic and epistemic logic, the usual proof system for these logics are Hilbert-style [10, 45]. However, the syntax of our logic is in the same style as the syntax of Dynamic Epistemic Logic (DEL) of Baltag, Moss, Solecki [10], which is based on the syntax of Propositional Dynamic Logic (PDL) [45]. We start with a brief overview of the syntax of PDL and its extension to DEL , then introduce our syntax, which is in some sense simpler than both of these. We then proceed by explaining our sequent calculus setting in intuitive terms and try not to refer to the algebra. This is done by providing an *intuitive reading* for each sequent and using it to read the rules, thus giving an intuitive meaning for rules. Also, we only present and explain the rules for connectives that are significant in dealing with dynamic epistemic scenarios. The full set of rules, together with formal definitions will be presented in the next chapter when we prove the soundness and completeness of our setting.

We refer to our logic as Intuitionistic Dynamic Epistemic Action Logic (IDEAL), which is a logic to reason about knowledge of agents in a multi-agent system where agents communicate and as a result their knowledge changes. The word Dynamic Epistemic comes from reasoning about knowledge and the changes induced to knowledge. In order to reason about these changes, we give an explicit formalization of the communication actions between agents, and that is where the word Action comes from. Finally, our logic is non-boolean, that is we do not have negation and classical implication and so we benefit from an Intuitionistic version of sequent calculus. It is interesting that IDEAL can encode and solve the epistemic puzzles that are usually dealt with in a full classical logic, and it does so in a much simpler manner. This is because of the power of the dynamic formalism: actions and the change they induce on knowledge compromises the lack of negation and implication. This is a precious quality, it enables us to stay minimal and constructive.

IDEAL has two sequent systems and thus two sets of rules: one for its propositional, which is a structural logic and another for its action setting, which is a substructural logic in the style of Lambek-calculus [56], or more precisely Intuitionistic Non-Commutative Linear Logic [44]. There are two

features in these rules that make them different from the usual propositional and action sequent calculi, firstly agents are explicitly encoded in sequents and interact with propositional and action connectives. On the action side, it is the first time that epistemic modalities are defined on actions. This feature makes us deal with context splitting for the action contexts and copying the context for the agent contexts, a feature absent from any other substructural logic we know. Secondly, we have some mixed rules where the two systems interact with each other to encode the effect of actions on propositions thus resulting in rules with two different kinds of sequents as input. These mixed rules have been discussed in a higher level of abstraction in Functor Logics of [18], however, it is for the first time in IDEAL that they get a more concrete treatment.

3.1 Historical Background

We start by introducing the syntax of Propositional Dynamic Logic PDL [45] and then show how it extends to Dynamic Epistemic Logic DEL [9, 10].

3.1.1 Propositional Dynamic Logic

Propositional Dynamic Logic is a logic to reason about interaction of computer programs with the system in Computer Science and is a stronger version of Hoare logic [47]. The syntax of PDL has two levels: propositions m and programs q and it is generated as as follows

$$\begin{aligned} m &::= \bot \mid \top \mid \neg m \mid m \wedge m \mid m \to m \mid [q]m \\ q &::= 1 \mid m? \mid q \bullet q \mid q \vee q \mid q^* \end{aligned}$$

Propositions of PDL stand for properties of the system and programs represent any computer program written in some programming language. So PDL has the usual propositional connectives, that is conjunction, disjunction, implication, and negation of these properties. Moreover, it has a new propositional connective $[q]m$, called *dynamic modality*and reads as 'after action q proposition m holds'. The dynamic modality bridges the propositional and the program levels and represents the *weakest precondition* of action q with regards to proposition m. This means that $[q]m$ is the weakest proposition that should be true before running q so that m becomes true after q. It enables us to reason about the output of a program, given the initial assumption on which the program was executed.

The connectives on the program level stand for basic operations on programs, which are sequential composition $q \bullet q'$ and non-deterministic choice $q \vee q'$ of programs. The composition of two programs $q \bullet q'$ means 'first do q then do q''. Sequential composition is a non-commutative operator, that is $q \bullet q' \neq q' \bullet q$. This is because running programs in different orders may result in different outputs. The star connective q^* stands for running a program for an infinite number of times is called iteration, it is based on infinitely many times composing q with itself and is used to define loop commands. 1 is the program that does nothing, it is the unit of sequential composition $q \bullet 1 = 1 \bullet q = q$ and is some

times referred to as *skip*. The choice of actions $q \vee q'$ means 'do either q or q''. The choice is non-deterministic in the sense that it is the system that decides which action is running and not us. Since we do not know the choice strategy of the system, it appears as non-deterministic to us. And finally the operation $m?$ is the 'test of proposition m, it is the action that tests the truth of a proposition m. It is used to define conditional commands such as `if-then-else`. Test can be seen as another bridge (other than dynamic modality) between the two levels: to each proposition m has a corresponding program: its test $m?$. So the dynamic modality $[q]m$ is a way to see actions as propositions and test $m?$ is a way to see propositions as actions. Test can be used together with the iteration to define conditional loop commands such as `while`.

PDL has two logical entailments: one between propositions and another between actions. The first one is the usual logical entailment between propositions: $m \vdash m'$ means proposition m entails proposition m'. The entailment between programs $q \vdash q'$ stands for the order of information or non-determinism of programs, that is $q \vdash q'$ means action q is more deterministic, or has more information, than action q'.

3.1.2 Dynamic Epistemic Logic

Our other logic, Dynamic Epistemic Logic or DEL for short, is an epistemic logic based on PDL. It benefits from the dynamic structure of PDL and enriches it with multi-agent *epistemic* modalities $\Box_A$. DEL adds a family of *epistemic modalities* to the propositional level of PDL and focuses on *epistemic action* in its action level, epistemic actions being actions that change the information state of agents. The syntax of DEL is generated as follows

$$\begin{aligned} m &::= \bot \mid \top \mid \neg m \mid m \wedge m \mid m \to m \mid [q]m \mid \Box_A m \\ q &::= 1 \mid m? \mid q \bullet q \mid q \vee q \mid q^* \mid m! \mid m!_\beta \end{aligned}$$

The epistemic modality $\Box_A$ represents the *knowledge* or *belief* of an agent A in the set of agents $\mathcal{A}$. In contexts where no wrong belief is allowed it can be read as knowledge, i.e. *justified true belief*, in the rest as *justified belief*. The knowledge proposition $\Box_A m$ says that agent A knows or believes that proposition m holds. The only knowledge axiom that $\Box_A$ satisfies is the K axiom of normal epistemic logics, that is

$$\Box_A(m \to m') \to (\Box_A m \to \Box_A m')$$

Axiom K is also referred to as the *monotonicity* axiom. Note that the knowledge modality of DEL does not satisfy the Truth axiom of epistemic logic that says the following

$$\Box_A m \to m$$

This feature enables DEL to deal with *wrong* belief, which is a suitable notion in dynamic situations.

For instance as a result of misinformation such as lying or cheating or a bad phone line, the agent might be deceived and thus get to believe in a wrong proposition.

The programs of DEL are *epistemic actions* in the sense that they change the information state of agents and they denote communication between agents. A full discussion of these notions in semantical terms is provided in chapter six. Two of these actions are public and private announcements of a proposition. The action of publicly announcing a proposition m denoted by $m!$ in DEL, is an epistemic action that changes the knowledge of all of the agents. Similarly the private announcement of m made only to a subgroup $\beta \subseteq \mathcal{A}$ of agents is denoted by $m!_\beta$ and is an epistemic action that changes the knowledge of agents who are in β. More complicated epistemic actions can be built by sequential composition or choice of these basic epistemic actions. This enables DEL to reason about the changes made to the *knowledge* or *belief* of agents after for example a public or private announcement is made to them. As mentioned in the introduction, the novelty of DEL in comparison with other update logics such as Gerbrandy and Groenveld [41, 42] and Plaza [72] is that it accounts for all sorts of updates or changes, including the negative ones that result in wrong belief and can thus reason about misinformation actions such as cheating and lying.

3.1.3 Intuitionistic Dynamic Epistemic Action Logic

Our IDEAL logic is based on DEL, but differs from it in several ways.

1. The propositions in DEL as well as in PDL are classical. We believe that the full classical setting is not necessary to reason about dynamic epistemic scenarios. We thus dismiss propositional negation and implication from our logic.

2. We consider knowledge and belief both on the propositional and the action levels. The propositional knowledge is the same as in DEL. The action knowledge enables our agents to acquire knowledge and belief with regard to actions. For example when a private announcement is made, agents that are in the subgroup know what is going on, but the outsiders do not know that an announcement is being made.

3. We base the agents' knowledge on both levels on a more basic notion of *appearance* and enrich the syntax with it. We will explain this new connective later.

4. The same thing is done with the dynamic modality, that is we base it on a the notion of *update* and enrich our syntax with it. The notion of update, or more precisely *epistemic update* originates from DEL but is not used in DEL's syntax.

5. IDEAL has an algebraic semantics, instead of the usual Kripke semantics of DEL. We have a representation theorem, which we will present in chapter six that constructs an algebraic semantics from the Kripke semantics of DEL.

6. Both PDL and DEL have Hilbert-style proof systems, we present a sound and complete sequent calculus for our logic.

3.2 Syntax of IDEAL

In this section we present the syntax of our logic, explain all the connectives: unary and binary, and also the unit constants. We explain each of these, with focus on the connectives that have epistemic or dynamic significance, leaving the other ones to our next chapter. The syntax of IDEAL is generated as follows

$$\begin{array}{rcl} m & ::= & \bot \mid \top \mid s \mid p \mid m \wedge m \mid m \vee m \mid \Box_A^M m \mid f_A^M(m) \mid [q]m \mid m.q \\ q & ::= & \bot \mid 1 \mid \sigma \mid q \bullet q \mid q \vee q \mid q \wedge q \mid q/q \mid q \setminus q \mid \Box_A^Q q \mid f_A^Q(q) \end{array}$$

where σ is in a set V_Q of atomic actions, s is in a set V_M of atomic propositions, A is in the set $\mathcal{A}$ of agents, and p is in the set Φ of facts.

3.2.1 Binary Connectives

We denote propositions by m and actions by q. The logic consists of three sorts of binary connectives:

1. **Between two propositions.** These are the usual binary connectives on propositions, that is classical conjunction $m_1 \wedge m_2$ and disjunction $m_1 \vee m_2$. Note that we do not have the propositional implication connective.

2. **Between two actions.** These are also the usual action operations, that is sequential composition $q_1 \bullet q_2$ and non-deterministic choice of actions $q_1 \vee q_2$. There are two implications between programs, referred to as *residuals* in the literature, q_1/q_2 and $q_1 \setminus q_2$, these are Galois adjoints to the sequential composition discussed in the previous chapter. For the reader familiar with Linear Logic notation, we present the following table for the correspondence between our binary connectives and the connectives in Intuitionistic Non-Commutative Linear Logic:

Q-system	Linear Logic
1	1
$\top$	$\top$
$\bot$	0
$\bullet$	$\cdot$
$/$	$\circ\!\!-$
$\setminus$	$-\!\!\circ$
$\vee$	$\oplus$
$\wedge$	$\&$

3. **Between a proposition and an action.** We have two connectives of this sort that are strongly related by adjunction. The first one is the PDL *dynamic modality* $[q]m$ or the weakest precondition of PDL. Given an action q and a proposition m, it returns the weakest proposition that should have been true before running q so that m becomes true afterwards. This proposition is the *weakest* in the sense that it is entailed by any other proposition m' that has the same property. Dynamic modality can be seen as a *before* operator with a backward nature: given the outputs, it provides with the weakest input that was true *before* the action and that caused this certain output. We have another binary connective, a new one, that complements the backward nature of dynamic modality $[q]m$. It is called *update* and denoted as $m.q$, given a proposition m and an action q, it tells you what proposition will be true after q, and thus can be seen as an *after* operator. More explicitly, it says if m is true at the input of action q, then $m.q$ will be true at the output of q. The relation between the dynamic modality and update is as follows:

$$(m.q \text{ entails } m') \quad \text{iff} \quad (m \text{ entails } [q]m')\,. \tag{3.1}$$

We call this relation *dynamic adjunction*; it says if an updated proposition $m.q$ implies another proposition m', then m implies that after running q, proposition m' holds and vice versa.

3.2.2 Unary Connectives or Modalities

We start with our epistemic modality on propositions $\Box_A m$. This modality, which is the same as in DEL, stands for knowledge or belief of agents. The knowledge modality is based on a more primitive notion, that of *appearance* $f_A(m)$, which a new connective of our logic. It stands for all the propositions that agent A considers possible when in fact m holds in the real world. f_A is monotone, that is if we have m entails m', then we also have that $f_A(m)$ entails $f_A(m')$. Knowledge can be derived from appearance as follows: if the appearance of m to an agent $f_A(m)$ entails m', then whenever proposition m holds, then A knows that m'. The other direction also holds, if in m agent A knows that m', then m appears to A as m', or the appearance of m to A entails m'. Thus we have

$$(f_A(m) \text{ entails } m') \quad \text{iff} \quad (m \text{ entails } \Box_A m')\,. \tag{3.2}$$

We call this relation *epistemic adjunction* , it is a Galois adjunction denoted as $f_A(m) \dashv \Box_A m$. This relation is the base of our epistemic reasoning and motivates a slogan: 'Our **knowledge** is the left adjoint to how the world **appears** to us.'

The same unary connectives are defined on actions, that is the appearance map of an agent A of an action $f_A(q)$, that is all the actions that an agent thinks are running when in reality action q is happening. The agent's knowledge about the current action is denoted as $\Box_A q$. Defining having epistemic modalities on actions is another novelty of our logic and will prove to be very useful in applications discussed in chapter five. When the context is not clear, we distinguish between the appearance of

the propositions and actions by denoting the former as f_A^Q and the latter as f_A^M, and similarly for the knowledge $\Box_A^Q$ and $\Box_A^M$. Note that these are our only unary connectives: we do not have negation.

3.2.3 Constants and Facts

True and False propositions are denoted by constants $\top$ and $\bot$. The true proposition $\top$ is the unit of conjunction and makes any disjunction true

$$m \wedge \top = m \qquad m \vee \top = \top$$

The false proposition $\bot$ has more properties, it is the unit of disjunction and makes the conjunction false

$$m \vee \bot = m\,, \qquad m \wedge \bot = \bot$$

Moreover, it appears as it is to all the agents

$$f_A(\bot) = \bot$$

that is, if a contradiction holds in the real world, every agent knows about it. also makes every update false:

$$\bot\,.\,q = \bot$$

So if we live in a contradictory world, i.e.. one in which a contradiction $\bot$ holds, then there is no action that can save us from this contradiction[1].

On the action side, the $\bot$ or the *false action* is the most deterministic action and has properties similar to the false proposition. That is, it is the unit of choice of actions

$$\bot \vee q = q$$

and makes the sequential composition of actions false

$$q \bullet \bot = \bot$$

and also its appearance as itself to every agent

$$f_A(\bot) = \bot$$

The dual notion of most non-deterministic action is the denoted as $\top$; this is the choice of all the actions and is the unit of conjunction of actions. But since conjunction of actions does not have any intuitive

[1]This goes against the para-consistent approach to logic e.g. Graham Priest's logic, that say the world contains contradiction. Since in our system the contradiction is contagious and will transfer from reality to all agents' minds, reasoning about which will have no added value.

meaning, we will not discuss it in this chapter.

The action that does not do any thing or the *skip* action is denoted as 1, it is the unit of sequential composition and update, that is

$$1 \bullet q = q \bullet 1 = q\,, \qquad m \cdot 1 = m$$

Not every proposition in an epistemic setting is epistemic. Some of propositions are objective in the sense that no epistemic action can change their truth value. These objective propositions are referred to as *facts* and we denote them by letter p, the set of all the facts is denoted as Φ. No update can change the truth value of a fact $p \in \Phi$, that is if p is true before running an action q, it will remain true after running the action q. Thus for any fact p and any action q, we have:

$$p \text{ entails } [q]p\,,$$

or equivalently by dynamic adjunction:

$$(p.q) \text{ entails } p\,.$$

We have now explained all of our connectives, so we move on to our sequent rules.

3.3 Sequent Calculus

Dynamic epistemic logic in its original form [9, 10] is a Hilbert-style logic. In this chapter we present the first Gentzen-style sequent calculus of its kind for a dynamic and epistemic logic.

3.3.1 Sequents and Sequences

Our calculus consist of two systems: an M-system for propositions with M-sequents denoted as $\vdash_M$, and a Q-system for actions with Q-sequents denoted as $\vdash_Q$. Both of these systems are intuitionistic in the sense that they only have one single formula on the right hand side of their sequents. We denote the M-sequents as follows

$$\Gamma \vdash_M m$$

and the Q-sequents as follows

$$\Gamma \vdash_Q q$$

In both cases we have a single formula on the right hand side of the turnstile, a proposition m in M-sequents and an action q in Q-sequents. The propositional sequence Γ is a finite sequence of propositions, actions, and agents

$$\Gamma = m_1, \ldots, m_n, q_1, \ldots, q_m, A_1, \ldots, A_k$$

The action sequence Γ is a finite sequence of actions and agents

$$\Gamma = q_1, \ldots, q_n, A_1, \ldots, A_m$$

In classical propositional sequents, where there are no actions or agents, commas are conjunction of propositions. In action logics such as Lambek calculus and Intuitionistic Linear Logic, there are no agents and thus commas stand for sequential composition of actions (or the $\cdot$ of Linear Logic). But in our setting we have more than one kind of formula in a sequent, thus commas get loaded with different meanings. Between two propositions they are conjunction and between two actions they are sequential composition:

$$\begin{array}{rll} m, m' \vdash_M m & \text{means} & m \wedge m' \vdash_M m \\ q, q' \vdash_Q q & \text{means} & q \bullet q' \vdash_Q q \end{array}$$

But between an agent and a proposition or action, the comma means the appearance of the agent of that proposition or action:

$$\begin{array}{rll} m, A \vdash_M m & \text{means} & f_A(m) \vdash_M m \\ q, A \vdash_Q q & \text{means} & f_A(q) \vdash_Q q \end{array}$$

The comma between a proposition and an action means the update of the proposition by the action

$$m, q \vdash_M m \text{ means } m \,.\, q \vdash_M m$$

Because we apply commas to left and we allow sequences of only one agent and one action, some exceptions arise in assigning meaning to commas. These exceptions are when our context on the left only has one agent, or only one action (in an M-sequence). We assign meaning to these cases as follows:

$$\begin{array}{rll} A \vdash_M m & \text{means} & f_A(\top) \\ A \vdash_Q q & \text{means} & f_A(1) \\ q \vdash_M m & \text{means} & \top.q \end{array}$$

In the first and last cases, we add the unit of conjunction $\top$ to the left of the agent or action in an M-sequence

$$A \cong \top, A \qquad \text{and} \qquad q \cong \top, q$$

In the middle case, we add the unit of sequential composition to the left of agent in a Q-sequence

$$A \cong 1, A$$

Empty Sequences. The empty sequence on the left hand side of a Q-sequent is the unit of sequential composition:

$$\vdash_Q q \quad \text{means} \quad 1 \vdash_Q q$$

We do not allow for an empty right hand side in Q-sequents. M-sequents, on the other hand, can have empty right hand side, which is $\bot$, that is the unit for disjunction:

$$\Gamma \vdash_M \quad \text{means} \quad \Gamma \vdash_M \bot$$

The empty left hand side in M-sequents means the True proposition, that is $\vdash_M m$ means $\top \vdash_M m$. The formal assignment of meaning to sequences is presented in the next chapter. Here we proceed by suggesting an intuitive reading for our sequences and sequents.

3.3.2 Intuitive Reading

We provide a way to read the M and Q sequents in natural language. This can be seen as capturing the *intuitive meaning* of a sequent.

- $\vdash_M m$ means that proposition m holds in all contexts.
- $\vdash_Q q$ means that action q is less deterministic than the action that does nothing, and thus might not change the truth-value of the proposition (on which it might act).
- $\Gamma, A, \Gamma' \vdash_M m$ means that in context Γ, agent A knows or believes that $\Gamma' \vdash_M m$ holds. So this captures features of A's own reasoning: the sequent $\Gamma' \vdash_M m$ is accepted by A in context Γ as a valid argument.
- $\Gamma, q, \Gamma' \vdash_M m$ means that, after action q happens on context Γ, the sequent $\Gamma' \vdash_M m$ will hold.
- $m, \Gamma \vdash_M m'$ means that, in context m (i.e. in any situation in which m is true), the sequent $\Gamma \vdash_M m'$ holds.
- $\Gamma, A, \Gamma' \vdash_Q q$ means agent A knows or believes that in context Γ action q is less-deterministic than the sequential composition of programs in Γ'.
- Finally $q, \Gamma \vdash_Q q'$ means that sequential composition of q with actions in Γ is more deterministic than action q.

This reading might seem backward in agent and action cases. The reason is that whenever we have an agent A, we are going to read the proposition or action to the left of it as the agent's knowledge or belief about them, where as we have encoded the agent A as his appearance map f_A and not his knowledge in our sequents. But the epistemic adjunction between the two $f_A \dashv \Box_A$ allows us to present the intuitive reading since we can take the appearance to the right hand side and read it as a knowledge connective.

This becomes clear below where we give examples. The same holds for the actions in propositional contexts, that is whenever we have an action we are going to update its left hand side and read it as 'after', where as the 'after' operation is the dynamic modality and the adjoint of update.

Example. The intuitive reading of the sequent $m, A, B \vdash_M m'$ is

'In context m, agent A knows that agent B knows that m''.

The formal meaning of this sequent will be

$$f_B(f_A(m)) \vdash_M m'$$

which by epistemic adjunction encode in the rules, to be presented later, is equivalent to

$$m \vdash_M \Box_A^M \Box_B^M m'$$

As another example consider the sequent $m, A, q, B \vdash_M m''$, which is intuitively read as:

In context m, agent A believes that after action q agent B will believe that proposition m'' must hold.

and formally means

$$f_B^M(f_A^M(m) \,.\, q) \vdash_M m''$$

equivalent to

$$m \vdash_M \Box_A^M [q] \Box_B^M m''$$

Resource Sensitivity. From this reading we can explain how our sequent calculus expresses two forms of resource sensitivity. One is the use-only-once form of Linear Logic [44]. We call these resources *dynamic resources*. They express the fact that repetition of actions matters in validity of sequents, and thus actions cannot be freely added to or deleted from the sequents. This is true in both our propositional and action sequents. For example in a propositional context, a proposition m might not entail m', that is $m \nvdash_M m'$, but if we update it with an action it will, that is $m, q \vdash_M m'$. An example would be when knowledge of an agent does not entail m', that is for example $\Box_A m \nvdash_M m'$, but if we announce m' to him via action q, then he will know it and thus we will have $\Box_A m, q \vdash m'$. The same holds for repetition of actions, for example we might not have $m, q \vdash_M m'$, but if we do q twice, then we will have $m, q, q \vdash_M m'$. A very good example is the muddy children puzzle where each repetition of the no answer yields new information in children. Another case would be if we do another action after q, for example q' then we will have $m, q, q' \vdash_M m'$. Similarly in the other direction, if we have $m \vdash_M m'$ and then update m with an action q, we might not get the same result $m, q \nvdash_M m'$, this for example the opposite of m' is announced to an agent. The same holds for action sequents, for example we might have $q \vdash_Q q''$, but after sequentially composing q with another action q', we do not maintain the same result, that is $q, q' \nvdash_M q''$. Similarly in the other direction, action q might not be

more deterministic than action q'', that is $q \nvdash_Q q''$, but sequentially composing it with q' will give us $q, q' \vdash_Q q''$.

The other form of our resource sensitivity deals with *epistemic resources*: these are resources that are available to each agent and enable him to reason in a certain way and for example to infer a conclusion from these resources. These resources are encoded in the way the context appears to the agent in sequents, for instance Γ in the sequent $\Gamma, A, \Gamma' \vdash_M m$ is the context, and hence $f_A(\Gamma)$ is the resource that enables agent A to do the $\Gamma' \vdash_M m$ reasoning. Note that $\Gamma' \vdash_M m$ might not be a valid sequent in the context Γ, but it is valid in the context given by Γ's appearance to agent A. That is we have Γ does not entail m in reality $\Gamma \nvdash_M m$ but agent A thinks it does $\Gamma, A \vdash_M m$. Also in the other direction, a sequent might hold in reality $\Gamma \vdash_M m$, but agent A is deceived and cannot do the same deduction, that is $\Gamma, A \nvdash_M m$. Exactly the same holds for action sequents, for example in reality an action q might be more deterministic than action q', that is $q \vdash_Q q'$, but not for agent A, that is $q, A \nvdash_Q q'$. In this way we can think of *presence of agents* as resources that make a difference in validity of sequents and cannot be freely added to or deleted from the sequents.

3.3.3 Axioms and Rules for Units and Constants

For each operation we develop two rules: one to introduce it on the right hand side, for short a right or R rule, and the other to introduce it on the left hand side or a left or L rule. The right rule tells us how a sequence on the left hand side of turnstile entails an operation. The left rule says how can the operation entails the proposition or action on the right hand side of turnstile. These rules express the properties of our propositional operations. In this section we explain the rules using our intuitive meaning, the formal meaning, connected to the algebra, will become clear in the next section when we prove the soundness and completeness. We introduce some notation: if we want to limit our attention to a sequence of only one entity, we subscript it with that entity. For example Γ_M is a sequence that only contains propositions, Γ_Q contains only actions and Γ_A is a sequence of only agents.

Axiom and rules for units in M-sequents.
The first group of our rules are to encode the properties of the constants $\bot$,$\top$ and 1. The M-sequents have the following rules for units

$$\frac{}{m \vdash_M m}\ id \qquad \frac{}{\bot \vdash_M m}\ \bot L \qquad \frac{\Gamma \vdash_M}{\Gamma \vdash_M \bot}\ \bot R \qquad \frac{}{\Gamma \vdash_M \top}\ \top R$$

Identity is the usual and only axiom of Gentzen systems, it says that each proposition entails itself. The left rule for $\bot$, (recall that $\bot$ in M-sequents is the false or contradictory proposition) encodes the usual logical meaning of contradiction: that it entails every proposition. The right rule for $\bot$ is the encoding of our notion of empty right hand side, which is the $\bot$. The right rule for $\top$ is also the usual encoding of the tautology proposition, the one that is true in every context, so every context entails it. The left

rule for $\top$ would be

$$\frac{\Gamma, \Gamma' \vdash_M m}{\Gamma, \top, \Gamma' \vdash_M m} \top L$$

but we do not need to state it, since it is derivable from the weakening rule that we will present later.

Axiom and rules for units in Q-sequents.
For Q-sequents we have the following unit rules

$$\frac{}{q \vdash_Q q} id \qquad \frac{\Gamma, \Gamma' \vdash_Q q}{\Gamma, 1, \Gamma' \vdash_Q q} 1L \qquad \frac{}{\vdash_Q 1} 1R \qquad \frac{}{\Gamma, \bot, \Gamma' \vdash_Q q} \bot L \qquad \frac{}{\Gamma \vdash_Q \top} \top R$$

The Identity axiom says that each action is more deterministic or equal to itself. The left rule for 1 encodes the neutrality of 1 in sequential composition, that it is the unit of sequential composition. Using the intuitive reading, it says that if sequential composition of two contexts of programs is more deterministic than q, then we can as well add the 1 action to the sequential composition, and everything will remain as it was. The rule for 1 on the right is the encoding of our notion of an empty left hand side in Q-sequent, as we said it is the unit of sequential composition. The left rule for $\bot$ encodes the fact that if one composes any action with the impossible action $\bot$, one will get an impossible action in return. The right rule for $\top$ encodes the fact that the top action is the most non-deterministic action since it is the choice of all actions and thus every action is more deterministic than it.

3.3.4 Operational rules for M-sequents

The second group of rules encode properties of the operations on propositions. We start with basic propositional connectives: conjunction and disjunction. The rules for disjunction are

$$\frac{\Gamma, m_1, \Gamma' \vdash_M m \quad \Gamma, m_2, \Gamma' \vdash_M m}{\Gamma, m_1 \vee m_2, \Gamma' \vdash_M m} \vee L \qquad \frac{\Gamma \vdash_M m}{\Gamma \vdash_M m \vee m'} \vee R1 \qquad \frac{\Gamma \vdash_M m'}{\Gamma \vdash_M m \vee m'} \vee R2$$

The rules for conjunction are

$$\frac{\Gamma, m_1, \Gamma' \vdash_M m}{\Gamma, m_1 \wedge m_2, \Gamma' \vdash_M m} \wedge L1 \qquad \frac{\Gamma, m_2, \Gamma' \vdash_M m}{\Gamma, m_1 \wedge m_2, \Gamma' \vdash_M m} \wedge L2 \qquad \frac{\Gamma \vdash_M m \quad \Gamma \vdash_M m'}{\Gamma \vdash_M m \wedge m'} \wedge R$$

We continue with appearance, which is our basic epistemic operation. The main property of appearance, as discussed before, is its *monotonicity*. This means that if a proposition m implies another proposition m, then its appearance would imply the appearance of the other proposition, that is if $m \vdash_M m$, then $f_A^M(m) \vdash_M f_A^M(m)$. In other words the appearance operation preserves the entailment relation between two propositions. This is the content of the right rule for appearance or $f_A^M R$

$$\frac{\Gamma \vdash_M m}{\Gamma, A \vdash_M f_A^M(m)} f_A^M R$$

The intuitive reading interpretation of this rule will be: if in context Γ proposition m holds, then in context Γ, agent A knows that his appearance of m holds. Note that $f_A^M(m)$ might not in reality be entailed by Γ, but agent A thinks it is. In other words, if an agent is present in a context, he will derive his own conclusions, which might not be the real (or true) ones!

The left rule for appearance $f_A^M L$ is the encoding of the meaning of comma between an agent and a proposition:

$$\frac{m', A, \Gamma \vdash_M m}{f_A^M(m'), \Gamma \vdash_M m} \; f_A^M L$$

Our other epistemic connective is the knowledge modality $\Box_A^M$. The rules for knowledge are derived from the rules for appearance using the epistemic adjunction between the two. The *epistemic adjunction* tells us if $f_A^M(m) \vdash m'$ then we have $m \vdash \Box_A^M m'$ and also the other way around. The first direction is encoded in the following rule (and thus this rule also holds in the other direction):

$$\frac{\Gamma, A \vdash_M m}{\Gamma \vdash_M \Box_A^M m} \; \Box_A^M R$$

It reads as: if in context Γ an agent knows that proposition m holds, then Γ entails that he knows that m. In other words, if the appearance of a context to an agent entails m, then in that context, the agent knows that m. This rule allows us to derive the knowledge of an agent given his appearances, which is encoded in the sequence Γ, A on the left hand side.

The left rule for $\Box_A$ expresses a property of knowledge that again descends from its adjunction to the appearance. This property says the appearance of knowledge does not add anything to the knowledge. In more exact terms, the appearance applied to the knowledge of a proposition $f_A^M(\Box_A^M m)$ implies the proposition m:

$$\frac{m, \Gamma \vdash_M m'}{\Box_A^M m, A, \Gamma \vdash_M m'} \; \Box_A^M L$$

The intuitive reading reveals the nature of this rule better: if in context m, sequence Γ entails proposition m', then if an agent knows the context, that is he knows that m, then he can derive, or he knows that the entailment $\Gamma \vdash_M m'$. In other words, if an agent knows all the assumptions, he can derive all the conclusions.

3.3.5 Operational rules for Q-sequents

The third group of our rules are to encode properties of operations on actions. As explained before, the entailment between actions $q \vdash_Q q'$ means that action q has more information (or is more deterministic) than action q', or q' is more non-deterministic than q. The meaning of a Q-sequent $\Gamma \vdash_Q q$ depends on the meaning of the sequence Γ, which is a finite sequence of actions and agents. As discussed before the comma between two actions means their sequential composition $q, q' = q \bullet q'$ and the comma between an action and an agent means the appearance of the agent of the action $q, A = f_A^Q(q)$.

The operations on actions consist of sequential composition $\bullet$, non-deterministic choice $\vee$, appearance f_A^Q and knowledge $\Box_A^Q$. We also have residuation, but since they do not have a specific epistemic meaning we only introduce their rules in the next chapter, when we prove completeness. The rules for non-deterministic choice are the same rules as in Intuitionistic Linear Logic, with the difference that we also consider agents in the context. The same goes with the rules for sequential composition, they are similar to the rules of non-commutative Intuitionistic Linear Logic generalized for an agent context. The rules for appearance of actions and knowledge about actions are new, but follow the same principles as the appearance and knowledge on propositions.

We will first discuss the rules for appearance and knowledge. This will facilitate the explanation of the agent context in other rules. The rules for appearance of actions are:

$$\frac{\Gamma \ \vdash_Q \ q}{\Gamma, A \ \vdash_Q \ f_A^Q(q)} \ f_A^Q R \qquad\qquad \frac{q', A, \Gamma \ \vdash_Q \ q}{f_A^Q(q'), \Gamma \ \vdash_Q \ q} \ f_A^Q L$$

The right rule for appearance expresses, same as in the propositional case, its monotonicity, that is if action q is more deterministic than action q', that is $q \ \vdash_Q \ q'$ then the appearance of q to A is more deterministic than the appearance of q' to A, that is $f_A(q) \vdash_Q \ f_A(q')$. The left rule is also the same as in M-sequent: it is the meaning of the comma between an action and an agent.

The rules for knowledge on Q-sequents $\Box_A^Q$ are also the same as the knowledge rules on M-sequents, since the $\Box_A^Q$ on actions has the same properties as $\Box_A^M$ on propositions. They are as follows:

$$\frac{\Gamma, A \vdash_Q q}{\Gamma \vdash_Q \Box_A^Q q} \ \Box_A^Q R \qquad\qquad \frac{q', \Gamma \vdash_Q q}{\Box_A^Q q', A, \Gamma \vdash_Q q} \ \Box_A^Q L$$

As we said before, sequential composition of actions behaves like conjunction on proposition. There is one difference: the relation between the appearance and conjunction is not the same as the relation between appearance and sequential composition. The appearance of sequential composition of two actions to an agent $f_A(q \bullet q')$ entails the sequential composition of their appearances $f_A(q) \bullet f_A(q')$, that is $f_A(q \bullet q') \ \vdash_Q \ f_A(q) \bullet f_A(q')$. The same thing does not hold for the conjunction (we did not assume any connection between appearance and conjunction). That is why although the left rule for $\bullet$ is the same as $\wedge L$, the right rule for $\bullet$ differs from $\wedge R$ since it asks for the same agent context in its top line sequents while splitting the action context. The rules are

$$\frac{\Gamma, q_1, q_2, \Gamma' \vdash_Q q}{\Gamma, q_1 \bullet q_2, \Gamma' \vdash_Q q} \bullet L \qquad\qquad \frac{\Gamma_Q, \Gamma_A \vdash_Q q_1 \quad \Gamma'_Q, \Gamma_A \vdash_Q q_2}{\Gamma_Q, \Gamma'_Q, \Gamma_A \vdash_Q q_1 \bullet q_2} \bullet R$$

This double treatment of contexts is a new feature in sequent rules: splitting of contexts is present in (and a novelty of) Linear Logic rules for tensor, but presence of both splitting and not-splitting in a rule is new and and worth proof-theoretic analysis.

The rules for non-deterministic choice are exactly the same as disjunction rules in M-sequents. The relation between the appearance and a disjunction or the appearance and a non-deterministic choice are the same, that is $f_A(q \vee q') = f_A(q) \vee f_A(q')$. So we do not need to mention the agent context:

$$\frac{\Gamma, q_1, \Gamma' \vdash_Q q \qquad \Gamma, q_2, \Gamma' \vdash_Q q}{\Gamma, q_1 \vee q_2, \Gamma' \vdash_Q q} \vee L \qquad \frac{\Gamma \vdash_Q q_1}{\Gamma \vdash_Q q_1 \vee q_2} \vee R1 \qquad \frac{\Gamma \vdash_Q q_2}{\Gamma \vdash_Q q_1 \vee q_2} \vee R2$$

We also have conjunction and its corresponding rules, but since conjunction does not have an intuitive meaning in the action contexts, we do not introduce the rules here. We will do so in the next chapter.

3.3.6 Mixed Rules

So far we have presented operational rules for propositions and also operational rules for actions. But actions can appear in propositional contexts via the *mixed* binary operations of update and dynamic modality. Here we present the *mixed* rules for these operators, where by *mixed* we mean rules that involve both M and Q sequents in their top line.

The update operator $-.-$ takes a proposition and an action and returns the updated proposition $m.q$. The left rule for update encodes the meaning of comma between a proposition and an action

$$\frac{\Gamma, q, \Gamma' \vdash_M m}{\Gamma.q, \Gamma' \vdash_M m} .L$$

The right rule for update encodes an important property, that how the update and appearance interact with each other and how what an agent knows before update connects to what he knows after update. In other words, how an agent gets to know more, or learn, from updating his past knowledge. The rule is:

$$\frac{\Gamma, \Gamma_A \vdash_M m \quad \Gamma_Q, \Gamma_A \vdash_Q q}{\Gamma, \Gamma_Q, \Gamma_A \vdash_M m.q} .R$$

According to the intuitive reading and assuming Γ_A has only one agent inside, it says that if in context Γ, an agent knows m, and after running a series of programs Γ_Q, he knows that an action q is running, then if he updates his knowledge with these actions, he will know the update of m by q. This rule enables us to calculate the updated knowledge of agents from their separate knowledge of the proposition and action. As we shall see in the next chapter, it corresponds to the *update inequality* in the algebra. Another important feature of this rule is that, similar to the left rule for sequential composition in Q-sequents, it splits the proposition and action contexts, that is Γ and Γ_Q, but copies the agents context Γ_A.

The rules for dynamic modality are somewhat dual to the rules for update (which is because they

are Galois adjoints):

$$\frac{m' \vdash_M m \quad \Gamma_Q \vdash_Q q}{[q]m', \Gamma_Q \vdash_M m}\ DyL \qquad\qquad \frac{\Gamma, q \vdash_M m}{\Gamma \vdash_M [q]m}\ DyR$$

The left rules says that if proposition m' entails m and the sequential composition of actions in Γ_Q is more deterministic than the single action q, then in the context where the weakest precondition of q with regard to m' holds, after doing the sequential composition of actions in Γ_Q, proposition m will hold. Note that the agent context is absent here, which is because we did not assume any relation between dynamic modality and appearance of agents.

Action connectives in propositional contexts.

Update can be done with a simple action, but also with sequential composition and choice of actions. So we need appropriate rules to encode these variants of update. These rules are very similar to their counterparts in Q-sequents, with the difference that they have propositional context and appear only in the left hand side of M-sequents. We thus need a left rule for the skip action, and also left rules for the $\bullet$ (also for residuals $/, \backslash$) and $\vee$ (also for $\wedge$) of actions[2] We label these rules with an extra M to distinguish them from the usual M rules.

The rule for skip action in an M-sequent encodes the neutrality of skip in update:

$$\frac{\Gamma, \Gamma' \vdash_M m}{\Gamma, 1, \Gamma' \vdash_M m}\ 1ML$$

According to the intuitive reading, if in context Γ, the sequent Γ' entails m, then after doing nothing on Γ, that sequent still holds.

The rule for sequential composition of programs in M-sequents is the encoding of the meaning of comma between two actions:

$$\frac{\Gamma, q_1, q_2, \Gamma' \vdash_M m}{\Gamma, q_1 \bullet q_2, \Gamma' \vdash_M m}\ \bullet ML$$

The rule for choice of actions in M-sequents is:

$$\frac{\Gamma, q_1 \vdash_M m \qquad \Gamma, q_2 \vdash_M m}{\Gamma, q_1 \vee q_2 \vdash_M m}\ \vee ML$$

It says if we update a context with action q_1 and the result entails m, and updating the same context with action q_2 yields the same result, then the update with the choice of these actions also gives us the same result.

[2]We do not need to add left rules for update with appearance and knowledge of actions, because they do not satisfy special properties with regard to update of propositions (as opposed to for example associativity of update over $\bullet$) and thus are not needed in proving completeness.

3.3.7 Structural rules

Propositions have the same structural rules as in intuitionistic logic: they can be weakened, contracted, and permuted as follows

$$\frac{\Gamma, \Gamma' \vdash m}{\Gamma, m', \Gamma' \vdash_M m}\ weakL \qquad \frac{\Gamma \vdash_M}{\Gamma \vdash_M m}\ weakR$$

$$\frac{\Gamma, m', m', \Gamma' \vdash_M m}{\Gamma, m', \Gamma' \vdash_M m}\ contr \qquad \frac{\Gamma, m'', m', \Gamma' \vdash_M m}{\Gamma, m', m'', \Gamma' \vdash_M m}\ exch$$

We have a restricted version of the usual Cut-rule for propositions as follows:

$$\frac{\Gamma' \vdash_M m' \qquad m', \Gamma'' \vdash_M m}{\Gamma', \Gamma'' \vdash_M m}\ Mcut$$

Moreover, we have a special structural rule for non-epistemic proposition, or fact. These have a special existence, they are stable under update, so we add one rule for facts

$$\frac{\Gamma \vdash_M p}{\Gamma, q \vdash_M p}\ fact$$

It says that if a fact p is true in a context Γ, then it remains true independent of any actions q happening on Γ. We have two structural rules for actions, one is a restricted version of the cut-rule as follows

$$\frac{\Gamma' \vdash_Q q \qquad q, \Gamma'' \vdash_Q q'}{\Gamma', \Gamma'' \vdash_Q q'}\ Qcut$$

The other one is a rule for agents

$$\frac{A \vdash_Q q}{1 \vdash_Q q}\ Agent$$

Actions cannot be contracted, weakened or permuted neither in M-sequents nor in Q-sequents. These induce actions as resources, fully discussed in the paragraph about resource-senstivity. Similarly, lack of structural rules for agents encode resource-sensitivity with regard to agents.

The table of all rules.

Axiom and Unit rules for M-sequents.

$$\frac{}{m \vdash_M m}\ id \qquad \frac{}{\bot \vdash_M m}\ \bot L \qquad \frac{\Gamma \vdash_M}{\Gamma \vdash_M \bot}\ \bot R \qquad \frac{}{\Gamma \vdash_M \top}\ \top R$$

Operational rules for M-sequents.

$$\frac{\Gamma \vdash_M m}{\Gamma, A \vdash_M f_A^M(m)}\ f_A^M R \qquad \frac{m, A, \Gamma \vdash_M m'}{f_A^M(m), \Gamma \vdash_M m'}\ f_A^M L$$

$$\frac{\Gamma, A \vdash_M m}{\Gamma \vdash_M \Box_A^M m}\ \Box_A^M R \qquad \frac{m, \Gamma \vdash_M m'}{\Box_A^M m, A, \Gamma \vdash_M m'}\ \Box_A^M L$$

$$\frac{\Gamma \vdash_M m_1 \quad \Gamma \vdash_M m_2}{\Gamma \vdash_M m_1 \wedge m_2}\ \wedge R \qquad \frac{\Gamma, m_1, \Gamma' \vdash_M m}{\Gamma, m_1 \wedge m_2, \Gamma' \vdash_M m}\ \wedge L1 \qquad \frac{\Gamma, m_2, \Gamma' \vdash_M m}{\Gamma, m_1 \wedge m_2, \Gamma' \vdash_M m}\ \wedge L2$$

$$\frac{\Gamma, m_1, \Gamma' \vdash_M m \quad \Gamma, m_2, \Gamma' \vdash_M m}{\Gamma, m_1 \vee m_2, \Gamma'}\ \vee L \qquad \frac{\Gamma \vdash_M m_1}{\Gamma \vdash_M m_1 \vee m_2}\ \vee R1 \qquad \frac{\Gamma \vdash_M m_2}{\Gamma \vdash_M m_1 \vee m_2}\ \vee R1$$

$$\frac{\Gamma, q, \Gamma' \vdash_M m}{\Gamma.q, \Gamma' \vdash_M m}\ .L \qquad \frac{\Gamma, \Gamma_A \vdash_M m \quad \Gamma_Q, \Gamma_A \vdash_Q q}{\Gamma, \Gamma_Q, \Gamma_A \vdash_M m.q}\ .R$$

$$\frac{m' \vdash_M m \quad \Gamma_Q \vdash_Q q}{[q]m', \Gamma_Q \vdash_M m}\ DyL \qquad \frac{\Gamma, q \vdash_M m}{\Gamma \vdash_M [q]m}\ DyR$$

$$\frac{\Gamma, \Gamma' \vdash_M m}{\Gamma, 1, \Gamma' \vdash_M m}\ 1ML \qquad \frac{\Gamma, q_1, q_2, \Gamma' \vdash_M m}{\Gamma, q_1 \bullet q_2, \Gamma' \vdash_M m}\ \bullet ML$$

$$\frac{\Gamma, q_1 \vdash_M m \qquad \Gamma, q_2 \vdash_M m}{\Gamma, q_1 \vee q_2 \vdash_M m}\ \vee ML$$

$$\frac{\Gamma_Q \vdash_Q q_2 \quad \Gamma, q_1 \vdash_M m}{\Gamma, q_1 / q_2, \Gamma_Q \vdash_M m}\ /ML \qquad \frac{\Gamma_Q \vdash_Q q_1 \quad \Gamma, q_2 \vdash_M m}{\Gamma, \Gamma_Q, q_1 \setminus q_2 \vdash_M m}\ \setminus ML$$

$$\frac{\Gamma, q_1, \Gamma' \vdash_M m}{\Gamma, q_1 \wedge q_2, \Gamma' \vdash_M m}\ \wedge ML1 \qquad \frac{\Gamma, q_2, \Gamma' \vdash_M m}{\Gamma, q_1 \wedge q_2, \Gamma' \vdash_M m}\ \wedge ML2$$

Structural rules for M-sequents.

$$\frac{\Gamma, \Gamma' \vdash m}{\Gamma, m', \Gamma' \vdash_M m}\ weakL \qquad \frac{\Gamma \vdash_M}{\Gamma \vdash_M m}\ weakR \qquad \frac{\Gamma, m', m', \Gamma' \vdash_M m}{\Gamma, m', \Gamma' \vdash_M m}\ contr$$

$$\frac{\Gamma, m'', m', \Gamma' \vdash_M m}{\Gamma, m', m'', \Gamma' \vdash_M m}\ exch \qquad \frac{\Gamma' \vdash_M m' \qquad m', \Gamma'' \vdash_M m}{\Gamma', \Gamma'' \vdash_M m}\ Mcut \qquad \frac{\Gamma \vdash_M p}{\Gamma, q \vdash_M p}\ fact$$

Axiom and Unit rules for Q-sequents.

$$\frac{}{q \vdash_Q q}\ id \qquad \frac{\Gamma, \Gamma' \vdash_Q q}{\Gamma, 1, \Gamma' \vdash_Q q}\ 1L \qquad \frac{}{\vdash_Q 1}\ 1R \qquad \frac{}{\Gamma, \bot, \Gamma' \vdash_Q q}\ \bot L \qquad \frac{}{\Gamma \vdash_Q \top}\ \top R$$

Operational rules for Q-sequents.

$$\frac{\Gamma \vdash_Q q}{\Gamma, A \vdash_Q f_A^Q(q)}\ f_A^Q R \qquad \frac{q', A, \Gamma \vdash_Q q}{f_A^Q(q'), \Gamma \vdash_Q q}\ f_A^Q L$$

$$\frac{\Gamma, A \vdash_Q q}{\Gamma \vdash_Q \Box_A^Q q}\ \Box_A^Q R \qquad \frac{q', \Gamma \vdash_Q q}{\Box_A^Q q', A, \Gamma \vdash_Q q}\ \Box_A^Q L$$

$$\frac{\Gamma, q_1, q_2, \Gamma' \vdash_Q q}{\Gamma, q_1 \bullet q_2, \Gamma' \vdash_Q q}\ \bullet L \qquad \frac{\Gamma_Q, \Gamma_A \vdash_Q q_1 \quad \Gamma'_Q, \Gamma_A \vdash_Q q_2}{\Gamma_Q, \Gamma'_Q, \Gamma_A \vdash_Q q_1 \bullet q_2}\ \bullet R$$

$$\frac{\Gamma, q_1, \Gamma' \vdash_Q q \qquad \Gamma, q_2, \Gamma' \vdash_Q q}{\Gamma, q_1 \vee q_2, \Gamma' \vdash_Q q}\ \vee L \qquad \frac{\Gamma \vdash_Q q_1}{\Gamma \vdash_Q q_1 \vee q_2}\ \vee R1 \qquad \frac{\Gamma \vdash_Q q_2}{\Gamma \vdash_Q q_1 \vee q_2}\ \vee R2$$

$$\frac{\Gamma, q_1, \Gamma' \vdash_Q q}{\Gamma, q_1 \wedge q_2, \Gamma' \vdash_Q q}\ \wedge L1 \qquad \frac{\Gamma, q_2, \Gamma' \vdash_Q q}{\Gamma, q_1 \wedge q_2, \Gamma' \vdash_Q q}\ \wedge L2 \qquad \frac{\Gamma \vdash_Q q_1 \qquad \Gamma \vdash_Q q_2}{\Gamma \vdash_Q q_1 \wedge q_2}\ \wedge R$$

$$\frac{\Gamma_Q \vdash_Q q_2 \quad q_1 \vdash_Q q}{q_1/q_2, \Gamma_Q \vdash_Q q}\ /L \qquad \frac{\Gamma, q_2 \vdash_Q q_1}{\Gamma \vdash_Q q_1/q_2}\ /R$$

$$\frac{\Gamma \vdash_Q q_1 \quad q_2 \vdash_Q q}{\Gamma, q_1 \setminus q_2 \vdash_Q q}\ \setminus L \qquad \frac{q_1, \Gamma_Q \vdash_Q q_2}{\Gamma_Q \vdash_Q q_1 \setminus q_2}\ \setminus R$$

Structural rule for Q-sequents.

$$\frac{\Gamma' \vdash_Q q \qquad q, \Gamma'' \vdash_Q q'}{\Gamma', \Gamma'' \vdash_Q q'}\ Qcut \qquad \frac{A \vdash_Q q}{1 \vdash_Q q}\ Agent$$

Chapter 4

Soundness and Completeness

In the previous section, we introduced our IDEAL sequent calculus, consisting of two systems: a Q system and an M-system, connected via the mixed rules of the M system. Given a distributive epistemic system, the Q-system is based on its quantale part, referred to as an *epistemic quantale*, and the M-system is based on its module part, referred to as an *epistemic module*. In this section we want to formalize this connection and to show that distributive epistemic systems are sound and complete algebraic models of IDEAL sequent systems. The soundness part states that every derivable sequent of the IDEAL system is a valid inequality in all distributive epistemic systems. The completeness part states the other direction: every valid inequality of any distributive epistemic system, is a derivable sequent of IDEAL.

4.1 Soundness

We provide definitions to prove two lemmas for the soundness of the Q and M-systems, starting with the Q-system.

4.1.1 Soundness of the Q-System

The formulae in this system are generated by the following syntax

$$q ::= \sigma \mid 1 \mid q \bullet q \mid q \setminus q \mid q/q \mid \bot \mid q \vee q \mid \top \mid q \wedge q \mid f_A^Q(q) \mid \Box_A^Q q$$

A sequence of this system is called a Q-*sequence*. It is denoted by Γ and is a list of actions and agents

$$\Gamma \in (L_Q \cup \mathcal{A})^*$$

where L_Q is the set of all formulae of the Q-system and $\mathcal{A}$ is set of all agents. Sequences that contain only agents are denoted by Γ_A and sequences of only actions are denoted by Γ_Q.

Sequents of this system are called Q-*sequents*. They are denoted by $\Gamma \vdash_Q q$ where q is a single action $q \in L_Q$ and Γ a sequence. The empty sequence on the left hand side is the unit of quantale multiplication, that is 1. So a sequent with an empty sequence on the left hand side $\vdash_Q q$ means $1 \vdash_Q q$. There is no empty sequent on the right[1].

Meaning of a Sequence. We assign *meaning* to the sequences of a Q-system by the following operation

$$- \odot_Q - \colon L_Q \times (L_Q \cup \mathcal{A}) \to L_Q$$

where

$$q \odot_Q q' = q \bullet q'$$
$$q \odot_Q A = f_A^Q(q)$$

We abuse the notation and use the same symbol[2] to extend this operation to sequences $\Gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n)$. This is done by induction as follows

$$\odot_Q \Gamma = (((1 \odot_Q \gamma_1) \odot_Q \gamma_2) \cdots \odot_Q \gamma_n)$$

This operation enables us to identify a sequence of Q-formulae $\Gamma \in (L_Q \cup \mathcal{A})^*$ with only one Q-formula $\odot_Q \Gamma \in L_Q$. We add the unit of sequential composition to the beginning of a sequence, and then apply the $\odot_Q$ operation to the left. For example a sequence $\Gamma = (q, A, q', B)$ is identified by

$$\odot_Q \Gamma = ((((1 \odot_Q q) \odot_Q A) \odot_Q q') \odot_Q B) = f_B^Q(f_A^Q(q) \bullet q')$$

Adding the unit makes the $\odot_Q$ operation well-defined by identifying a sequence of only one action $\Gamma = (q)$ with itself $1 \odot_Q q = 1 \bullet q = q$ and a sequence of only one agent $\Gamma = (A)$ with the appearance of that agent of the unit $1 \odot_Q A = f_A^Q(1)$.

Satisfaction Relation. Given a distributive epistemic system $(M, Q, \{f_A\}_{A \in \mathcal{A}})$, we define an interpretation map α from the Q formulae to the quantale part of the epistemic system:

$$\alpha : L_Q \to Q$$

This map assigns to each Q-formula $q \in L_Q$, an element of the quantale $\alpha(q)$[3]. Note that in order to know the interpretation of a sequent Γ, we apply α to $\odot_Q \Gamma$. The types of this composition match since

[1] If we have an empty sequence on the right it would be the unit of Linear Logic inverted ampersand on the right, that is Linear Logic $\bot$, which does not exist in our language.

[2] Another option would be to use a new symbol; in [7] we use $\bigodot_Q$ for this extended operation.

[3] This is nothing but the semantic map $\alpha(q) = [\![q]\!]$. In [7] we skip the interpretation step and denote the semantics of a formula by the formula itself, that is we use q for $[\![q]\!]$. We follow this abuse of notation later on in this chapter to make the soundness proof easier to read.

we have

$$\alpha \circ \odot_Q : (L_Q \cup \mathcal{A})^* \to L_Q \to Q$$

For example interpretation of $\Gamma = q, A$ will be $\alpha(\odot(q, A)) = \alpha(f_A^Q(q))$. The α interpretation satisfies the following structure-preserving properties

$$\alpha(\bot) = \bot \quad \text{and} \quad \alpha(\top) = \top \quad \text{and} \quad \alpha(1) = 1$$

and for the meet, join, and multiplication (and its residuals) connectives we have:

$$\alpha(q) \bigcirc \alpha(q') = \alpha(q \bigcirc q')$$

where $\bigcirc = \{\wedge, \vee, \bullet, /, \backslash\}$, and also for the epistemic connectives

$$\alpha(f_A^Q(q)) = f_A^Q(\alpha(q)) \quad \text{and} \quad \alpha(\Box_A^Q\, q) = \Box_A^Q\, \alpha(q)$$

Definition 4.1.1 Given a distributive epistemic system $(M, Q, \{f_A\}_{A\in\mathcal{A}})$ and its interpretation map $\alpha\colon L_Q \to Q$, a Q-sequence Γ and a Q-formula q', we define a satsifaction relation as follows

$$\Gamma \models_Q q' \quad \text{iff} \quad \alpha(\odot_Q \Gamma) \leq \alpha(q')$$

Definition 4.1.2 A sequent $\Gamma \vdash_Q q$ is valid if and only if for any distributive epistemic system $(M, Q, \{f_A\}_{A\in\mathcal{A}})$ and its interpretation map $\alpha\colon L_Q \to Q$ we have $\Gamma \models_Q q$.

Lemma 4.1.3 *Every derivable Q-sequent is valid.*

Proof. The proof is done by proving that the rules of Q-system preserve validity of sequents. That is, if the sequents on the top line of a rule are valid, so are the sequents on the bottom line.

We start by proving soundness of the axioms and rules for units $1, \top, \bot$, given by

$$\frac{}{q \vdash_Q q}\ id \qquad \frac{\Gamma, \Gamma' \vdash_Q q}{\Gamma, 1, \Gamma' \vdash_Q q}\ 1L \qquad \frac{}{\vdash_Q 1}\ 1R \qquad \frac{}{\Gamma, \bot, \Gamma' \vdash_Q q}\ \bot L \qquad \frac{}{\Gamma \vdash_Q \top}\ \top R$$

The identity axiom is sound because it corresponds to the reflexivity of the partial order of the quantale, we have

$$q \vdash_Q q \quad \text{is valid} \quad \text{iff} \quad q \models_Q q \quad \text{iff} \quad \alpha(q) \leq \alpha(q)$$

For the left rule of 1 we have to show that if the top line is valid, then so is the bottom line:

$$\text{If} \quad \Gamma, \Gamma' \vdash_Q q \quad \text{is valid then} \quad \Gamma, 1, \Gamma' \vdash_Q q \quad \text{is also valid.}$$

This, by definition of validity, is equivalent to

$$\text{If} \quad \Gamma, \Gamma' \models_Q q \quad \text{then} \quad \Gamma, 1, \Gamma' \models_Q q\,,$$

which in turn, by definition of satisfaction is equivalent to

$$\text{If} \quad \alpha(\odot_Q(\Gamma, \Gamma')) \leq \alpha(q) \quad \text{then} \quad \alpha(\odot_Q(\Gamma, 1, \Gamma')) \leq \alpha(q)\,.$$

This conditional is true since we have $\odot_Q(\Gamma, \Gamma') = \odot(\Gamma, 1, \Gamma')$ and thus we have $\alpha(\odot(\Gamma, \Gamma')) = \alpha(\odot(\Gamma, 1, \Gamma'))$. In order to see that $\odot_Q(\Gamma, \Gamma') = \odot(\Gamma, 1, \Gamma')$, observe that if Γ and Γ' are sequences of actions we have $\odot_Q(\Gamma, \Gamma') = \odot_Q\Gamma \bullet \odot_Q\Gamma' = \odot_Q\Gamma \bullet 1 \bullet \odot_Q\Gamma'$, which is equal to $\odot_Q(\Gamma, 1, \Gamma')$. If they are both only agents, for example $\Gamma = A$ and $\Gamma' = B$, then we have $\odot_Q(\Gamma, \Gamma') = f_B^Q(f_A^Q(1))$, which is equal to $f_B^Q(f_A^Q(1) \bullet 1)$, and which is $\odot_Q(\Gamma, 1, \Gamma')$.

For the soundness of the right rule for 1, we have to show that $\vdash_Q 1$ is valid. An empty sequence on the left hand side of a sequent is the unit of sequential composition, so $\vdash_Q 1$ means $1 \vdash_Q 1$, which is valid since $\alpha(\odot_Q 1) \leq \alpha(\odot_Q 1)$ holds by reflexivity of the partial order on the quantale. For the soundness of the left rule for $\bot$ we have to show that $\Gamma, \bot, \Gamma' \vdash_Q q$ is valid, that is $\alpha(\odot_Q(\Gamma, \bot, \Gamma')) \leq \alpha(q)$. This is again trivial since $\odot_Q(\Gamma, \bot, \Gamma') = \bot$ and $\alpha(\bot) = \bot$, which is the least element of the quantale and thus less than any other element $\bot \leq \alpha(q)$. For the soundness of the right rule for $\top$ we have to show $\Gamma \vdash_Q \top$ is valid, that is $\alpha(\Gamma) \leq \alpha(\top)$, which is true since $\alpha(\top) = \top$, and $\top$ is the greatest element of the quantale and everything is less than it, $\alpha(\Gamma) \leq \top$.

The rules for sequential composition are

$$\frac{\Gamma, q_1, q_2, \Gamma' \vdash_Q q}{\Gamma, q_1 \bullet q_2, \Gamma' \vdash_Q q}\ \bullet L \qquad\qquad \frac{\Gamma_Q, \Gamma_A \vdash_Q q_1 \quad \Gamma'_Q, \Gamma_A \vdash_Q q_2}{\Gamma_Q, \Gamma'_Q, \Gamma_A \vdash_Q q_1 \bullet q_2}\ \bullet R$$

For the left rule we have to show

$$\text{If} \quad \alpha(\odot_Q(\Gamma, q_1, q_2, \Gamma')) \leq \alpha(q) \quad \text{then} \quad \alpha(\odot_Q(\Gamma, q_1 \bullet q_2, \Gamma')) \leq \alpha(q)\,,$$

which is true since $\odot_Q(\Gamma, q_1, q_2, \Gamma') = \odot_Q(\Gamma, q_1 \bullet q_2, \Gamma')$.

For the right rule first assume that we have only one agent in our agent context, that is $\Gamma_A = A$. So we have to show the following

$$\text{If } \alpha(\odot_Q(\Gamma, A)) \leq \alpha(q_1) \text{ and } \alpha(\odot_Q(\Gamma'_Q, A)) \leq \alpha(q_2) \quad \text{then} \quad \alpha(\odot_Q(\Gamma_Q, \Gamma'_Q, A)) \leq \alpha(q_1 \bullet q_2)$$

By applying the $\odot_Q$'s to their arguments we get an equivalent simpler version

$$\text{If } \alpha(f_A^Q(\odot_Q\Gamma)) \leq \alpha(q_1) \text{ and } \alpha(f_A^Q(\odot_Q\Gamma'_Q)) \leq \alpha(q_2) \quad \text{then} \quad \alpha(f_A^Q(\odot_Q\Gamma_Q \bullet \odot_Q\Gamma'_Q)) \leq \alpha(q_1 \bullet q_2)$$

Assume that the precedent holds, that is

$$\alpha(f_A^Q(\odot_Q\Gamma)) \leq \alpha(q_1) \quad \text{and} \quad \alpha(f_A^Q(\odot_Q\Gamma'_Q)) \leq \alpha(q_2)\,,$$

by order-preservation of the multiplication on the quantale we can multiply both sides of these inequalities and we get

$$\alpha(f_A^Q(\odot_Q\Gamma)) \bullet \alpha(f_A^Q(\odot_Q\Gamma'_Q)) \leq \alpha(q_1) \bullet \alpha(q_2)\,,$$

which is by structure-preservation of interpretation on f_A^Q and is equal to

$$f_A^Q(\alpha(\odot_Q\Gamma)) \bullet f_A^Q(\alpha(\odot_Q\Gamma'_Q)) \leq \alpha(q_1) \bullet \alpha(q_2)\,.$$

By the relation between appearance maps and multiplication on the quantale we have

$$f_A^Q(\alpha(\odot_Q\Gamma) \bullet \alpha(\odot_Q\Gamma'_Q)) \leq f_A^Q(\alpha(\odot_Q\Gamma)) \bullet f_A^Q(\alpha(\odot_Q\Gamma'_Q))\,,$$

which implies the following

$$f_A^Q(\alpha(\odot_Q\Gamma) \bullet \alpha(\odot_Q\Gamma'_Q)) \leq \alpha(q_1) \bullet \alpha(q_2)\,.$$

and again by structure preservation of interpretation, this time on the $\bullet$, we get

$$f_A^Q(\alpha(\odot_Q\Gamma \bullet \odot_Q\Gamma'_Q)) \leq \alpha(q_1 \bullet q_2)$$

and equivalently by structure preservation of α over f_A^Q

$$\alpha(f_A^Q(\odot_Q\Gamma_Q \bullet \odot_Q\Gamma'_Q)) \leq \alpha(q_1 \bullet q_2)$$

which is exactly what we wanted to prove, that is the validity of the bottom line of the rule.

If Γ_A has more than one agent $\Gamma_A = A_1, \ldots, A_n$ then we have to show that if

$$\alpha(f_{A_n}^Q(f_{A_{n-1}}^Q(\ldots f_{A_1}^Q(\odot_Q\Gamma)))) \leq \alpha(q_1) \quad \text{and} \quad \alpha(f_{A_n}^Q(f_{A_{n-1}}^Q(\ldots f_{A_1}^Q(\odot_Q\Gamma'_Q)))) \leq \alpha(q_2)$$

then

$$\alpha(f_{A_n}^Q(f_{A_{n-1}}^Q(\ldots f_{A_1}^Q(\odot_Q\Gamma_Q \bullet \odot_Q\Gamma'_Q)))) \leq \alpha(q_1 \bullet q_2)$$

The proof for this case is done similarly, except that after multiplying the two sides of the assumption by $\bullet$, we have to apply the inequality for f_{A_i} and the quantale multiplication n times, that is once for each agent $A_i \in \Gamma_A$, starting from the innermost one f_{A_n} and ending with the outmost one f_{A_1}.

The proof of soundness of other rules is done similarly, that is by following the same steps. In order to avoid the repetition of symbols in the proof of each rule and get cleaner proofs with less symbols,

we abuse the notation and denote the interpretation of a Q-formula by the formula itself. So instead of $\alpha(q)$, we write q. It can be understood from the context which one we mean, since a Q-formula q will appear in a sequent $\Gamma \vdash_Q q$, whereas its interpretation appears in an order relation $\odot_Q \Gamma \leq q$.

The rules for right residuation are

$$\frac{\Gamma_Q \vdash_Q q_2 \quad q_1 \vdash_Q q}{q_1/q_2, \Gamma_Q \vdash_Q q} \; /L \qquad\qquad \frac{\Gamma, q_2 \vdash_Q q_1}{\Gamma \vdash_Q q_1/q_2} \; /R$$

For the left rule, by the top line assumptions we have $\odot_Q \Gamma_Q \leq q_2$ and $q_1 \leq q$. Since sequential composition is order preserving, we compose the two sides of these two inequalities and we get $q_1 \bullet \odot_Q \Gamma_Q \leq q \bullet q_2$, which is by residuation equal to $q_1/q_2 \bullet \odot_Q \Gamma_Q \leq q$, and what we want for the bottom line, since Γ_Q is an action-only sequence and $\odot_Q(q_1/q_2, \Gamma_Q) = q_1/q_2 \bullet \odot_Q \Gamma_Q$.

For the right rule we have to show that if $\odot_Q \Gamma \bullet q_2 \leq q_1$ then $\odot_Q \Gamma \leq q_1/q_2$. First assume that Γ does not start with agents. Then the rule becomes true by the definition of adjunction $- \bullet q_2 \dashv -/q_2$, which says $\odot_Q \Gamma \bullet q_2 \leq q_1$ iff $\odot_Q \Gamma \leq q_1/q_2$. The iff definition of adjunction makes the other direction of this rule also sound, that is if the bottom line is true, then so is the top line. For the case that Γ starts with agents, for simplicity assume it has only one agent, that is $\Gamma = A$, then we have to show

$$\frac{A, q_2 \vdash_Q q_1}{A \vdash_Q q_1/q_2} \; /R$$

By the definition of a sequence starting with agents above this means that

$$\text{if} \quad f_A(1) \bullet q_2 \leq q_1 \quad \text{then} \quad f_A(1) \leq q_1/q_2$$

which is true by definition of adjunction and the rule holds in both directions.

The rules for left residuation are

$$\frac{\Gamma \vdash_Q q_1 \quad q_2 \vdash_Q q}{\Gamma, q_1 \setminus q_2 \vdash_Q q} \; \setminus L \qquad\qquad \frac{q_1, \Gamma_Q \vdash_Q q_2}{\Gamma_Q \vdash_Q q_1 \setminus q_2} \; \setminus R$$

For the left rule, the top line assumptions are $\odot_Q \Gamma \leq q_1$ and $q_2 \leq q$, we compose both sides and we get $\odot_Q \Gamma \bullet q_2 \leq q_1 \bullet q$, which is by residuation equal to $\odot_Q \Gamma \bullet (q_1 \setminus q_2) \leq q$, that is what we want for the bottom line, since $\odot_Q(\odot_Q \Gamma, q_1 \setminus q_2) = \odot_Q \Gamma \bullet (q_1 \setminus q_2)$.

The right rule, similar to the right rule for the right residuation, follows by definition of adjunction $q_1 \bullet - \dashv q_1 \setminus -$, which says $q_1 \bullet \odot_Q \Gamma_Q \leq q_2$ iff $\odot_Q \Gamma_Q \leq q_1 \setminus q_2$. The iff definition of adjunction makes the other direction of this rule also sound, that is if the bottom line is true, then so is the top line. Note that the right rule for left residuation is weaker from the right rule for the right residuation in the sense that the context after q_1, that is Γ_Q can only contain actions, where as in the right rule for the right residuation, we could have both. The action-only context is necessary here since if we have, for

example, only one agent after q_1, that is if $\Gamma = A$, then we have to show:

$$\frac{q_1, A \vdash_Q q_2}{A \vdash_Q q_1 \setminus q_2} \setminus R$$

which is not sound since

$$f_A(q_1) \leq q_2 \quad \text{does not imply} \quad f_A(1) \leq q_1 \setminus q_2$$

The rules for choice are

$$\frac{\Gamma, q_1, \Gamma' \vdash_Q q \qquad \Gamma, q_2, \Gamma' \vdash_Q q}{\Gamma, q_1 \vee q_2, \Gamma' \vdash_Q q} \vee L \qquad \frac{\Gamma \vdash_Q q_1}{\Gamma \vdash_Q q_1 \vee q_2} \vee R1 \qquad \frac{\Gamma \vdash_Q q_2}{\Gamma \vdash_Q q_1 \vee q_2} \vee R2$$

For the proof of the left rule note that by the definition of join in the quantale, we have that $q_1 \leq q$ and $q_2 \leq q$ implies $q_1 \vee q_2 \leq q$. By the top line assumptions we have $\odot_Q(\odot_Q \Gamma \bullet q_1, \Gamma') \leq q$ and $\odot_Q(\odot_Q \Gamma \bullet q_2, \Gamma') \leq q$ from which we obtain $\odot_Q(\odot_Q \Gamma \bullet q_1, \Gamma') \vee \odot_Q(\odot_Q \Gamma \bullet q_2, \Gamma') \leq q$. Assume first that Γ' is an action-only sequence, then by join preservation of $\bullet$ we have

$$\odot_Q(\odot_Q \Gamma \bullet q_1, \Gamma') \vee \odot_Q(\odot_Q \Gamma \bullet q_2, \Gamma') = (\odot_Q \Gamma \bullet q_1 \bullet \odot_Q \Gamma') \vee (\odot_Q \Gamma \bullet q_2 \bullet \odot_Q \Gamma') = (\odot_Q \Gamma \bullet (q_1 \vee q_2) \bullet \odot_Q \Gamma')$$

This is equal to $\odot_Q(\Gamma, (q_1 \vee q_2), \Gamma')$ and we obtain $\odot_Q(\Gamma, (q_1 \vee q_2), \Gamma') \leq q$. For the case that Γ' is an agent-only sequence, without loss of generality we assume it contains only one agent A. Then by join preservation of f_A and $\bullet$ we obtain

$\odot_Q(\odot_Q \Gamma \bullet q_1, A) \vee \odot_Q(\odot_Q \Gamma \bullet q_2, A) =$
$f_A(\odot_Q \Gamma \bullet q_1) \vee f_A(\odot_Q \Gamma \bullet q_2) = f_A((\odot_Q \Gamma \bullet q_1) \vee (\odot_Q \Gamma \bullet q_2)) = f_A(\odot_Q \Gamma \bullet (q_1 \vee q_2))$
This is equal to $\odot_Q(\Gamma, (q_1 \vee q_2), A')$ and thus $\odot_Q(\Gamma, (q_1 \vee q_2), A') \leq q$. For the case where Γ' is a mixture of actions and agents, soundness follows from both of the above two cases.

The right rules follow directly from the definition of join in the quantale, that is if $\odot_Q \Gamma \vdash_Q q_2$, since $q_2 \leq q_1 \vee q_2$ then $\odot_Q \Gamma \vdash q_1 \vee q_2$ and the same for the other one.

The rules for meet on the quantale are

$$\frac{\Gamma, q_1, \Gamma' \vdash_Q q}{\Gamma, q_1 \wedge q_2, \Gamma' \vdash_Q q} \wedge L1 \qquad \frac{\Gamma, q_2, \Gamma' \vdash_Q q}{\Gamma, q_1 \wedge q_2, \Gamma' \vdash_Q q} \wedge L2 \qquad \frac{\Gamma \vdash_Q q_1 \qquad \Gamma \vdash_Q q_2}{\Gamma \vdash_Q q_1 \wedge q_2} \wedge R$$

The left rules follow from the definition of meet on the quantale $q_1 \wedge q_2 \leq q_1$ and $q_1 \wedge q_2 \leq q_2$. Consider the first left rule, by the top line we have $\odot_Q(\odot_Q \Gamma \bullet q_1, \Gamma') \leq q$, since $q_1 \wedge q_2 \leq q_1$ we obtain $\odot_Q(\odot_Q \Gamma \bullet (q_1 \wedge q_2), \Gamma') \leq \odot_Q(\odot_Q \Gamma \bullet q_1, \Gamma')$. Thus $\odot_Q(\odot_Q \Gamma \bullet (q_1 \wedge q_2), \Gamma') \leq q$, which is the meaning of the bottom sequent. The soundness of the second left rule is proven similarly. The right rule follows by the definition of meet in the quantale: if $\Gamma \leq q_1$ and $\Gamma \leq q_2$ then $\Gamma \leq q_1 \wedge q_2$.

The rules for the appearance map are

$$\frac{q', A, \Gamma \vdash_Q q}{f^Q_A(q'), \Gamma \vdash_Q q}\ f^Q_A L \qquad\qquad \frac{\Gamma \vdash_Q q}{\Gamma, A \vdash_Q f^Q_A(q)}\ f^Q_A R$$

The left rule follows from definition of comma between an agent and an action, both of the left sequences on the bottom and top lines mean $\odot_Q(f^Q_A(q'), \Gamma)$, which is by the top line assumption less than or equal to q. The right rule follows by the order preservation of f^Q_A, that is if $\odot_Q\Gamma \leq q$ then we have $f^Q_A(\odot_Q\Gamma) \leq f^Q_A(q)$, which is the meaning of the bottom line.

The rules for knowledge on the quantale are:

$$\frac{q', \Gamma \vdash_Q q}{\Box^Q_A q', A, \Gamma \vdash_Q q}\ \Box_A L \qquad\qquad \frac{\Gamma, A \vdash_Q q}{\Gamma \vdash_Q \Box^Q_A q}\ \Box_A R$$

For the left rule assume $\odot_Q(q', \Gamma) \leq q$, and we have to show $\odot_Q(f^Q_A(\Box^Q_A q'), \Gamma) \leq q$. By composition of adjoints on the f^Q_A and $\Box^Q_A$, we have $f^Q_A(\Box^Q_A q') \leq q'$. Since both f^Q_A and $\bullet$ are order preserving, no matter what Γ consists of, we can apply the $\odot_Q\Gamma$ to both sides of this inequality. As a result we obtain $\odot_Q(f^Q_A(\Box^Q_A q'), \Gamma) \leq \odot_Q(q', \Gamma)$ and this is by the top line assumption less than q. For the right rule we assume $f^Q_A(\odot_Q\Gamma) \leq q$ which is equal, by adjunction to $\odot_Q\Gamma \leq \Box^Q_A q$. So this rule is sound also on the other direction.

The cut rule on Q sequents is

$$\frac{\Gamma' \vdash_Q q \qquad q, \Gamma'' \vdash_Q q'}{\Gamma', \Gamma'' \vdash_Q q'}\ Qcut$$

The first assumption means $\odot_Q\Gamma' \leq q$, from which we obtain $\odot_Q(\odot_Q\Gamma', \Gamma'') \leq \odot_Q(q, \Gamma'')$, since $\odot_Q$ is order preserving. By the second assumption we have $\odot_Q(q, \Gamma'') \leq q'$ and thus $\odot_Q(\odot_Q\Gamma', \Gamma'') \leq q'$, which is what we need for the bottom line.

The structural rules for agents is

$$\frac{A \vdash_Q q}{1 \vdash_Q q}\ Agent$$

By the $\odot_Q$ operation and validity, the top lime sequent means $f^Q_A(1) \leq q$, by the multiplication inequality eq. (2.1) we have $1 \leq f^Q_A(1)$, so by transitivity we get $1 \leq q$, which is what we want for the bottom line sequent.

4.1.2 Soundness of the M-System

The formulae of the M-system, are called M-formulae and are generated by the following syntax

$$m ::= s \mid p \mid \top \mid m \wedge m \mid \bot \mid m \vee m \mid f^M_A(m) \mid \Box^M_A\, m \mid m \,.\, q \mid [q]m$$

A sequence in this system is called an M*-sequence*. It is denoted by Γ and is a list of propositions, actions, and agents

$$\Gamma \in (L_M \cup L_Q \cup \mathcal{A})^*$$

with L_M is the set of all M-formulae, L_Q the set of all Q-formulae and $\mathcal{A}$, as before, set of all agents. Sequences that contain only propositions are denoted by Γ_M, sequences that contain only agents are denoted by Γ_A, and same as in the Q-system, sequences of only actions are denoted by Γ_Q.

Sequents of this system are called M*-sequents*. They are denoted as $\Gamma \vdash_M m$ where m is a single proposition $m \in L_M$ and Γ is a sequence. The empty sequence on the left hand side is the unit of conjunction, that is $\top$. So a sequent with an empty sequence on the left hand side $\vdash_M m$ means $\top \vdash_M m$. Here we can have an empty sequence on the right because it corresponds to the unit of $\vee$, which is $\bot$. So we have that $\Gamma \vdash_M$ means $\Gamma \vdash_M \bot$.

Meaning of a Sequence. We assign *meaning* to the sequences of an M-system via the following operation

$$- \odot_M - : L_M \times (L_M \cup L_Q \cup L_{\mathcal{A}}) \to L_M$$

which similar to the Q-system is defined as

$$\begin{aligned} m \odot_M m' &= m \wedge m' \\ m \odot_M A &= f_A^M(m) \\ m \odot_M q &= m.q \end{aligned}$$

This operation is applied to sequences inductively, for example a sequence

$$\Gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n)$$

has the following meaning[4]

$$\odot_M \Gamma = (((\top \odot_M \gamma_1) \odot_M \gamma_2) \cdots \odot_M \gamma_n)$$

This operation enables us to identify a sequence of M-formulae Γ with only one M-formula $\odot\Gamma \in L_M$. For example $\Gamma = (m, A, q, B, m')$ has the following meaning

$$\odot_M \Gamma = (((((\top \odot_M m) \odot_M A) \odot_M q) \odot_M B) \odot_M m') = f_B^M((f_A^M(m).q)) \wedge m'$$

By adding the unit of conjunction to the left of the sequence, we identify a sequence of only one agent $\Gamma = A$ with the appearance of that agent of top of the module, which is the unit of conjunction $\odot_M \Gamma = f_A^M(\top)$. Similarly a sequence of only action $\Gamma = q$ is identified with the update of the top of

[4]Here, we abuse the notation and use the same symbol $\odot_M$ for meaning of a sequence; in [7] we use the slightly different symbol of $\bigodot_M$.

module with that action $\odot_M \Gamma = \top.q$.

Interpretation. Given a distributive epistemic system $(M, Q, \{f_A\}_{A\in\mathcal{A}})$ and its quantale interpretation map $\alpha\colon L_Q \to Q$, we define a module interpretation map β from the M-formulae to the module part of the epistemic system as follows:

$$\beta : L_M \to M$$

This maps assigns an element of the module $\beta(m)$ to each M-formula m. In order to interpret a sequent Γ, we first apply $\odot_M$, and then the β map. For example the interpretation of a sequence like $\Gamma = m, A$ and will be $\beta(\odot(m, A)) = \beta(f_A^M(m))$, and similarly the interpretation of $\Gamma = m, q$ will be $\beta(\odot(m, q)) = \beta(m.q)$. This composition is well-defined since we have:

$$\beta \circ \odot : (L_M \cup L_Q \cup \mathcal{A})^* \to L_M \to M$$

The β map has the usual structure-preserving properties:

$$\beta(\bot) = \bot \quad \text{and} \quad \beta(\top) = \top$$

and for the join and meet connectives we have

$$\beta(m) \vee \beta(m') = \beta(m \vee m') \quad \text{and} \quad \beta(m) \wedge \beta(m') = \beta(m \wedge m')$$

and also

$$\beta(f_A^M(m)) = f_A^M(\beta(m)) \quad \text{and} \quad \beta(\Box_A^M\, m) = \Box_A^M\, \beta(m)$$

But moreover we have the following two for the mixed operations between quantale and module

$$\beta(m.q) = \beta(m).\alpha(q) \quad \text{and} \quad \beta([q]m) = [\alpha(q)]\beta(m)$$

where α is the interpretation map between the Q-system and the quantale.

Definition 4.1.4 For a distributive epistemic system $(M, Q, \{f_A\}_{A\in\mathcal{A}})$, its interpretation maps $\alpha\colon L_Q \to Q, \beta\colon L_M \to M$, an M-sequence Γ, and an M-formula m', we define a satisfaction relation as follows

$$\Gamma \models_M m' \quad \text{iff} \quad \beta(\odot_M \Gamma) \leq \beta(m')$$

Definition 4.1.5 A sequent $\Gamma \vdash_M m'$ is valid whenever for any distributive epistemic system $(M, Q, \{f_A\}_{A\in\mathcal{A}})$ and its interpretation maps $\alpha\colon L_Q \to Q, \beta\colon L_M \to M$ we have $\Gamma \models_M m'$.

Lemma 4.1.6 *Every derivable M-sequent is valid.*

Proof. We prove that the rules of our M-system preserve validity of sequents by showing that if the

sequents on the top line of a rule are valid (this includes validity of the Q-sequents of the mixed rules), so are the sequents on the bottom of the line.

Before starting the proof, we make the same convention as in the Q-systems, to avoid repeating the proof steps: the interpretation of each M-formula is denoted by the formula itself. That is, we write m instead of $\beta(m)$. We start our proof with the axiom and rules for units, which are as follows:

$$\frac{}{m \vdash_M m}\ id \qquad \frac{}{\bot \vdash_M m}\ \bot L \qquad \frac{\Gamma \vdash_M}{\Gamma \vdash_M \bot}\ \bot R \qquad \frac{}{\Gamma \vdash_M \top}\ \top R$$

Soundness of the identity axiom follows by reflexivity of order on the module $m \leq m$. The left rule for $\bot$ is sound since $\bot$ is less than every other element of the module $\bot \leq m$. The right rule for $\bot$ follows by the definition of empty sequence on the right hand side, which is $\bot$ itself. The right rule for $\top$ follows by $\top$ being the top element of the module, that is every other element is less than it $\odot_M \Gamma \leq \top$. There is no need to state a left rule for $\top$, which would be

$$\frac{\Gamma, \Gamma' \vdash_M m}{\Gamma, \top, \Gamma' \vdash_M m}\ \top L$$

since it is derivable from the weakening rule of the module, to be discussed below. The rules for disjunction are

$$\frac{\Gamma, m_1, \Gamma' \vdash_M m \quad \Gamma, m_2, \Gamma' \vdash_M m}{\Gamma, m_1 \vee m_2, \Gamma'}\ \vee L \qquad \frac{\Gamma \vdash_M m_1}{\Gamma \vdash_M m_1 \vee m_2}\ \vee R1 \qquad \frac{\Gamma \vdash_M m_2}{\Gamma \vdash_M m_1 \vee m_2}\ \vee R1$$

For the left rule we have $\odot_M(\Gamma, m_1, \Gamma') \leq m$ and $\odot_M(\Gamma, m_2, \Gamma') \leq m$, from which we obtain $\odot_M(\Gamma, m_1, \Gamma') \vee \odot_M(\Gamma, m_2, \Gamma') \leq m$ by definition of join in the module. First consider the case where Γ' contains only propositions, so we have

$$\odot_M(\Gamma, m_1, \Gamma') \vee \odot_M(\Gamma, m_2, \Gamma') = (\odot_M \Gamma \wedge m_1 \wedge \odot_M \Gamma') \vee (\odot_M \Gamma \wedge m_2 \wedge \Gamma')$$

By distributivity of meet over join we obtain

$$\odot_M \Gamma \wedge (m_1 \vee m_2) \wedge \odot_M \Gamma' \leq m$$

and thus $\odot_M(\Gamma, m_1 \vee m_2, \Gamma') \leq m$, that is the bottom line. Now consider the case where Γ is an agent-only sequence and without loss of generality contains only one agent A. Then we have

$$\odot_M(\Gamma, m_1, A) \vee \odot_M(\Gamma, m_2, A) = f_A(\odot_M \Gamma \wedge m_1) \vee f_A(\odot_M \Gamma \wedge m_2)$$

By join-preservation of f_A and distributivity of meet over join we obtain the following

$$f_A((\odot_M \Gamma \wedge m_1) \vee (\odot_M \Gamma \wedge m_2)) = f_A(\odot_M \Gamma \wedge (m_1 \vee m_2)) \leq m$$

and thus it follows that $\odot_M(\Gamma, m_1 \vee m_2, A) \leq m$. Finally, consider the case that Γ' is an action-only sequence. In this case we have

$$\odot_M(\Gamma, m_1, \Gamma) \vee \odot_M(\Gamma, m_2, \Gamma) = ((\odot_M \Gamma \wedge m_1) \cdot \odot_Q \Gamma') \vee ((\odot_M \Gamma \wedge m_2) \cdot \odot_Q \Gamma')$$

By join-preservation of $\cdot$ and distributivity of meet over join we obtain the following

$$((\odot_M \Gamma \wedge m_1) \vee (\odot_M \Gamma \wedge m_2)) \cdot \odot_Q \Gamma' = (\odot_M \Gamma \wedge (m_1 \vee m_2)) \cdot \odot_Q \Gamma' \leq m$$

This it follows that $\odot_M(\Gamma, m_1 \vee m_2, \Gamma') \leq m$. The soundness of cases where Γ' is a mixture of actions, agents, and propositions follows from the above three cases.

For the first (and similarly second) right rule assume $\odot_M \Gamma \leq m_1$ then by definition of join in the module we have $m_1 \leq m_1 \vee m_2$ and thus it follows that $\odot_M \Gamma \leq m_1 \vee m_2$.

The rules for conjunction are

$$\frac{\Gamma, m_1, \Gamma' \vdash_M m}{\Gamma, m_1 \wedge m_2, \Gamma' \vdash_M m} \wedge L1 \qquad \frac{\Gamma, m_2, \Gamma' \vdash_M m}{\Gamma, m_1 \wedge m_2, \Gamma' \vdash_M m} \wedge L2 \qquad \frac{\Gamma \vdash_M m_1 \quad \Gamma \vdash_M m_2}{\Gamma \vdash_M m_1 \wedge m_2} \wedge R$$

For the first (and similarly the second) left rule assume $\odot_M(\Gamma, m_1, \Gamma') \leq m$, since $m_1 \wedge m_2 \leq m_1$ and $\odot_M$ is order preserving we obtain $\odot_M(\Gamma, m_1 \wedge m_2, \Gamma') \leq m$. For the right rule assume $\odot_M \Gamma \leq m_1$ and $\odot_M \Gamma \leq m_2$, from this by the definition of meet we obtain $\odot_M \Gamma \leq m_1 \wedge m_2$.

The rules for appearance maps are

$$\frac{m', A, \Gamma \vdash_M m}{f^M_A(m'), \Gamma \vdash_M m} f^M_A L \qquad \frac{\Gamma \vdash_M m}{\Gamma, A \vdash_M f^M_A(m)} f^M_A R$$

For the left rule observe that the sequences of the top and bottom lines have the same meanings, that is $\odot_M(f^M_A(m'), \Gamma)$. The right rule follows by order preservation of appearance maps, if $\odot_M \Gamma \leq m$ then we can apply f^M_A to both sides and get $f^M_A(\odot_M \Gamma) \leq f^M_A(m)$ and thus the bottom sequent.

Rules for the knowledge modality on the module are

$$\frac{m', \Gamma \vdash_M m}{\Box^M_A m', A, \Gamma \vdash_M m} \Box^M_A L \qquad \frac{\Gamma, A \vdash_M m}{\Gamma \vdash_M \Box^M_A(m)} \Box^M_A R$$

For the left rule, assume the top line, which is $\odot_M(m', \Gamma) \leq m$. By composition of adjoints f^M_A and $\Box^M_A$ we have $f^M_A(\Box^M_A m') \leq m'$. Since $\cdot$, f^M_A and $\wedge$ are all order preserving, we apply $\odot_M$ with Γ to both sides and get $\odot_M(f^M_A(\Box^M_A m'), \Gamma) \leq \odot_M(m', \Gamma)$. By the top line assumption and transitivity we get $\odot_M(f^M_A(\Box^M_A m'), \Gamma) \leq m$, which is what we want for the bottom line. The right rule follows directly from the definition of adjunction. By the top line we have $f^M_A(\odot_M \Gamma) \leq m$, which is by adjunction equivalent to $\odot_M \Gamma \leq \Box^M_A m$. Similar to the knowledge rule in the Q-system, this rule is also true on the other direction, that is the bottom line also implies the top line.

The cut rule for the M-system is as follows

$$\frac{\Gamma' \vdash_M m' \qquad m', \Gamma'' \vdash_M m}{\Gamma', \Gamma'' \vdash_M m} \; cut$$

By the first assumption we have $\odot_M \Gamma' \leq m'$, from which we obtain $\odot_M(\odot_M \Gamma', \Gamma'') \leq \odot_M(m, \Gamma'')$ by order preservation of $\odot_M$. By the second assumption we have $\odot_M(m, \Gamma'') \leq m'$ and thus by transitivity $\odot_M(\odot_M \Gamma', \Gamma'') \leq m'$, which is what we want for the bottom line.

The rule for factual propositions is

$$\frac{\Gamma \vdash_M p}{\Gamma, q \vdash_M p} \; fact$$

The validity of the top line sequent says $\odot_M \Gamma \leq p$, we update both sides with q and we get $\odot_M \Gamma \,.\, q \leq p \,.\, q$, by the definition of facts we have that $p \,.\, q \leq p$, and by transitivity we get $\odot_M \Gamma \,.\, q \leq p$, which is what we want for the validity of the bottom line sequent.

Other structural rules of the module are

$$\frac{\Gamma, \Gamma' \vdash m}{\Gamma, m', \Gamma' \vdash_M m} \; weakL \qquad\qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash_M m} \; weakR$$

$$\frac{\Gamma, m', m', \Gamma' \vdash_M m}{\Gamma, m', \Gamma' \vdash_M m} \; contr \qquad\qquad \frac{\Gamma, m'', m', \Gamma' \vdash_M m}{\Gamma, m', m'', \Gamma' \vdash_M m} \; exch$$

For the left weakening assume the top line, that is $\odot_M(\odot_M \Gamma, \Gamma') \leq m$. Since $\odot_M \Gamma \wedge m' \leq \odot_M \Gamma$ and $\odot_M$ is order preserving, we obtain $\odot_M(\odot_M \Gamma \wedge m', \Gamma') \leq m$, that is the bottom line. The right weakening follows since $\odot_M \Gamma \leq \bot$ is equivalent to $\odot_M \Gamma = \bot$ and $\bot \leq m$. Contraction is sound since we have $\odot_M \Gamma \wedge m' \wedge m' = \odot_M \Gamma \wedge m'$ and $\odot_M$ is order preserving. Exchange follows by commutativity of meet $m'' \wedge m' = m' \wedge m''$ and order preservation of $\odot_M$.

The rules for epistemic update are

$$\frac{m', q, \Gamma \vdash_M m}{m'.q, \Gamma \vdash_M m} \; .L \qquad\qquad \frac{\Gamma, \Gamma_A \vdash_M m \quad \Gamma_Q, \Gamma_A \vdash_Q q}{\Gamma, \Gamma_Q, \Gamma_A \vdash_M m.q} \; .R$$

The left rule follows from the definition of comma between a proposition and an action $m', q = m'.q$ and order preservation of $\odot_M$. For the right rule, first assume that we have only one agent in our agent context, that is $\Gamma_A = A$. By the first assumption of the top line we have $f^M_A(\odot_M \Gamma) \leq m$ and by the second assumption we have $f^Q_A(\odot_Q \Gamma_Q) \leq q$. Since update is order preserving, we can update both sides of these two assumption by each other and get $f^M_A(\odot_M \Gamma).f^Q_A(\odot_Q \Gamma_Q) \leq m.q$. Now by update inequality we have $f^M_A(\odot_M \Gamma. \odot_Q \Gamma_Q) \leq f^M_A(\odot_M \Gamma).f^Q_A(\odot_Q \Gamma_Q) \leq m.q$, which is what we want for the bottom line and we are done. If we have more than one agent, that is $\Gamma_A = A_1, \ldots, A_n$, then we follow the same line except that we have to apply the update inequality n times, starting from the

innermost agent A_1 to the outmost one A_n, that is

$$f^M_{A_n}(f^M_{A_{n-1}}(\dots f^M_{A_1}(\odot_M \Gamma \,.\, \odot_Q \Gamma_Q))) \leq m \,.\, q$$

The rules for dynamic modality are

$$\frac{m' \vdash_M m \quad \Gamma_Q \vdash_Q q}{[q]m', \Gamma_Q \vdash_M m}\ DyL \qquad\qquad \frac{\Gamma, q \vdash_M m}{\Gamma \vdash_M [q]m}\ DyR$$

For the left rule start from the second assumption $\odot_Q \Gamma_Q \leq q$, since update is order preserving, this inequality is preserved under update of the proposition $[q]m'$ as follows

$$[q]m' \cdot \odot_Q \Gamma_Q \leq [q]m' \cdot q$$

By adjunction between update and dynamic modality we have $[q]m' \,.\, q \leq m'$, and thus

$$[q]m' \cdot \odot_Q \Gamma_Q \leq m'$$

now by the first assumption of the top line we have $m' \leq m$ and by transitivity we get

$$[q]m' \cdot \odot_Q \Gamma_Q \leq m$$

which is exactly what we want for the bottom line. The right rule follows directly by definition of adjunction. The top line assumption says $\odot_M \Gamma \,.\, q \leq m$, which by adjunction is equivalent to $\odot_M \Gamma \leq [q]m$, which is the bottom line. This rule holds in both direction.

We now prove the soundness of the rules that deal with occurrences of actions in the M-sequences. Recall that actions can only occur on the left hand side of M-sequents, so we have left rules for all the operations on actions, including the unit of sequential composition. The rule for update with unit of sequential composition in the M-system is

$$\frac{\Gamma, \Gamma' \vdash_M m}{\Gamma, 1, \Gamma' \vdash_M m}\ 1ML$$

By unity of 1 we have $\odot_M \Gamma.1 = \odot_M \Gamma$, and thus $\odot_M(\Gamma, \Gamma') = \odot_M((\odot_M \Gamma.1), \Gamma')$. So by the top line assumption and transitivity we get $\odot_M((\odot_M \Gamma.1), \Gamma') \leq m$.

The rule for update with sequential composition of actions in the module is

$$\frac{\Gamma, q_1, q_2, \Gamma' \vdash_M m}{\Gamma, q_1 \bullet q_2, \Gamma' \vdash_M m}\ \bullet ML$$

The top line assumption means $\odot_M(((\odot_M\Gamma\,.\,q_1)\,.\,q_2),\Gamma') \leq m$, by module equation we have

$$(\odot_M\Gamma\,.\,q_1)\,.q_2 = \odot_M\Gamma\,.\,(q_1 \bullet q_2)$$

and so we get $\odot_M(\odot_M\Gamma\,.\,(q_1 \bullet q_2),\Gamma') \leq m$, which is the meaning of the bottom line.

The rules for update with right and left residuals in the M-sequents are

$$\frac{\Gamma_Q \vdash_Q q_2 \quad \Gamma, q_1 \vdash_M m}{\Gamma, q_1/q_2, \Gamma_Q \vdash_M m}\ /ML \qquad\qquad \frac{\Gamma_Q \vdash_Q q_1 \quad \Gamma, q_2 \vdash_M m}{\Gamma, \Gamma_Q, q_1 \setminus q_2 \vdash_M m}\ \setminus ML$$

For the right residual we have two top line assumptions: $\odot_Q\Gamma_Q \leq q_2$ and $\odot_M\Gamma.q_1 \leq m$. Start from the first assumption $\odot_Q\Gamma_Q \leq q_2$ and compose both sides with q_1 on the left and we get $q_1 \bullet \odot_Q\Gamma_Q \leq q_1 \bullet q_2$, which is by residuation equal to $q_1/q_2 \bullet \odot_Q\Gamma_Q \leq q_1$. Now update the propositional sequent $\odot_M\Gamma$ with this inequality and we get $\odot_M\Gamma\,.\,(q_1/q_2 \bullet \odot_Q\Gamma_Q) \leq \odot_M\Gamma\,.\,q_1$. By the second assumption of the top line $\odot_M\Gamma\,.\,q_1 \leq m$ and so by transitivity we have $\odot_M\Gamma\,.\,(q_1/q_2 \bullet \odot_Q\Gamma_Q) \leq m$. By the module equation this inequality is equivalent to $(\odot_M\Gamma\,.\,q_1/q_2)\,.\,\odot_M\Gamma_Q \leq m$. Since we have $(\odot_M\Gamma\,.\,q_1/q_2)\,.\,\odot_M\Gamma_Q = \odot_M(\Gamma, q_1/q_2, \Gamma_Q)$, we obtain $\odot_M(\Gamma, q_1/q_2, \Gamma_Q) \leq m$, which is what we need for the bottom line.

The proof of the left residual is similar, we start by the first assumption of the top line $\odot_Q\Gamma_Q \leq q_1$ and compose it on both sides with q_2 on the right and we get $\odot_Q\Gamma_Q \bullet q_2 \leq q_1 \bullet q_2$, which is by residuation equal to $\odot_Q\Gamma_Q \bullet q_1 \setminus q_2 \leq q_2$, now update both sides with the propositional context $\odot_M\Gamma$ on the left and we get $\odot_M\Gamma\,.\,(\odot_Q\Gamma_Q \bullet q_1 \setminus q_2) \leq \odot_M\Gamma\,.\,q_2$. By module equation this is equivalent to $(\odot_M\Gamma\,.\,\odot_Q\Gamma_Q)\,.\,q_1 \setminus q_2 \leq \odot_M\Gamma\,.\,q_2$. Now we use the second assumption of the first line that says $\odot_M\Gamma\,.\,q_2 \leq m$ and by transitivity of order we get $(\odot_M\Gamma\,.\,\odot_Q\Gamma_Q)\,.\,q_1 \setminus q_2 \leq m$, which is what we want for the bottom line, since $\odot_M(\Gamma, \Gamma_Q, q_1 \setminus q_2) = (\odot_M\Gamma\,.\,\odot_Q\Gamma_Q)\,.\,q_1 \setminus q_2$.

The rule for update with choice of actions in M-sequents is

$$\frac{\Gamma, q_1 \vdash_M m \qquad \Gamma, q_2 \vdash_M m}{\Gamma, q_1 \vee q_2 \vdash_M m}\ \vee ML$$

Assume the top line sequents: $\odot_M\Gamma.q_1 \leq m$ and $\odot_M\Gamma.q_2 \leq m$. By definition of join we obtain $(\odot_M\Gamma\,.\,q_1) \vee (\odot_M\Gamma\,.\,q_2) \leq m$. Since update is join preserving we get $(\odot_M\Gamma\,.\,q_1) \vee (\odot_M\Gamma\,.\,q_2) = \odot_M\Gamma\,.\,(q_1 \vee q_2)$, so $\odot_M\Gamma\,.\,(q_1 \vee q_2) \leq m$, which is what we want for the bottom line.

We have two left rules for update with meet of actions

$$\frac{\Gamma, q_1, \Gamma' \vdash_M m}{\Gamma, q_1 \wedge q_2, \Gamma' \vdash_M m}\ \wedge ML1 \qquad\qquad \frac{\Gamma, q_2, \Gamma' \vdash_M m}{\Gamma, q_1 \wedge q_2, \Gamma' \vdash_M m}\ \wedge ML2$$

For the left rule, assume the top sequent, that is $\odot_M((\odot_M\Gamma.q_1),\Gamma') \leq m$. Since $q_1 \wedge q_2 \leq q_1$ and $\odot_M$ is order preserving, we obtain $\odot_M((\odot_M\Gamma.(q_1 \wedge q_2)),\Gamma') \leq m$, which is what we want for the bottom line. The second line is proven in the same way.

Theorem 4.1.7 *The rules of* IDEAL *are sound with respect to the algebraic semantics in terms of distributive epistemic systems.*

Proof follows directly from lemmas 4.1.3 and 4.1.6. □

4.2 Completeness

We provide two lemmas for the completeness of the Q and M systems, starting with the Q system.

4.2.1 Completeness of the Q-system

Lemma 4.2.1 If a sequent is valid in the quantale part of all distributive epistemic systems, then it is derivable in the Q-system.

Proof. We show the contrapositive by building the Lindenbaum-Tarski algebra of the Q-formulae, and showing that it satisfies all the properties of the quantale of a distributive epistemic system. The construction is by forming the equivalence class of all Q-formulae over the logical consequence $\cong_Q$ defined as $\vdash_Q \dashv$. We denote this set of all these equivalence classes by Q_0, so we have $Q_0 = Q \backslash \cong_Q$. The proof proceeds as follows:

1. We interpret the Q-formulae in our model Q_0 by mapping them to their corresponding equivalence classes. Thus we have to first show that this interpretation is well-defined.

2. We define an order $\leq$ between these equivalence classes, using the provability of the Q-system and check that this order is well-defined and a partial order.

3. We show that the $(Q_0, \leq)$ has a least and a greatest element, that is a top and a bottom.

4. We define meet and join operators in $(Q_0, \leq)$ and show that it forms a lattice (not a complete one yet).

5. Similarly we define a unital monoid multiplication and show that it satisfies the finite versions of equations of a quantale, that is preservation of binary joins instead of arbitrary joins.

6. We define endomorphisms on Q_0 and show that these satisfy the finite versions of the equations of the appearance maps, that is preservation of binary joins. We call our endowed Q_0 a *pre-epistemic* quantale, since it does not have arbitrary joins.

7. Finally we extend our finite model Q_0 to the infinite case Q by the ideal construction [28, 17] on Q_0.

4.2.2 Proof of the Finitary Case

Interpretation and Order We map each formula of our Q-system to its equivalence class in Q_0, that is

$$\alpha : L_Q \to Q_0 \quad \text{where} \quad \alpha(q) = [q]$$

We define an order between the equivalence classes of Q_0, using the logical consequence of the Q-system as follows

$$[q] \leq [q'] \quad \text{iff} \quad q \vdash_Q q'$$

we have to show that this order is well-defined. That is we have to show

$$[q_1] = [q_1'] \text{ and } [q_2] = [q_2'] \text{ and } [q_1] \leq [q_2] \quad \text{implies} \quad [q_1'] \leq [q_2']$$

which is equivalent to show the following

$$q_1 \vdash_Q \dashv q_1' \text{ and } q_2 \vdash_Q \dashv q_2' \text{ and } q_1 \vdash_Q q_2 \quad \text{implies} \quad q_1' \vdash_Q q_2'$$

the proof tree for which is

$$\dfrac{q_1' \vdash_Q q_1 \qquad \dfrac{q_1 \vdash_Q q_2 \quad q_2 \vdash_Q q_2'}{q_1 \vdash_Q q_2'}\, QCut}{q_1' \vdash_Q q_2'}\, QCut$$

We also have to show that our order is a partial order. The reflexivity $[q_1] \leq [q_1]$ follows by the identity axiom $q_1 \vdash_Q q_1$. The transitivity says if $[q_1] \leq [q_2]$ and $[q_2] \leq [q_3]$ then $[q_1] \leq [q_3]$, which follows from the cut rule

$$\dfrac{q_1 \vdash_Q q_2 \quad q_2 \vdash_Q q_3}{q_1 \vdash_Q q_3}\, QCut$$

The anti-symmetry says if $[q_1] \leq [q_2]$ and $[q_2] \leq [q_1]$ then $[q_1] = [q_2]$, which follows directly from our equivalence, that is $q_1 \cong_Q q_2$ is defined as $q_1 \vdash_Q q_2$ and $q_2 \vdash_Q q_1$. Thus we have proved that $(Q_0, \leq)$ is a partial order.

Greatest and Least Elements. We have to show that $(Q_0, \leq)$ has a bottom element $[\bot]$, which is less than any other element $[q] \in Q_0$, that is we have to show $[\bot] \leq [q]$, which follows by the $\bot L$ axiom

$$\dfrac{}{\bot \vdash_Q q}\, \bot L$$

Similarly we have to show that $(Q_0, \leq)$ has a top element $[\top]$, greater than any other element $[q] \leq [\top]$, which follows by the $\top$ right axiom

$$\dfrac{}{q \vdash \top}\, \top R$$

Join and Meet. We define join and meet operations on $(Q_0, \leq)$ using the disjunction and conjunction

of the Q-system as follows

$$[q] \vee [q'] := [q \vee q'] \quad \text{and} \quad [q] \wedge [q'] := [q \wedge q']$$

We show that these definitions are well-defined, that is

$$[q_1] = [q_1'] \text{ and } [q_2] = [q_2'] \quad \text{imply} \quad [q_1 \vee q_2] = [q_1' \vee q_2']$$

and similarly for meet as follows

$$[q_1] = [q_1'] \text{ and } [q_2] = [q_2'] \quad \text{imply} \quad [q_1 \wedge q_2] = [q_1' \wedge q_2']$$

For each case we have four assumptions $q_1 \vdash_Q q_1', q_1' \vdash_Q q_1$ and also $q_2 \vdash_Q q_2'$ and $q_2' \vdash_Q q_2$ and we have to prove two directions. So for the first case, i.e. well-definedness of join, we have to show that firstly $q_1 \vee q_2 \vdash_Q q_1' \vee q_2'$ and also $q_1' \vee q_2' \vdash_Q q_1 \vee q_2$, using our four assumptions: $q_1 \vdash_Q q_2,\ q_2 \vdash_Q q_1$ and $q_1' \vdash_Q q_2',\ q_2' \vdash_Q q_1'$. The proof trees for these are

$$\dfrac{\dfrac{\dfrac{q_1 \vdash_Q q_1'}{q_1 \vdash_Q q_1' \vee q_2'} \vee R1 \qquad \dfrac{q_2 \vdash_Q q_2'}{q_2 \vdash_Q q_1' \vee q_2'} \vee R2}{q_1 \vee q_2 \vdash_Q q_1' \vee q_2'} \vee L \qquad \dfrac{\dfrac{\dfrac{q_1' \vdash_Q q_1}{q_1' \vdash_Q q_1 \vee q_2} \vee R1 \qquad \dfrac{q_2' \vdash_Q q_2}{q_2' \vdash_Q q_1 \vee q_2} \vee R2}{q_1' \vee q_2' \vdash_Q q_1 \vee q_2} \vee L$$

The proof trees for the second case, i.e. well-definedness of meet are similar, except that we first do the right rules and then the left rules. That is:

$$\dfrac{\dfrac{\dfrac{q_1 \vdash_Q q_1'}{q_1 \wedge q_2 \vdash_Q q_1'} \wedge L1 \qquad \dfrac{q_2 \vdash_Q q_2'}{q_1 \wedge q_2 \vdash_Q q_2'} \wedge L2}{q_1 \wedge q_2 \vdash_Q q_1' \wedge q_2'} \wedge R \qquad \dfrac{\dfrac{\dfrac{q_1' \vdash_Q q_1}{q_1' \wedge q_2' \vdash_Q q_1} \wedge L1 \qquad \dfrac{q_2' \vdash_Q q_2}{q_1' \wedge q_2' \vdash_Q q_2} \wedge L2}{q_1' \wedge q_2' \vdash_Q q_1 \wedge q_2} \wedge R$$

Multiplication. Now we extend our lattice to a quantale by defining a multiplication operator on our Q_0 using the sequential composition of the Q-system

$$[q] \bullet [q'] := [q \bullet q']$$

We have to show that this definition is well-defined, that is

$$\text{If} \quad [q_1] = [q_1'] \quad \text{and} \quad [q_2] = [q_2'] \quad \text{then} \quad [q_1 \bullet q_2] = [q_1' \bullet q_2']$$

The proof trees for these are

$$\dfrac{\dfrac{q_1 \vdash_Q q_1' \qquad q_2 \vdash_Q q_2'}{q_1, q_2 \vdash_Q q_1' \bullet q_2'} \bullet R}{q_1 \bullet q_2 \vdash_Q q_1' \bullet q_2'} \bullet L \qquad \dfrac{\dfrac{q_1' \vdash_Q q_1 \qquad q_2' \vdash_Q q_2}{q_1', q_2' \vdash_Q q_1 \bullet q_2} \bullet R}{q_1' \bullet q_2' \vdash_Q q_1 \bullet q_2} \bullet L$$

The unit of this multiplication is the equivalence class of the unit of sequential composition in the Q-system, that is $[1]$ for which we have to show the following two cases

$$[q] \bullet [1] = [q] \qquad \text{and} \qquad [1] \bullet [q] = [q]$$

which are equal to the following by definition of multiplication on Q_0

$$[q \bullet 1] = [q] \qquad \text{and} \qquad [1 \bullet q] = [q]$$

In terms of logical consequence we have to show

$$q \bullet 1 \vdash_Q \dashv q \qquad \text{and} \qquad 1 \bullet q \vdash_Q \dashv q$$

The proof trees for the first case are

$$\dfrac{\dfrac{}{q, 1 \vdash_Q q}\, 1L}{q \bullet 1 \vdash_Q q}\, \bullet L \qquad\qquad \dfrac{q \vdash_Q q \quad \dfrac{}{\vdash_Q 1}\, 1R}{q \vdash_Q q \bullet 1}\, \bullet R$$

The other permutation has similar proof trees.

Now we have to show that this multiplication preserves joins, that is

$$([q_1] \vee [q_2]) \bullet [q_3] = ([q_1] \bullet [q_3]) \vee ([q_2] \bullet [q_3]) \quad \text{and} \quad [q_1] \bullet ([q_2] \vee [q_3]) = ([q_1] \bullet [q_2]) \vee ([q_2] \bullet [q_3])$$

which is equal to the following by definition of join and multiplication on Q_0

$$[(q_1 \vee q_2) \bullet q_3] = [(q_1 \bullet q_3) \vee (q_2 \bullet q_3)] \quad \text{and} \quad [q_1 \bullet (q_2 \vee q_3)] = [(q_1 \bullet q_2) \vee (q_2 \bullet q_3)]$$

In logical consequence terms we have to prove the following

$$(q_1 \vee q_2) \bullet q_3 \vdash_Q \dashv (q_1 \bullet q_3) \vee (q_2 \bullet q_3) \quad \text{and} \quad q_1 \bullet (q_2 \vee q_3) \vdash_Q \dashv (q_1 \bullet q_2) \vee (q_2 \bullet q_3)$$

The proof of join-preservation of multiplication on its left argument consists of two directions: $(q_1 \vee q_2) \bullet q_3 \vdash_Q (q_1 \bullet q_3) \vee (q_2 \bullet q_3)$ and $(q_1 \bullet q_3) \vee (q_2 \bullet q_3) \vdash_Q (q_1 \vee q_2) \bullet q_3$. The proof tree for the first direction is

$$\dfrac{\dfrac{\dfrac{\dfrac{q_1 \vdash_Q q_1 \quad q_3 \vdash_Q q_3}{q_1, q_3 \vdash_Q q_1 \bullet q_3}\, \bullet R}{q_1, q_3 \vdash_Q (q_1 \bullet q_3) \vee (q_2 \bullet q_3)}\, \vee R1 \qquad \dfrac{\dfrac{q_2 \vdash_Q q_2 \quad q_3 \vdash_Q q_3}{q_2, q_3 \vdash_Q q_2 \bullet q_3}\, \bullet R}{q_2, q_3 \vdash_Q (q_1 \bullet q_3) \vee (q_2 \bullet q_3)}\, \vee R2}{q_1 \vee q_2, q_3 \vdash_Q (q_1 \bullet q_3) \vee (q_2 \bullet q_3)}\, \vee L}{(q_1 \vee q_2) \bullet q_3 \vdash_Q (q_1 \bullet q_3) \vee (q_2 \bullet q_3)}\, \bullet L$$

The proof tree for the second direction is

$$\dfrac{\dfrac{\dfrac{\dfrac{q_1 \vdash_Q q_1}{q_1 \vdash_Q q_1 \vee q_2}\vee R1 \qquad q_3 \vdash_Q q_3}{q_1, q_3 \vdash_Q (q_1 \vee q_2) \bullet q_3}\bullet R}{q_1 \bullet q_3 \vdash_Q (q_1 \vee q_2) \bullet q_3}\bullet L \qquad \dfrac{\dfrac{\dfrac{\dfrac{q_2 \vdash_Q q_2}{q_2 \vdash_Q q_1 \vee q_2}\vee R2 \qquad q_3 \vdash_Q q_3}{q_2, q_3 \vdash_Q (q_1 \vee q_2) \bullet q_3}\bullet R}{q_2 \bullet q_3 \vdash_Q (q_1 \vee q_2) \bullet q_3}\bullet L}{(q_1 \bullet q_3) \vee (q_2 \bullet q_3) \vdash_Q (q_1 \vee q_2) \bullet q_3}\vee L$$

The proofs for join preservation of multiplication on its second argument are similar. We also have to show that our multiplication preserves the empty join, that is

$$[\bot] \bullet [q] = [\bot] \qquad \text{and} \qquad [q] \bullet [\bot] = [\bot]$$

which by definition of multiplication on Q_0 is equivalent to

$$[\bot \bullet q] = [\bot] \qquad \text{and} \qquad [q \bullet \bot] = [\bot]$$

and in logical consequence terms we have to show the following

$$\bot \bullet q \vdash_Q \dashv \bot \qquad \text{and} \qquad q \bullet \bot \vdash_Q \dashv \bot$$

The proof trees for the two directions of this congruence are

$$\dfrac{\dfrac{}{\bot, q \vdash_Q \bot}\bot L}{\bot \bullet q \vdash_Q \bot}\bullet L \qquad\qquad \dfrac{}{\bot \vdash_Q \bot \bullet q}\bot L$$

The second case is proved similarly.

We have now proved that $(Q_0, \leq, \vee, \wedge, \bullet, 1)$ is a pre-quantale, that is, it satisfies the binary versions of the axioms of a quantale. We verify some details about other connectives below.

Residuals. The residuals of multiplication are defined using the residuals of the Q-system and we have to show their well-definedness, that is for the right residual we have to show

$$\text{If} \quad [q_1] = [q_1'] \quad \text{and} \quad [q_2] = [q_2'] \quad \text{then} \quad [q_1/q_2] = [q_1'/q_2']$$

The proof trees for it are:

$$\dfrac{\dfrac{q_2' \vdash_Q q_2 \qquad q_1 \vdash_Q q_1'}{q_1/q_2, q_2' \vdash_Q q_1'}/L}{q_1/q_2 \vdash_Q q_1'/q_2'}/R \qquad\qquad \dfrac{\dfrac{q_2 \vdash_Q q_2' \qquad q_1' \vdash_Q q_1}{q_1'/q_2', q_2 \vdash_Q q_1}/L}{q_1'/q_2' \vdash_Q q_1/q_2}/R$$

And similarly for the left residual we have to show

$$\text{If} \quad [q_1] = [q_1'] \quad \text{and} \quad [q_2] = [q_2'] \quad \text{then} \quad [q_1 \setminus q_2] = [q_1' \setminus q_2']$$

the proof trees for it are

$$\dfrac{\dfrac{q_1' \vdash q_1 \qquad q_2 \vdash q_2'}{q_1', q_1 \setminus q_2 \vdash_Q q_2'}\setminus L}{q_1 \setminus q_2 \vdash_Q q_1' \setminus q_2'}\setminus R \qquad\qquad \dfrac{\dfrac{q_1 \vdash q_1' \qquad q_2' \vdash q_2}{q_1, q_1' \setminus q_2' \vdash_Q q_2}\setminus L}{q_1' \setminus q_2' \vdash_Q q_1 \setminus q_2}\setminus R$$

We have to show that these residuals are indeed adjoints to multiplication. That is we have to show the following two equations hold:

$$(1)\, [q_1 \bullet q_2] \leq [q_3] \quad \text{iff} \quad [q_1] \leq [q_3/q_2] \quad \text{and} \quad (2)\, [q_1 \bullet q_2] \leq [q_3] \quad \text{iff} \quad [q_2] \leq [q_1 \setminus q_3]$$

The proof for the two sides of the first equations are

$$\dfrac{\dfrac{\dfrac{q_1 \vdash_Q q_1 \quad q_2 \vdash_Q q_2}{q_1, q_2 \vdash_Q q_1 \bullet q_2}\bullet R \qquad q_1 \bullet q_2 \vdash_Q q_3}{q_1, q_2 \vdash_Q q_3}QCut}{q_1 \vdash_Q q_3/q_2}/R \qquad\qquad \dfrac{q_1 \vdash_Q q_3/q_2 \qquad \dfrac{q_2 \vdash_Q q_2 \quad q_3 \vdash_Q q_3}{q_3/q_2, q_2 \vdash_Q q_3}/L}{q_1, q_2 \vdash_Q q_3}QCut}{q_1 \bullet q_2 \vdash_Q q_3}\bullet L$$

The proofs of the second equations are very similar to the first one. Both residuals preserve meet on one of their arguments. So for the right residual we have to show the following

$$[(q_1 \wedge q_2)/q_3] = [(q_1/q_3) \wedge (q_2/q_3)]$$

The proof tree for the first direction of this congruence is

$$\dfrac{\dfrac{\dfrac{q_3 \vdash_Q q_3 \quad \dfrac{q_1 \vdash_Q q_1}{q_1 \wedge q_2 \vdash_Q q_1}\wedge L1}{(q_1 \wedge q_2)/q_3, q_3 \vdash_Q q_1}/L}{(q_1 \wedge q_2)/q_3 \vdash_Q q_1/q_3}/R \qquad \dfrac{\dfrac{q_3 \vdash_Q q_3 \quad \dfrac{q_2 \vdash_Q q_2}{q_1 \wedge q_2 \vdash_Q q_2}\wedge L2}{(q_1 \wedge q_2)/q_3, q_3 \vdash_Q q_2}/L}{(q_1 \wedge q_2)/q_3 \vdash_Q q_2/q_3}/R}{(q_1 \wedge q_2)/q_3 \vdash_Q (q_1/q_3) \wedge (q_2/q_3)}\wedge R$$

The proof tree of the second direction is

$$\dfrac{\dfrac{\dfrac{\dfrac{q_3 \vdash_Q q_3 \quad q_1 \vdash_Q q_1}{q_1/q_3, q_3 \vdash_Q q_1}/L}{(q_1/q_3) \wedge (q_2/q_3), q_3 \vdash_Q q_1}\wedge L1 \qquad \dfrac{\dfrac{q_3 \vdash_Q q_3 \quad q_2 \vdash_Q q_2}{q_2/q_3, q_3 \vdash_Q q_2}/L}{(q_1/q_3) \wedge (q_2/q_3), q_3 \vdash_Q q_2}\wedge L2}{(q_1/q_3) \wedge (q_2/q_3), q_3 \vdash_Q q_1 \wedge q_2}\wedge R}{(q_1/q_3) \wedge (q_2/q_3) \vdash_Q (q_1 \wedge q_2)/q_3}/R$$

For the left residual we have

$$[q_1 \setminus (q_2 \wedge q_3)] = [(q_1 \setminus q_2) \wedge (q_1 \setminus q_3)]$$

The proof of the first direction of the this congruence is

$$\dfrac{\dfrac{\dfrac{q_1 \vdash_Q q_1 \quad \dfrac{q_2 \vdash_Q q_2}{q_2 \wedge q_3 \vdash_Q q_2}\wedge L2}{q_1, q_1 \setminus (q_2 \wedge q_3) \vdash_Q q_2}\setminus L}{q_1 \setminus (q_2 \wedge q_3) \vdash_Q q_1 \setminus q_2}\setminus R \qquad \dfrac{\dfrac{\dfrac{q_1 \vdash_Q q_1 \quad \dfrac{q_3 \vdash_Q q_3}{q_2 \wedge q_3 \vdash_Q q_3}\wedge L2}{q_1, q_1 \setminus (q_2 \wedge q_3) \vdash_Q q_3}\setminus L}{q_1 \setminus (q_2 \wedge q_3) \vdash_Q q_1 \setminus q_3}\setminus R}{q_1 \setminus (q_2 \wedge q_3) \vdash_Q (q_1 \setminus q_2) \wedge (q_1 \setminus q_3)}\wedge R$$

and the proof tree of the second direction is

$$\dfrac{\dfrac{\dfrac{\dfrac{q_1 \vdash_Q q_1 \quad q_2 \vdash_Q q_2}{q_1, q_1 \setminus q_2 \vdash_Q q_2}\setminus L}{q_1, (q_1 \setminus q_2) \wedge (q_1 \setminus q_3) \vdash_Q q_2}\wedge L1 \qquad \dfrac{\dfrac{q_1 \vdash_Q q_1 \quad q_3 \vdash_Q q_3}{q_1, q_1 \setminus q_3 \vdash_Q q_3}\setminus L}{q_1, (q_1 \setminus q_2) \wedge (q_1 \setminus q_3) \vdash_Q q_3}\wedge L2}{q_1, (q_1 \setminus q_2) \wedge (q_1 \setminus q_3) \vdash_Q q_2 \wedge q_3}\wedge R}{(q_1 \setminus q_2) \wedge (q_1 \setminus q_3) \vdash_Q q_1 \setminus (q_2 \wedge q_3)}\setminus R$$

The meet-preservation of the second argument of the left residual is proved similarly. Both residuals preserve the empty meet

$$\top / q \cong_Q \top \qquad \text{and} \qquad q \setminus \top \cong_Q \top$$

The proof trees for the right residual are

$$\dfrac{}{\top / q \vdash_Q \top}\top R \qquad\qquad \dfrac{\dfrac{}{\top, q \vdash_Q \top}\top R}{\top \vdash_Q \top / q}/R$$

and the proof trees for the left residual are

$$\dfrac{}{q \setminus \top \vdash_Q \top}\top R \qquad\qquad \dfrac{\dfrac{}{q, \top \vdash_Q \top}\top R}{\top \vdash_Q q \setminus \top}\setminus R$$

Appearance and Knowledge. We define appearance maps on our quantale $(Q_0, \leq, \vee, \wedge, \bullet, 1)$, using the f_A^Q maps of the Q-system:

$$f_A^Q([q]) := [f_A^Q(q)]$$

and have to show that this definition is well-defined, that is

$$\text{If} \quad [q_1] = [q_1'] \quad \text{then} \quad [f_A^Q(q_1)] = [f_A^Q(q_1')]$$

The proof tree follows:

$$\dfrac{\dfrac{q_1 \vdash_Q q_1'}{q_1, A \vdash_Q f_A^Q(q_1')}\, f_A^Q R}{f_A^Q(q_1) \vdash_Q f_A^Q(q_1')}\, f_A^Q L \qquad \dfrac{\dfrac{q_1' \vdash_Q q_1}{q_1', A \vdash_Q f_A^Q(q_1)}\, f_A^Q R}{f_A^Q(q_1') \vdash_Q f_A^Q(q_1)}\, f_A^Q L$$

The knowledge modality is defined similarly as follows

$$\Box_A^Q\,[q] = [\Box_A^Q\, q]$$

For its well-definedness we have to show

$$\text{If} \quad [q_1] = [q_1'] \quad \text{then} \quad [\Box_A^Q\, q_1] = [\Box_A^Q\, q_1']$$

whose proof trees are

$$\dfrac{\dfrac{q_1 \vdash_Q q_1'}{\Box_A^Q\, q_1, A \vdash q_1'}\, \Box_A^Q L}{\Box_A^Q\, q_1 \vdash_Q \Box_A^Q\, q_1'}\, \Box_A^Q R \qquad \dfrac{\dfrac{q_1' \vdash_Q q_1}{\Box_A^Q\, q_1', A \vdash q_1}\, \Box_A^Q L}{\Box_A^Q\, q_1' \vdash_Q \Box_A^Q\, q_1}\, \Box_A^Q R$$

It remains to show that appearance and knowledge are adjoint, that is

$$[f_A^Q(q)] \leq [q'] \quad \text{iff} \quad [q] \leq [\Box_A^Q\, q']$$

The two proof trees for these follow

$$\dfrac{\dfrac{q \vdash_Q q}{q, A \vdash_Q f_A^Q(q)}\, f_A^Q R \quad f_A^Q(q) \vdash_Q q'}{\dfrac{q, A \vdash_Q q'}{q \vdash_Q \Box_A^Q\, q'}\, \Box_A^Q R}\, QCut \qquad \dfrac{q \vdash_Q \Box_A^Q\, q' \quad \dfrac{q' \vdash_Q q'}{\Box_A^Q\, q', A \vdash_Q q'}\, \Box_A^Q L}{\dfrac{q, A \vdash_Q q'}{f_A^Q(q) \vdash_Q q'}\, f_A^Q L}\, QCut$$

Join Preservation of Appearance. The appearance maps preserve binary joins, that is we have to show

$$[f_A^Q(q_1 \vee q_2)] = [f_A^Q(q_1) \vee f_A^Q(q_2)]$$

The proof of the first direction of preservation of joins is

$$\dfrac{\dfrac{\dfrac{\dfrac{q_1 \vdash_Q q_1}{q_1, A \vdash_Q f_A^Q(q_1)}\, f_A^Q R}{q_1, A \vdash_Q f_A^Q(q_1) \vee f_A^Q(q_2)}\, \vee R1 \qquad \dfrac{\dfrac{q_2 \vdash_Q q_2}{q_2, A \vdash_Q f_A^Q(q_2)}\, f_A^Q R}{q_2, A \vdash_Q f_A^Q(q_1) \vee f_A^Q(q_2)}\, \vee R2}{q_1 \vee q_2, A \vdash_Q f_A^Q(q_1) \vee f_A^Q(q_2)}\, \vee L}{f_A^Q(q_1 \vee q_2) \vdash_Q f_A^Q(q_1) \vee f_A^Q(q_2)}\, f_A^Q L$$

The proof tree for the second direction is

$$\dfrac{\dfrac{\dfrac{\dfrac{q_1 \vdash_Q q_1}{q_1 \vdash_Q q_1 \vee q_2}\, \vee R1}{q_1, A \vdash_Q f_A^Q(q_1 \vee q_2)}\, f_A^Q R}{f_A^Q(q_1) \vdash_Q f_A^Q(q_1 \vee q_2)}\, f_A^Q L \qquad \dfrac{\dfrac{\dfrac{q_2 \vdash_Q q_2}{q_2 \vdash_Q q_1 \vee q_2}\, \vee R2}{q_2, A \vdash_Q f_A^Q(q_1 \vee q_2)}\, f_A^Q R}{f_A^Q(q_2) \vdash_Q f_A^Q(q_1 \vee q_2)}\, f_A^Q L}{f_A^Q(q_1) \vee f_A^Q(q_2) \vdash_Q f_A^Q(q_1 \vee q_2)}\, \vee L$$

Multiplication and Appearance. Appearance maps on the quantale are related to the multiplication through an inequality, so we have to show the following

$$[f_A^Q(q_1 \bullet q_2)] \leq [f_A^Q(q_1) \bullet f_A^Q(q_2)]$$

The proof of which is

$$\dfrac{\dfrac{\dfrac{\dfrac{q_1 \vdash_Q q_1}{q_1, A \vdash_Q f_A^Q(q_1)}\, f_A^Q R \qquad \dfrac{q_2 \vdash_Q q_2}{q_2, A \vdash_Q f_A^Q(q_2)}\, f_A^Q R}{q_1, q_2, A \vdash_Q f_A^Q(q_1) \bullet f_A^Q(q_2)}\, \bullet R}{q_1 \bullet q_2, A \vdash_Q f_A^Q(q_1) \bullet f_A^Q(q_2)}\, \bullet L}{f_A^Q(q_1 \bullet q_2) \vdash_Q f_A^Q(q_1) \bullet f_A^Q(q_2)}\, f_A^Q L$$

The appearance maps also preserve the empty join

$$[f_A^Q(\bot)] = [\bot]$$

The proof trees are

$$\dfrac{\dfrac{\dfrac{}{\bot, A \vdash_Q \bot}\, \bot L}{f_A^Q(\bot) \vdash_Q \bot}\, f_A^Q L \qquad\qquad \dfrac{}{\bot \vdash_Q f_A^Q(\bot)}\, \bot L$$

Unit and Appearance. The unit is related to its appearance via the unit inequality eq. (2.1), so we

have to show the following

$$[1] \leq [f^Q_A(1)]$$

The proof tree is as follows

$$\dfrac{\dfrac{\dfrac{}{\vdash_Q 1}\,1R}{A \vdash_Q f^Q_A(1)}\,f^Q_A R}{1 \vdash_Q f^Q_A(1)}\,Agent$$

Meet preservation of Knowledge. Dually the knowledge operators preserve meets

$$[\Box^Q_A(q_1 \wedge q_2)] = [\Box^Q_A q_1 \wedge \Box^Q_A q_2]$$

The proof tree for the first direction is

$$\dfrac{\dfrac{\dfrac{\dfrac{q_1 \vdash_Q q_1}{q_1 \wedge q_2 \vdash_Q q_1}\,\wedge L1}{\Box^Q_A(q_1 \wedge q_2), A \vdash_Q q_1}\,\Box^Q_A L}{\Box^Q_A(q_1 \wedge q_2) \vdash_Q \Box^Q_A q_1}\,\Box^Q_A R \qquad \dfrac{\dfrac{\dfrac{q_2 \vdash_Q q_2}{q_1 \wedge q_2 \vdash_Q q_2}\,\wedge L2}{\Box^Q_A(q_1 \wedge q_2), A \vdash_Q q_2}\,\Box^Q_A L}{\Box^Q_A(q_1 \wedge q_2) \vdash_Q \Box^Q_A q_2}\,\Box^Q_A R}{\Box^Q_A(q_1 \wedge q_2) \vdash_Q \Box^Q_A q_1 \wedge \Box^Q_A q_2}\,\wedge R$$

The proof tree for the second direction is

$$\dfrac{\dfrac{\dfrac{\dfrac{q_1 \vdash_Q q_1}{\Box^Q_A q_1, A \vdash_Q q_1}\,\Box^Q_A L}{\Box^Q_A q_1 \wedge \Box^Q_A q_2, A \vdash_Q q_1}\,\wedge L1 \qquad \dfrac{\dfrac{\dfrac{q_2 \vdash_Q q_2}{\Box^Q_A q_2, A \vdash_Q q_2}\,\Box^Q_A L}{\Box^Q_A q_1 \wedge \Box^Q_A q_2, A \vdash_Q q_2}\,\wedge L2}{\Box^Q_A q_1 \wedge \Box^Q_A q_2, A \vdash_Q q_1 \wedge q_2}\,\wedge R}{\Box^Q_A q_1 \wedge \Box^Q_A q_2 \vdash_Q \Box^Q_A(q_1 \wedge q_2)}\,\Box^Q_A R$$

Also dually, the knowledge operators preserve the empty meet

$$[\Box^Q_A \top] = [\top]$$

for which the proof trees are

$$\dfrac{}{\Box^Q_A \top \vdash_Q \top}\,\top R \qquad\qquad \dfrac{\dfrac{}{\top, A \vdash_Q \top}\,\top R}{\top \vdash_Q \Box^Q_A \top}\,\Box^Q_A R$$

So we have shown that $(Q_0, \{f^Q_A\}_{A \in \mathcal{A}})$ satisfies the binary and thus finite versions of the axioms of an epistemic quantale. In other words, $(Q_0, \{f^Q_A\}_{A \in \mathcal{A}})$ is a *pre-epistemic quantale*.

4.2.3 Proof of the Infinitary Case

In this section we extend our complete binary setting of a pre-epistemic quantale to the infinite setting of an epistemic quantale. As it is usual in this procedure, we do so by *ideal* construction on Q_0 and defining infinite meets, joins, multiplication, appearance and knowledge on the ideals. We show that these definitions are consistent with the corresponding operations on Q_0, and that thus the pre-epistemic quantale is faithfully embedded in the epistemic quantale. This is used to show that the finite version of the equations of the pre-epistemic quantale extends to the infinite case of the epistemic quantale. Finally, we show how the proof of completeness extends to the ideal setting.

Define Q as the family of all ideals on Q_0:

$$Q := Idl(Q_0)$$

where an ideal is a non-empty subset of a lattice, which is downward closed and is also closed under finite joins:

$$I \in Idl(Q_0) \quad \text{iff} \quad \begin{cases} I \subseteq Q_0, I \neq \emptyset \\ x \in I, y \leq x \quad \Rightarrow y \in I \\ x, y \in I \quad \Rightarrow x \vee y \in I \end{cases}$$

We want to show that this family of ideals is an epistemic quantale. So we define infinite operations on ideals, as follows, but in order to distinguish these operators from the binary operators in Q_0, we put a bar on them:

$$\begin{aligned} \overline{\bigwedge_i} I_i &:= \bigcap_i I_i \\ \overline{\bigvee_i} I_i &:= \downarrow\{\vee Y \mid Y \text{ finite } \subseteq \bigcup_i I_i\} \\ I_1 \,\overline{\bullet}\, I_2 &:= \downarrow\{q_1 \bullet q_2 \mid \forall q_1 \in I_1 \text{ and } \forall q_2 \in I_2\} \\ \overline{f_A^Q}(I) &:= \downarrow\{f_A^Q(q) \mid \forall q \in I\} \end{aligned}$$

We have to show that these operations are ideal preserving, that is the meet, join, multiplication and appearance of ideals is an ideal. We start with meet, we have to show that $\overline{\bigwedge_i} I_i$ is an ideal. For down ward closure assume that $x \in \overline{\bigwedge_i} I_i$, this means $x \in I_i$ for any I_i, so for any $y \leq x$ we have $y \in I_i$. Similarly for closure under joins assume that $x, y \in \overline{\bigwedge_i} I_i$, then $x, y \in I_i$, which means $x \vee y \in I_i$, since this is for any I_i, we have $x \vee y \in \overline{\bigwedge_i} I_i$.

For the join of ideals we have to show that $\overline{\bigvee_i} I_i$ is an ideal, the downward closure follows from the definition. For closure under joins assume that $x, y \in \overline{\bigvee_i} I_i$, then $x = \vee Y_1$ and $y = \vee Y_2$, for Y_1, Y_1 finite subsets of the unions of I_i's, that is $Y_1 \subseteq I_1$ and $Y_2 \subseteq I_2$. We have $x \vee y = (\vee Y_1) \vee (\vee Y_2) = \vee(Y_1 \vee Y_2)$, since $Y_1 \vee Y_2 \subseteq I_1 \cup I_2$, it is also a finite subset of union of I_i's and thus $x \vee y \in \overline{\bigvee_i} I_i$.

For the multiplication, we have to show $I_1 \,\overline{\bullet}\, I_2$ is an ideal. Downward closure follows from the

definition. For closure under join assume given $x, y \in I_1 \,\overline{\bullet}\, I_2$, we have $x = q_1 \bullet q_2$ where $q_1 \in I_1$ and $q_2 \in I_2$. Similarly for y we have $y = q_1' \bullet q_2'$ where $q_1' \in I_1$ and $q_2' \in I_2$. So we have $q_1 \vee q_1' \in I_1$ and $q_2 \vee q_2' \in I_2$. Since multiplication of Q_0 is join preserving we have that $(q_1 \bullet q_2) \vee (q_1' \bullet q_2') \leq (q_1 \vee q_1') \bullet (q_2 \vee q_2')$ and since $(q_1 \vee q_1') \bullet (q_2 \vee q_2') \in I_1 \,\overline{\bullet}\, I_2$, we have that $x \vee y = (q_1 \bullet q_2) \vee (q_1' \bullet q_2') \in I_1 \,\overline{\bullet}\, I_2$.

For the appearance of ideals we have to show that $\overline{f_A^Q}(I)$ is an ideal. Downward closure follows from the definition. For closure under joins assume that $x, y \in \overline{\bigvee}_i I_i$, then $x \leq \bigvee Y_1$ and $y \leq \bigvee Y_2$, for Y_1, Y_2 finite subsets of the unions of I_i's, that is $Y_1 \subseteq I_1$ and $Y_2 \subseteq I_2$. We have $x \vee y \leq (\bigvee Y_1) \vee (\bigvee Y_2) = \bigvee (Y_1 \vee Y_2)$, since $Y_1 \vee Y_2 \subseteq I_1 \cup I_2$, it is also a finite subset of union of I_i's and thus $\bigvee (Y_1 \vee Y_2)$ is an element of $\overline{\bigvee}_i I_i$. Since $x \vee y$ lives in the down set of $\bigvee (Y_1 \vee Y_2)$, we obtain $x \vee y \in \overline{\bigvee}_i I_i$.

Next step is to show that these infinite operators are consistent with their binary counterparts in Q_0. We do so by mapping Q_0 to Q and showing that this map is an embedding. The map is defined as follows and sends each of the elements of Q_0 to its down-set:

$$e : Q_0 \hookrightarrow Q\,, \qquad :: q \mapsto q{\downarrow}$$

we have to show that e is an embedding, that is for $q_1, q_2 \in Q_0$:

$$e(q_1) \bigcirc e(q_2) = e(q_1 \bigcirc q_2)$$

for $\bigcirc \in \{\overline{\bigvee}, \overline{\bigwedge}, \overline{\bullet}\}$ and similarly for the appearance map:

$$e(f_A^Q(q)) = \overline{f_A^Q}(e(q))$$

Proofs.

Meet. For the meet operation on ideals we have to show

$$e(q_1 \wedge q_2) = e(q_1) \,\overline{\wedge}\, e(q_2)$$

or equivalently

$$\downarrow(q_1 \wedge q_2) = \downarrow q_1 \cap \downarrow q_2$$

We show this equality by proving its two inequalities. For the first direction we have:

$$x \in \downarrow(q_1 \wedge q_2) \;\Rightarrow\; x \leq (q_1 \wedge q_2) \;\Rightarrow\; x \leq q_1 \text{ and } x \leq q_2$$

but this is equivalent to

$$x \in \downarrow q_1 \text{ and } x \in \downarrow q_2 \;\Rightarrow\; x \in (\downarrow q_1 \cap \downarrow q_2)\,.$$

For the other direction we have

$$x \in (\downarrow q_1 \cap \downarrow q_2) \;\Rightarrow\; x \in \downarrow q_1 \text{ and } x \in \downarrow q_2 \;\Rightarrow\; x \leq q_1 \text{ and } x \leq q_2$$

which implies

$$x \leq q_1 \wedge q_2 \;\Rightarrow\; x \in \downarrow(q_1 \wedge q_2)$$

and we are done.

Join. For the join of ideals we have to show

$$e(q_1 \vee q_2) = e(q_1) \,\overline{\vee}\, e(q_2)$$

that is

$$(q_1 \vee q_2)\downarrow = \downarrow q_1 \,\overline{\vee}\, \downarrow q_2$$

We first show that the left hand side is a subset of the right hand side. So we take $x \in \downarrow(q_1 \vee q_2)$, which means $x \leq q_1 \vee q_2$. We want to show that $x \in \downarrow q_1 \,\overline{\vee}\, \downarrow q_2$ where by definition of join of ideals we have

$$\downarrow q_1 \,\overline{\vee}\, \downarrow q_2 = \downarrow \{\vee Y \mid Y \text{ finite } \subseteq q_1\downarrow \cup\, q_2\downarrow\}$$

Since $q_1 \in \downarrow q_1$ and $\downarrow q_1 \subseteq \downarrow q_1 \cup \downarrow q_2$, we have that $q_1 \in \downarrow q_1 \cup \downarrow q_2$ and similarly $q_2 \in \downarrow q_1 \cup \downarrow q_2$. We take the join of both sides

$$q_1 \vee q_2 \in \vee(\downarrow q_1 \cup \downarrow q_2)$$

since $\downarrow q_1 \cup \downarrow q_2$ is a finite subset of $\downarrow q_1 \cup \downarrow q_2$, we have that

$$\vee(\downarrow q_1 \cup \downarrow q_2) \in \downarrow q_1 \,\overline{\vee}\, \downarrow q_2$$

and thus

$$q_1 \vee q_2 \in \downarrow q_1 \,\overline{\vee}\, \downarrow q_2$$

Now since $x \leq q_1 \vee q_2$ and $\downarrow q_1 \,\overline{\vee}\, \downarrow q_2$ is downward closed we get that $x \in \downarrow q_1 \,\overline{\vee}\, \downarrow q_2$.
For the other direction, we show that right hand side is a subset of left hand side, that is

$$\downarrow q_1 \,\overline{\vee}\, \downarrow q_2 \subseteq \downarrow(q_1 \vee q_2)$$

We start with an element of right hand side, which is, by the definition of join of ideals, in the form $\vee Y$, where each Y is a finite subset of $\downarrow q_1 \cup \downarrow q_2$ and this means that

$$\forall y_i \in Y \qquad \text{we have that} \qquad y_i \in \downarrow q_1 \quad \text{or} \quad y_i \in \downarrow q_2$$

The join of all these y_i's, which is the join of elements of Y, will be less than $q_1 \vee q_2$, that is

$$\vee Y = \vee_i y_i \ \leq \ q_1 \vee q_2$$

so we have shown that any element $\vee Y$ of $\downarrow q_1 \ \overline{\triangledown} \ \downarrow q_2$ is also an element of $\downarrow(q_1 \vee q_2)$ and we are done.

Multiplication. For the multiplication of ideals we have to show

$$e(q_1 \bullet q_2) = e(q_1) \ \overline{\bullet} \ e(q_2)$$

that is we have to show

$$\downarrow(q_1 \bullet q_2) = \downarrow q_1 \ \overline{\bullet} \ \downarrow q_2 = \downarrow\{x \bullet y \mid \forall x \in \downarrow q_1 \text{ and } \forall y \in \downarrow q_2\}$$

We first show that the left hand side is a subset of the right hand side. So we take $x \in \downarrow(q_1 \bullet q_2)$, which means $x \leq (q_1 \bullet q_2)$. But by definition of multiplication of ideals we have that $q_1 \bullet q_2 \in \downarrow q_1 \ \overline{\bullet} \ \downarrow q_2$, which is downward closed, so we have $x \in \downarrow q_1 \ \overline{\bullet} \ \downarrow q_2$.
For the other direction we take an element of the right hand side $x \in \downarrow q_1 \ \overline{\bullet} \ \downarrow q_2$, this means that x is of the form $x = y_1 \bullet y_2$ where $y_1 \bullet y_2$ is an element of $\downarrow q_1 \ \overline{\bullet} \ \downarrow q_2$. This means that $y_1 \leq q_1$ and $y_2 \leq q_2$, so we multiply both sides and we get $y_1 \bullet y_2 \leq q_1 \bullet q_2$, which means $x \leq q_1 \bullet q_2$ and thus $x \in \downarrow(q_1 \bullet q_2)$ and we are done.

Appearance. For the appearance of ideals we have to show

$$e(f_A^Q(q)) = \overline{f_A^Q}(e(q))$$

that is

$$\downarrow f_A^Q(q) \ = \overline{f_A^Q}(\downarrow q) \ = \downarrow\{f_A^Q(x) \mid \forall x \in \downarrow q\}$$

For the first direction we we take an element of the left hand side $x \leq f_A^Q(q)$ and since $q \leq q$, we get $x \in \overline{f_A^Q}(\downarrow q)$.
For the other direction we take an element of the right hand side $x \in \overline{f_A^Q}(\downarrow q)$, which means $x \leq f_A^Q(y)$ for some $y \leq q$. Since f_A^Q is monotone, we take apply it to both sides of $y \leq q$ and we get $f_A^Q(y) \leq f_A^Q(q)$, so we have that $x \leq f_A^Q(q)$, that is an element of the left hand side.

Knowledge. The knowledge operator on ideals can now be defined as the right adjoint to appearance:

$$\overline{\Box_A^Q} \, I \ := \ \overline{\triangledown}\{I' \mid \overline{f_A^Q}(I') \ \subseteq \ I\} \, .$$

It follows then that

$$e(\Box_A^Q \, q) \ = \ \overline{\Box_A^Q}\,(e(q))$$

and we can easily verify that

$$\downarrow(\Box_A^Q\, q) \;=\; \overline{\Box_A^Q}\,(\downarrow q)$$

To see this assume $x \leq \Box_A^Q\, q$ but by adjunction this is if and only if $f_A^Q(x) \leq q$, which implies $x \in \overline{\Box_A^Q}\, q$, by definition. The other direction is done similarly.

Units. It remains to show that Q has the right units for multiplication, meet, and join. The unit of multiplication of ideals is the down set of the unit of multiplication in Q_0, that is

$$e(1) \;= \downarrow 1$$

It is easily checked that $\downarrow 1$ is an ideal, since for any $x, y \leq 1$, we have that $x \vee y \leq 1 \vee 1 = 1$. In order to show that $\downarrow 1$ is indeed the unit of ideal multiplication, we have to verify the following

$$\downarrow 1 \,\overline{\bullet}\, I \;= I$$

For one direction we have to show $I \subseteq \downarrow 1 \,\overline{\bullet}\, I$ and we proceed as follows

$$I = \downarrow\{1 \bullet y \mid y \in I\} \;\subseteq \downarrow\{x \bullet y \mid x \leq 1, y \in I\} = \downarrow 1 \,\overline{\bullet}\, I$$

For the other direction we have to show $\downarrow 1 \,\overline{\bullet}\, I \subseteq I$ and we proceed similarly as follows

$$x \bullet y \;\in\; (\downarrow 1 \,\overline{\bullet}\, I)$$

which means $x \leq 1$ and $y \in I$, now multiply both sides of $x \leq 1$ with y and we get $x \bullet y \leq 1 \bullet y$, for which we have

$$1 \bullet y \;\in \downarrow\{1 \bullet y \mid y \in I\} \;=\; I$$

and thus $x \bullet y \in I$.

The unit of join, or the bottom of Q, is the singleton of the bottom of Q_0:

$$e(\bot) \;=\; \{\bot\}$$

and it is easily seen that it has the properties of $\bot$, that is for example

$$\{\bot\} \,\overline{\bullet}\, I \;= \downarrow\{\bot \bullet q \mid \forall q \in I\} \;= \downarrow\{\bot\} \;=\; \{\bot\}$$

The unit of meet, or the top of Q, is the ideal generated by the whole Q_0, that Q_0 itself

$$e(\top) \;=\; Q_0$$

It is again easily seen that

$$Q_0 \mathbin{\overline{\wedge}} I \;=\; Q_0 \cap \; I \;=\; I$$

and also that

$$Q_0 \mathbin{\overline{\vee}} I \;= \downarrow\{\vee Y \mid Y \text{ finite } Y \subseteq \; (Q_0 \;\cup\; I) = Q_0\} \;=\; Q_0$$

We have shown that the main infinite operations on Q are consistent with their finite counterparts in Q_0, that is our map e is an embedding. It remains to show that Q is an epistemic quantale, that is multiplication of ideas preserves arbitrary join of ideals, appearance of ideas preserves arbitrary join of ideals, and that the appearance of ideals satisfies the inequality with regard to multiplication of ideals. For first case we have to show

$$(\overline{\bigvee_i} I_i) \mathbin{\overline{\bullet}} I' = \overline{\bigvee_i}(I_i \mathbin{\overline{\bullet}} I')$$

We start from the left hand side and unfold the definition to get to the right hand side as follows:

$$\begin{aligned}
(\overline{\bigvee_i} I_i) \mathbin{\overline{\bullet}} I' &= \downarrow\{q \bullet q' \mid q \in \overline{\bigvee_i} I_i \text{ and } q' \in I'\} \\
&= \downarrow\{q \bullet q' \mid q = \vee Y,\ Y \text{ finite} \subseteq \bigcup_i I_i \text{ and } q' \in I'\} \\
&= \downarrow\{(\vee Y) \bullet q' \mid q = \vee Y,\ Y \text{ finite} \subseteq \bigcup_i I_i \text{ and } q' \in I'\}
\end{aligned}$$

now since binary multiplication preserves finite joins in Q_0 we have this is equal to the following

$$\downarrow\{\vee(Y \bullet q') \mid q = \vee Y,\ Y \text{ finite} \subseteq \bigcup_i I_i \text{ and } q' \in I'\} = \overline{\bigvee_i}(I_i \bullet I')$$

For the appearance of ideals we have to show

$$\overline{f_A^Q}(\overline{\bigvee_i} I_i) = \overline{\bigvee_i} \overline{f_A^Q}(I_i)$$

We start from the left hand side

$$\begin{aligned}
\overline{f_A^Q}(\overline{\bigvee_i} I_i) &= \downarrow\{f_A^Q(\overline{\bigvee_i} I_i) \mid I_i \text{ is an ideal}\} \\
&= \downarrow\{f_A^Q(\vee Y) \mid Y \text{ finite } \subseteq \bigcup_i I_i\} \\
&= \downarrow\{\vee f_A^Q(Y) \mid Y \text{ finite } \subseteq \bigcup_i I_i\}
\end{aligned}$$

which is equal to $\overline{\bigvee_i} \overline{f_A^Q}(I_i)$.

It remains to show the inequality between appearance and multiplication, that is

$$\overline{f_A^Q}(I_1 \mathbin{\overline{\bullet}} I_2) \leq \overline{f_A^Q}(I_1) \mathbin{\overline{\bullet}} \overline{f_A^Q}(I_2)$$

For the left hand side we have

$$\overline{f_A^Q}(I_1 \mathbin{\overline{\bullet}} I_2) \quad = \quad \downarrow\{f_A^Q(q_1 \bullet q_2) \mid q_1 \in I_1, q_2 \in I_2\}$$

we can now apply the inequality of f_A^Q over multiplication in Q_0 and get

$$\downarrow\{f_A^Q(q_1 \bullet q_2) \mid q_1 \in I_1, q_2 \in I_2\} \subseteq \downarrow\{f_A^Q(q_1) \bullet f_A^Q(q_2) \mid q_1 \in I_1, q_2 \in I_2\}$$

which is equal to the right hand side. So we have shown that Q is an epistemic quantale. In the rest of this section we show how completeness extends from Q_0 to Q.

Extension of Completeness. We showed in the previous section that our pre-epistemic quantale Q_0 is a complete model of the Q-system. That is we have the following in Q_0:

$$\text{If} \quad \Gamma \nvdash_Q q \quad \text{then} \quad \alpha(\odot_Q \Gamma) \not\leq_{Q_0} \alpha(q)$$

This is extended to our epistemic quantale Q. Since the embedding of Q_0 in Q is a homomorphism, we have

$$\alpha(\odot_Q \Gamma) \not\leq_{Q_0} \alpha(q) \quad \Leftrightarrow \quad e(\Gamma) \not\leq_Q e(q)$$

So it follows that:

$$\text{If} \quad \Gamma \nvdash_Q q \quad \text{then} \quad e(\Gamma) \not\leq_Q e(q)$$

which makes Q a complete model of the Q-system.

4.2.4 Completeness of the M-system

Lemma 4.2.2 If a sequent is valid in the module part of all distributive epistemic systems, then it is derivable in the M-system.

Proof. We show the contrapositive by building the Lindenbaum-Tarski algebra of the M-formulae, by $M_0 = M \backslash \cong_M$, that is the set of all equivalence classes of M-formulae under the logical consequence $\cong_M$ defined as $\vdash_M \dashv$. We then show that M_0 satisfies all the properties of a module in a distributive epistemic system (this requires using the Lindenbaum-Tarski algebra of the Q-system for operations with actions). These are listed below

1. Each M-formula is mapped to its equivalence class in M_0.

2. We define an order $\leq$ between these equivalence classes, using the provability of the M-system and check that this order is well-defined and a partial order.

3. We show that the $(M_0, \leq)$ has a least and a greatest element, that is a top and a bottom.

4. We define meet and join operators in $(M_0, \leq)$ and show that it forms a lattice.

5. We define an update operation on M_0 and Q_0 and show that it satisfies the binary versions of the properties of the action of quantale on the module (preservation of binary joins).

6. We define endomorphisms on M_0 and show that these satisfy the finite versions of the equations of the appearance maps on the module. We call M_0 a *pre-epistemic right module* over Q_0.

7. Finally we extend our finite model M_0 to the infinite case M by the ideal construction on M_0.

4.2.5 Proof of the Finitary Case

The proof for the items one to four above are the same as in the quantale. The order is defined as follows

$$[m] \leq [m'] \quad \text{iff} \quad m \vdash_M m'$$

and it is well defined since if we have

$$[m_1] \cong_M [m_1'] \text{ and } [m_2] \cong_M [m_2'] \text{ and } [m_1] \leq [m_2] \quad \text{imply} \quad [m_1'] \leq [m_2']$$

by the following proof tree

$$\dfrac{m_1' \vdash_M m_1 \qquad \dfrac{m_1 \vdash_M m_2 \quad m_2 \vdash_M m_2'}{m_1 \vdash_M m_2'}\, MCut}{m_1' \vdash_M m_2'}\, MCut$$

It is very easy to see that this order is a partial order, transitivity being satisfied by the MCut rule

$$\dfrac{m_1 \vdash_M m_2 \quad m_2 \vdash_M m_3}{m_1 \vdash_M m_3}\, MCut$$

So $(M_0, \leq)$ is a partially ordered set and $[\top]$ and $[\bot]$ are its greatest and least elements by the axioms for $\top$ and $\bot$ in M-systems:

$$\dfrac{}{\bot \vdash_M m}\, \bot L \qquad\qquad \dfrac{}{m \vdash_M \top}\, \top R$$

Join and meet are defined as follows

$$[m] \vee [m'] := [m \vee m'] \quad \text{and} \quad [m] \wedge [m'] := [m \wedge m']$$

We have to show that they are both well-defined. The proof trees for well-definedness of meet and join are exactly the same as in the Q-systems case, since the rules for meet and join are the same in both systems. For example to prove that join is well-defined we have to show the following

$$[m_1] = [m_2] \text{ and } [m_1'] = [m_2'] \quad \text{imply} \quad [m_1 \vee m_1'] = [m_2 \vee m_2']$$

The proof trees for these are as follows

$$\dfrac{\dfrac{\dfrac{m_1 \vdash_M m_1'}{m_1 \vdash_M m_1' \vee m_2'} \vee R1 \quad \dfrac{m_2 \vdash_M m_2'}{m_2 \vdash_M m_1' \vee m_2'} \vee R2}{m_1 \vee m_2 \vdash_M m_1' \vee m_2'} \vee L \qquad \dfrac{\dfrac{\dfrac{m_1' \vdash_M m_1}{m_1' \vdash_M m_1 \vee m_2} \vee R1 \quad \dfrac{m_2' \vdash_M m_2}{m_2' \vdash_M m_1 \vee m_2} \vee R2}{m_1' \vee m_2' \vdash_M m_1 \vee m_2} \vee L$$

We show that meet and join are distributive by proving the following in logical consequence terms

$$\begin{aligned} m_1 \vee (m_2 \wedge m_3) \quad &\vdash_M \dashv \quad (m_1 \vee m_2) \wedge (m_1 \vee m_3) \\ m_1 \wedge (m_2 \vee m_3) \quad &\vdash_M \dashv \quad (m_1 \wedge m_2) \vee (m_1 \wedge m_3) \end{aligned}$$

The proof trees for the first direction of the distributivity of join over meet is

$$\dfrac{\dfrac{\dfrac{\dfrac{m_1 \vdash_M m_1}{m_1 \vdash_M m_1 \vee m_2} \vee R1 \quad \dfrac{\dfrac{m_2 \vdash_M m_2}{m_2 \vdash_M m_1 \vee m_2} \vee R2}{m_2 \wedge m_3 \vdash_M m_1 \vee m_2} \wedge L1}{m_1 \vee (m_2 \wedge m_3) \vdash_M m_1 \vee m_2} \vee L \quad \dfrac{\dfrac{\dfrac{m_1 \vdash_M m_1}{m_1 \vdash_M m_1 \vee m_3} \vee R1 \quad \dfrac{\dfrac{m_3 \vdash_M m_3}{m_3 \vdash_M m_1 \vee m_3} \vee R2}{m_2 \wedge m_3 \vdash_M m_1 \vee m_3} \wedge L2}{m_1 \vee (m_2 \wedge m_3) \vdash_M m_1 \vee m_3} \vee L}{m_1 \vee (m_2 \wedge m_3) \vdash_M (m_1 \vee m_2) \wedge (m_1 \vee m_3)} \wedge R$$

The proof tree of the other direction is

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{m_1 \vdash_M m_1}{m_1 \vdash_M m_1 \vee (m_2 \wedge m_3)} \vee R1}{m_1, m_1 \vee m_3 \vdash_M m_1 \vee (m_2 \wedge m_3)} weakL \quad \dfrac{\dfrac{\dfrac{m_1 \vdash_M m_1}{m_2, m_1 \vdash_M m_1} weakL}{m_2, m_1 \vdash_M m_1 \vee (m_2 \wedge m_3)} \vee R1 \quad \dfrac{\dfrac{m_2 \vdash_M m_2}{m_2, m_3 \vdash_M m_2} weakL \quad \dfrac{m_3 \vdash_M m_3}{m_2, m_3 \vdash_M m_3} weakL}{m_2, m_3 \vdash_M m_2 \wedge m_3} \wedge R}{m_2, m_3 \vdash_M m_1 \vee (m_2 \wedge m_3)} \vee R2}{m_2, m_1 \vee m_3 \vdash_M m_1 \vee (m_2 \wedge m_3)} \vee L}{m_1 \vee m_2, m_1 \vee m_3 \vdash_M m_1 \vee (m_2 \wedge m_3)} \wedge L2}{m_1 \vee m_2, (m_1 \vee m_2) \wedge (m_1 \vee m_3) \vdash_M m_1 \vee (m_2 \wedge m_3)} \wedge L1}{(m_1 \vee m_2) \wedge (m_1 \vee m_3), (m_1 \vee m_2) \wedge (m_1 \vee m_3) \vdash_M m_1 \vee (m_2 \wedge m_3)} contr}{(m_1 \vee m_2) \wedge (m_1 \vee m_3) \vdash_M m_1 \vee (m_2 \wedge m_3)}$$

The proof trees of the first direction of the distributivity of meet over join is as follows

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{m_1 \vdash_M m_1}{m_1, m_2 \vdash_M m_1}\, weakL \quad \dfrac{m_2 \vdash_M m_2}{m_1, m_2 \vdash_M m_2}\, weakL}{m_1, m_2 \vdash_M m_1 \wedge m_2}\, \wedge R}{m_1, m_2 \vdash_M (m_1 \wedge m_2) \vee (m_1 \wedge m_3)}\, \vee R1 \quad \dfrac{\dfrac{\dfrac{m_1 \vdash_M m_1}{m_1, m_3 \vdash_M m_1}\, weakL \quad \dfrac{m_3 \vdash_M m_3}{m_1, m_3 \vdash_M m_3}\, weakL}{m_1, m_3 \vdash_M m_1 \wedge m_3}\, \wedge R}{m_1, m_3 \vdash_M (m_1 \wedge m_2) \vee (m_1 \wedge m_3)}\, \vee R2}{m_1, m_2 \vee m_3 \vdash_M (m_1 \wedge m_2) \vee (m_1 \wedge m_3)}\, \vee L$$

$$\dfrac{m_1, m_2 \vee m_3 \vdash_M (m_1 \wedge m_2) \vee (m_1 \wedge m_3)}{m_1, m_1 \wedge (m_2 \vee m_3) \vdash_M (m_1 \wedge m_2) \vee (m_1 \wedge m_3)}\, \wedge L2$$

$$\dfrac{m_1 \wedge (m_2 \vee m_3), m_1 \wedge (m_2 \vee m_3) \vdash_M (m_1 \wedge m_2) \vee (m_1 \wedge m_3)}{m_1 \wedge (m_2 \vee m_3) \vdash_M (m_1 \wedge m_2) \vee (m_1 \wedge m_3)}\, \wedge L1\ contr$$

The proof tree of the second direction is as follows

$$\dfrac{\dfrac{\dfrac{\dfrac{m_1 \vdash_M m_1}{m_1 \wedge m_2 \vdash_M m_1}\, \wedge L1 \quad \dfrac{m_1 \vdash_M m_1}{m_1 \wedge m_3 \vdash_M m_1}\, \wedge L2}{(m_1 \wedge m_2) \vee (m_1 \wedge m_3) \vdash_M m_1}\, \vee L \quad \dfrac{\dfrac{\dfrac{m_2 \vdash_M m_2}{m_1 \wedge m_2 \vdash_M m_2}\, \wedge L2}{m_1 \wedge m_2 \vdash_M m_2 \vee m_3}\, \vee R1 \quad \dfrac{\dfrac{m_3 \vdash_M m_3}{m_1 \wedge m_3 \vdash_M m_3}\, \wedge L2}{m_1 \wedge m_3 \vdash_M m_2 \vee m_3}\, \vee R2}{(m_1 \wedge m_2) \vee (m_1 \wedge m_3) \vdash_M m_2 \vee m_3}\, \vee L}{(m_1 \wedge m_2) \vee (m_1 \wedge m_3) \vdash_M m_1 \wedge (m_2 \vee m_3)}\, \wedge R$$

The appearance maps and knowledge operators are also defined in exactly the same way:

$$f_A^M([m]) := [f_A^M(m)] \quad \text{and} \quad \Box_A^M\,[m] := [\Box_A^M\, m]$$

Since the rules for these two are identical to the Q-system, their well-definedness and being adjoints is proved in exactly the way as in the Q-systems, and also in exactly the same way we can show that f_A^M's are join and $\bot$ preserving, where as $\Box_A^M$'s are meet and $\top$ preserving.

So far we have shown that $(M_0, \leq, \wedge, \vee)$ is a non-distributive lattice and that $(M_0, \{f_A^M\}_{A\in\mathcal{A}})$ is an epistemic module. Now we have to show that our previously constructed epistemic quantale $((M_0, \{f_A - Q\}_{A\in\mathcal{A}})$ acts on the module, that is M_0 is indeed the right module of Q_0.

Update and Dynamic Modality. We define an update product on the pair (M_0, Q_0) using the update operator of our M-systems

$$[m].[q] := [m.q]$$

For the proof of well-definedness of this operator we have to show

$$\text{If} \quad [m] = [m'] \quad \text{and} \quad [q] = [q'] \quad \text{then} \quad [m.q] = [m'.q']$$

For the proof we use both M and Q systems. The proof tree for one direction is:

$$\dfrac{\dfrac{m \vdash_M m' \quad q \vdash_Q q'}{m, q \vdash_M m'.q'}\, .L}{m.q \vdash_M m'.q'}\, .R$$

The proof tree for the other direction is drawn similarly. We define a dynamic modality on the pair (M_0, Q_0) as follows

$$[[q]]\,[m] := [[q][m]]$$

since both the equivalence class and dynamic modality use the [ ] sign, the notation looks confusing. Note that on the left hand side $[[q]]$ is the equivalence class of the dynamic operator $[q]$ and on the right hand side $[[q][m]]$ is the equivalence class of the dynamic modality $[q]$ being applied to equivalence class of m. We have to show that this definition is well-defined, that is we have to show the following

$$[m] = [m'] \quad \text{and} \quad [q] = [q'] \quad \text{implies} \quad [[q]m] = [[q']m']$$

or in logical consequence terms

$$m \vdash_Q \dashv m' \quad \text{and} \quad q \vdash_Q \dashv q' \quad \text{implies} \quad [q]m \vdash_Q \dashv [q']m'$$

the proof trees for this are

$$\dfrac{\dfrac{m \vdash_M m' \quad q' \vdash_Q q}{[q]m, q' \vdash_M m'}\, DyL}{[q]m \vdash_M [q']m'}\, DyR$$

The proof tree for the other direction is drawn similarly. Now we have to show that update and dynamic modality are adjoint operators, that is

$$[m.q] \leq [m'] \quad \text{iff} \quad [m] \leq [[q]m']$$

the proof trees for which are

$$\dfrac{\dfrac{m \vdash_M m \quad q \vdash_Q q}{m, q \vdash_M m.q}\, .R \qquad m.q \vdash_M m'}{\dfrac{m, q \vdash_M m'}{m \vdash_M [q]m'}\, DyR}\, MCut \qquad \dfrac{m \vdash_M [q]m' \qquad \dfrac{\dfrac{m' \vdash_M m' \quad q \vdash_Q q}{[q]m', q \vdash_M m'}\, DyL}{m, q \vdash_M m'}\, MCut}{m.q \vdash_M m'}\, .L$$

Associativity of update and multiplication. The action of quantale on the module and the multiplication of quantale are related to each other via the following equation

$$[m] \,.\, ([q] \bullet [q']) = ([m] \,.\, [q]) \,.\, [q']$$

which is equal to the following by definition of update in M_0

$$[m \,.\, (q \bullet q')] = [(m \,.\, q) \,.\, q']$$

which is derivable in our pair (M_0, Q_0) by the following proof trees:

$$\dfrac{\dfrac{\dfrac{q' \vdash_Q q' \quad \dfrac{m \vdash_M m \quad q \vdash_Q q}{m, q \vdash_M m.q}\, .R}{m, q, q' \vdash_M (m.q).q'}\, .R}{m, q \bullet q' \vdash_M (m.q).q'}\, \bullet ML}{m.(q \bullet q') \vdash_M (m.q).q'}\, .L$$

Note that in applying the right rule for update, that is $.R$, we take $\Gamma = m, q$ and $\Gamma_Q = q'$, instead of the tempting, but wrong choice of $\Gamma = m$ and $\Gamma_Q = q, q'$.

$$\dfrac{\dfrac{\dfrac{m \vdash_M m \quad \dfrac{q \vdash_Q q \quad q' \vdash_Q q'}{q, q' \vdash_Q q \bullet q'}\, \bullet R}{m, q, q' \vdash_M m.(q \bullet q')}\, .R}{(m.q), q' \vdash_M m.(q \bullet q')}\, .L}{(m.q).q' \vdash_M m.(q \bullet q')}\, .L$$

In this proof, in order to apply the right rule for update, that is $.R$, we make a different choice from the previous proof. Here we take our Γ to be only m and our $\Gamma_Q = q, q'$, which was the wrong tempting choice of the previous proof.

Update preserves unit of multiplication. Unit of multiplication in M_0 is $[1]$ and we have to show that update preserves it, that is

$$[m] \,.\, [1] = [m]$$

which is equal to $[m \,.\, 1] = [m]$ and in logical consequence terms we have to show the following

$$m.1 \vdash_M \dashv m$$

the proof trees for which are

$$\dfrac{\dfrac{m \vdash_Q m}{m, 1 \vdash_M m}\, 1ML}{m.1 \vdash_M m}\, .L \qquad\qquad \dfrac{m \vdash_M m \quad \dfrac{}{\vdash_Q 1}\, 1R}{m \vdash_M m.1}\, .R$$

Join preservation of update and meet preservation of dynamic modality. We show that update preserves binary joins in its both arguments, that is both in M_0 and in Q_0, as follows

$$[m.(q \vee q')] = [(m.q) \vee (m.q')] \quad \text{and} \quad [(m \vee m').q] = [(m.q) \vee (m'.q)]$$

or in logical consequence terms

$$m.(q \vee q') \vdash_M \dashv (m.q) \vee (m.q') \quad \text{and} \quad (m \vee m').q \vdash_M \dashv (m.q) \vee (m'.q)$$

The proof trees for the first direction of the first case is

$$\dfrac{\dfrac{\dfrac{\dfrac{m \vdash_M m \quad q \vdash_Q q}{m, q \vdash_M m.q}\,.R}{m, q \vdash_M (m.q) \vee (m.q')}\,\vee R1 \quad \dfrac{\dfrac{m \vdash_M m \quad q' \vdash_Q q'}{m, q' \vdash_M m.q'}\,.R}{m, q' \vdash_M (m.q) \vee (m.q')}\,\vee R2}{m, q \vee q' \vdash_M (m.q) \vee (m.q')}\,\vee ML}{m.(q \vee q') \vdash_M (m.q) \vee (m.q')}\,.L$$

Similarly for the second direction of the first case we have

$$\dfrac{\dfrac{m \vdash_M m \quad \dfrac{q \vdash_Q q}{q \vdash_Q q \vee q'}\,\vee R1}{m, q \vdash_M m.(q \vee q')}\,.R}{m.q \vdash_M m.(q \vee q')}\,.L \quad \dfrac{\dfrac{m \vdash_M m \quad \dfrac{q' \vdash_Q q'}{q' \vdash_Q q \vee q'}\,\vee R2}{m, q' \vdash_M m.(q \vee q')}\,.R}{m.q' \vdash_M m.(q \vee q')}\,.L}{(m.q) \vee (m.q') \vdash_M m.(q \vee q')}\,\vee L$$

The proof tree for the first direction of the second case is

$$\dfrac{\dfrac{\dfrac{\dfrac{m \vdash_M m \quad q \vdash_Q q}{m, q \vdash_M m.q}\,.R}{m, q \vdash_M (m.q) \vee (m'.q)}\,\vee R1 \quad \dfrac{\dfrac{m' \vdash_M m' \quad q \vdash_Q q}{m', q \vdash_M m'.q}\,.R}{m', q \vdash_M (m.q) \vee (m'.q)}\,\vee R2}{m \vee m', q \vdash_M (m.q) \vee (m'.q)}\,\vee L}{(m \vee m').q \vdash_M (m.q) \vee (m'.q)}\,.L$$

Similarly the proof tree for the second direction is

$$\dfrac{\dfrac{q \vdash_Q q \quad \dfrac{m \vdash_M m}{m \vdash_M m \vee m'}\,\vee R1}{m, q \vdash_M (m \vee m').q}\,.R}{m.q \vdash_M (m \vee m').q}\,.L \quad \dfrac{\dfrac{q \vdash_Q q \quad \dfrac{m' \vdash_M m'}{m' \vdash_M m \vee m'}\,\vee R2}{m', q \vdash_M (m \vee m').q}\,.R}{m'.q \vdash_M (m \vee m').q}\,.L}{(m.q) \vee (m'.q) \vdash_M (m \vee m').q}\,\vee L$$

Dually we have to show that the dynamic modality preserves meets in both argument, that is:

$$[q](m \wedge m') \vdash_M \dashv [q]m \wedge [q]m' \quad \text{and} \quad [q \wedge q']m \vdash_M \dashv [q]m \wedge [q']m$$

The proof tree for the first direction of the first case is

$$\dfrac{\dfrac{\dfrac{\dfrac{q \vdash_Q q \quad \dfrac{m \vdash_M m}{m \wedge m' \vdash_M m}\,\wedge L1}{[q](m \wedge m'), q \vdash_M m}\,DyL}{[q](m \wedge m') \vdash_M [q]m}\,DyR \quad \dfrac{\dfrac{q \vdash_Q q \quad \dfrac{m' \vdash_M m'}{m \wedge m' \vdash_M m'}\,\wedge L2}{[q](m \wedge m'), q \vdash_M m'}\,DyL}{[q](m \wedge m') \vdash_M [q]m'}\,DyR}{[q](m \wedge m') \vdash_M [q]m \wedge [q]m'}\,\wedge R$$

Similarly, the proof tree for the second direction of the first case is

$$\dfrac{\dfrac{\dfrac{\dfrac{q \vdash_Q q \quad m \vdash_M m}{[q]m, q \vdash_M m}\, DyL}{[q]m \wedge [q]m', q \vdash_M m}\, \wedge L1 \quad \dfrac{\dfrac{q \vdash_Q q \quad m' \vdash_M m'}{[q]m' q \vdash_M m'}\, DyL}{[q]m \wedge [q]m', q \vdash_M m'}\, \wedge L2}{[q]m \wedge [q]m', q \vdash_M m \wedge m'}\, \wedge R}{[q]m \wedge [q]m' \vdash_M [q](m \wedge m')}\, DyR$$

The proof tree for the first direction of the second case is

$$\dfrac{\dfrac{m \vdash_M m \quad \dfrac{q \vdash_Q q}{q \wedge q' \vdash_Q q}\, \wedge L1}{[q \wedge q']m, q \vdash_M m}\, DyL}{[q \wedge q']m \vdash_M [q]m}\, DyR \quad \dfrac{\dfrac{m \vdash_M m \quad \dfrac{q' \vdash_Q q'}{q \wedge q' \vdash_Q q'}\, \wedge L2}{[q \wedge q']m, q' \vdash_M m}\, DyL}{[q \wedge q']m \vdash_M [q']m}\, DyR}{[q \wedge q']m \vdash_M [q]m \wedge [q']m}\, \wedge R$$

And finally the proof tree for the second direction of the second case is

$$\dfrac{\dfrac{\dfrac{\dfrac{q \vdash_Q q \quad m \vdash_M m}{[q]m, q \vdash_M m}\, DyL}{[q]m, q \wedge q' \vdash_M m}\, \wedge ML}{[q]m \wedge [q']m, q \wedge q' \vdash_M m}\, \wedge L}{[q]m \wedge [q']m \vdash_M [q \wedge q']m}\, DyR$$

We also have to show that update preserves the $\bot$ of the module and dually dynamic modality preserves the $\top$ of the module:

$$\bot.q \vdash_M \dashv \bot \quad \text{and} \quad [q]\top \vdash_M \dashv \top$$

which are very easily done:

$$\dfrac{\dfrac{\dfrac{}{\bot, q \vdash_M \bot}\, \bot L}{\bot.q \vdash_Q \bot}\, .L \qquad \dfrac{}{\bot \vdash_M \bot.q}\, \bot L \qquad \dfrac{}{[q]\top \vdash_M \top}\, \top R \qquad \dfrac{\dfrac{}{\top, q \vdash_M \top}\, \top R}{\top \vdash_M [q]\top}\, DyR$$

Update Inequality. The last thing to show for the proof of completeness is that the appearance map satisfies the update inequality

$$[f_A^M(m.q)] \leq [f_A^M(m).f_A^Q(q)]$$

The proof tree for the inequality is as follows

$$\dfrac{\dfrac{\dfrac{m \vdash_M m}{m, A \vdash_M f_A^M(m)}\, f_A^M R \quad \dfrac{q \vdash_Q q}{q, A \vdash_Q f_A^Q(q)}\, f_A^Q R}{m, q, A \vdash_M f_A^M(m).f_A^Q(q)}\, .R}{m.q, A \vdash_M f_A^M(m).f_A^Q(q)}\, .L}{f_A^M(m.q) \vdash_M f_A^M(m).f_A^Q(q)}\, f_A^M L$$

So we have shown that $(M_0, \{f_A^M\}_{A\in\mathcal{A}})$ is satisfies the binary (and thus finite) version of the axioms of an epistemic module and is a right module of the binary version of epistemic quantale $(Q_0, \{f_A^Q\}_{A\in\mathcal{A}})$ discussed in the previous section.

4.2.6 Proof of the Infinitary Case

This is done in exactly the same way as in the Q-system. We form the family of ideals over M_0:

$$M \;:=\; Idl(M_0)$$

and define meet, join, appearance, top and bottom of ideals in exactly the same way as for the ideals of Q_0. It remains to define the update operations of ideals and check that it is consistent with the update in M_0. We define the update as

$$I^M \cdot I^Q \;= \downarrow\{x.y \mid \forall x \in I^M, \forall y \in I^Q\}$$

We have to show that that the update of two ideals is an ideal. The downward closure follows from the definition. Given $m, m' \in I^M \cdot I^Q$, we have $m = x.y$ and $m' = x'.y'$ where $x, x' \in I^M$ and $y, y' \in I^Q$. So we have $x \vee x' \in I^M$ and $y \vee y' \in I^Q$, thus we also have that $(x \vee x').(y \vee y') \in I^M \cdot I^Q$. Since update of Q_0 preserves binary join, we have $(x.y) \vee (x'.y') \leq (x \vee x').(y \vee y')$ and thus $m \vee m' \in I^M \cdot I^Q$

We embed Q_0 in Q via the following map

$$e' : M_0 \hookrightarrow M \qquad :: m \mapsto \downarrow m$$

we have to show that this map is an embedding. The proof for join, meet, and appearance operations are the same as in the quantale case (since they have a similar definition). It remains to show that update of ideals is consistent with the update of Q_0, that is we have to show the following

$$e'(m.q) \;=\; e'(m) \cdot e'(q)$$

that is

$$\downarrow(m.q) \ = \downarrow m \centerdot \downarrow q \ = \downarrow\{x.y \mid \forall x \leq m, \forall y \leq q\}$$

For the first direction we assume

$$m' \leq m.q$$

since $m \leq m$ and $q \in q$, we have $m.q \in \{x.y \mid \forall x \leq m, \forall y \leq q\}$ and thus

$$m' \leq \{x.y \mid \forall x \leq m, \forall y \leq q\}\,.$$

For the other direction we have

$$m' \in \downarrow\{x.y \mid \forall x \leq m, \forall y \leq q\}$$

that is $m' \leq x'.y'$ for some x', y' such that $x' \leq m$ and $y' \leq q$. Now since update is monotone, $m' \leq x'.y' \leq m.q$.

Next step is to show that M satisfies the module equations and thus it is the right module for our previously discussed Q. We have to firstly show that ideal update preserves the unit of ideal multiplication, that is

$$I^M \centerdot \downarrow 1 = I^M$$

which is easily seen since

$$I^M \centerdot \downarrow 1 \ = \downarrow\{x \bullet 1 \mid x \in I^M, 1 \in \downarrow 1\} \ = \downarrow\{x \mid x \in I^M\} \ = \ I^M$$

Secondly we have to show that update of ideals is associative over multiplication of ideals, that is we have to show the following

$$I^M \centerdot (I_1^Q \mathbin{\overline{\bullet}} I_2^Q) = (I^M \centerdot I_1^Q) \centerdot I_2^Q$$

which follows by unfolding the definitions and using the corresponding associativity in the binary case, that is

$$I^M \centerdot (I_1^Q \mathbin{\overline{\bullet}} I_2^Q) \ = \downarrow\{x.(y \bullet z) \mid x \in I^M, y \in I_1^Q, z \in I_2^Q\}$$

since binary update of M_0 is associative over binary multiplication in Q_0, this is equal to

$$\downarrow\{(x.y).z \mid x \in I^M, y \in I_1^Q, z \in I_2^Q\} \ = \ (I^M \centerdot I_1^Q) \centerdot I_2^Q$$

Finally we have to show that update of ideals preserves join of ideals in both arguments, that is

$$(\overline{\bigvee_i} I_i^M) \centerdot I^Q = \overline{\bigvee_i}(I_i^M \centerdot I^Q) \qquad \text{and} \qquad I^M \centerdot (\overline{\bigvee_i} I_i^Q) = \overline{\bigvee_i}(I^M \centerdot I_i^Q)$$

which again follows by unfolding definitions, for example for the first argument we have

$$(\overline{\bigvee_i} I_i^M) \dot{-} I^Q \ = \downarrow\{\vee Y.q \mid Y \text{ finite } \subseteq \bigcup_i I_i, q \in I^Q\}$$

since binary update of M_0 preserves finite joins in Q_0, this is equal to the following

$$\downarrow\{\vee(Y.q) \mid Y \text{ finite } \subseteq \bigcup_i I_i, q \in I^Q\} \ = \ \overline{\bigvee_i}(I_i^M \dot{-} I^Q)$$

So we have shown that M is a right module for Q. The last step is to show that M with the appearance of ideals defined above is indeed an epistemic module, that is we have to firstly show that appearance of ideals preserves joins of ideals

$$\overline{f_A^M}(\overline{\bigvee_i} I_i) = \overline{\bigvee_i} \overline{f_A^M}(I_i)$$

and is proved in exactly the same way as for the appearance and join of ideals on our epistemic quantale Q. It remains to show that appearance of ideals on the module satisfies the inequality for update of ideals, that is

$$\overline{f_A^M}(I_M \dot{-} I_Q) \leq \overline{f_A^M}(I_M) \dot{-} \overline{f_A^Q}(I_Q)$$

This easily seen since we have

$$\overline{f_A^M}(I_M \dot{-} I_Q) \ = \downarrow\{f_A^M(m.q) \mid m \in I^M, q \in I^Q\} \subseteq \{f_A^M(m).f_A^Q(q) \mid m \in I^M, q \in I^Q\}$$

which is exactly the definition of the right hand side. So we are done, we have proved that module $M = Idl(M_0)$ is an epistemic module for our epistemic quantale $Q = Idl(Q_0)$, and so we have that $(M, Q, \{\overline{f_A}\}_{A \in \mathcal{A}})$ is a distributive epistemic system.

Extension of Completeness. Similarly to the quantale case, we show that our completeness result extends from the pre-epistemic module to our epistemic module. We showed in the previous section that our pre-epistemic module M_0 is a complete model of the M-system. That is we have the following in M_0:

$$\text{If} \quad \Gamma \nvdash_M m \quad \text{then} \quad \beta(\odot_M \Gamma) \not\leq_{M_0} \beta(m)$$

This is extended to our epistemic module M. Since the embedding of M_0 in M is a homomorphism, we have

$$\beta(\odot_M \Gamma) \not\leq_{M_0} \beta(m) \quad \Leftrightarrow \quad e'(\Gamma) \not\subseteq_M e'(m)$$

So it follows that

$$\text{If} \quad \Gamma \nvdash_M m \quad \text{then} \quad e'(\Gamma) \not\leq_M e'(m)$$

Theorem 4.2.3 *The rules of* IDEAL *are complete with respect to the algebraic semantics in terms of distributive epistemic systems.*

Proof follows directly from lemmas 4.2.1 and 4.2.2. □

Chapter 5

Application to Security Protocols

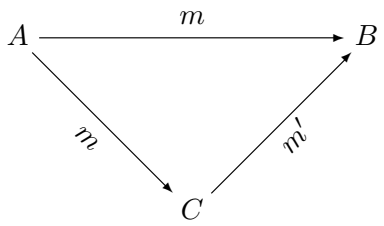
The logic developed in this thesis is a logic to reason about knowledge of agents in a multi-agent system where agents communicate and as a result their knowledge changes. In the previous chapters, I have presented an algebraic axiomatic and a sequent calculus for this purpose, I have applied the algebra to solve a challenging epistemic puzzle: the muddy children puzzle and also more interesting versions of it with misinformation actions such as cheating and lying. In this section I will show how the ability of this setting in formalizing such actions makes it an appropriate logic for a serious domain of applications: reasoning about safety of security protocols. In a way this is not a surprise, since the setting of security protocols is an example of a multi-agent system where the principals involved in the protocol communicate via message passing and the goal is to, for example make sure that each principal knows with whom he is communicating. The difference between these message passing actions and the actions we dealt with in our previous examples is that the communication channel in which the messages are sent and received is not safe. This means that there is always a chance that a malicious agent will intercept the messages, so for example a message that was sent will never be received. In this chapter, I will show how a slight recast of the formalism of previous chapters enables us to deal with these actions. The distinguishing features of this formalism are its ability to methodically deal with misinformation actions, make agents suspect the related such actions (via their appearance maps), and then use these suspicions to compute the knowledge of agents by adjunction. These features offer a modular and compositional way of analyzing and also designing protocols for safe communications. Thus one of the difficulties of the field of security, that safety of protocols do not compose and every new protocols needs a new proof of safety, will be tackled in our setting, since our proofs of safety is based on suspicions of agents, which preserve both composition and choice of protocols.

It is worth noting that our logic is related to the compositional logic of Meadows, Mitchell, and Pavlovic [27, 64], since both logics use the dynamic modality of Propositional Dynamic Logic [45]. The novelty of our approach is enriching the setting of dynamic logic with suspicion-based epistemic modalities and systematically connecting them to the dynamic modality. Thus overcoming the weakness of their approach in dealing with more complex epistemic operations such as conditional and

nested knowledge of agents.

5.1 A Brief Background Story

Consider a simple but typical security setting, we have three agents A, B, C where A and B are honest and C is a malicious intruder. A and B want to communicate a secret through a communication channel, for example the internet, but since the communication channel is not safe C can intercept the message. For example in the picture below, A sends a message containing m to B, but C intercepts the message by changing the content to m' and sends it to B, still in A's name.



So B receives the message in A's name but with a different content. The intruder C can also change the name of the claimed sender, or stop the message from arriving to destination. So when A sends a message to B, he cannot make sure that B received the message in the first place, and that if he receives it, it is the same message that was sent by A and not changed by C on the way. Similarly when B receives a message with A's name on it as claimed sender, he cannot be sure if the message was really sent by A, or the intruder has faked A's name on it. Also he is not sure if the content of the message is the original content that was sent by A, since maybe the intruder has changed the content on the way. In security terms, agents A and B cannot *authenticate* and make sure they are talking to each other. Authentication is the first step towards sending secrets over the channel: if A is sure that B receives his messages as they were sent, that is if A authenticates with B, he can send his secret to B. On the other side, if B is sure that the message he received from A is really sent by A and has not been intercepted on the way, that is if B authenticates with A, then he knows that he can receive a secret form A. Authentication is not easy to achieve over unsafe channels like internet. This is why simple-message passing cannot be the base of sharing secrets over unsafe channels and one has to design protocols involving series of messages and encryption. Designing such protocols and proving that they are safe, that is agents involved in them correctly reach authentication after running the protocol, constitutes one of the areas of the field of security. Proving the safety property is not an easy task: it involves having to consider many factors and possibilities and in many cases flaws are discovered in them. A well-known example is the Needham-Schroeder protocols [68] that was proven to be safe for 15 years using BAN logic [22], an epistemic logic tailored for security purposes. It was shown by Lowe [59] that the protocol, although proven to be safe, was not safe by building a path according to which the agents would wrongly authenticate with an intruder.

In what follows I will show how by adding dynamics to epistemic logic (or epistemics to dynamic logic) and taking into account the epistemic structure of actions to encode misinformation actions, one can encode *suspicions* of agents about the interception actions and prevent the false authentication. I will show how this way of encoding security protocols leads to the discovery of the path of Lowe-like attacks and thus would not result in the wrong safety proofs.

5.2 Message Passing Actions

The communication actions in a security protocol are secret message passing actions. These are similar to the *misinformation* actions that we dealt with earlier, for example the referee of the coin-toss example taking a peek and the children in the muddy children puzzle cheating or lying. So when agent A sends a message containing m to B, he is secretly communicating m to B, an action denoted as

$$q^{A,m,B}$$

The problem with this single action encoding is that it consists of different actions: the action of A sending m and the action of B receiving m. Such an encoding will work in the situations that the communication channel is safe and every send is followed by its receive. For example in the muddy children, child 2 secretly tells to child 3 via action π that he is dirty and child 3 hears it immediately. Where as when A sends m to B, he might not receive it at all, or receive m' instead. So not every send is followed by its corresponding receive.

An option would be to continue treating this action as the secret communication action, but instead of reading it as 'A secretly communicates m to B', read it as 'A sends m to B and B receives it'. The problem would then be that secret communication actions appear as they are to the agents involved in them. So for example the cheating action π of the muddy children appeared as it was to the cheating children 2 and 3

$$f^Q_{C_2}(\pi) = f^Q_{C_3}(\pi) = \pi$$

So we should have the following for our message passing action:

$$f^Q_A(q^{A,m,B}) = f^Q_B(q^{A,m,B}) = q^{A,m,B}$$

which is not true, since when A sends m to B, he does not think that B will receive it.

Decomposition. The way to go is to decompose the message passing action to two sub-actions:

$$q^{A,m,B} \begin{cases} q^{A,s,m,B} & A \text{ sends } m \text{ to } B \\ q^{B,r,m,A} & B \text{ receives } m \text{ in } A's \text{ name} \end{cases}$$

where in the send action A is the real sender, s says that this action is a send action, m is the propo-

sitional content of the message, and B is the intended receiver that might not turn out to be the real receiver. The receive action has a similar format: r says that this is a receive action, A is the claimed sender, B is the agent that receives the message, and m is the received content of the message. The send and receive sub-actions have different f_A^Q maps, however, since they have the same content m, they stand for the same epistemic actions, in the sense that they result in the same updates. In this sense, any secret communication can be seen as a sequential composition of its two sub-actions

$$q^{A,m,B} \quad \text{can be seen as} \quad q^{A,s,m,B} \bullet q^{B,r,m,A}$$

where the order of composition does not matter since the channel is safe and the send and receive are assumed to happen at the same time:

$$q^{A,m,B} \quad \text{can be seen as} \quad q^{A,s,m,B} \bullet q^{B,r,m,A} = q^{B,r,m,A} \bullet q^{A,s,m,B}$$

In order to maintain this aspect of our decomposing, we have to do a unification of the two decomposed sub-actions. So we ask our quantale to satisfy a weak unification via the following two axioms:

Unification. For two actions $q^{A,s,m,B}$ and $q^{B,r,m,A}$ with the same content $m \in M$, we have:

$$q^{A,s,m,B} \bullet q^{B,r,m,A} \leq q^{A,s,m,B} \tag{5.1}$$

$$q^{A,s,m,B} \bullet q^{B,r,m,A} \leq q^{B,r,m,A} \tag{5.2}$$

This implies that the update induced by the sequential composition of a send and receive action with the same content and between the same agents, is stronger than and thus entails the update induced by any of its send or receive sub-actions. In terms of the order on the quantale, it means that the sequential composition of a send action followed by its corresponding receive action is more deterministic than the send or receive actions on their own. We refer to these axioms as the *deterministic send and receive* axioms respectively. These axioms will be used to derive that after A sends m to B and B receives it, A knows that he did the send action and similarly B know that he did the receive action.

5.3 Suspicions about Actions

In the previous chapters, we interpreted the endomorphisms of the quantale, that is the f_A^Q maps as the appearance of agents about an action. In the security setting, we read these maps as *suspicions* that each agent has about the messages he sends or receives. For example $f_A^Q(q)$ stands for all the actions agent A suspects that could have happened where q is the action that has really happened. As before the adjoints to these maps stand for *knowledge of agents about actions*. The adjunction equations below

$$\frac{f_A^Q(q) \leq q'}{q \leq \Box_A^Q q'}$$

will now reads as 'if A's suspicions about action q are more deterministic than action q' then q is more deterministic than A's knowledge about action q' and vise-versa'. This reading is not very intuitive. We can re-read it as 'if when (or after) q happens, agent A *suspects* that q' has happened, then when (or after) q happens, agent A *knows* that q' has happened and vice versa. As before, two consequences of this adjunction are

$$(1) \quad f_A^Q(\Box_A^Q\, q) \leq q \qquad \text{and} \qquad (2) \quad q \leq \Box_A^Q\, f_A^Q(q)$$

The first one says that when A knows that q, he also suspects that q. The second one says that after action q, agent A knows all of his suspicions about q. This second consequence is used to express knowledge of agents after a series of messages have been passed in a security protocol.

We have to assign suspicions to the send and receive actions for each agent, that is suspicions of the sender about the send and receive actions and also suspicions of the receiver about the send and receive actions. From these four groups, the following two are the important ones

1. Suspicions of a sender about the receive of the content of his message in his name
2. Suspicions of a receiver about the originality of the content and the name of the claimed sender of the received message.

The other two groups are identities, since sender is sure about his send action and similarly the receiver has no doubts about his receive actions. But they both have suspicions about the corresponding actions of the other party.

When agent A sends a message containing proposition m to agent B, we assume that he suspects the following five things about the receive of his message by agent B:

1. He suspects that agent B might have received the message unchanged, that is exactly as it was sent: he received m in A's name, which is the following action

$$q^{B,r,m,A}$$

2. He suspects that the intruder C might have changed the content of his message to another proposition m'. In this case the intruder's actions are: he received A's message and sent another message to B with a fake content m' but kept A's name on it, so B received a message in A's name but with a different content, which is the following sequential composition

$$q^{C,r,m,A} \bullet q^{C,s,m',B} \bullet q^{B,r,m',A}$$

3. He suspects that the intruder C might have changed the sender's name from A to his own name C, but kept the original content unchanged, that is putting C in the claimed sender's field, and

then sending it to B. These actions of C form the following sequential composition

$$q^{C,r,m,A} \bullet q^{C,s,m,B} \bullet q^{B,r,m,C}$$

4. He suspects that the intruder C might have changed both the original content, for example m to m', and the claimed sender from A to C. His actions are

$$q^{C,r,m,A} \bullet q^{C,s,m',B} \bullet q^{B,r,m',C}$$

5. The last option might be that C stopped the message and took no further actions, thus B received nothing. In this case, C's actions are

$$q^{C,r,m,A} \bullet 1$$

Agent A has all these suspicions and is not sure which one has really happened in reality. So we use the non-deterministic choice of the quantale to put all these cases together and form the suspicions of agent A about the receive action:

$$\begin{aligned} f_A(q^{B,r,m,A}) \;=\; & q^{B,r,m,A} \\ \vee\; & (q^{C,r,m,A} \bullet q^{C,s,m',B} \bullet q^{B,r,m',A}) \\ \vee\; & (q^{C,r,m,A} \bullet q^{C,s,m,B} \bullet q^{B,r,m,C}) \\ \vee\; & (q^{C,r,m,A} \bullet q^{C,s,m',B} \bullet q^{B,r,m',C}) \\ \vee\; & (q^{C,r,m,A} \bullet 1) \end{aligned}$$

This says that A suspects either of these disjuncts could have happened. Although very suspicious about the receive of his message, agent A has no suspicions about the action originated from his own side, that is the send action. This is denoted by making the suspicion operator act as identity:

$$f_A(q^{A,s,m,B}) = q^{A,s,m,B}$$

Now assume that after agent A sent his message, agent B received the message exactly as it was, but of course he does not know that he has received the message unchanged. So what does B suspect about the message he has received? We assume that B's suspicions about the send action are the following four cases

1. B suspects that the message might have been sent exactly as he received it, that is containing m and sent by A, that is

$$q^{A,s,m,B}$$

2. But that it might as well have been that A sent another content m' and the intruder changed it to

m on the way. These form the following sequential composition

$$q^{A,s,m',B} \bullet q^{C,r,m',A} \bullet q^{C,s,m,B}$$

3. Or it might have been the case that A intended the message to C, but C is redirecting it to B without changing anything. These form the following sequential composition

$$q^{A,s,m,C} \bullet q^{C,r,m,A} \bullet q^{C,s,m,B}$$

4. It might have been the case that A sent another message containing m' to C and C changed both the content to m and the intended receiver's name and redirected it to B in A's name, that is

$$q^{A,s,m',C} \bullet q^{C,r,m',A} \bullet q^{C,s,m',B}$$

Note that B can also suspect that A was not the original sender, but we ignore this option for the time. Because if we want to consider it, we either have to add another agent other than C as the real sender, and this will double the length of all suspicions, or assume A can also be an intruder, which is contradictory with our other assumption that C was the only intruder. Ignoring these suspicions, however, will not change our results about authentication[1].

We use the non-deterministic choice to put all these cases together and form the suspicions of B about the send action:

$$\begin{aligned} f_B(q^{A,s,m,B}) &= q^{A,s,m,B} \\ &\vee \ (q^{A,s,m',B} \bullet q^{C,r,m',A} \bullet q^{C,s,m,B}) \\ &\vee \ (q^{A,s,m,C} \bullet q^{C,r,m,A} \bullet q^{C,s,m,B}) \\ &\vee \ (q^{A,s,m',C} \bullet q^{C,r,m',A} \bullet q^{C,s,m,B}) \end{aligned}$$

Similar to the previous case, B is sure about his own actions, that is the receive of the message:

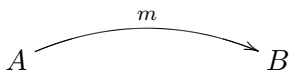
$$f_B(q^{B,r,m,A}) = q^{B,r,m,A}$$

We have now associated suspicions about each action to each honest agent involved in the protocol. These form the base of our setting. In the next section we show how suspicions of agents about protocols (sequences of send and receive actions) can be compositionally calculated from these suspicions.

[1] If we parametrize the agents and contents, then this option then we would have a better way to encode suspicions and can add these suspicions as well.

5.4 Suspicions about Protocols

We can build protocols by sequentially composing the send and receive actions. For example a one message protocol α between A and B is:



and can be written compositionally as:

$$\alpha = q^{A,s,m,B} \bullet q^{B,r,m,A}$$

Agent A's suspicions about the whole protocol is the sequential composition of his suspicions about each action in the protocol:

$$f_A(\alpha) = f_A(q^{A,s,m,B} \bullet q^{B,r,m,A}) \leq f_A(q^{A,s,m,B}) \bullet f_A(q^{B,r,m,A})$$

which is equal to

$$\begin{aligned} f_A(\alpha) \quad \leq \quad & q^{A,s,m,B} \bullet \\ & (q^{B,r,m,A} \ \vee (q^{C,r,m,A} \bullet q^{C,s,m',B} \bullet q^{B,r,m',A}) \ \vee \\ & (q^{C,r,m,A} \bullet q^{C,s,m,B} \bullet q^{B,r,m,C}) \quad \vee \\ & (q^{C,r,m,A} \bullet q^{C,s,m',B} \bullet q^{B,r,m',C}) \ \vee \\ & (q^{C,r,m,A} \bullet 1)) \end{aligned}$$

By distributivity of join over multiplication we get the following choices

$$\begin{aligned} f_A(\alpha) \quad \leq \quad & (q^{A,s,m,B} \bullet q^{B,r,m,A}) \ \vee \\ & (q^{A,s,m,B} \bullet q^{C,r,m,A} \bullet q^{C,s,m',B} \bullet q^{B,r,m',A}) \ \vee \\ & (q^{A,s,m,B} \bullet q^{C,r,m,A} \bullet q^{C,s,m,B} \bullet q^{B,r,m,C}) \ \vee \\ & (q^{A,s,m,B} \bullet q^{C,r,m,A} \bullet q^{C,s,m',B} \bullet q^{B,r,m',C}) \ \vee \\ & (q^{A,s,m,B} \bullet q^{C,r,m,A} \bullet 1) \end{aligned}$$

This says that A cannot distinguish between the choice of the above sequences of messages: he is not sure which one has really taken place. In particular, he is not sure if B received his message unchanged. This is because it is not the case that every disjunct is less than or equal to $q^{B,r,m,A}$ (or $q^{B,r,m,A}$ is not part of all of the suspicions). In other words, we cannot prove that $f_A(\alpha) \leq q^{B,r,m,A}$ from our assumptions, so it is fair to say

$$f_A(\alpha) \not\leq \ q^{B,r,m,A}$$

Similarly we can calculate $f_B(\alpha)$ and see that B is also not sure about the originality of the message he received

$$f_B(\alpha) \not\leq q^{A,s,m,B}$$

In knowledge terms, after A sent his message to B and B received it, A does not know if B received his message (unchanged) and B does not know if the message was really sent by A:

$$\alpha \not\leq \Box_A\, q^{B,r,m,A} \qquad \text{and} \qquad \alpha \not\leq \Box_A\, q^{A,s,m,B}$$

The only things they know are the trivialities, that is actions done by themselves and also each agent knows his own suspicions:

$$\begin{aligned} \alpha \leq \Box_A\, q^{A,s,m,B} \qquad &\text{and} \qquad \alpha \leq \Box_B\, q^{B,r,m,A} \\ \alpha \leq \Box_A\, f_A(\alpha) \qquad &\text{and} \qquad \alpha \leq \Box_B\, f_B(\alpha) \end{aligned}$$

To see that for example $\alpha \leq \Box_A\, q^{A,s,m,B}$, recall the *deterministic send* axiom

$$q^{A,s,m,B} \bullet q^{B,r,m,A} \leq q^{A,s,m,B}$$

Since f_A is order-preserving, we can apply it to both sides

$$f_A(q^{A,s,m,B} \bullet q^{B,r,m,A}) \leq f_A(q^{A,s,m,B})$$

Now we know that $f_A(q^{A,s,m,B}) = q^{A,s,m,B}$ so

$$f_A(q^{A,s,m,B} \bullet q^{B,r,m,A}) \leq q^{A,s,m,B}$$

which is by adjunction equivalent to

$$q^{A,s,m,B} \bullet q^{B,r,m,A} \leq \Box_A\, q^{A,s,m,B}$$

By using one of the consequences of suspicion-knowledge adjunction (also the third case above) $\alpha \leq \Box_A\, f_A(\alpha)$, we can show that A knows that a choice of actions might have happened to what B received:

$$\alpha \leq \Box_A\, (q^{B,r,m,A} \vee q^{B,r,m',A} \vee q^{B,r,m,C} \vee q^{B,r,m',C})$$

similarly for B, after he received the message from A, he knows a choice of actions could have happened on A's side, but he is not sure which one, in particular why he is not sure it was A who sent him m. We are now going to use our knowledge operator to define authentication between two agents A and B

Definition 5.4.1 Authentication. After agent A sends a message to agent B and B receives it, he authenticates with B if the following holds

$$q^{A,s,m,B} \bullet q^{B,r,m,A} \leq \Box_A \, q^{B,r,m,A}$$

Note that this is an authentication on both data and identity. Similarly, agent B authenticates with A if the following holds

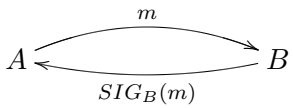
$$q^{A,s,m,B} \bullet q^{B,r,m,A} \leq \Box_B \, q^{A,s,m,B}$$

As we have showed above, that after a one-message protocol agents A and B cannot authenticate. In the next section we take one step towards authentication by extending and enriching this simple protocol.

5.5 Challenge-Response with Signature

The Challenge-Response protocol with digital signature on a fresh content (nonce) is a two message protocol that was thought to be safe before an attack was discovered on it. By 'thought to be safe' we mean that it was proven in a logic that agents could safely reach authentication after running the protocol. The attack then showed a path according to which this authentication could not be reached because an intruder would make one of the agents wrongly authenticate with him. We encode the protocol in our logic and show that after running it, our agents would not reach authentication in the first place, and more interestingly the reason they would not do so is because they will suspect the path of the attack according to the base suspicions we set before.

In this protocol, agent A sends m to agent B, this being a fresh content never communicated before. Upon receive, agent B has to sign this content with his unforgeable signature and send it back to A. The protocol is depicted as



The sequential composition of messages (after A has freshly created m[2]) in this protocol are

$$\alpha = q^{A,s,m,B} \bullet q^{B,r,m,A} \bullet q^{B,s,SIG_B(m),A} \bullet q^{A,r,SIG_B(m),B}$$

The suspicions of agent A about the protocol are the sequential composition of his suspicions about each message:

$$f_A(\alpha) \leq f_A(q^{A,s,m,B}) \bullet f_A(q^{B,r,m,A}) \bullet f_A(q^{B,s,SIG_B(m),A}) \bullet f_A(q^{A,r,SIG_B(m),B})$$

[2]We cannot encode non-epistemic actions such as creating a nonce in this setting, but we can encode these actions as epistemic ones. For example we can make a fresh nonce being announced privately to A.

Agent A's suspicions about B receiving the first message $f_A(q^{A,s,m,B})$ are exactly as before. His suspicions about B sending the second message $f_A(q^{B,s,SIG_B(m),A})$ can be similarly set:

$$\begin{aligned} f_A(q^{B,s,SIG_B(m),A}) &= q^{B,s,SIG_B(m),A} \\ &\vee \ (q^{B,s,m',A} \bullet q^{C,r,m',B} \bullet q^{C,s,SIG_B(m),A}) \\ &\vee \ (q^{B,s,m,C} \bullet q^{C,r,m,B} \bullet q^{C,s,SIG_B(m),A}) \\ &\vee \ (q^{B,s,m',C} \bullet q^{C,r,m',B} \bullet q^{C,s,SIG_B(m),A}) \end{aligned}$$

and as before A is sure about his own actions.

$$f_A(q^{A,s,m,B}) = q^{A,s,m,B} \qquad \text{and} \qquad f_A(q^{A,r,SIG_B(m),B}) = q^{A,r,SIG_B(m),B}$$

Substitute these suspicions in $f_A(\alpha)$ and distribute the sequential composition over joins and A gets twenty different scenarios, nineteen of them rivals to reality α.

$$f_A(\alpha) \leq \alpha \vee (\bigvee_{i=2}^{20} \alpha_i)$$

Fortunately, most of them will not be valid scenarios. For example some of these alternatives are

$$\begin{aligned} \alpha_2 &= q^{A,s,m,B} \bullet q^{B,r,m,A} \bullet q^{B,s,m',A} \bullet q^{C,r,m',B} \bullet q^{C,s,SIG_B(m),A} \bullet q^{A,r,SIG_B(m),B} \\ \alpha_3 &= q^{A,s,m,B} \bullet q^{B,r,m,A} \bullet q^{B,s,SIG_B(m),C} \bullet q^{C,r,SIG_B(m),B} \bullet q^{C,s,SIG_B(m),A} \bullet q^{A,r,SIG_B(m),B} \\ \alpha_4 &= q^{A,s,m,B} \bullet q^{B,r,m,A} \bullet q^{B,s,m',C} \bullet q^{C,r,m',B} \bullet q^{C,s,SIG_B(m),A} \bullet q^{A,r,SIG_B(m),B} \\ \alpha_5 &= q^{A,s,m,B} \bullet q^{C,r,m,A} \bullet q^{C,s,m',B} \bullet q^{B,r,m',A} \bullet q^{B,s,SIG_B(m'),A} \bullet q^{C,r,SIG_B(m'),B} \bullet \\ &\quad q^{C,s,SIG_B(m),A} \bullet q^{A,r,SIG_B(m),B} \\ \alpha_6 &= q^{A,s,m,B} \bullet q^{B,r,m,A} \bullet q^{B,s,SIG_B(m),A} \bullet q^{C,r,SIG_B(m),B} \bullet q^{C,s,SIG_B(m),A} \bullet q^{A,r,SIG_B(m),B} \\ \alpha_7 &= q^{A,s,m,B} \bullet q^{C,r,m,A} \bullet q^{C,s,m,B} \bullet q^{B,r,m,A} \bullet q^{B,s,SIG_B(m),A} \bullet q^{A,r,SIG_B(m),B} \\ \alpha_8 &= q^{A,s,m,B} \bullet q^{C,r,m,A} \bullet q^{C,s,m,B} \bullet q^{B,r,m,C} \bullet q^{B,s,SIG_B(m),C} \bullet q^{C,r,SIG_B(m),B} \bullet \\ &\quad q^{C,s,SIG_B(m),A} \bullet q^{A,r,SIG_B(m),B} \end{aligned}$$

The first three are not valid, since they contradict agent B's honesty. For example in α_2, when B receives m from A, why would he reply with m' and not with $SIG_B(m)$? He is aware he is running the protocol with A and knows his role. Agent A is also aware of this and thus he will discard this alternative scenario. In order to implement this in the system, we design axioms for honesty by assigning $\perp$ of quantale, which is the unit of $\vee$, to the contradictory scenarios, and thus eliminate them from A's suspicions. For example the following will be an instance of honesty axioms

$$q^{B,r,m,A} \bullet q^{B,s,m',A} = \perp$$

and as a result the scenario containing it gets eliminated from A's suspicions:

$$\alpha_2 = \bot \quad \Rightarrow \quad f_A(\alpha) \leq \alpha \vee (\bigvee_{i=3}^{20} \alpha_i)$$

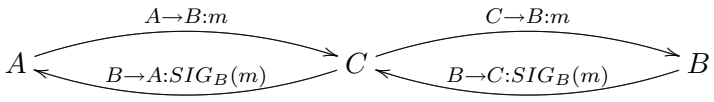
Scenarios 3 and 4 get eliminated in the same way, that is according to honesty axioms. Scenario α_5 is also not valid, but according to axioms of digital signature on fresh nonces. Since the digital signature is not forgeable by the intruder and m is freshly generated by A, it could not be the case that intruder C receives B's signature on m' and forges his signature on m (or uses B's signature from an old message) and then sends in to A. In order to deal with these cases, we design axioms for honesty and signature on fresh nonces, for example the following will be an instance of signature axioms

$$q^{C,r,SIG_B(m'),B} \bullet q^{C,s,SIG_B(m),A} = \bot$$

The 13 other scenarios starting from α_9 also get discarded by either honesty or signature axioms. What remains are the three scenarios $\alpha_6, \alpha_7, \alpha_8$, these do not get discarded by any axiom and remain as valid alternative scenarios for A. The first two say that C has been reading the messages, but not doing any harm to them. On the other hand, the last one, that is α_8 repeated below

$$\begin{aligned} \alpha_8 \quad = \quad & q^{A,s,m,B} \bullet q^{C,r,m,A} \bullet q^{C,s,m,B} \bullet q^{B,r,m,C} \bullet q^{B,s,SIG_B(m),C} \bullet q^{C,r,SIG_B(m),B} \bullet \\ & q^{C,s,SIG_B(m),A} \bullet q^{A,r,SIG_B(m),B} \end{aligned}$$

This is exactly the path that stops A from authenticating with B since in this path B is intending his second message to C and not to A. The path can be pictured as follows:



This path suggests a scenario in which B did not receive A's first message in A's name (he received it in C's name) and thus did not intend his second message for A (it was intended for C). So although A receives B's signature on his nonce, B did not intend it for him.

Now that we have discarded the contradictory suspicions, we can proceed and calculate A's knowledge, using its adjunction with suspicions

$$\frac{f_A(\alpha) \leq \alpha \vee \alpha_6 \vee \alpha_7 \vee \alpha_8}{\alpha \leq \Box_A (\alpha \vee \alpha_6 \vee \alpha_7 \vee \alpha_8)}$$

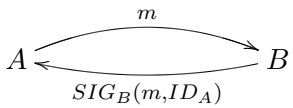
So A is not sure, that is he does not know, which one of these scenarios has happened in reality. In particular, he does not know if B received A's message as it was sent

$$\alpha \leq \Box_A (q^{B,r,m,A} \vee q^{B,r,m,C})$$

Also he does not know if B's second message was intended for him:

$$\alpha \leq \Box_A \, (q^{B,s,SIG_B(m),A} \vee q^{B,s,SIG_B(m),C})$$

Adding Identities. It is now well-known that in order to avoid the attack to the above protocol, one has to add identities to the signature [27]. We show that if one does so in our setting, the alternative path α_8 will also get discarded and A gets to authenticate with B. In this version of the protocol B is supposed to include the identity of the claimed sender of the first message in his signature. We call this version α' and picture it as follows



Now the alternative attack scenario α_8 will become

$$\alpha_8 = q^{A,s,m,B} \bullet q^{C,r,m,A} \bullet q^{C,s,m,B} \bullet q^{B,r,m,C} \bullet q^{B,s,SIG_B(m,ID_C),C} \bullet \\ q^{C,r,SIG_B(m,ID_C),B} \bullet q^{C,s,SIG_B(m,ID_A),A} \bullet q^{A,r,SIG_B(m,ID_A),B}$$

but $q^{C,r,SIG_B(m,ID_C),B} \bullet q^{C,s,SIG_B(m,ID_A),A}$ is against the signature being unforgeable and gets eliminated by signature axiom. After the protocol α', agent A can finally authenticate with B, that is we can prove the following two inequalities

$$\alpha' \leq \Box_A \, q^{B,r,m,A} \qquad \text{and} \qquad \alpha' \leq \Box_A \, q^{B,s,SIG_B(m,ID_A),A}$$

The two other rival scenarios are still valid, but as before, they do not do any harm to A's knowledge, just making A suspect that the whole thing has been done under C's eyes. The same authentication result can be obtained in the shared hashes version of challenge response [27] and using the proper axioms for hash.

5.6 Axioms for Honesty and Signature

In this section we add proper axioms to our quantale in order to formalize the honesty of agents and the unforgeability of digital signatures. These are the axioms that will discard the contradictory alternative scenarios from the suspicions of agents. We assume that m and $SIG_B(m)$ are propositions, that is elements of the module

$$m, SIG_B(m) \in M$$

For example m can be the proposition that says 'number m is a nonce'. Assume also that
(i) x, y, z are variables ranging over propositions,
(ii) A, B, C are the agents; with A being the honest challenger, B the honest responder, and C the

non-honest intruder,
(iii) Y, Z are variables ranging over agents.

Honesty axioms

We have two axiom schemas for honesty:

1. Honesty axiom schema one

$$\text{If} \quad q^{B,r,x,A} \bullet q^{B,s,y,A} \quad \text{and} \quad y \neq SIG_B(x) \quad \text{then} \quad q^{B,r,x,A} \bullet q^{B,s,y,A} = \perp$$

   It says that since B is the honest responder in a Challenge-Response with signatures, he acts according to his role and will only respond with his signature on what he receives. So it is impossible that he responds with anything else.

2. Honesty axiom schema two

$$\text{If} \quad q^{B,r,x,Y} \bullet q^{B,s,y,Z} \quad \text{and} \quad Y \neq Z \quad \text{then} \quad q^{B,r,x,Y} \bullet q^{B,s,y,Z} = \perp$$

   This says that, again since B is honest, he will only respond to the claimed sender of the message he receives. So it is impossible that he replies to someone else.

Here are the instances of these schemas in the alternative scenarios of Challenge Response with signature. The first three are instances of the first schema and the rest instances of the second one.

$$\begin{aligned}
1- \quad & q^{B,r,m,A} \bullet q^{B,s,m',A} = \perp \\
2- \quad & q^{B,r,m',A} \bullet q^{B,s,SIG_B(m),A} = \perp \\
3- \quad & q^{C,s,m',A} \bullet q^{A,r,SIG_B(m),B} = \perp \\
4- \quad & q^{B,r,m',A} \bullet q^{B,s,m',A} = \perp \\
5- \quad & q^{B,r,m,C} \bullet q^{B,s,SIG_B(m),A} = \perp \\
6- \quad & q^{B,r,m,C} \bullet q^{B,s,m',A} = \perp \\
7- \quad & q^{B,r,m',C} \bullet q^{B,s,SIG_B(m),A} = \perp \\
8- \quad & q^{B,r,m',C} \bullet q^{B,s,m',A} = \perp
\end{aligned}$$

Axiom for Digital Signature on a Fresh Nonce

With the assumption that z ranges over fresh propositions, we have the following schemas for signature:

$$\text{If} \quad q^{C,r,x,B} \bullet q^{C,s,y,A} \quad \text{and} \quad y = SIG_B(z), x \neq SIG_B(z) \quad \text{then} \quad q^{C,r,x,B} \bullet q^{C,s,y,A} = \perp$$

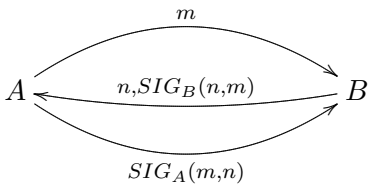
It says that the intruder cannot forge B's signature (on a fresh nonce), that is, if he receives a not-signed proposition from B, it is impossible that he creates B's signature on it and sends it (to any agent). Also that if he receives B's signature on a proposition, he cannot transfer it to another proposition and send

it signed to A. Instances of this schema in our example are

$$\begin{aligned} 1- \quad & q^{C,r,SIG_B(m),B} \bullet q^{C,s,SIG_B(m'),A} = \bot \\ 2- \quad & q^{C,r,SIG_B(m'),B} \bullet q^{C,s,SIG_B(m),A} = \bot \end{aligned}$$

5.7 Challenge-Response with Three Messages

We have shown how agent A gets to authenticate with agent B in a Challenge Response with signatures and identities, but B has still no clue to whom he is talking. Three message Challenge-Response [27] is designed so that agent B can also authenticate with agent A. As before, we start by the three message version without identities and show that B suspects the attack path and thus will not authenticate with A, then we show how adding identities solves the problem. The protocol is pictured as follows:



We denote this protocol by γ. Exactly in the same lines as for agent A in the two-message protocols above and using our base suspicions, we calculate suspicions of agent B about this protocol. As before we get a disjunct of alternative scenarios, most of which get discarded by the axioms, some of the remaining ones are with a passive intruder watching over messages and not changing them. The following two scenarios are the active remaining paths that survive the signature and honesty axioms:

$$f_B(\gamma) \leq \gamma_1 \vee \gamma_2$$

From these two the first one γ_1 suggests a similar path as in Challenge Response with two messages, according to which A cannot authenticate with B since C intercepts his messages and makes B intend the responses for C, as opposed to A. This scenario is as follows

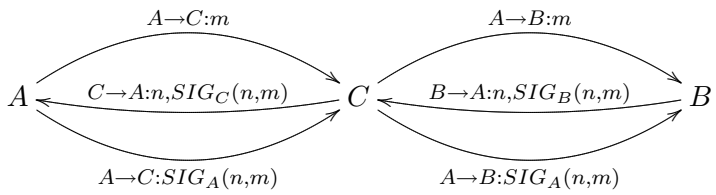
$$\begin{aligned} \gamma_1 \quad = \quad & q^{A,s,m,B} \bullet q^{C,r,m,A} \bullet q^{C,s,m,B} \bullet q^{B,r,m,C} \\ & \bullet q^{B,s,\{n,SIG_B(n,m)\},C} \bullet q^{C,r,\{n,SIG_B(n,m)\},B} \bullet q^{C,s,\{n,SIG_B(n,m)\},A} \bullet q^{A,r,\{n,SIG_B(n,m)\},B} \\ & \bullet q^{A,s,SIG_A(n,m),B} \bullet q^{C,r,SIG_A(n,m),A} \bullet q^{C,s,SIG_A(n,m),B} \bullet q^{B,r,SIG_A(n,m),C} \end{aligned}$$

The second scenario is the path along which B cannot authenticate with A. In this scenario, B suspects that A will somehow starts a run of the protocol with C and then C uses A's messages that were intended for C, to make B think that he is communicating with A, were as it is C who is on the

other side. This scenario is as follows

$$\begin{aligned}\gamma_2 \;=\;& q^{A,s,m,C} \bullet q^{C,r,m,A} \bullet q^{C,s,m,B} \bullet q^{B,r,m,A} \\ & \bullet q^{B,s,\{n,SIG_B(n,m)\},A} \bullet q^{C,r,\{n,SIG_B(n,m)\},B} \bullet q^{C,s,\{n,SIG_C(n,m)\},A} \bullet q^{A,r,\{n,SIG_C(n,m)\},C} \\ & \bullet q^{A,s,SIG_A(n,m),C} \bullet q^{C,r,SIG_A(n,m),A} \bullet q^{C,s,SIG_A(n,m),B} \bullet q^{B,r,SIG_A(n,m),A}\end{aligned}$$

and can be pictured as follows:



The scenario starts when A sends m to C and C sends it to B in A's name. So B thinks that A wants to run the protocol with him, he signs m and produces a fresh n and sends it along to A. The intruder stops this message, now that he has both m and n, he signs them with his own signature and sends them in the expected format, that is $\{n, SIG_C(n,m)\}$ to A. Then A signs both n and m and sends them to C, where they are sent exactly as they are to B, but in A's name. At this point B will think that A intended this message for him, where as he is wrong. It is along this suspected path that B will not authenticate with A, that is

$$\gamma \not\leq \Box_B\, q^{A,s,SIG_A(n,m),B}$$

he can also not be sure that A received the message in B's name, that is

$$\gamma \not\leq \Box_B\, q^{A,r,\{n,SIG_B(n,m)\},B}$$

This prevents B from authenticating with A in the challenge response with three messages and signatures. In order to show how the other scenarios get discarded we need to change our axioms for honesty and signature and extend them to this three message protocol. The reason our previous formalization will not work is that there honest agents where only challenger or responder, so B's role as the responder was to sign what he receives and send it back. Where as in the three message case, these roles increase: B also gets a challenger roles and thus A has to sign what he receives.

Axioms for honesty and signature. As before, we assume that n and $SIG_B(n,m)$ are both propositions $n, SIG_B(n,m) \in M$ and that $\{n, SIG_B(n,m)\} = n \wedge SIG_B(n,m)$, where $\wedge$ is the meet on the module. So to say that for example n is included in $\{n, SIG_B(n,m)\}$, we can say $\{n, SIG_B(n,m)\} \leq n$. The axioms schemas for honesty and signature can now be extended to

1. Honesty axiom schema one

$$\begin{aligned}&\text{If} \quad q^{B,r,x,A} \bullet q^{B,s,y,A} \quad \text{and} \quad y \neq \{z, SIG_B(z,x)\} \quad \text{then} \quad q^{B,r,x,A} \bullet q^{B,s,y,A} = \bot \\ &\text{If } q^{A,r,\{z,SIG_B(z,x)\},B} \bullet q^{A,s,y,B} \text{ and } y \neq SIG_A(z,x) \quad \text{then} \quad q^{A,r,\{z,SIG_B(z,x)\},B} \bullet q^{A,s,y,B} = \bot\end{aligned}$$

These encode the fact that A and B respond with what they are supposed to. It is an extension of the previous axiom since it also formalizes A's role in signing.

2. Honesty axiom schema two

$$\begin{array}{llllll} \text{If} & q^{B,r,x,Y} \bullet q^{B,s,y,Z} & \text{and} & Y \neq Z & \text{then} & q^{B,r,x,Y} \bullet q^{B,s,y,Z} = \bot \\ \text{If} & q^{A,r,x,Y} \bullet q^{A,s,y,Z} & \text{and} & Y \neq Z & \text{then} & q^{A,r,x,Y} \bullet q^{A,s,y,Z} = \bot \end{array}$$

These encode the fact that A and B respond to whom they are supposed to. It is an extension of our previous axiom since it also encodes A's role as the honest responder to the claimed sender of the messages that his receives. These axioms can be unified by parameterizing over honest agents, so for $V \in \{A, B\}$ we have the following for honesty axiom schema two

$$\text{If} \quad q^{V,r,x,Y} \bullet q^{V,s,y,Z} \quad \text{and} \quad Y \neq Z \quad \text{then} \quad q^{V,r,x,Y} \bullet q^{V,s,y,Z} = \bot$$

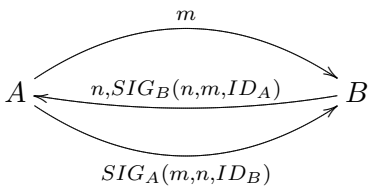
3. Signature axiom schema

$$\begin{array}{llllll} \text{If} & q^{C,r,x,B} \bullet q^{C,s,y,A} & \text{and} & y = SIG_B(z), x \neq SIG_B(z) & \text{then} & q^{C,r,x,B} \bullet q^{C,s,y,A} = \bot \\ \text{If} & q^{C,r,x,A} \bullet q^{C,s,y,B} & \text{and} & y = SIG_A(z), x \neq SIG_A(z) & \text{then} & q^{C,r,x,A} \bullet q^{C,s,y,B} = \bot \end{array}$$

This axiom says that C cannot forge neither A's nor B's signatures. It extends our previous axiom by adding A's signature to the set of unforgeable signatures. In fact these two axioms can be unified if we use variables V, W to range over honest agents A and B as follows:

$$\text{If} \quad q^{C,r,x,V} \bullet q^{C,s,y,W} \quad \text{and} \quad y = SIG_V(z), x \neq SIG_V(z) \quad \text{then} \quad q^{C,r,x,V} \bullet q^{C,s,y,W} = \bot$$

Adding Identities.
If we add identities, like in the two message case, then the alternative scenarios will also get discarded and as a result B can authenticate with A. This protocol is pictured as



The alternative scenarios γ_1 and γ_2 both get discarded by the signature axiom. Now A authenticates with B in the same way as in the Challenge-Response with signature and identities. Moreover, B also authenticates with A on the arrival of second message and sent of third message as follows

$$\gamma \leq \Box_B \, q^{A,r,\{n,SIG_B(n,m,ID_A)\},B} \qquad \text{and} \qquad \gamma \leq \Box_B \, q^{A,s,SIG_B(m,n,ID_B),B}$$

That is after the challenge response with digital signature and identities, agent B knows that agent A received the second message and it was indeed A who sent him the third message.

5.8 Derived Properties of Suspicion and Knowledge

In our setting, suspicions are quantale homomorphisms: they are join and composition preserving. Composition is also join preserving. All of these are order preserving. These relations enable us to put together simple protocols by composition and non-deterministic choice and build new more complicated protocols. We can then derive interesting properties for the suspicions of agents about these new protocols. Moreover, we can compare different agents' suspicions about one protocols, and suspicions of one agent about different protocols. Consequently, we can reason about and compare knowledge of agents about composition and choice of protocols. The following are examples of these derived properties:

- Composition of protocols and suspicion
  If after protocol α agent A suspects that action q has happened, and after protocol β he suspects that action q' has happened, then after the composition of protocols α and β he suspects the composition of his previous suspicions $q \bullet q'$.

$$f_A(\alpha) \leq q \quad \text{and} \quad f_A(\beta) \leq q' \quad \text{implies} \quad f_A(\alpha \bullet \beta) \leq q \bullet q'$$

- Composition of protocols and knowledge (1)
  If we apply the suspicion-knowledge adjunction to the above property, we get an equivalent one for knowledge, which says if after protocol α agent A knows that q and after protocol β he knows that q', then after the composition of these two protocols he knows the compositions of his knowledge:

$$\alpha \leq \Box_A\, q \quad \text{and} \quad \beta \leq \Box_A\, q' \quad \text{implies} \quad \alpha \bullet \beta \leq \Box_A\, (q \bullet q')$$

- Composition of protocols and knowledge (2)
  The same assumptions lead to another property for knowledge, by simply composing the two sides of the inequalities

$$\alpha \leq \Box_A\, q \quad \text{and} \quad \beta \leq \Box_A\, q' \quad \text{implies} \quad \alpha \bullet \beta \leq (\Box_A\, q) \bullet (\Box_A\, q')$$

  which is not equal to the previous one since knowledge does not necessarily preserve composition (it only preserves meet)

$$\Box_A\, (q \bullet q') \neq (\Box_A\, q) \bullet (\Box_A\, q')$$

- Choice of protocols and suspicion
  If after α agent A suspects that q and after β he suspects that q', then after the choice of α and β he suspects either of his previous suspicions

$$f_A(\alpha) \leq q \quad \text{and} \quad f_A(\beta) \leq q' \quad \text{implies} \quad f_A(\alpha \vee \beta) \leq q \vee q'$$

- Choice of protocols and knowledge (1)
  Applying adjunction to the above property gives us an equivalent property for knowledge:

$$\alpha \leq \Box_A\, q \quad \text{and} \quad \beta \leq \Box_A\, q' \quad \text{implies} \quad \alpha \vee \beta \leq \Box_A\, (q \vee q')$$

- Choice of protocols and knowledge (2)
  Same as with composition, we get another property for knowledge and choice by simply taking the choice of two sides:

$$\alpha \leq \Box_A\, q \quad \text{and} \quad \beta \leq \Box_A\, q' \quad \text{implies} \quad \alpha \vee \beta \leq (\Box_A\, q) \vee (\Box_A\, q')$$

  which is, as before, not equal to the previous property.

- Comparing knowledge of different agents about the same protocol
  If agent B has more suspicions about α than A, then A has more knowledge than B after α

$$f_A(\alpha) \leq f_B(\alpha) \quad \text{and} \quad \alpha \leq \Box_B\, q \quad \text{then} \quad \alpha \leq \Box_A\, q$$

  That is, everything that B knows after α, for example q, agent A knows too, but perhaps A knows more. This encodes the fact that the more you suspect, the less you know! By applying the adjunction, we get an equivalent property for suspicion.

- Comparing knowledge of one agent about different protocols
  If agent A has more suspicions about β than about α, then A's knowledge less β than about α:

$$f_A(\alpha) \leq f_A(\beta) \quad \text{and} \quad \beta \leq \Box_A\, q \quad \text{then} \quad \alpha \leq \Box_A\, q$$

  Similarly, this says that everything that A knows after protocol β, for example q, he knows after protocol α, and perhaps he knows more after α. The suspicion equivalent can easily be derived.

Note that since suspicion is join-preserving, its adjoint, that is, knowledge will be meet preserving:

$$\Box_A\, (q \wedge q') = \Box_A\, q \wedge \Box_A\, q'$$

In a propositional setting meet is read as conjunction, but in a program setting it does not have an intuitive reading. The knowledge operator may provide us with an intuition: we can read $\Box_A\, (q \wedge q')$

as agent A knows both actions q and q' are happening (or have happened), but is not sure about the order of the happening. Here we are using the ambiguity of context to give a propositional meaning to the knowledge about actions and use it to read the conjunction in a propositional way where the order matters. The other side of the equality $\Box_A\, q \wedge \Box_A\, q'$ can be read easier: agent A knows that action q has happened, *and* he also knows that action q' has happened. We can then use order properties of meet and derive properties for meet of knowledge. For example

- Conjunction of knowledge
  If after α agent A knows that actions q has happened and he also knows that action q' has happened, then he knows both of them have happened

$$\alpha \leq \Box_A\, q \quad \text{and} \quad \alpha \leq \Box_A\, q' \quad \text{then} \quad \alpha \leq \Box_A\, (q \wedge q')$$

5.9 Future Work

Nested Knowledge We have shown above that after adding identities to our challenge response protocol with signatures, the challenger A knows that the responder B has received the first message and has intended his message (the second message of the protocols) for A. The responder, on the contrary, has no knowledge about his challenger, that is he does not if A was the real sender of the first message, and that he received the second message. All the responder knows is his suspicions about the protocol, that is

$$\alpha' \leq \Box_B\, f_B(\alpha')$$

It is easily seen that this inequality holds, since by adjunction it is equivalent to the following

$$f_B(\alpha') \leq f_B(\alpha')$$

In this section we are interested in calculating the nested knowledge of the agents, that is what does B know about the knowledge of A. In particular does he know that A knows that he received the first message and sent the second one, that is do the following hold

$$\alpha' \leq \Box_B \Box_A\, q^{B,r,m,A} \qquad \text{and} \qquad \alpha' \leq \Box_B \Box_A\, q^{B,s,SIG_B(m,ID_A),A}$$

Consider the first inequality, which is by adjunction equivalent to

$$f_B(\alpha') \leq \Box_A\, q^{B,r,m,A}$$

which is itself, again by adjunction, equivalent to

$$f_A(f_B(\alpha')) \leq q^{B,r,m,A}$$

So calculating the nested knowledge of B about A is equivalent to calculating the nested suspicions of A about B. We do this calculation as follows:

$$\begin{aligned} f_A(f_B(\alpha')) &= f_A\left(f_B(q^{A,s,m,B} \bullet q^{B,r,m,A} \bullet q^{B,s,SIG_B(m,ID_A),A} \bullet q^{A,r,SIG_B(m,ID_A),B})\right) \\ &\leq f_A(f_B(q^{A,s,m,B})) \bullet f_A(q^{B,r,m,A}) \bullet f_A(q^{B,s,SIG_B(m,ID_A),A}) \\ &\quad \bullet f_A(f_B(q^{A,r,SIG_B(m,ID_A),B})) \end{aligned}$$

So far we have only assigned suspicions to the actions of the honest agents. But in order to calculate this composition we also have to assign f_A's to the actions of the intruder. For example we have to decide about the following:

$$f_A(q^{C,r,m',A}) \qquad \text{and} \qquad f_A(q^{C,s,m,B})$$

Since we have assumed that there is only one intruder in the system, A has no uncertainties about the receive actions of the intruder, that is

$$f_A(q^{C,r,m',A}) = q^{C,r,m',A}$$

But he suspects for example three possibilities about the send actions are

$$f_A(q^{C,s,m,B}) = q^{C,s,m,B} \vee q^{C,s,m',B} \vee 1$$

After assigning suspicions to all the intruder actions involved in the above expression, we have to analyze a considerable amount of disjuncts. In fact the number is so large that any thought of even starting the calculation without automation seems infeasible. So in order to be able to perform an exact analysis of the nested knowledge, we need to automize the reasoning.

On the other hand, calculating the nested knowledge of A about B, that is

$$\alpha' \leq \Box_A \Box_B f_B(\alpha')$$

is easier, this is because the above inequality is equivalent to

$$f_B(f_A(\alpha')) \leq f_B(\alpha')$$

and we have done a perfect analysis of $f_A(\alpha')$ before, in which we discarded 17 cases of the 19 disjuncts and had to deal with only 2 cases other than reality. So we have the following

$$f_B(f_A(\alpha')) \leq f_B(\alpha' \vee \alpha'_6 \vee \alpha'_7) = f_B(\alpha') \vee f_B(\alpha'_6) \vee f_B(\alpha'_7) \not\leq f_B(\alpha')$$

So agent A does not know agent B's suspicions, that is

$$f_B(f_A(\alpha')) \not\leq f_B(\alpha') \quad \cong \quad \alpha' \not\leq \Box_A \Box_B f_B(\alpha')$$

We now know what A does **not** know, but what about the things that he knows? We can show that A knows that B is uncertain about the first message

$$\alpha' \leq \Box_A \Box_B (q^{A,s,m,B} \vee q^{A,s,m',B} \vee q^{A,s,m,C} \vee q^{A,s,m',C})$$

and also that A knows that B knows that he received the second message

$$\alpha' \leq \Box_A \Box_B \, q^{B,r,m,A}$$

Agent A has these pieces of nested knowledge because he has refined suspicions that lead to his acquiring some knowledge. But agent B was not able to do any refinement on his suspicions in the CR with two messages and as a result calculating his nested knowledge involves checking many cases. In the CR with three messages and identities γ', agent B also refines his suspicions and we can show that

$$\gamma' \leq \Box_B \Box_A \, q^{B,r,m,A} \qquad \text{also} \qquad \gamma' \leq \Box_B \Box_A \, q^{B,s,\{n,SIG_B(n,m,ID_A)\},A}$$

Another form of nested knowledge, is the nested knowledge of the intruder, that is calculating knowledge of C about the knowledge of the other two honest agents. But this can be easily calculated since we have only dealt with clear text messages. So the intruder does not have any suspicions and f_C is identity on all the messages and as a result he knows everything that each agent knows, for example

$$\alpha' \leq \Box_C \Box_A \, q^{B,s,SIG_B(m),A} \qquad \text{and} \qquad \alpha' \leq \Box_C \Box_A q^{B,r,m,A}$$

But the situation changes if cipher texts are used, in which case C does not know the content of the messages that are encrypted in keys that he does not have. This constitutes future work and will be discussed in another point below.

Conditional Knowledge As it stands, in the CR with two messages α', agent B does not know that A actually knows that he received the first message and sent the second message to A. But if he knows that A received his second message as it was sent, then he, exactly like A, discards his suspicions. That is if he knows that A received the second message, he knows that A knows that he received the first message and so on. We can express this using the adjoints (residuals) to sequential composition: as discussed in the chapter on the algebra, sequential composition is join-preserving and non-commutative, thus it has two adjoints presented in chapter two.

Here we use the first residual to express B's conditional knowledge:

$$\alpha' \leq \Box_B\, f_A(\alpha')/\Box_B\, q^{A,r,SIG_B(m),B}$$

which is equivalent to

$$\alpha' \bullet \Box_B\, q^{A,r,SIG_B(m),B} \leq \Box_B\, f_A(\alpha')$$

equivalent to

$$f_B(\alpha') \bullet q^{A,r,SIG_B(m),B} \leq f_A(\alpha')$$

Enriching the setting so that these sort of inequalities can be proven in it constitutes further work. For example, we have to add axioms to discard the following invalid sequences of messages

$$q^{A,r,m',B} \bullet q^{A,r,SIG_B(m),B} = \bot$$

We also need to add axioms to discard repetition of factual messages, for example

$$q^{A,r,SIG_B(m),B} \bullet q^{A,r,SIG_B(m),B} \leq q^{A,r,SIG_B(m),B}$$

Lack of Knowledge . Another interesting thing we can express using residuals is lack of knowledge. We can define two kinds of negations (using each residual) for actions, for example by using the right residual we can define a *right negation* as $\neg q = \bot/q$. We can then express that it is impossible for A to know if B received his message right after he sent it

$$q^{A,s,m,B} \bullet q^{B,r,m,A} \leq \neg\Box_A\, q^{B,r,m,A}$$

for which we have to show

$$q^{A,s,m,B} \bullet q^{B,r,m,A} \bullet \Box_A\, q^{B,r,m,A} = \bot$$

In order to prove this we need the axiom about repetition of factual messages. The rest goes by noting that $f_A(\bot) = \bot$, taking f_A on both sides, and recalling that $f_A(\Box_A\, q^{B,r,m,A}) \leq q^{B,r,m,A}$.

Contents of messages So far in this chapter, we have showed how one can reason about knowledge of agents about actions in a security protocol. Each action has a propositional content, about which the agents also have knowledge. For example when B receives a message, he gets to know its content. Reasoning about the propositional knowledge is done in the module where we use the dynamic modality, exactly in the same lines as for the muddy children puzzle. For example, if the initial situation is encoded in a proposition $s_0 \in M$ we have to prove the following inequality to show that after receiving a message, B knows its content

$$s_0 \leq [q^{B,r,m,A}]\Box_B\, m$$

On the other hand, after A sends his message to B, we do not have that B knows the content, since C might have stopped or changed it, that is

$$s_0 \not\leq [q^{A,s,m,B}]\Box_B\, m$$

Moreover, agent A is aware of this:

$$s_0 \not\leq [q^{A,s,m,B}]\Box_A\, \Box_B\, m$$

In this setting we can prove that after a protocol with only one message, agent B knows the content of the message he has received, that is

$$s_0 \leq [q^{A,s,m,B} \bullet q^{B,r,m,A}]\Box_B\, m$$

but A is not aware of it

$$s_0 \not\leq [q^{A,s,m,B} \bullet q^{B,r,m,A}]\Box_A \Box_B\, m$$

The proofs of these cases are derivable from the proofs of the single action cases. For example, we have the following claim:

$$\text{If} \quad s_0 \leq [q^{B,r,m,A}]\Box_B\, m \quad \text{then} \quad s_0 \leq [q^{A,s,m,B} \bullet q^{B,r,m,A}]\Box_B\, m$$

To prove this claim we start from our *unifying* axiom on the quantale

$$q^{A,s,m,B} \bullet q^{A,r,m,A} \leq q^{B,r,m,A}$$

now we update the initial situation on both sides and we get

$$s_0 \,.\, (q^{A,s,m,B} \bullet q^{A,r,m,A}) \leq s_0 \,.\, q^{B,r,m,A}$$

we then apply f_B to both sides

$$f_B(s_0 \,.\, (q^{A,s,m,B} \bullet q^{A,r,m,A})) \leq f_B(s_0 \,.\, q^{B,r,m,A})$$

but the right hand side is less than m by our if part of the claim

$$f_B(s_0 \,.\, q^{B,r,m,A}) \leq m$$

so we have

$$f_B(s_0 \,.\, (q^{A,s,m,B} \bullet q^{A,r,m,A})) \leq m$$

which is equivalent to the then part of our claim

$$s_0 \leq [q^{A,s,m,B} \bullet q^{B,r,m,A}]\Box_B\, m$$

and we are done. So all that needs to be done is to encode the propositional part of each security protocol in our module so that we can prove propositional knowledge of agents, that is for example the if part of the claim. For this we have to analyze the initial situation s_0 and assign propositional appearances to it for each agent, that is $f_B(s_0)$ and $f_A(s_0)$. We also have to assign kernel to each of our actions. In fact, the kernel of the send and its corresponding receive will be the same, since they have the same propositional content.

Secrecy So far we have only considered messages in clear text and did not use encryption. This means that each agent, when he receives the message, will know its content and this includes the intruder. This knowledge is included in the knowledge of actions, that is we have shown how to prove the following

$$q^{C,r,m,A} \leq \Box_C\, q^{C,r,m,A}$$

which says that after the intruder C receives a messages containing m in A's name, he will know he has received this message with all the particulars. This should result in the derivation of the following propositional knowledge on the module

$$s_0 \leq [q^{C,r,m,A}]\Box_C\, m$$

But when the messages are encrypted, things are not the same. We denote by $\{m\}_K$ an encrypted proposition m in the key K. Suppose that the key is only known by A and B and not by C. So we have the following inequality for B

$$q^{C,r,\{m\}_K,A} \leq \Box_B\, q^{C,r,\{m\}_K,A}$$

but C will not get to know the decrypted content, that is

$$s_0 \not\leq [q^{C,r,\{m\}_K,A}]\Box_C\, m$$

and we only have that C knows the encrypted and not the real content

$$s_0 \leq [q^{C,r,\{m\},A}]\Box_C\, \{m\}_K$$

which does not imply that C also knows the real content. The situation is different for A and B, for example we have the following for agent B

$$s_0 \leq [q^{B,r,\{m\}_K,A}]\Box_B\, m$$

Adding secrecy, reduces the powers of the intruder: he is not anymore the agent who knows everything. Encoding secrecy constitutes future work, we have to encode the initial assumptions in such a way the we can derive the above properties.

Chapter 6

Algebraic Representation of Kripke Semantics

The usual semantics for epistemic logic is the relational or Kripke models that encode the appearances as accessibility relations on a set of states that stand for possible worlds for agents and calculate knowledge set-theoretically. These models have been extended by Baltag Moss and Solecki [10] to model communication actions and their effects on the knowledge of agents. The syntax of their logic DEL, has been discussed in chapter three. In this chapter we explain the Kripke semantics of DEL and show how it can be recasted and represented in our order-theoretic semantics of Epistemic Systems, presented in chapter two. The novelty of DEL is that it models actions as states as Kripke models and then formalizes the effect of an action on knowledge by forming the (partial) product of the two structures. Our theorem shows that models of DEL are instances or concrete versions of models of IDEAL. We start with defining Kripke models for states and actions and the product of the two. Examples will be presented along the way to make the understanding of concepts easier. We then abstract over these Kripke models and build abstract DEL models in order to state our theorem. The proofs are straightforward and follow from the way we abstract the state and action models. This means that any valid formula in a model of DEL is valid in its corresponding order structure built by our theorem and also the other way around. Although there exist dualities [28, 49] between Kripke models of epistemic logic and order-theoretic structures, for instances boolean algebras with operators are algebraic models of classical modal logic [51, 50], nothing similar has been done for the setting of DEL. The other direction of the construction of this chapter, mentioned in the joint work [8] is the first of its kind.

6.1 Kripke Models

For a set of *facts* Φ and a finite set of *agents* $\mathcal{A}$, a *Kripke state model* is a triple

$$\mathbf{S} = (S, \xrightarrow{A}, \mu)_{A \in \mathcal{A}}$$

where S is the set of *states*, $\xrightarrow{A}$ is the *accessibility relation* for each agent $A \in \mathcal{A}$, that is

$$\xrightarrow{A} \subseteq S \times S\,,$$

and μ is the *valuation map* defined as follows

$$\mu : S \to \mathcal{P}(\Phi)\,,$$

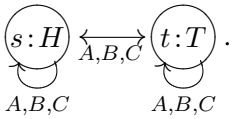
that encodes the following satisfaction relation

$$s \models \phi \quad \text{iff} \quad \phi \in \mu(s)\,.$$

The "facts" $\phi \in \Phi$ are simple, objectives features of the world ("objective" in the sense of non-epistemic, i.e. independent of the agents' knowledge or believes), and the valuation maps tell us what facts hold in a given state $s \in S$.

Example. Consider a coin-toss scenario where in front of two agents A and B, a referee C throws a coin and covers it. So non of the agents including C himself know on which face the coin has landed. This scenario can be modeled by the following Kripke structure

(Toss)



In this model we have two states, one in which the coin lands heads up denoted as s, and another in which the coin lands tails, denoted by t. So the set of states is $S = \{s, t\}$. The accessibility relation for A tells us if s is the real world, agent A considers the worlds s and t as possible, because he does not know on which face the coin has landed. So the set of accessibility relation for agent A is

$$\xrightarrow{A} = \{(s,s),(s,t),(t,t),(t,s)\}$$

and similarly for agents B and C, that is

$$\xrightarrow{B} = \xrightarrow{C} = \{(s,s),(s,t),(t,t),(t,s)\}$$

The set of facts is $\{H, T\}$, where H is the fact that the coin is heads and T is the fact that the coin is tails. The valuations are as follows

$$s \models H \quad \text{and} \quad t \models T$$

or in μ terms:

$$\mu(s) = \{H\} \quad \text{and} \quad \mu(t) = \{T\}$$

This says that each state satisfies its corresponding facts.

Repackaging of Accessibility Relations Each accessibility relation can be repackaged as (or lifted t) a map from the set of states to the power set of states as follows

$$f_A : S \to \mathcal{P}(S) :: s \mapsto f_A(s) := \{t \in S \mid s \xrightarrow{A} t\},$$

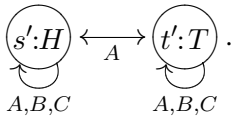
which corresponds to our algebraic *appearance map* of an agent A. The significance of the appearance maps is as follows: if $t \in f_A(s)$ then, whenever agent A is in state s he considers state t as a 'possible world'. In other words, if the actual state of the system is s, agent A thinks t may be the actual state. For example in our coin-toss model above we have

$$f_A(s) = \{s, t\} \quad \text{and} \quad f_A(t) = \{s, t\}$$

and similarly for B and C.

As another example consider a case in which agents B and C can see the face of the coin, but agent A cannot see it (although he knows that the others see it), so he is still uncertain if the coin is heads or tails. This scenario is depicted in the following Kripke model called PToss:

(PToss)



In this case only agent A is uncertain about the face of the coins and thus has several arrows between states, that is

$$f_A(s') = f_A(t') = \{s', t'\}$$

whereas agents B and C have only one arrow in each state, that is

$$f_B(s') = f_C(s') = \{s'\} \quad \text{and} \quad f_B(t') = f_C(t') = \{t'\}$$

This means that if the coin is heads up, B and C know it and similarly for tails up.

Epistemic Propositions We continue the repackaging by defining a new notion of proposition:

Definition 6.1.1 *An* epistemic proposition P over a state model $\mathbf{S}$ *is a subset P of S, containing all the states at which the proposition is 'true'.*

We have to show how our valuations and appearance maps extend to this new notion of proposition. The maps μ and f_A of the state model are extended to elements of P as follows

$$f_A(P) := \bigcup \{f_A(s) \mid s \in P\} \in \mathcal{P}(S) \qquad \mu(P) := \bigcap \{\mu(s) \mid s \in P\} \in \mathcal{P}(\Phi)$$

Since epistemic propositions are just subsets of the set of states, appearance maps can be extend to them point wisely, . So in order to calculate the appearance map of a set of states, we take the union of the appearance maps of each element. For the valuations, we first form the set of μ maps of each element and then take the intersection of these sets. We use intersection and not union in defining $\mu(P)$ since a fact is entailed by an epistemic proposition when it holds at all the states of the proposition. This will become clear by our example below. This is called a *contravariant* passage from $\mathcal{P}(S)$ to $\mathcal{P}(\Phi)$, that is the μ is order reversing. In other words, the actual algebra of facts is $\mathcal{P}(\Phi)^{op}$, that is, the complete boolean algebra $\mathcal{P}(\Phi)$ where the order is reversed i.e.

$$\phi_1 \leq^{op} \phi_2 \Leftrightarrow \phi_1 \supseteq \phi_2 \,.$$

While facts are simple and non-epistemic, and thus cannot be altered by epistemic actions (as explained in chapter two), epistemic propositions can express complex features of the world, which may depend on the agents' knowledge (and so can be changed by epistemic actions). Facts can also be repackaged as epistemic propositions, each fact $\phi \in \Phi$ corresponds to an epistemic proposition as follows

$$P_\phi := \{s \in S \mid \phi \in \mu(s)\} \,,$$

saying that the fact holds in these state.

In the **Toss** model, H and T are facts expressing the heads up or tails up of the coin. The epistemic propositions that correspond to these facts are the states in which the fact holds, that is $P_H = \{s\}$ and $P_T = \{t\}$. The epistemic propositions are

$$\emptyset, \{s\}, \{t\}, \{s,t\} \subseteq \{s,t\} \,.$$

Where $\emptyset$ is the *falsum* (i.e. the trivially false epistemic proposition over $\mathbf{S}$), and the set $S = \{s,t\}$ is the true proposition or a tautology. The appearance map of the falsum to any agent is itself, that is $f_A(\emptyset) = \emptyset$. The appearance and μ maps of the singleton sets $\{s\}$ and $\{t\}$ are the same as their single states, that is

$$f_A(\{s\}) = f_A(s) \qquad \text{and} \qquad \mu(\{s\}) = \mu(s)$$

The interesting case here is the epistemic proposition $\{s,t\}$. Its appearance is

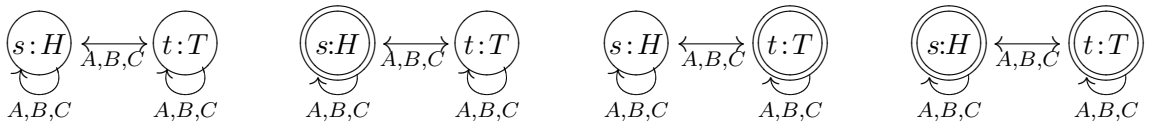
$$f_A(\{s,t\}) = f_A(s) \cup f_A(t) = \{s,t\} \cup \{s,t\} = \{s,t\}$$

and it valuation map is

$$\mu(\{s,t\}) = \mu(s) \cap \mu(t) = \{H\} \cap \{T\} = \emptyset$$

this means that there is no fact in our model which is true at both states s and t, if we had taken the union in our passage, we would get the set $\{H,T\}$ as result, which would be wrong since it would mean both heads and tails are true in proposition $\{s,t\}$, something we do not want.

Given a state model, an epistemic proposition over a it can be depicted by double-circling the included states, hence the double-circled states in the following state models represent the four epistemic propositions of **Toss** as follows



When a proposition P has exactly one state $s \in P$ (i.e. $P = \{s\}$ is a singleton), we can use systematic ambiguity, identifying the proposition with the state and writing e.g. s instead of $\{s\}$.

6.2 Action Models

Given a state model $\mathbf{S}$, *an action model over* $\mathbf{S}$ is a triple

$$\Sigma = (\Sigma, \xrightarrow{A}, \mu)$$

which is similar to a state model except that we think of the elements of Σ as possible *actions* instead of possible states and the valuation map defined as follows

$$\mu : \Sigma \to \mathcal{P}(S)\,,$$

assigns to each action σ a *precondition*, i.e. a proposition $\mu(\sigma)$ defining the domain of applicability of σ, that is

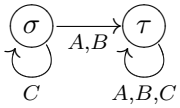
$$\text{action } \sigma \text{ can happen in a state } s \quad \text{iff} \quad s \in \mu(\sigma)$$

e.g. a truthful announcement of a proposition can only happen in those states where that proposition holds. Note that since $\mathcal{P}(S)$ is boolean we can equivalently consider the states at which the action *cannot take place* , denoted as

$$Ker(\sigma) := S \setminus \mu(\sigma) \quad \text{for each} \quad \sigma \in \Sigma\,.$$

The accessibility relations are as before, for example $\sigma_1 \xrightarrow{A} \sigma_2$ says that if action σ_1 is happening in the real world, agent A thinks, or it appears to him that action σ_2 is happening.

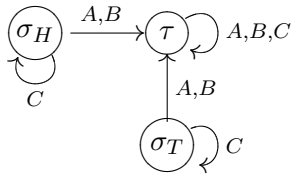
As an example, we introduce an action model over **Toss**. After catching the coin in his hand, the referee might secretly take a peek at the coin before covering it while nobody notices this. The action model for this cheating is depicted as



where σ is the 'cheating' action and τ is the action in which 'nothing happens'. If we assume that in action σ the coin has landed heads, its precondition is the states in the state model **Toss** where the fact H holds, that is

$$\mu(\sigma) = \{s\}$$

We can also make a more precise action model to express that when the referee takes a peek, the coin can be either heads or tails. This action model is depicted as follows:



We have replaced the single action σ by two actions σ_H and σ_T where $\mu(\sigma_H) = \{s\}$ and $\mu(\sigma_T) = \{t\}$, specifying what the referee saw when he took a peek.

Epistemic Programs The accessibility relations are repackaged as appearance maps in exactly the same way as in state models. We define a notion of epistemic program in the same lines as for epistemic propositions as follows:

Definition 6.2.1 An epistemic program π over an action model $\mathbf{\Sigma}$ is a subset π of Σ.

The μ and f_A maps are both extended to these subsets point wisely

$$\mu(\pi) := \bigcup\{\mu(\sigma) \mid \sigma \in \pi\} \in \mathcal{P}(S) \quad \text{and} \quad f_A(\pi) := \bigcup\{f_A(\sigma) \mid \sigma \in \pi\} \in \mathcal{P}(\Sigma)\,.$$

The union in the definition of μ maps for programs says that an epistemic program is applicable where at least one of its actions is applicable. If we had that the applicability for *all of its actions*, then the passage would be, like for the valuations of epistemic propositions, contravariant. But the covariant passage of precondition, makes the Ker map follow contravariantly, since it is the boolean negation of precondition i.e. $Ker(\pi) = S \setminus \mu(\pi)$. That is we will have

$$Ker(\pi) := \bigcap\{Ker(\sigma) \mid \sigma \in \pi\} \in \mathcal{P}(S)$$

Note that we can have the notion of an empty program $\emptyset$ which stands for the *impossible program*, that is a program that can never be performed, so its kernel is the set of all the states in our state model:

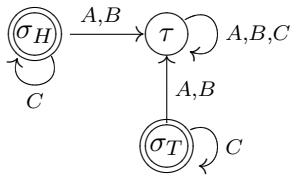
$$Ker(\emptyset) = S \qquad \text{and dually} \qquad \mu(\emptyset) = \emptyset$$

We also have the notion of a program in which nothing happens, that is our τ in the coin-toss example. This program can be performed everywhere since it does not do any thing and thus does not need any

precondition, so its kernel is the empty set:

$$Ker(\tau) = \emptyset \qquad \text{and dually} \qquad \mu(\tau) = S$$

Similar to epistemic propositions, we depict a program over an action model by double-circling the including actions of that program. Hence the picture of the program $\pi = \{\sigma_H, \sigma_T\}$ over Σ is



We also have the notion of a *deterministic* program, that is a program that contains only one action, for example $\pi = \{\sigma\}$. As in the case of states and propositions, we use systematic ambiguity to identify these programs with their unique underlying action, so we write σ instead of $\{\sigma\}$.

6.3 Epistemic Update

So far we have introduced state models for propositions and action models for programs. Programs act on propositions and thus affect their truth value. In this section we formalize this notion via an operation on the state and action models.

Given a state model $\mathbf{S}$ and an action model Σ over $\mathbf{S}$ we define their *update product* $\mathbf{S} \otimes \Sigma$ to be a new state model with the following set of states

$$S \otimes \Sigma := \bigcup_{\sigma \in \Sigma} \mu(\sigma) \times \{\sigma\}$$

This means that we take the cartesian product of the actions with states in which the precondition of action holds. This can also be defined as follows

$$S \otimes \Sigma := \{(s, \sigma) \mid s \in S,\ \sigma \in \Sigma,\ s \in \mu(\sigma)\}$$

which expresses that update is a partial cartesian product between the set of states and the set of action;

$$S \otimes \Sigma \subseteq S \times \Sigma$$

It is partial since we through away the pairs $(s, \sigma) \in S \times \Sigma$ where the state does not satisfy the precondition of the action $s \notin \mu(\sigma)$, so we have $(s, \sigma) \notin S \otimes \Sigma$.

The appearance maps are extended to these pairs point wisely, that is as follows

$$\text{for each } (s, \sigma) \in S \otimes \Sigma, \quad f_A(s, \sigma) := (f_A(s) \times f_A(\sigma)) \cap (S \otimes \Sigma)$$

This says that for each pair in the updated state model, we connect it to the pairs whose states were connected to the state in the state model and whose actions were connected to the action in the action model, of course only if the resulting pair is included in the set $S \otimes \Sigma$. This can be equivalently defined as

$$f_A(s,\sigma) = \{(s',\sigma') \mid (s',\sigma') \in S \otimes \Sigma,\ s' \in f_A(s),\ \sigma' \in f_A(\sigma)\}$$

Hence the appearance map of a pair is also a partial cartesian product of the sets of appearances of the state and that of the action:

$$f_A(s,\sigma) \subseteq f_A(s) \times f_A(\sigma)$$

The valuations maps remain the same in the updated model

$$\mu(s,\sigma) := \mu(s),$$

that is if a state state s had the valuation $\mu(s)$, then if it remains in the updated model, it will still have the same valuation.

In our example, after the cheating action σ_H where the coin has lied Heads up, A and B do not know the face of the coin. But since C took a peek, he knows the face of the coin! We want to show this by showing the effect of the cheating on the original state model, that is by updating the state model with the action model of cheating. So we form the update product of the two models **Toss** and σ_H, that is

The Cartesian product of the set of states of the state model and the set of actions of the action model is

$$\textbf{Toss} \times \sigma_H = \{(s,\sigma_H),(s,\tau),(t,\sigma_H),(t,\tau)\}$$

from which the pair (t,σ_H) gets eliminated since t does not satisfy the precondition of σ_H, that is $t \notin \mu(\sigma_H)$. So we have

$$\textbf{Toss} \otimes \sigma_H = \{(s,\sigma_H),(s,\tau),(t,\tau)\}$$

Note that the action τ can be applied anywhere, that is any proposition satisfies its preconditions. The appearance maps are extended to this pair point wisely, that is since $s \xrightarrow{A} s$ in **Toss** and $\sigma_H \xrightarrow{A} \tau$ in σ_H, we have that

$$(s,\sigma_H) \xrightarrow{A} (s,\tau)$$

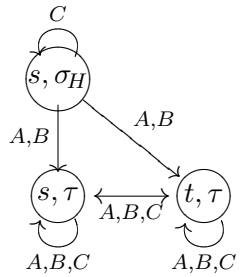
and similarly for other pairs, another example would be

$$s \xrightarrow{A} t \quad \text{and} \quad \sigma_H \xrightarrow{A} \tau \quad \text{thus} \quad (s,\sigma_H) \xrightarrow{A} (t,\tau)$$

Other arrows are obtained in exactly the same way. The valuations remain the same, that is

$$\mu(s, \sigma_H) = \mu(s, \tau) = \mu(s) \quad \text{and} \quad \mu(t, \tau) = \mu(t)$$

The resulting Kripke model of this update is pictured as follows



We see that in this model there are no uncertainty arrows for agent C from the real state (s, σ_H): the only possible state for C is the same state. So in this model agent C is no more uncertain about the face of the coin, he knows it is heads. This is reflected in the valuation of the real state $\mu(s, \sigma_H) = \{H\}$. But agents A and B are still uncertain: they arrow to both states (s, τ) and (t, τ): in the first one the coin is heads $\mu(s, \tau) = \{H\}$, and in the second it is tails $\mu(t, \tau) = \{T\}$. Note that agents A and B think that agent C is also uncertain about the face of the coin, since they do not know about the cheating, that is why we have uncertainty arrows for C in the states that are accessible from the real states for A and B.

Epistemic Propositions Updated by Epistemic Programs We have defined the update of an action model with a state model, we now extend it to update between epistemic programs and epistemic propositions as follows:

Definition 6.3.1 We define the update product of an epistemic proposition P over $\mathbf{S}$ and an epistemic program π over Σ *as the epistemic proposition*

$$P \otimes \pi := \bigcup_{\sigma \in \pi} (\mu(\sigma) \cap P) \times \{\sigma\} \subseteq \ P \times \pi \ \text{ over } \ \mathbf{S} \otimes \Sigma.$$

This is a point wise extension, or restriction since here we have subsets of the original set of states and actions, of the update of the state and action models. One way to obtain $P \otimes \pi$ is to update the state model with the action model, but only consider the states in proposition P and the actions in program π. One can also first update the whole models and then reduce it to the subsets of states and actions.

It can be seen that an update results in the empty sets when none of the propositions on which we want to do the update, satisfy the precondition of the program, that is

$$\text{if} \quad P \otimes \pi = \emptyset \quad \text{then} \quad P \cap \mu(\pi) = \emptyset$$

where $\emptyset$ is the *falsum* (i.e. the trivially false epistemic proposition over $\mathbf{S}$).

6.4 Modalities

So far we have defined state and action models and propositions and programs over them. Since propositions and programs are sets, we can operate on them via the usual set theoretic operations of union and intersection. We have also defined the update of a proposition by a program via the set theoretic notion of a partial cartesian product. In this section we define two more operations: epistemic and dynamic modalities, these are also defined set-theoretically but stand for more abstract categorical operations of adjunction. The epistemic modality is usually defined by de Morgan dualities and using accessibility relations of a Kripke model. We show that our repackaging leads to the definition of epistemic modality as the right adjoint to the appearance maps (repackaging of accessibility relations). The dynamic modality, on the other hand, is known to arise from adjunction [47, 45], and we show how in our setting it arises from epistemic update.

Epistemic Modality We define the *epistemic modality* for each agent $A \in \mathcal{A}$ as the unary connective which assigns to proposition $P \subseteq S$ over $\mathbf{S}$ another proposition as follows

Definition 6.4.1 The epistemic modality $\Box_A P$ is the knowledge of an agent about the proposition P defined as

$$\Box_A P := \left\{ s \in S \;\middle|\; f_A(s) \subseteq P \right\} \text{ over } \mathbf{S}.$$

We read $\Box_A P$ as 'agent A knows or believes P'[1]. So the states in which agent A knows that proposition P holds, that is $\Box_A P$, are the states that access the states of P, or in other words, all the states that access P (all the states in which P holds). So if for all t accessible from s we have $t \in P$, then we also have that $t \in \Box_A P$:

$$f_A(s) \subseteq P \quad \text{iff} \quad s \in \Box_A P$$

In other words agent A knows the common part of all his appearances, if a state is in all his appearances, then he knows it. We can say that appearances correspond to uncertainty and possibility, where knowledge, being the common part of all appearances, corresponds to certainty and necessity. An agent knows a proposition if it is consistently part of all his appearances. This relation is exactly the categorical notion of adjunction: it says that appearances and knowledge form and adjoint pair $(f_A, \Box_A)$, and that moreover knowledge is the right adjoint to appearance, that is $f_A \dashv \Box_A$. This is is equivalent to say the following

$$f_A(P) \subseteq Q \quad \text{iff} \quad P \subseteq \Box_A Q$$

[1] Taking either 'knows' or 'believes' depends on the context.

which can easily be seen from our definition of knowledge above:

$$t \in \Box_A P \quad \text{iff} \quad f_A(t) \in P$$

Dynamic Modality We define the *dynamic modality* for each epistemic program π over Σ as the unary connective which assigns to proposition $P \subseteq S$ over $\mathbf{S}$ another proposition.

Definition 6.4.2 The dynamic modality $[\pi]P$ is read as 'after doing program π, proposition P holds' and is defined as follows

$$[\pi]P := \big\{ s \in S \;\big|\; \{s\} \otimes \pi \subseteq P \big\} = \bigcup \big\{ Q \in \mathcal{P}(S) \;\big|\; Q \otimes \pi \subseteq P \big\} \text{ over } \mathbf{S}\,.$$

The states in which after π, proposition P holds, are the states that when updated with program π, will satisfy P, that is if $s \otimes \pi$ is in P then it is also in $[\pi]P$:

$$\text{if} \quad \{s\} \otimes \pi \subseteq P \quad \text{then} \quad s \in [\pi]P \quad \text{and vice versa}$$

So if we put all such states in a set, that is take the union of all of them, we have the proposition $[\pi]P$. In this sense, the proposition $[\pi]P$ is the set of all the states on which you can do π and after that P will become true. This says that dynamic modality forms an adjoint pair with update $(- \otimes \pi, [\pi]-)$ and that it is the right adjoint of update $- \otimes \pi \dashv [\pi]-$. This is equivalent to the following

$$Q \otimes \pi \subseteq P \quad \text{iff} \quad Q \subseteq [\pi]P$$

which can easily be derived from our definition of dynamic modality. The dynamic modality $[\pi]P$ is also referred to as *weakest precondition* for a program π in literature [47], it is the union of all the propositions that should be true before π so that P is true afterwards. In this sense the updated proposition $P \otimes \pi$ provides the *strongest postcondition* for P with respect to program π: for each state in $P \otimes \pi$ the proposition P holds before running the π.

6.5 Operations on Action Models

Union and intersection of sets of states in a state model corresponds to logical disjunction and conjunction of epistemic programs defined over that state model. However, only union makes sense in the context of programs. We can of course form the intersection of a sub set of actions, but program wise it would not correspond to a meaningful program operations based on its subset programs. Natural operations on programs are choice of two programs and also sequential composition of them. In this section we show how these two connectives can be defined in our setting.

Non-Deterministic Choice We first introduce the notion of *non-determinism* on epistemic programs using the inclusion between the two: whenever a program is a subset of another one $\pi_1 \subseteq \pi_2$ then the bigger program π_2 is obtained from the smaller one π_1 by increasing non-determinism. So we have the following

$$\pi = \{\sigma_1, \sigma_2\} \quad \text{stands for "either action } \sigma_1 \text{ or action } \sigma_2 \text{ takes place"}.$$

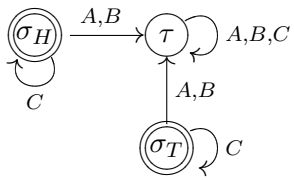
That is for example program π_1 has only one state but π_2 has two states, one of them he shares with π_1:

$$\pi_1 = \{\sigma_1\} \subseteq \{\sigma_1, \sigma_2\} = \pi_2$$

so we say that since π_2 has more states, it can perform either of them, and so it is firstly non-deterministic and also more non-deterministic than π_1, since in this example π_1 only has one state and is very deterministic. We can also have inclusions like the following

$$\pi_2 = \{\sigma_1, \sigma_2\} \subseteq \{\sigma_1, \sigma_2, \sigma_3\} = \pi_3$$

where π_2 is more deterministic than π_3, since π_3 has three states either of which can be performed, where as π_2 has two.
In our example where the referee took a peek, pictured below



we have three actions σ_H, σ_T and τ and the epistemic program $\{\sigma_H, \sigma_T\}$ stands for the non-deterministic action σ, which says that what the referee sees after taking a peek, can be heads σ_H or tails σ_T, either can happen and it is not the referee that controls it.

Definition 6.5.1 We define the *non-deterministic choice* of two epistemic programs Σ_1 and Σ_2 over $\mathbf{S}$ of two action models Σ_1 and Σ_2 as the union of them

$$\Sigma_1 \cup \Sigma_2$$

It means either do Σ_1 or do Σ_2. The set of states of this program is the union of the set of states of Σ_1 and Σ_2. The appearance maps of the union is the union of appearance maps and the precondition of the unions is also the union of preconditions.

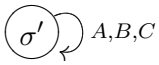
Sequential Composition Another natural operation on programs is the sequential composition of them. This cannot be defined as easy as the choice, we have to form the cartesian product of the two programs that are sequentially composing, and build a new action model for the composition.

Definition 6.5.2 The sequential composition $\Sigma_1 \bullet \Sigma_2$ over $\mathbf{S}$ of two action models Σ_1 and Σ_2 both over $\mathbf{S}$ means 'first do Σ_1 and then do Σ_2' and is defined as

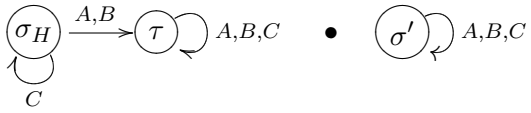
$$\Sigma_1 \bullet \Sigma_2 := \Sigma_1 \times \Sigma_2 \quad f_A(\sigma_1, \sigma_2) := f_A(\sigma_1) \times f_A(\sigma_2) \quad \mu(\sigma_1, \sigma_2) := \mu(\sigma_1) \cap [\sigma_1]\mu(\sigma_2).$$

This construction is very similar to the update of an action model and a state model, the first difference is that there we had partial cartesian product, here we have the full product set. This means that we assume any program can be sequentially composed with another program, although when updating, the composed program might not go through. This is because of the other difference, which is about calculating the precondition of the composition. The precondition of the composition of two actions, is the intersection of the precondition of the first one and the weakest precondition that should be true before the second one so that the precondition of the second one becomes true afterwards. So if the first action can be performed on a state, but it results in a state that does not satisfy the precondition of the second action, then the composition can not go through, although its first action was successful. This says that a composition only goes through if firstly, the first action can go through and secondly, the resulting states of the first update satisfy the precondition of the second action.

As an example consider the sequential composition of the taking a peek (discussed before) and an announcements of heads. So the referee C, first takes a peek and sees that for example the coin is heads, and then announces the result publicly to every one. The action model for the announcement has just one state call it σ', which is accessible to all the agents (the action is public) and its precondition is heads H. It is pictured as follows



We want to compose this with the action of taking a peek, that is we want to form the following sequential composition



If we call the first action model Σ_1 and the second one Σ_2, the set of the states of the result action model is

$$\Sigma_1 \times \Sigma_2 = \{(\sigma_H, \sigma'), (\tau, \sigma')\}$$

The appearance map of agent A on the state (σ_H, σ') is calculated as follows

$$f_A(\sigma_H, \sigma') = f_A(\sigma_H) \times f_A(\sigma') = \{\tau\} \times \{\sigma'\} = \{(\tau, \sigma')\}$$

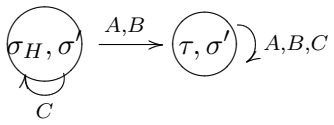
which is also equal to $f_B(\sigma_H, \sigma')$. The appearance of C on this state is

$$f_C(\sigma_H, \sigma') = f_C(\sigma_H) \times f_C(\sigma') = \{\sigma_H\} \times \{\sigma'\} = \{(\sigma_H, \sigma')\}$$

In the same way the appearance of the three of them of the second state (τ, σ') is

$$f_A(\tau, \sigma') = f_B(\tau, \sigma') = f_C(\tau, \sigma') = \{(\tau, \sigma')\}$$

The model of the composition is pictured as follows



The preconditions for the first state is calculated as follows

$$\mu(\sigma_H, \sigma') = \mu(\sigma_H) \cap [\sigma_H]\mu(\sigma') = \{H\} \cap \{H\} = \{H\}$$

since in order for σ_H to perform, the coin should be heads, which is the same as the precondition of the announcement of heads in σ'. For the second state we have

$$\mu(\tau, \sigma') = \mu(\tau) \cap [\tau]\mu(\sigma') = \{H, T\} \cap \{H\} = \{H\}$$

Note that if for example T was announced in σ', then we had $\mu(\tau, \sigma') = \emptyset$, which means the composition could not go through and update our state model.

We define the sequential composition of the epistemic programs, or the subsets of our actions as follows

Definition 6.5.3 *We define the sequential composition of two epistemic programs π_1 over Σ_1 and π_2 over Σ_2* as the epistemic proposition $\pi_1 \bullet \pi_2 := \pi_1 \times \pi_2$ over $\Sigma_1 \bullet \Sigma_2$.

Before proceedings to state our theorem, we need to construct an action model from the action that does nothing, that is τ. We need this since we want to (later) close our action models under sequential composition.

The action model over a state model $\mathbf{S}$ is a τ model iff

$$\tau = \{\tau\} \qquad \mu_\tau = S \qquad f_A(\tau) = \{\tau\}\,.$$

Notice the use of systematic ambiguity: we denoted with the same name τ both the program τ and its only action. It is easy to see that this action is a unit, up to isomorphism, both for update product and sequential composition, that is

$$P \otimes \tau \cong P \quad \text{and} \quad \pi \bullet \tau \cong \pi$$

6.6 The Theorem

We have introduced and repackaged DEL and its set-theoretic constructions in a way that enables us to talk about it in an order-theoretic system. Our main repackaging was the repackaging of accessibility relations of a Kripke structure as a subset of the set of states, rather than a relation on it. This helped us to bring together all the states accessible to a state in one set, rather having to browse through the relation. In the same lines, we have considered subsets of set of states of a model (state of action) as our main elements (propositions and programs) and showed how operations of DEL, and most importantly update, can be defined in terms of these subsets. This repackaging enabled us to define our epistemic and dynamic modalities as categorical adjoints, defined accordingly in terms of appearances and update, which also enabled us to provide each modality with a set of answers, rather than having to check all the accessibility relations each time we need to know a modal proposition is true. In this section we show, how these repackagings help us to define an order-theoretic model for DEL, to which we refer to as *concrete epistemic systems*, which are variants (more restricted) of epistemic systems, since concrete epistemic systems are based on completely atomistic boolean algebras where as epistemic systems are based on sup-lattices, .

Concrete epistemic systems and DEL Models Given a state model $\mathbf{S}$ and an action model Σ, we want to build a larger model to reason about knowledge of agents about all the states and actions, including their updates and sequential composition and choice. This larger model should contain all the proposition on the state model and all the programs of the action model, which means all the subsets of the states and actions, obtained by taking the power set of the states and action. But it should also contain the resulting states of any operation that can be done on them, for example the updated propositions and sequentially composed programs. So before taking the power set of our state and action model, we have to close them under update product and sequential composition, and also add the unit of composition, that is our τ model, to the action model. This model is defined below

Definition 6.6.1 A DEL model is a pair $(\mathbf{S}, \Sigma)$ where $\mathbf{S}$ is a state model and Σ is an action model over $\mathbf{S}$ such that $\tau \in \Sigma$, $(S \otimes \Sigma) \subseteq S$ and $(\Sigma \bullet \Sigma) \subseteq \Sigma$.

Now we have all the propositions and programs, including updated ones, we form the power sets of each element, which is a complete lattice but has more properties, This will be our concrete order-theoretic model. It is defined as follows:

Definition 6.6.2 Given a DEL model $(\mathbf{S}, \Sigma)$, a *concrete epistemic system* is the following triple

$$(\mathcal{P}(S), \mathcal{P}(\Sigma), \{f_A\}_{A \in \mathcal{A}}) .$$

The Theorem and its Proof Note that the concrete epistemic system pair goes equipped with valuation μ, appearance maps $\{f_A\}_{A \in \mathcal{A}}$ and all other operations of the DEL model extended to $\mathcal{P}(S)$ and

$\mathcal{P}(\Sigma)$ as we repackaged above. With all these operations, it is easy to show that a concrete model is actually a pair quantale and its right module endowed with appearance endomorphisms. The power sets form complete lattices, so both $\mathcal{P}(\mathbf{S})$ and $\mathcal{P}(\Sigma)$ are sup-lattices. The joins are the unions in each power set, on the propositions and also on the programs. The power set of programs $\mathcal{P}(\Sigma)$ has a multiplication, which is the sequential composition of the epistemic programs as defined above. It follows from our construction that this multiplication preserves unions, this is because sequential composition is a cartesian product, which preserve unions. The unit of multiplication is our τ program that does nothing. So $(\mathcal{P}(\Sigma), \subseteq, \cup, \bullet, \tau)$ forms a quantale. The action of the quantale on the module is our epistemic update, it preserves unions since it is also a (partial) cartesian product. We state and prove some lemmas before proving the main theorem.

Lemma 6.6.3 *The following are true:*
i. *Epistemic programs $\mathcal{P}(\Sigma)$ with $\bigcup$ as $\bigvee$, sequential composition as $\bullet$ and τ as 1 form a quantale.*
ii. *Epistemic propositions $\mathcal{P}(S)$ with $\bigcup$ as $\bigvee$ and update product as $\otimes$ form a right $\mathcal{P}(\Sigma)$-module.*
iii. *The pair $(\mathcal{P}(S), \mathcal{P}(\Sigma))$ is an atomistic system. The atoms of the module $\mathcal{P}(S)$ correspond to the* states *$s \in S$, while the atoms of the quantale $\mathcal{P}(\Sigma)$ correspond to the* actions *$\sigma \in \Sigma$.*

Proof. For the first part, since power sets are complete lattices, we just have to show that sequential composition preserves unions, that is for π and α_i epistemic programs over an action model Σ, we have to show the following

$$\pi \bullet \bigcup_i \alpha_i = \bigcup_i (\pi \bullet \alpha_i)$$

and similarly for the other argument. By definition of sequential composition of epistemic propositions we have

$$\pi \bullet \bigcup_i \alpha_i = \pi \times \bigcup_i \alpha_i$$

which is equal to the following by the property of cartesian product (it preserves unions)

$$\bigcup_i (\pi \times \alpha_i) = \bigcup_i (\pi \bullet \alpha_i)$$

The proof for the other direction is done symmetrically. We also have to show that τ is the unit of sequential composition

$$\pi \bullet \tau = \tau \bullet \pi = \tau$$

Consider the first equation, by definition it is equal to

$$\pi \times \{\tau\} \cong \pi$$

which is isomorphic to π, the singleton set $\{\tau\}$ being the unit of cartesian product.

For the second part, since a power set is a complete lattice we have that $\mathcal{P}(S)$ is a sup-lattice, so we just have to show that update product is the action of the quantale $\mathcal{P}(\Sigma)$ on $\mathcal{P}(S)$. We first show that it is join-preserving, that is for $P, P_i \subseteq S$ and $\pi, \pi_i \subset \Sigma$) we should have

$$\bigcup_i P_i \otimes \pi = \bigcup_i (P_i \otimes \pi) \quad \text{and} \quad P \otimes \bigcup_i \pi_i = \bigcup_i (P \otimes \pi_i)$$

For the first one we have by definition the following

$$\bigcup_i P_i \otimes \pi = \{(s_i, \sigma) \mid s_i \in \bigcup_i P_i, \sigma \in \pi, s_i \in \mu(\sigma)\}$$

which is equal to the following

$$\bigcup_i \{(s_i, \sigma) \mid s_i \in P_i, \sigma \in \pi, s_i \in \mu(\sigma)\} = \bigcup_i (P_i \otimes \pi)$$

The proof for the other argument is done symmetrically. The second thing we have to show is that update is associative over the sequential composition, that is

$$P \otimes (\pi_1 \bullet \pi_2) = (P \otimes \pi_1) \otimes \pi_2$$

We start from the left hand side

$$P \otimes (\pi_1 \bullet \pi_2) = \{(s, (\sigma_1, \sigma_2)) \mid s \in P, \sigma_1 \in \pi_1, \sigma_2 \in \pi_2, s \in \mu(\sigma_1) \cap [\sigma_1]\mu(\sigma_2)\}$$

each element of which is by re-bracketing isomorphic to $((s, \sigma_1), \sigma_2)$. We have to show that the pre-conditions also hold, that is

$$s \in \mu(\sigma_1) \cap [\sigma_1]\mu(\sigma_2) \quad \text{iff} \quad s \in \mu(\sigma_1) \text{ and } s \otimes \sigma_1 \in \mu(\sigma_2)$$

now by adjunction between update and dynamic modality we get

$$s \in \mu(\sigma_1) \cap [\sigma_1]\mu(\sigma_2) \quad \text{iff} \quad s \in \mu(\sigma_1) \text{ and } s \in [\sigma_1]\mu(\sigma_2)$$

which gets us to the right hand side. The last thing we have to show is that update preserves the unit of sequential composition, that is

$$P \otimes \tau = P$$

which is again a very easy proof, since every state satisfies the precondition of τ and we have the following isomorphism

$$P \otimes \tau = \{(s, \tau) \mid s \in P, s \in \mu(\tau)\} \cong \{s \mid s \in P\} = P$$

We have proved parts (i) and (ii) of the proposition and by these it follows that $(\mathcal{P}(S), \mathcal{P}(\Sigma))$ is a system. The atomistic condition follows since both the module and quantale are power sets, and more over if s is a state and σ an action, then by the product construction $(s \otimes \sigma) = \{(s, \sigma)\}$ is a state since it does not contain a union. And similarly on the quantale we have that if σ_1 and σ_2 are two actions, so is $\sigma_1 \bullet \sigma_2 = \{(\sigma_1, \sigma_2)\}$. □

We now extend our pair of quantale and module to an epistemic system, using the appearance maps:

Lemma 6.6.4 *The following are true*
i. *The appearance maps $f_A : \mathcal{P}(S) \to \mathcal{P}(S)$ are sup-homomorphisms.*
ii. *The appearance maps on actions $f_A : \mathcal{P}(\Sigma) \to \mathcal{P}(\Sigma)$ are sup-homomorphisms and satisfy the following for π_1, π_2 epistemic programs*

$$f_A(\pi_1 \bullet \pi_2) \cong f_A(\pi_1) \bullet f_A(\pi_2)$$

iii. *The following holds between the update product and the appearance maps*

$$f_A(P \otimes \pi) \cong f_A(P) \otimes f_A(\pi)$$

Proof. The first property is easily verified by definition of appearance maps of epistemic propositions:

$$f_A(\bigcup_i P_i) = \bigcup \{f_A(s) \mid s \in \bigcup_i P_i\}$$

which is equal to

$$\bigcup_i \bigcup \{f_A(s) \mid s \in P_i\} = \bigcup_i f_A(P_i)$$

The join preservation of appearance of epistemic programs is verified in the same way as above. It remains to show the equality between appearance of sequential composition and sequential composition of appearances:

$$f_A(\pi_1 \bullet \pi_2) = \bigcup \{f_A(\sigma_1 \bullet \sigma_2) \mid \sigma_1 \bullet \sigma_2 \in \pi_1 \bullet \pi_2\}$$

which is equal to the following by definition of appearance of sequential composition

$$\bigcup \{f_A(\sigma_1) \times f_A(\sigma_2) \mid \{\sigma_1\} \times \{\sigma_2\} \subseteq \pi_1 \times \pi_2\}$$

and this is equal to

$$\bigcup \{f_A(\sigma_1) \mid \sigma_1 \in \pi_1\} \times \bigcup \{f_A(\sigma_2) \mid \sigma_2 \in \pi_2\} = f_A(\pi_1) \times f_A(\pi_2) = f_A(\pi_1) \bullet f_A(\pi_2)$$

The reason for equality rather than the inequality of epistemic systems is that in DEL sequential composition of any two programs is allowed, where as in our algebraic setting, we do not allow any sequential composition, if the outcome of first program does not satisfy the precondition of the second one, their sequential composition, by the definition in our algebra, will be impossible (that is $\perp$). In DEL this is only reflected in the update of the sequential composition, that is if the sequential composition is impossible, it is still formed, but cannot perform an update on the propositions.

For the third part, we show that the following two sets are equivalent

$$\begin{aligned} f_A(P \otimes \pi) &= \bigcup \{ f_A(s, \sigma) \mid s \in P, \sigma \in \pi, s \in \mu(\sigma) \} \\ f_A(P) \otimes f_A(\pi) &= \{ (s', \sigma') \mid s' \in f_A(P), \sigma' \in f_A(\pi), s' \in \mu(\sigma') \} \end{aligned}$$

Since we have closed the set of propositions under all updates $S \otimes \Sigma \subseteq S$, in a concrete epistemic system the update map has become a total map. So for $P \subseteq S$ and $\pi \subseteq \Sigma$ if we have $P \otimes \pi = \emptyset$ then it should be the case that either $P = \emptyset$ or $\pi = \emptyset$. As a result of this, the μ conditions in the definition of f_A's of update above can be ignored. This makes the above two sets equivalent and thus the stronger equality version of the update inequality true. □

Theorem 6.6.5 *The concrete epistemic system $(\mathcal{P}(S), \mathcal{P}(\Sigma), \{f_A\}_{A \in \mathcal{A}})$ is an atomistic epistemic system.*

Proof. Follows by lemmas 6.3, 6.4, and 6.6 above. □

In order to be consistent with the terminology of [8], we call an epistemic system with the equality versions of the update and mutiplication inequalities as follows

Definition 6.6.6 *An epistemic system where the update and multiplication inequalities lift to equalities is called a strong epistemic system.*

So the above theorem becomes as follows

Theorem 6.6.7 *The concrete epistemic system $(\mathcal{P}(S), \mathcal{P}(\Sigma), \{f_A\}_{A \in \mathcal{A}})$ is a strong atomistic epistemic system.*

6.7 Variations on Epistemic Modalities

So far we have only had two unary operators on epistemic propositions and we saw how one can be seen as a knowledge modality. As discussed in the chapter on algebra, one can get more modalities by asking the module to be a boolean algebra (as is the case here), or to ask more properties for appearances, or compose the adjoints. In this section we will do the same construction but in a set-theoretic way.

Properties of the Module In chapter two we showed how the diamond epistemic modality arises in a Boolean Algebra. In the boolean setting of a powerset $\mathcal{P}(S)$, each relation $R \subseteq S \times S$ can be lifted to a sup-map $f_R : \mathcal{P}(S) \to \mathcal{P}(S)$ where f_R assigns the image of R to the element of each singleton, that is as follows

$$f_R(\{x\}) = \{y \in S \mid xRy\}$$

It can easily be seen that f_R is union preserving and thus a sup-map and thus it has a Galois right adjoint denoted as $f_R^* : \mathcal{P}(S) \to \mathcal{P}(S)$, that is

$$f_R \dashv f_R^* .$$

Moreover each relation $R \subseteq S \times S$ has an inverse $R^{-1} \subseteq S \times S$, which can also be lifted to a sup map $f_{R^{-1}}$. This sup map is called the *linear adjoint* of f_R and denoted as follows

$$f_{R^{-1}} = f_R^+ : \mathcal{P}(S) \to \mathcal{P}(S) .$$

The boolean setting also provides us with a full classical negation, which is defined using the complement operation on sets. That is for any subset $X \subseteq S$ it negation is defined as $X^c := S \setminus X$. The linear adjoint and negation give rise to the following proposition:

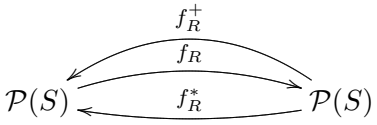
Proposition 6.7.1 In a Boolean Algebra $\mathcal{P}(S)$, every pair of maps $f, g : \mathcal{P}(S) \to \mathcal{P}(S)$ that form an adjunction $f \dashv g$ gives rise to another pair of adjoint maps on their linear adjoints $f^+ \dashv g^+$ defined as $f^+ = g(X^c)^c$ and $g^+ = f(X^c)^c$.

Proof. For $P, Q \subseteq S$:

$$\begin{array}{rcl} f(P) & \dashv & g(P) \\ f(P^c) \subseteq Q^c & \Leftrightarrow & P^c \subseteq g(Q^c) \\ (Q^c)^c \subseteq (f(P^c))^c & \Leftrightarrow & (g(Q^c))^c \subseteq (P^c)^c \\ Q \subseteq (f(P^c))^c & \Leftrightarrow & (g(Q^c))^c \subseteq P \\ Q \subseteq g^+(P) & \Leftrightarrow & f^+(Q) \subseteq P \\ f^+(P) & \dashv & g^+(P) \end{array}$$

□

Thus the linear adjoint f^+ of a map f is the De Morgan dual of its categorical (Galois) adjoint f^*. Pictorially we have



where

$$f_R \dashv f_R^* \quad \text{and} \quad f_R^+(X) = (f_R^*(X^c))^c .$$

Using the above proposition we can calculate the linear adjoint to our appearance mops that is f_A^+, recall that f_A's were calculated by lifting from accessibility relations, as follows:

$$\begin{aligned} f_A^+(P) = (\Box_A P^c)^c &= \{s \in S \mid \forall t \in f_A(s), t \in P^c\}^c \\ &= \{s \in S \mid \forall t \in f_A(s), t \notin P\}^c \\ &= \mathcal{P}(S) \setminus \{s \in S \mid \forall t \in f_A(s), t \notin P\} \\ &= \{s \in S \mid \exists t \in f_A(P), t \in P\}\,. \end{aligned}$$

This operation is the Diamond modality of epistemic logic

$$\Diamond_A P = \{s \in S \mid \exists t \in f_A(s), t \in P\}\,,$$

If we interpret $\Box_A P$ as the *past of (all of) proposition P*, that is propositions that hold before P holds now, then we can interpret $\Diamond_A P$ as *past of part of P* (as opposed to *past of all of P* in $\Box_A$). We can similarly calculate the linear adjoint to the box modality, that is $\Box_A^+$ and we get

$$\begin{aligned} \Box_A^+ P = f_A(P^c)^c &= \bigcup \{f_A(s) \mid s \in P^c\}^c \\ &= \bigcup \{s \in S \mid s \notin f_A(P^c)\}\,. \end{aligned}$$

The epistemic significance of linear adjoint to epistemic modality $f_A(P^c)^c$ is not yet clear to me. It can be read as all the propositions an agent does not consider true if P does not hold in the real world. Temporally, it signifies the propositions that do not hold in the future of P^c. Note that 'future of P' or $f_A(P)$ and 'future of not P' or $f_A(P^c)$ might not be distinct $f_A(P) \cap f_A(P^c) \neq \emptyset$. That is future of P^c is **not** the complement of the future of P, $f_A(P^c) \neq (f_A(P))^c$. Similarly 'future of P' or $f_A(P)$ and 'not future of not P' or $(f_A(P^c))^c$ might have a non-empty intersection $f_A(P) \cap (f_A(P^c)^c) \neq \emptyset$, and moreover $f_A(P) \neq (f_A(P^c))^c$.

Properties of Appearance As discussed before, our epistemic modality $\Box_A$ has the properties of the K modality of normal epistemic logics. In the semantics chapter we showed how one gets different modalities, e.g. T and $S4$, by closure and co-closure properties of f_A maps. In this section we go through the same constructions but using set-theoretic constructions on accessibility relations. As mentioned before, the relational properties that are usually asked for accessibility relations, will not work with our repackaged appearance maps. We need to ask for order properties. For example in the usual Kripke structures, the transitivity of accessibility relation leads to positive introspection for the epistemic modality. If we translate the transitivity of the accessibility relation R_A to the appearance maps f_A derives from it, we get the following

$$Q \subseteq f_A(P) \wedge W \subseteq f_A(Q) \Rightarrow W \subseteq f_A(P)$$

But his does not lead to positive introspection of knowledge, that is

$$(Q \subseteq f_A(P) \wedge W \subseteq f_A(Q) \Rightarrow W \subseteq f_A(P)) \not\Rightarrow \Box_A P \subseteq \Box_A \Box_A P\,.$$

The reason is that by appearance-knowledge adjunction, $\Box_A P \subseteq \Box_A \Box_A P$ is equivalent to $f_A(f_A(\Box_A P)) \subseteq P$. So to prove $\Box_A P \subseteq \Box_A \Box_A P$ it is enough to show $f_A(f_A(\Box_A P)) \subseteq P$, but this cannot be proven by our transitivity assumptions. As discussed chapter two, the right way to go to prove for example positive introspection of knowledge, is to assume f_A is idempotent. That is

$$f_A(f_A(P)) \subseteq f_A(P) \Rightarrow \Box_A P \subseteq \Box_A \Box_A P\,.$$

The idempotence of f_A enables us to say $f_A(f_A(\Box_A P)) \subseteq P$ is equal to $f_A(\Box_A P) \subseteq P$, which is true by appearance-knowledge adjunction.

Composition of Adjoints Following the same path as chapter two, we can compose the appearance map with knowledge to get two more modalities. These composition modalities are defined set theoretically as

$$\begin{aligned} \bigcirc_A := f_A(\Box_A P) &= \bigcup \{f_A(s) \mid f_A(s) \subseteq P\} \\ \bigcirc'_A := \Box_A f_A(P) &= \{s \in S \mid f_A(s) \subseteq f_A(P)\} \end{aligned}$$

The second equation can be more simplified to $\bigcirc'_A = \{s \in S \mid s \subseteq P\}$. Given a proposition P, $\bigcirc'_A$ returns the states in which P holds. The first composition modality $\bigcirc_A$ returns the accessible states in which P holds. Note that these modalities are both monotone, but neither preserve disjunction or conjunction of propositions.

Chapter 7

Appendix: Sup-Enriched Categorical Semantics

In this appendix we show how sup-enriched categories provide semantics for our epistemic systems. The theory of quantales and modules in an enriched categorical setting has been studied in [20, 58] and also investigated in detail in [85]. First, we go over the construction of a tensor product for sup lattices and show how this tensor makes the category sup a monoidal closed category. By this it follows that sup is enriched in itself. Then, we recast our epistemic setting in the sup-enriched category sup. There are two main feature to this categorical semantics:

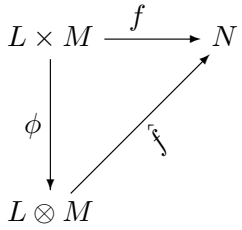
1. Each agent has his own propositions, updates, facts and kernels. Reality is a fixed agent of the setting and this encodes real propositions, updates, facts and kernel of actions.

2. Appearance of each agent is the lax sup-enriched natural transformation between reality and each agent's propositions.

These features allow us to encode more interesting cases of epistemic scenarios such as muddy children. For example when the update ability of each child, together with his set of facts are different from that of other children and also different from reality and this leads to a different reasoning scheme for each agent. It then becomes very interesting to investigate how these personalized setting affect the problem of logical omniscience, mentioned in the introduction.

7.1 Sup as a Sup-Enriched Category

Consider two sup-lattices L and M in the category of sup-lattices and join-preserving maps, that is Sup, and their tensor product $L \otimes M$ defined in terms of the meet preserving maps $Inf(L^{op}, M)$. We show that this definition of tensor satisfies the universal property:



where $\times$ is a direct product, i.e. cartesian product equipped with point wise order (cf. Coecke and Moore in [25]). The universal property expressed in this diagram says that given two join-preserving maps $\phi : L \times M \to L \otimes M$ and $f : L \times M \to N$, there exists a unique join-preserving map $\hat{f} : L \otimes M \to N$ that makes the above diagram commute. In the other direction, given ϕ and any join-preserving map $\hat{f}$ from $L \otimes M$ to N, the composition $\phi; \hat{f}$ provides us with a map from $L \times M$ to N.

For $L \otimes M = Inf(L^{op}, M)$ the ϕ map defined below inputs a pair $(a, b) \in L \times M$ and outputs a meet-preserving map $\phi(a, b) \in L \otimes M$:

$$\phi(a,b) : L^{op} \to M :: \begin{cases} \top \mapsto \top \\ \{\uparrow a\} \setminus \{1\} \mapsto b \\ \{\uparrow a\}^c \mapsto \bot \end{cases} \tag{7.1}$$

Note that $\phi(a, b)$ is a mapping that lives in $L \otimes M$ and maps the empty meet $\bigwedge \emptyset = \top$ in L^{op} to $\top$ in M, so it preserves the empty meet in L^{op}. It can be shown that it also preserves all other meets. On the other hand, ϕ should preserve all joins including the empty ones in both arguments. That is, it has to map both $(\bot, b)$ and $(a, \bot)$ to the smallest map in $L \otimes M$, which sends $\top$ to $\top$ and everything else to $\bot$. It is easy to verify that ϕ preserves the empty joins in both arguments and that it is order preserving.

For a given f, the unique $\hat{f} : L \otimes M \to N$ is derived by $g \mapsto \bigvee_{a \in L} f(a, g(a))$. It can be shown that $f(a, b) = \bigvee_{x \in L} f(x, \phi(a, b)(x))$ and this makes the above diagram commute by replacing $\phi(a, b)$ for g. The uniqueness of $\hat{f}$ can be shown by proving that all other maps g in $L \otimes M \setminus Img(\phi)$ can be written in terms of ϕ using the equation $g = \bigvee_{a \in L} \phi(a, g(a))$.

Using the universal property of tensor and observing that direct product (point wise cartesian product) of sup-lattices is the categorical product in Sup, it can be shown that $\otimes$ is a symmetric monoidal tensor in Sup with $I = 2$ (the lattice with two elements $\bot$ and $\top$) equipped with two morphisms $l : I \otimes M \to M$ and $r : M \otimes I \to M$ that correspond to the isomorphism $M \otimes I \cong M$ and satisfy coherence axioms. Each morphism $2 \to M$ sends $\bot$ to $\bot$ and $\top$ to an arbitrary element in M. Moreover and by using the universal property and closedness of direct product, it can be shown that $L \multimap M$, defined as $Sup(L, M)$, is the co-tensor and thus $Sup(L \otimes M, N) \cong Sup(L, M \multimap N)$. The morphism $(L \multimap M) \otimes L \to M$ is the evaluation morphism of [20] denoted as $ev_{L,M}$. By the isomorphism $(Inf(L^{op}, M^{op}))^{op} \cong Sup(L, M)$ we get $L \multimap M \cong (L \otimes M^{op})^{op}$ and thus the *-autonomy of Sup.

It has to be noted that all these hold by taking $L \otimes M = Gal(L, M)$ defined in [71].

Since Sup is monoidal closed, it is enriched in itself [20]. Closedness of sup can be seen by observing that for all objects L, M in Sup, $L \multimap M = Sup(L, M)$ is also a sup-lattice and thus an object of Sup (the object of morphism). For all L, M, N in Sup, the composition morphism

$$Sup_{L,M,N} : Sup(L, M) \otimes Sup(M, N) \to Sup(L, N)$$

can be rewritten as

$$(L \multimap M) \otimes (M \multimap N) \to (L \multimap N)\,,$$

By adjunction and symmetry, this corresponds to the following composite

$$(L \multimap M) \otimes L \otimes (M \multimap N) \to M \otimes (M \multimap N) \to N\,.$$

For each L in Sup, the identity morphism on L is $u_L : I \to Sup(L, L)$ and by adjunction corresponds to the isomorphism $I \otimes L \cong L$.

7.2 Quantale as a One-Object Sup-Enriched Category

Consider a one object sup-enriched category Q and its only object $*$. The morphism object in Sup $Q(*, *)$ corresponds to the elements of a quantale Q. The composition morphism

$$Q_{*,*,*} : Q(*, *) \otimes Q(*, *) \to Q(*, *)$$

corresponds to the quantale multiplication $(q, q') \mapsto q \bullet q'$ by the universal property of tensor. The identity morphism on $*$ i.e. $u_* : 2 \to Q(*, *)$ picks the unit of quantale from $Q(*, *)$ and makes the following diagram (interaction between unit of quantale and unit of Sup) and a similar one for r commute:

$$\begin{array}{ccc} 2 \otimes Q(*,*) & \xrightarrow{u_* \otimes id_Q} & Q(*,*) \otimes Q(*,*) \\ \Big\downarrow{\scriptstyle l} & & \Big\downarrow{\scriptstyle Sup_{Q,Q,Q}} \\ Q(*,*) & = & Q(*,*) \end{array}$$

Note that $u_* \in Sup(2, Q)$, which is also isomorphic to Q. To see this recall $2 \cong 2^{op}$ and $(Sup(2^{op}, Q))^{op} \cong Inf(2, Q^{op}) \cong Q^{op}$ and thus $Sup(2^{op}, Q) \cong Q$.

7.3 Modules as Sup-Enriched Functors

A right module M over a quantale Q with the right action $\phi : M \otimes Q \to M$ is a sup-enriched functor $\mathcal{M} : Q \to Sup$. It assigns to $*$ a sup-lattice $\mathcal{M}(*) = M \in Sup$ and a sup-morphism

$$\mathcal{M}_{*,*} : Q(*,*) \to Sup(\mathcal{M}(*), \mathcal{M}(*)) .$$

That is to say each element q of the quantale is sent to a map $\phi(-, q) \in Sup(M, M)$. These data are required to make the following diagram commute,

$$\begin{array}{ccc} Q(*,*) \otimes Q(*,*) & \xrightarrow{\mathcal{M}_{*,*} \otimes \mathcal{M}_{*,*}} & Sup(M,M) \otimes Sup(M,M) \\ \downarrow{\scriptstyle Sup_{*,*,*}} & & \downarrow{\scriptstyle Sup_{M,M,M}} \\ Q(*,*) & \xrightarrow[\mathcal{M}_{*,*}]{} & Sup(M,M) \end{array}$$

This diagram corresponds to the module equation $\phi(m, q \bullet q') = \phi(\phi(m, q), q')$. We should also have that $u_* \circ \mathcal{M}_{*,*} = u_{\mathcal{M}(*)}$, which corresponds to the other module equation $\phi(m, 1) = m$. Diagrammatically, the following should commute

$$\begin{array}{ccc} I & \xrightarrow{u_*} & Q(*,*) \\ & \searrow^{u_{\mathcal{M}(*)}} & \downarrow{\scriptstyle \mathcal{M}_{*,*}} \\ & & Sup(M,M) . \end{array}$$

A system (M, Q) can now be depicted as

$$Q \xrightarrow{\mathcal{M}} Sup$$

where Q is a one object sup-enriched category, and $\mathcal{M}$ is a sup-enriched functor.

7.4 Appearances as Sup-Enriched Natural Transformations

In previous chapters we showed how *epistemic actions* form a quantale Q and epistemic propositions form a Q-right module M and that the action of the module is the epistemic update of a proposition. This setting is based on the same update for all the agents. However, it is very reasonable to consider different update schemes for different agents. Moving to the categorical setting equips us with a better

mean to personalize the update of each agent[1]. This is done by considering different sup-enriched functors $\mathcal{M}_A, \mathcal{M}_B, \cdots$ for each agent. For example, a functor $\mathcal{M}_A$ results in propositions that are true in agent A's mind, that is $\mathcal{M}_A(*) = M_A$ together with her personal updates $\mathcal{M}_A(q) = \phi_A(-, q)$. The inequality $\mathcal{M}_A(q) \leq \mathcal{M}_A(q')$ says that the update by q is stronger than the update by q' in the sense than the latter is implied by the former (the passage is contravariant) i.e. $\phi_A(m_A, q) \leq \phi_A(m_A, q')$. In the same way the update that implies and implied by top $\phi_A(m_A, q) = \top$ in M_A is the weakest update. Similarly $m_A \leq \phi_A(m_A, q)$ means a negative update, since the proposition after update is derivable even before update.

We fix an agent R to metaphorically represent the reality and $\mathcal{M}_R$ stands for the 'real world', that is the real propositions and updates. The appearance maps of agents can be seen as the way real propositions and updates appear to each agents. The connection between real and each agent's propositions is established through a sup-enriched natural transformation for each agent $\alpha_A : \mathcal{M}_R \Rightarrow \mathcal{M}_A$

$$Q \xrightarrow[\Downarrow^{\alpha_A}]{\mathcal{M}_R \atop \mathcal{M}_A} Sup\,.$$

This natural transformation consists in giving for $* \in Q$, a morphism $\alpha_A^* : 2 \to Sup(M_R, M_A)$ in Sup, which satisfies the axiom of naturality [20]. The lax such natural transformation expresses our appearance-update inequality, where the appearance of real update $\phi_R(-, q)$ to agent A is stronger than the agent A's personalized update $\phi_A(-, q)$ on his own appearances. Abusing the notation, the instance α_A^* of natural transformation will be noted as the natural transformation itself α_A. So we have

$$\mathcal{M}_R(q); \alpha_A \leq \alpha_A; \mathcal{M}_A(q)$$

that is

$$\alpha_A(\phi_R(m_R, q)) \leq \phi_A(\alpha_A(m_R), q)\,.$$

This corresponds to the following lax diagram

$$\begin{array}{ccc} \mathcal{M}_R(*) & \xrightarrow{\mathcal{M}_R(q)} & \mathcal{M}_R(*) \\ \Big\downarrow{\scriptstyle \alpha_A} & \geq & \Big\downarrow{\scriptstyle \alpha_A} \\ \mathcal{M}_A(*) & \xrightarrow[\mathcal{M}_A(q)]{} & \mathcal{M}_A(*)\,. \end{array}$$

Two times pasting the laxity diagram results in an inequality for the appearance of update with sequen-

[1]This can also be done in the algebraic setting, by assuming a family of updates $\{\cdot_A\}_{A \in \mathcal{A}}$ one for each agent, making the setting rather crowded.

tial composition of actions

$$\mathcal{M}_R(q' \bullet q); \alpha_A \leq \alpha_A; \mathcal{M}_A(q' \bullet q)\,.$$

or diagrammatically

$$\begin{array}{ccccc}
\mathcal{M}_R(*) & \xrightarrow{\mathcal{M}_R(q)} & \mathcal{M}_R(*) & \xrightarrow{\mathcal{M}_R(q')} & \mathcal{M}_R \\
\Big\downarrow{\scriptstyle \alpha_A} & \geq & & \geq & \Big\downarrow{\scriptstyle \alpha_A} \\
\mathcal{M}_A(*) & \xrightarrow[\mathcal{M}_A(q)]{} & \mathcal{M}_A(*) & \xrightarrow[\mathcal{M}_A(q')]{} & \mathcal{M}_A
\end{array}$$

The meet-preserving Galois right adjoint to the appearance of each agent $\alpha_A \dashv \alpha_A^\dagger$ is itself a natural transformation in $Inf(M_R, M_A)$. The composition $\alpha_A^\dagger \circ \alpha_A$ of this adjoint natural transformation pair $(\alpha_A, \alpha_A^\dagger)$ enables us to compare the appearance of each agent to reality. One can think of this composition as *knowledge* of the agent. For example the extreme case when α_A and $\alpha_A^\dagger$ are inverses, we have that $\alpha_A^\dagger(\alpha_A(m_R)) = m_R$, which expresses agent A's certain knowledge of reality. In another extreme case where $\alpha_A^\dagger(\alpha_A(m_R)) = \top_{M_R}$, agent A has no knowledge of what is *really* going on! Another interesting case is when agent A is deceived about the reality. In this case $m_R \not\leq m'_R$ but $\alpha_A^\dagger(\alpha_A(m_R)) \leq \alpha_A^\dagger(\alpha_A(m'_R))$. This composition should indeed be, as it is in these cases, consistent with the adjoint inequalities

$$\alpha_A(\alpha_A^\dagger(m_A)) \leq m_A \qquad \text{and} \qquad m_A \leq \alpha_A^\dagger(\alpha_A(m_A))\,.$$

We can compare this composition for different agents and compare knowledge of these agents. For example $\alpha_A^\dagger(\alpha_A(m_R)) \leq \alpha_B^\dagger(\alpha_B(m_R))$ says that agent A has more knowledge of reality than agent B. In the same way, we can talk about the way agent A appears to agent B and the other way around (how B appears to A) by looking at natural transformations between the modules of the two, that is $\alpha_{AB} : \mathcal{M}_A \Rightarrow \mathcal{M}_B$ and $\alpha_{BA} : \mathcal{M}_B \Rightarrow \mathcal{M}_A$ both satisfying similar update inequalities

$$\alpha_{AB}(\phi_A(m_A, q)) \leq \phi_B(\alpha_{AB}(m_A), q) \quad \text{and} \quad \alpha_{BA}(\phi_B(m_B, q)) \leq \phi_A(\alpha_{BA}(m_B), q)\,.$$

Facts are also personalized, so the 'real facts' are

$$F_R = \{f_R \in M_R \mid \forall q \in Sup(Q, Q), \phi_R(f_R, q) = f_R\}\,.$$

Each agent has its own set of facts (we can call these dogmas) stable under his own updates

$$F_A = \{f_A \in M_A \mid \forall q \in Sup(Q, Q), \phi_A(f_A, q) = f_A\}\,.$$

We have the following, by the fact equality for real facts and the lax natural transformations

$$\alpha_A(f_R) = \alpha_A(\phi_R(f_R, q)) \leq \phi_A(\alpha_A(f_R), q)$$

One can establish some consistencies between the real and personalized facts. For example, if we ask $\alpha_A(f_R) \in F_A$ then we get $\phi_A(\alpha_A(f_R), q) = f_A$ and thus $\alpha_A(f_R) = f_A$. This means that appearance of real facts to agents are a subset of the facts of the agents and so appearance preserve real facts. The kernels of each action can also be personalized for each agent

$$ker_A(q) = \{m_A \in M_A \mid \phi_A(m_A, q) = \bot\}$$

Using the laxity diagram we can show

$$\alpha_A(m_R) \in ker_A(q) \quad \text{implies} \quad \alpha_A(\phi_R(m_R, q)) = \bot\,.$$

On the other hand,

$$m \notin ker_R(q) \quad \text{implies} \quad \alpha_A(m) \notin ker_A(q)\,.$$

This is due to the strict inequality $\bot < \mathcal{M}_R(q)(m)$, order preservation of α, i.e. $\alpha(\bot) = \bot < \mathcal{M}_R(q); \alpha_A$ and the laxity $\mathcal{M}_R(q); \alpha_A \leq \alpha_A; \mathcal{M}_A(q)$. That is $\mathcal{M}_A(q)(\alpha_A(m)) \neq \bot$. It can also be shown that

$$m \leq m' \quad \text{and} \quad m' \in ker_A(q) \quad \text{implies} \quad m \in ker_A(q)\,.$$

Based on this, $\alpha_A(\alpha_A^\dagger(m))$ and $\alpha_A(\alpha_A^\dagger(m'))$ are also in $ker_A(q)$. So some consistency between the real and personalized kernels follows.

To conclude, the categorical semantics establishes agents as different types and distinguishes between their abilities. This provides us with more *room* in the formalism. The extra room can be used to model reasoning of non-uniform agents in multi-agent systems, and thus makes us get closer to real life scenarios. Further contemplation on and implementation of these issues constitutes future work.

Chapter 8

Bibliography

Bibliography

[1] S. Abramsky, 'Domain Theory in Logical Form', *Proceedings of IEEE Symposium on Logic in Computer Science*, pp. 47-53, 1987.

[2] S. Abramsky and S. Vickers, 'Quantales, observational logic and process semantics'. *Mathematical Structures in Computer Science* **3**, pp. 161-227, 1993.

[3] M. Adams and W. Dziobiak (eds.), Special Issue on Priestley Duality, *Studia Logica* **56**, 1996.

[4] C. Alchourron, P. Gardenfors and D. Makinson, 'On the logic of theory change: partial meet contraction and revision functions', *Journal of Symbolic Logic* **50**, pp. 510-535, 1985.

[5] A. Baltag, 'A coalgebraic semantics for epistemic programs', *Electronic Notes in Theoretical Computer Science* **82**, Issue 1, 22 pages, 2003.

[6] A. Baltag, 'A Logic for Suspicious Players: Epistemic Actions and Belief Updates in Games', *Bulletin of Economic Research* **54**, pp. 1-46, 2002.

[7] A. Baltag, B. Coecke, and M. Sadrzadeh, 'Epistemic actions as resources' accepted for publication in *Journal of Logic and Computation*, `http://eprints.ecs.soton.ac.uk/12824`.

[8] A. Baltag, B. Coecke, and M. Sadrzadeh, 'Algebra and Sequent Calculus for Epistemic Actions', *Electrical Notes in Computer Science* **126**, pp. 27-52, 2005.

[9] A. Baltag and L.S. Moss, 'Logics for epistemic programs', *Synthese* **139**, pp. 165-224, 2004.

[10] A. Baltag, L.S. Moss and S. Solecki, 'The logic of public announcements, common knowledge and private suspicions', CWI Technical Report SEN-R9922, 1999.

[11] A. Baltag and M. Sadrzadeh, 'The Algebra of Multi-Agent Dynamic Belief Revision', *Electronic Notes in Theoretical Computer Science* **157**, Issue 4, pp. 37-56, 2006.

[12] J. Barwise, D. Gabbay and C. Hartonas. 'On the logic of information flow'. *Bulletin of the Interest Group in Pure and Applied Logics* **3**, pp. 7-49, 1995.

[13] C.H. Bennet, 'Quantum Cryptography Using Any Two Nonorthogonal Sttes', *Physical Review Letters* **68**, pp. 3121-3124, 1992.

[14] C.H. Bennet, G. Brassard and N.D. Mermin, 'Quantum Cryptography without Bell's Theorem', *Physical Review Letters* **68**, pp. 557-559, 1992.

[15] C.H. Bennet and G. Brassard, 'Quantum Cryptography: Public Key Distribution and Coin Tossing', *Proceedings of International Conference on Computers Systems and Signal Processing*, 1984.

[16] G, Birkhoff, *Lattice Theory*, American Mathematical Society Colloquium Publications, vol. 25, 1940.

[17] P. Blackburn, M. de Rijke and Y. Venema, *Modal Logic*, Cambridge, Cambridge University Press, 2002.

[18] R. Blute, J.R.B. Cockett and R.A.G. Seely, 'The Logic of Linear Functors', *Mathematical Structures in Computer Science* **12**, pp. 513-539, 2002.

[19] G. Boole, *An Investigation into the Laws of Thought*, London, 1854 (reprinted by Dover Publication, 1951).

[20] F. Borceaux, *Handbook of Categorical Algebra (3 volumes)*, Encyclopedia of Mathematics and its Applications, Cambridge, Cambridge University Press, 1994.

[21] G. Brassard, C. Crépeau, D. Mayers and L. Salvail, 'A Brief Review on the Impossibility of Quantum Bit Commitment', *Quantum Physics Archives*, arXiv: quant-ph/9712023, 1997.

[22] M. Burrows, M. Abadi and R. Needham, 'A Logic of Authentication', *ACM Transactions on Computer Systems* **8**, pp. 18-36, 1990.

[23] B. Coecke and K. Martin. *A Partial Order on Classical and Quantum States*. Research Report PRG-RR-02-07, Oxford University Computing Laboratory, 2002. `http://web.comlab.ox.ac.uk/oucl/publications/tr/rr-02-07.html`

[24] B. Coecke, D. J. Moore and I. Stubbe. 'Quantaloids describing causation and propagation of physical properties'. *Foundations of Physics Letters* **14**, pp. 133-145, 2001.

[25] B. Coecke, D.J. Moore and A. Wilce, 'Operational Quantum Logic: An Overview', B. Coecke, D. Moore, A. Wilce (eds.), *Current Research in Operational Quantum Logic*, Fundamental Theories of Physics 111, Kluwer Academic Publishers, 2000.

[26] V. Danos, E. Kashefi and P. Panangaden, 'The Measurement Calculus', *Quantum Physics Archives*, arXiv: quant-ph/0412135, 2005.

[27] A. Datta, A. Derek, J.C. Mitchell and D. Pavlovic, 'A derivation system and compositional logic for security protocols', *Journal of Computer Security* **13**, pp. 423-482, 2005.

[28] B.A. Davey and H.A. Priestley, *Introduction to Lattices and Order*, Cambridge, Cambridge University Press, 1990.

[29] A. de Morgan,'On the Syllogism, no. IV, and on the Logic of Relations', *Transactions of the Cambridge Philosophical Society* **10**, pp. 331-358, 1964.

[30] E. de Vink and J. Rutten, 'Bisimulation for Probabilistic Transition Systems, A Coalgebraic Approach', *Theoretical Computer Science* **221**, pp. 271-293, 1999.

[31] E.W. Dijkstra. *A Discipline of Programming*. Prentice-Hall, 1976.

[32] R.P. Dilworth, 'Non-Commutative Residuated Lattices', *Transactions of the American Mathematical Society* **46**, pp. 426-444, 1939.

[33] R.P. Dilworth and M. Ward, 'Residuated Lattices', *Transactions of the American Mathematical Society* **45**, pp. 335-354, 1939.

[34] J. Dubucs, 'Feasibility in Logic', *Synthese*, **132**, pp.213-237, 2002.

[35] J. Dubucs and M. Marion, 'Radical Antirealism and Substructural Logics', to appear in *Proceedings of the contributed papers of LMPS'99*, Dordrecht, Kluwer, 2003.

[36] J.M. Dunn, 'Partial Gaggles Applied to Logics with Restricted Structural Rules', *Substructural Logics*, P. Schroeder-Heister and K. Dosen (eds.), Studies in Logic and Computation 2, New York, Oxford University Press, pp. 63-108, 1993.

[37] M. Dunn, M. Gehrke and A. Palmigiano, 'Canonical Extensions and Relational Completeness of Some Substructural Logics', to appear in *The Journal of Symbolic Logic*.

[38] A.K. Ekert, 'Quantum Cryptography Based on Bell's Theorem', *Physical Review Letters* **67**, pp. 661-663, 1991.

[39] R. Fagin, J. Y. Halpern, Y. Moses and M. Y. Vardi. *Reasoning about Knowledge*. MIT Press, 1995.

[40] P. Gardenförs, 'Belief Revision: An Introduction', Cambridge Tracts in Computer Science, Cambridge University Press, 1992.

[41] J. Gerbrandy, 'Dynamic Epistemic Logic', in L.S. Moss, et al (eds.) *Logic, Language, and Information* **2**, Stanford University, CSLI Publication, 1999.

[42] J. Gerbrandy, and W. Groenveld, 'Reasoning about information change', *Journal of Logic, Language, and Information* **6**, pp. 147-169, 1997.

[43] G. Gierz, K. H. Hofmann, K. Keimel, J. D. Lawson, M. W. Mislove and D. S. Scott. *A Compendium of Continuous Lattices*. Springer-Verlag, 1980.

[44] J-Y. Girard. 'Linear logic'. *Theoretical Computer Science* **50**, pp. 1-102, 1987.

[45] D. Harel, D. Kozen and J. Tiuryn. *Dynamic Logic*. MIT Press, 2000.

[46] J. Hintikka, *Knowledge and Belief: an Introduction to the Logic of Two Notions*, New York, Cornell University Press, 1962.

[47] C. A. R. Hoare and Jifeng, HE. 'The weakest prespecification'. *Information Processing Letters* **24**, pp. 127-132, 1987.

[48] A. Hommersom, J.J. Meyer and E. De Vink, 'Update Semantics of Security Protocols', *Synthese* **142**, pp. 289-327, 2004.

[49] P. T. Johnstone. *Stone Spaces*. Cambridge University Press, 1982.

[50] B. Jonsson and A. Tarski, 'Boolean Algebras with Operators II', *American Journal of Mathematics* **74**, pp. 127-162, 1952.

[51] B. Jonsson and A. Tarski, 'Boolean Algebras with Operators I', *American Journal of Mathematics* **73**, pp. 891-939, 1951.

[52] A. Joyal. 'Free lattices, communication and money games'. M. L. Dalla Chiara et al. (eds.), *Logic and Scientific Methods*, Kluwer, pp. 29-68, 1997.

[53] A. Joyal and M. Tierney. 'An extension of the Galois theory of Grothendieck'. *Memoirs of the American Mathematical Society* **309**, 1984.

[54] D. Kan, 'Adjoint Functors', *Transactions of the American Mathematical Society* **87**, pp. 294-329, 1958.

[55] G.M. Kelly, *Basic Concepts of Enriched Category Theory*, London Mathematical Society Lecture Notes **64**, Cambridge, Cambridge University Press, 1982.

[56] J. Lambek. 'The mathematics of sentence structure'. *American Mathematics Monthly* **65**, pp. 154-169, 1958.

[57] D. Larchy-Wendling and D. Galmiche, 'Quantales as Completions of Ordered Monoids: Revised Semantics for Intuitionistic Linear Logic', *Electronic Notes in Computer Science* **35**, pp. 1-15, 2000.

[58] W. Lawvere, 'Metric Spaces, Generalized Logic, and Closed Categories', *Rend. Sem. Mat. Fis. Milano* **43**, pp. 135-166, 1973,

[59] G. Lowe, 'An Attack on the Needham-Schroeder Public-Key Authentication Protocol',Information Processing Letters **56**, pp. 131-133, 1995.

[60] C. Lutz and F. Wolter, 'Complexity and Succinctness of Public Announcement Logic', *LTCS Technical Report* 05-09, Technische Universitat Dresden, 2005.

[61] S. Mac Lane, *Categories for the Working Mathematician*, Graduate Texts in Mathematics, New York, Springer-Verlag, 1998.

[62] M. Marion and M. Sadrzadeh. 'Reasoning about knowledge in linear logic: modalities and complexity'. D. Gabbay, S. Rahman, J. M. Torres and J.-P. Van Bendegem (eds.), *Logic, Epistemology, and the Unity of Science*, pp. 327-350, Kluwer, 2004.

[63] D. Mayers, 'Unconditionally Secure Bit Commitment Is Impossible', *Quantum Physics Archives*, arXiv:quant-ph/9605044, 1997.

[64] A. Meadows and D. Pavlovic, 'Deriving, attacking and defending the GDOI protocol', *Lecture Notes in Computer Science* **3193**, pp. 53-72, 2004.

[65] J.J.C. Meyer and W. van der Hoek, *Epistemic Logic for Computer Science and Artificial Intelligence*, in Cambridge Tracts in Theoretical Computer Science, vol. 41, Cambridge, Cambridge University Press, 1995.

[66] L.S. Moss, 'Coalgebraic Logic', *Annals of Pure and Applied Logic* **96**, pp. 277-317, 1999.

[67] C. J. Mulvey. &. *Supplemento ai Rendiconti del Circolo Matematico di Palermo* **II**, pp. 99-104, 1992.

[68] R.M. Needham and M.D. Schroeder, 'Using Encryption for Authentication in Large Networks of Computers', *C*ommunications of the ACM **21**, pp. 993-999, 1978.

[69] P. W. O'Hearn and D. J. Pym. 'The logic of bunched implications'. *Bulletin of Symbolic Logic* **5**, pp. 215–244, 1999.

[70] J. Paseka and J. Rosický. 'Quantales'. In: B. Coecke, D. J. Moore and A. Wilce (eds.), *Current Research in Operational Quantum Logic: Algebras, Categories, Languages*, Kluwer, pp. 245-262, 2000.

[71] J. Picado, 'A Quantale of Galois Connections', *Algebra Universalis* **52**, pp. 527-540, 2004.

[72] J. Plaza, 'Logics of public communications', *Proceedings of 4th International Symposium on Methodologies for Intelligent Systems*, 1989.

[73] R. Raussendorf, D.E. Browne and H.J. Briegel, 'The oneway quantum computer a nonnetwork model of quantum computation', *Journal of Modern Optics* **49**, 1299, 2002.

[74] P. Resende. 'Quantales and observational semantics'. In: B. Coecke, D. J. Moore and A. Wilce (eds.), *Current Research in Operational Quantum Logic: Algebras, Categories, Languages*, Kluwer, pp. 263-288, 2000.

[75] G. Restall, *An Introduction to Substructural Logics*, London, Routledge, 2000.

[76] K. Rosenthal, 'Modules Over a Quantale and Models for the operator ! in Linear Logic', *Cahiers de Topologie et Geometrie Differentielle Categoriques* **XXXV-4**, pp. 329-333, 1994.

[77] K. I. Rosenthal. *Quantales and their Applications*. Pitman Research Notes in Mathematics Series **234**, Longman, 1990.

[78] J.J.M.M. Rutten, 'Universal Coalgebra: A Theory of Systems', *Theoretical Computer Science* **249**, pp. 3-80, 2000.

[79] M. Ryan and M. Huth, *Logic in Computer Science*, Cambridge, Cambridge University Press, 2004.

[80] Peter Ryan, Steve Schneider, Michael Goldsmith, Gavin Lowe and Bill Roscoe, *Modelling and Analysis of Security Protocols*, Addison-Wesley, 2001.

[81] M. Sadrzadeh, 'Modal Linear Logic in Higher Order Logic, an experiment in Coq', *Emerging Trends Proceedings of Theorem Proving in Higher Order Logics*, D. Basin and W. Burkhart (eds.), Rome, ARACNE, No. 187, pp.75-93, 2003.

[82] K. Segeberg, 'Two traditions in the logic of belief: bringing them together', in *Logic, Language, and Reasoning***II**, H. Ohlbach and U.Reyle (eds.), pp. 105-134, 1999.

[83] R.M. Smullyan, *First-Order Logic*, New York, Dover Publications, 1995.

[84] M.H. Stone, 'The Theory of Representations for Boolean Algebras', *Transactions of American Mathematical Society* **40**, pp. 37-111, 1936.

[85] I. Stubbe. *Categorical Structures Enriched in a Quantaloid: Categories and Semicategories*. Ph. D. Thesis, Université Catholique de Louvain, 2003.

[86] A. Tarski, *Logic, Semantics, Metamathematics*, Translated by H. Woodger, Oxford, Clarendon Press, 1956.

[87] A.S. Troelstra and H. Schwichtenberg, *Basic Proof Theory*, Cambridge, Cambridge University Press, 1996.

[88] J. Van Benthem. 'Logic in action'. *Journal of Philosophical Logic* **20**, pp. 225-263, 1989.

[89] B. Von Karger, 'Temporal Algebra', *Mathematical Structures in Computer Science* **8**, pp. 277-320, 1998.

[90] M. Ward, 'Residuation in Structures over which a Multiplication is Defined', *Duke Mathematical Journal* **3**, pp. 627-636, 1937.

[91] M. Ward, 'Structure Residuation', *Annals of Mathematics* **39**, pp. 558-568, 1938.

[92] T. Williamson, *Knowledge and Its Limits*, Oxford, Oxford University Press, 2000.

[93] F. Wolter and M. Zakharyaschev. 'The relation between intuitionistic and classical modal logics'. *Algebra and logic* **36**, pp. 73-92, 1997.

[94] D.N. Yetter, 'Quantales and (non-commutative) Linear Logic', *Journal of Symbolic Logic* **55**, pp. 41-64, 1990.