INSTITUTO SUPERIOR TÉCNICO
Universidade Técnica de Lisboa

Dynamic Probabilistic Epistemic Logic

towards information security

Andreia Filipa Torcato Mordido

Dissertação para obtenção do Grau de Mestre em

Matemática e Aplicações

Júri

Presidente:	Prof.ª Doutora Maria Cristina Sales Viana Serodio Sernadas
Orientador:	Prof. Doutor Carlos Manuel Costa Lourenço Caleiro
Vogal:	Prof. Doutor Paulo Alexandre Carreira Mateus

Dezembro 2011

Agradecimentos

Ao Professor Carlos Caleiro agradeço este último ano: o que me ensinou, a capacidade que tem de simplificar até o que é inerentemente complexo, mas acima de tudo agradeço a escolha do tema, nenhum outro me motivaria tanto para os tempos que se seguem.

Ao Professor Paulo Mateus pelo interesse que as aulas de Criptografia despertaram em mim para a área da segurança de informação.

Aos Professores Filipe Oliveira e Fabio Chalub agradeço a amizade, o contágio do gosto pela matemática e a motivação que sempre me deram. O meu agradecimento permanente ao Professor Luís Trabucho pela honra que senti por assistir às suas lições.

À família agradeço os sorrisos, os poemas e a dedicação.

Resumo

Pretendemos estudar na literatura uma lógica que permita raciocinar sobre aspectos relevantes em segurança de informação. Tipicamente num problema de segurança precisamos de raciocinar sobre o conhecimento do intruso, a incerteza associada à distribuição dos objectos desconhecidos e ainda sobre actualizações de informação. A lógica dinâmica probabilistica e epistémica parece cobrir todos estes requisitos e impõe-se suficientemente expressiva para modelar situações simples mas pertinentes em segurança. Neste texto faremos uma revisão da lógica dinâmica probabilistica e epistémica e culminamos com a aplicação desta lógica a duas situações simples mas bastante significativas em segurança de informação. A primeira aplicação surge no âmbito da criptanálise e baseia-se na descoberta de um segredo por parte de um atacante que tem a capacidade de interagir com o sistema. O segundo problema prende-se com os conhecidos *chosen-plaintext attack* e *chosen-chiphertext attack* e desenvolve-se em torno da importante noção de indistinguibilidade computacional.

A lógica dinâmica probabilistica epistémica prova ser importante no contexto da segurança de informação, apresentando potencialidades para no futuro ser a base da correcção de alguns protocolos em segurança.

Palavras-chave: lógica modal, lógica epistémica, lógica probabilistica epistémica, lógica dinâmica probabilistica epistémica, segurança de informação, indistinguibilidade computacional.

Abstract

We pretend to study in the literature a logic that allows us to reason about relevant issues in information security. Typically in a security problem we need to reason about the intruder's knowledge, the uncertainty related with the distribution of the unknown objects and still about updates of information. The dynamic probabilistic epistemic logic seems to cover all these requirements and imposes itself to be expressive enough to model simple but relevant situations in security. In this text we make an overview of the dynamic probabilistic epistemic logic and we end up applying this logic to a couple of simple but quite significant situations in information security. The first application arises in the context of cryptanalysis and is based upon the discovery of a secret by an attacker who is able to interact with the system. The second problem is related to the known chosen-plaintext attack and chosen-ciphertext attack and is developed around the important notion of computational indistinguishability.

The dynamic probabilistic epistemic logic proves to be importance worthy in the context of information security, with the potential to constitute in the future the basis of the correctness of some security protocols.

Key words: modal logic, epistemic logic, probabilistic epistemic logic, dynamic probabilistic epistemic logic, information security, computational indistinguishability.

Contents

Chapter 1

Introduction

Information security is a topic that has been shown essential nowadays. We live in a world full of electronic communications and commerce, which requires a growing need for security. Actually, information security has been the subject of much research in the last years.

To study secure communication protocols, two approaches have been used. The formal approach adopts the Dolev and Yao attacker under an idealization of the cryptographic systems. Despite assuming an idealization of the cryptographic primitives, this approach represented a significant breakthrough in research in recent years, in fact it is scalable and automatable. Nevertheless this approach is not perfect and omits many of the concrete problems in cryptography. On the contrary, the computational approach seems to be closer to reality. In this approach all the issues of computational complexity, resource-bounded attackers and probabilities of attack are taken into consideration. Since it stands closer to reality, it is far from being scalable or automatable. Recently, there has been an effort into making these approaches closer and getting profit from the advantages of both of them. One way of approaching the problem is to incorporate equational theories, probabilities, and to a certain extent complexity issues, into a full-fledged security logic, and this is our long term objective.

For now, this work consists in preparing the ground for the subsequent construction of the information security logics we have in mind. Typically, in problems of information security we need to reason about the intruder's knowledge, the uncertainty related with the distribution of the unknown objects and still with updates of information. We shall therefore

concern ourselves with studying the literature on logics for knowledge and probability that also allow us to reason about information changes. The purpose of this text is to present an overview of dynamic probabilistic epistemic logic and then test it by modeling original applications on security motivated questions.

Reasoning about knowledge (see [7] for an overview) is an interesting topic of research since early in economics, philosophy and more recently in computer science and mathematics. It was a very exploited area until a strong interest in talking about uncertainty emerged and in 1976 Aumann began introducing probabilities on his papers. However, a proper logic with a language that allows us to reason about both knowledge and probability was just presented in 1988 with the preliminary versions of [5] and [6]. After Gerbrandy's [8] concern on introducing a dynamical component on the epistemic case, in 2003 Kooi [15] pieced together the probabilistic epistemic case of [5] with the dynamical epistemic case of [8]. More recently [3] presents a more complete approach of dynamic probabilistic epistemic logic.

Often, in problems of information security we focus on the behavior of the attacker thus confining ourselves to the study of a single-agent in the system. The applications that we will study at the end of this text rely on this. Therefore we will not concern ourselves on defining common knowledge not even distributed knowledge as usual in the literature.

This text is divided into two major parts. In the first one (Chapter 3) we recall the construction of the logic for knowledge, probability and information updates, step by step. This first part consists of an overview of the already known results of probabilistic epistemic logic with a dynamical component. In the second part (Chapter 4) we test the logic in a couple of original applications that depict two simple but quite significant situations in information security.

In Section 3.1 we begin by introducing and making an overview of epistemic logic. This logic allows us to reason about the knowledge of the agents in static scenarios. Then we increment the logic, introducing uncertainty in Section 3.2 and obtaining probabilistic epistemic logic. Pairing this definitions together with the proofs of soundness and completeness we get the logic for the static case. With this static logic we make a detour on the single agent case in Subsection 3.2.1 and study complexity-related questions in this simpler case. Then we come back to the general case to remember we need to reason about information updates and with this purpose in Chapter 3.3 we begin introducing a particular case of

update, the public announcements. Hence we generalize this approach to the case where, in fact, updates are not deterministic and occur with a given probability.

In the closing Chapter 4 we dedicate ourselves on applying this theory to a pair of original applications towards information security. In this last chapter, the logic is reduced to the single agent case, focusing the analysis on the intruder's behavior.

In the first application, the logic is used to model a usual problem associated with cryptanalysis: there is a secret and an attacker who interacts with the system, gets information and so reduces the uncertainty associated to the secret and eventually ends up discovering its value. The second application is based on the important concept of computational indistinguishability, which is crucial in information security, namely it is the base of the semantic characterization of asymmetric encryption schemes such as chosen-plaintext attack or chosen-ciphertext attack. We introduce the definition of computational indistinguishability and after analyzing its possible variations use dynamic probabilistic epistemic logic in order to express it.

Chapter 2

Preliminary

This preliminary section aims to make this text self contained. We define several notions in logic and present some introductory results.

The development of a logic consists in defining a formal language and in specifying a procedure to obtain valid reasoning patterns.

Definition 2.0.1 *A logic consists of a language and a consequence operator, $\mathcal{L} = (L, \vdash)$, where $L \neq \emptyset$ and $\vdash \subseteq 2^L \times L$ verifies the following conditions:*

(i) $\Gamma \vdash A$ *if* $A \in \Gamma$

(ii) *if* $\Gamma \subseteq \Delta$ *and* $\Gamma \vdash A$ *then* $\Delta \vdash A$

(iii) *if* $\Gamma \vdash A$ *for all* $A \in \Delta$ *and* $\Delta \vdash B$ *then* $\Gamma \vdash B$.

In axiomatizable logics it still verifies

(iv) *if* $\Gamma \vdash A$ *then there exists a finite* $\Gamma_0 \subseteq \Gamma$ *such that* $\Gamma_0 \vdash A$.

Notice that if the language L have some structure and some connectives then the consequence operator may verify some extra conditions.

Notation: Most of the times we confuse the notation of language L with $\mathcal{L}$.

We must establish a consequence relation. With this purpose we can use either the deductive way or the semantic way. We begin by introducing a consequence relation by means

of the deductive approach. For this we need to characterize a deductive system.

Definition 2.0.2 *A rule of inference has the form* $\frac{A_1,\ldots,A_n}{A}$. *The formulas* $A_1,\ldots,A_n$ *are the premises and* A *is termed the conclusion.*
A set of formulas is closed for an inference rule $\frac{A_1\ldots,A_n}{A}$ *if whenever the set contains all the premises then it also contains the conclusion.*
We define an axiom to be an inference rule without premises.

Notation: We denote an axiom

$$\frac{}{A}$$

without the horizontal bar, i.e

$$A.$$

Definition 2.0.3 *An inference system is a collection of axioms and inference rules.*

To reason in a logic we need to establish a relation between formulas and it can be achieved through the notion of derivability.

Definition 2.0.4 *Consider an inference system. A proof consists of a sequence of formulas, each of which is an hypothesis, an instance of an axiom or is the result of applying an inference rule to the previous formulas.*
We say that we have a proof of φ *from* Γ *if we have a proof where* φ *is the last formula in the sequence and all the hypotheses belong to* Γ.
Moreover, we say that φ *is provable (or* φ *is a theorem), and write* $\vdash \varphi$, *if we have a proof of* φ.

Notation: To simplify the notation, we write $\psi_1,\ldots,\psi_n \vdash \varphi$ instead of $\{\psi_1,\ldots,\psi_n\} \vdash \varphi$. Moreover we denote $\Gamma \vdash A$ and $\Gamma \vdash B$ by $\Gamma \vdash A, B$.

Now that we already introduced the notion of consequence relation in a deductive way, we care about the definition of a consequence relation in a semantic approach. So we need to clarify the notion of a model for a logic.

Models for a logic are structures that attribute a meaning to formulas of the language.

Definition 2.0.5 *Let* $\mathcal{L}$ *be a logic. A satisfaction relation is such that* $\Vdash \subseteq \mathcal{M} \times L$, *where* $\mathcal{M}$ *is the class of models for* $\mathcal{L}$ *and* L *is the language.*

We say we are in the presence of a semantics when it is defined a class of models $\mathcal{M}$ and a satisfaction relation $\Vdash$.

Definition 2.0.6 *Let $\mathcal{L}$ be a logic, $\mathcal{M}$ the class of models for $\mathcal{L}$ and $\varphi \in \mathcal{L}$ a formula. We say that*

φ is valid, $\Vdash \varphi$, if φ is true in all the models in $\mathcal{M}$,

φ is satisfiable if exists a model in $\mathcal{M}$ that makes the formula φ true,

φ is semantic consequence of a set $\Gamma \subseteq \mathcal{L}$, $\Gamma \models \varphi$, if in any model where all the formulas of Γ are valid, φ is also valid.

Definition 2.0.7 *Let $\mathcal{L}$ be a logic and consider a semantics $\mathcal{M}$, $\Vdash$.*
We say that the inference system is strongly sound for $\mathcal{L}$ if for every set of formulas $\Gamma \subseteq \mathcal{L}$, any formula that is provable from Γ, follows semantically from Γ,

$$\text{if } \Gamma \vdash \varphi \text{ then } \Gamma \models \varphi.$$

An inference system is weakly sound if every formula provable in $\mathcal{L}$ is valid with respect to every model M, i.e.

$$\text{if } \vdash \varphi \text{ then } \Vdash \varphi.$$

Reciprocally, an inference system is strongly complete for $\mathcal{L}$ if for every set of formulas $\Gamma \subseteq \mathcal{L}$, any formula which semantically follows from Γ is derivable from Γ,

$$\text{if } \Gamma \models \varphi \text{ then } \Gamma \vdash \varphi.$$

An inference system is weakly complete for $\mathcal{L}$ if every valid formula is provable, i.e.,

$$\text{if } \Vdash \varphi \text{ then } \vdash \varphi.$$

Definition 2.0.8 *Let $\mathcal{L}$ be a logic and $\Psi \subseteq \mathcal{L}$ be a set of formulas. We define*

$$\Psi \text{ to be } \vdash\text{-consistent if exists } \psi \in \mathcal{L} \text{ such that } \Psi \nvdash \psi.$$

If Ψ is not $\vdash$-consistent , we say Ψ is $\vdash$-inconsistent .

The notion of (in)consistency is very important. Definition 2.0.8 expresses pretty well the concept of inconsistency, however there is another approach to this notion that in the more specific context where we will work is equivalent to the previous one, and it is quite easy to use in the proofs we will have to do.

For this reason we now reduce the level of generality and specify the logics with which we will deal.

Definition 2.0.9 *A set C provided with a function $f : C \longrightarrow \mathbb{N}_0$ is called a set of constructors. The function f assigns to each constructor $c \in C$ its arity $f(c) \in \mathbb{N}_0$.*

Typically, the language is constructed inductively from a set of primitive propositions and a set of constructors.

Definition 2.0.10 *Given a set Φ of primitive propositions and C a set of constructors, a language L is defined inductively as follows:*

- $P \subseteq L$
- *if $c \in C$ and $\varphi_1, \ldots, \varphi_{f(c)} \in L$ then $c\left(\varphi_1, \ldots, \varphi_{f(c)}\right) \in L$*

Later on we are interested in modal logics, so in particular we want to talk about classical based logics. With this purpose we assume from now that the language is constructed at least with the connectives $\neg, \wedge, \rightarrow, \vee$. In addition assume some properties over these connectives:

i. $\Gamma, A \vdash B$ *iff* $\Gamma \vdash A \rightarrow B$

ii. $\Gamma \vdash A, B$ *iff* $\Gamma \vdash A \wedge B$

iii. $\Gamma \vdash A$ or $\Gamma \vdash B$ *iff* $\Gamma \vdash A \vee B$

iv. if $\Gamma \vdash A$ *then* $\Gamma \nvdash \neg A$

v. $A, \neg A \vdash B$,

where $A, B \in \mathcal{L}$ are any formulas.

As stated above, the notion of inconsistency is very important and the approach of consistency with connectives is easier to use, therefore consider the following

Definition 2.0.11 *Let $\mathcal{L}$ be a logic, $\varphi, \varphi_1, \ldots, \varphi_n \in \mathcal{L}$ formulas and $\Psi \subseteq \mathcal{L}$ an infinite set of formulas. We define*

- *φ to be $\vdash$-consistent if $\nvdash \neg\varphi$;*
- *$\{\varphi_1, \ldots, \varphi_n\}$ to be $\vdash$-consistent if $\varphi_1 \wedge \ldots \wedge \varphi_n$ is $\vdash$-consistent ;*
- *Ψ is $\vdash$-consistent if all its finite subsets are $\vdash$-consistent .*

If Ψ is not $\vdash$-consistent , we say Φ is $\vdash$-inconsistent .

Proposition 2.0.1 *Let $\mathcal{L}$ be a logic (with the assumptions above).*

Definition 2.0.8 and Definition 2.0.11 are equivalent.

Proof: Since the classical negation is *explosive*, i.e.

$$\text{for all } \Lambda \subseteq \mathcal{L},\ A, B \in \mathcal{L} \text{ we have } \Lambda, A, \neg A \vdash B,$$

Definition 2.0.8 is equivalent to the following definition

$$\Psi \text{ is } \vdash\text{-inconsistent} \quad \textit{iff} \quad \text{exists a formula } B \text{ such that } \Psi \vdash B, \neg B. \tag{2.1}$$

Let φ be any formula.
Assume φ is $\vdash$-inconsistent in the sense of Definition 2.0.11. Then we have $\vdash \neg\varphi$. So $\varphi \vdash \varphi, \neg\varphi$, so (2.1) holds.
Reciprocally, assume φ is $\vdash$-inconsistent wrt Definition 2.0.8. Then $\varphi \vdash \neg\varphi$. By the assumption of local deduction, we can use deduction metatheorem (property i.) and it follows that $\vdash \varphi \to \neg\varphi$. Since we are working with classical negation we have $\vdash \neg\varphi$. ■

Definition 2.0.12 *Consider an inference system and let $\Upsilon, \Delta \subseteq \mathcal{L}$ be any sets of formulas.*
Υ is a maximal consistent subset of Δ if

- *Υ is $\vdash$-consistent*
- *$\Upsilon \subseteq \Delta$*
- *for all $\varphi \in \Delta \setminus \Upsilon$, the set $\Upsilon \cup \{\varphi\}$ is $\vdash$-inconsistent .*

Lemma 2.0.13 *Consider an inference system and let $\Delta \subseteq \mathcal{L}$ a countable set of formulas which is closed with respect to classical negation and conjunction.*
Then, every $\vdash$-consistent set $\Upsilon \subseteq \Delta$ can be extended to a maximal consistent subset of Δ.
If Υ is a maximal consistent subset of Δ then

(i) for every formula $\varphi \in \Delta$ exactly one of φ and $\neg\varphi$ belongs to Υ,

(ii) if $\varphi \wedge \psi \in \Delta$ then $\varphi \wedge \psi \in \Upsilon$ iff $\varphi \in \Upsilon$ and $\psi \in \Upsilon$,

(iii) if $\varphi, (\varphi \Rightarrow \psi) \in \Upsilon$ then $\psi \in \Upsilon$,

(iv) if φ is provable then $\varphi \in \Upsilon$.

Proof: Let $\Upsilon \subseteq \Delta$ be an $\vdash$-consistent set. Δ is a countable set of formulas, say $\Delta = \{\psi_i\}_{i\in\mathbb{N}}$.
Now consider the following construction of the extension of Υ to a maximal consistent subset of Δ:

$$\begin{array}{lcl} \Upsilon_0 & = & \Upsilon \\ \Upsilon_{i+1} & = & \begin{cases} \Upsilon_i \cup \{\psi_{i+1}\} & \text{if } \Upsilon_i \cup \{\psi_{i+1}\} \text{ is } \vdash\text{-consistent} \\ \Upsilon_i & \textit{otherwise} \end{cases} \end{array}$$

Let $\tilde{\Upsilon} = \bigcup_{i=0}^{\infty} \Upsilon_i$.
Each finite subset Λ of $\tilde{\Upsilon}$ is contained in some Υ_k, $k \in \mathbb{N}$. Since Υ_k is $\vdash$-consistent so is Λ. Therefore $\tilde{\Upsilon}$ is $\vdash$-consistent .
Let $\varphi \in \Delta$ be a formula such that $\varphi \notin \tilde{\Upsilon}$ and $\varphi \in \Delta = \{\psi_i\}_{i\in\mathbb{N}}$, say $\varphi = \psi_m$. If $\Upsilon_m \cup \{\psi_m\}$ is $\vdash$-consistent , then $\Upsilon_{m+1} = \Upsilon_m \cup \{\psi_m\} \subseteq \tilde{\Upsilon}$ and $\psi_m \in \tilde{\Upsilon}$, which is a contradiction. So $\Upsilon_m \cup \{\psi_m\} \subseteq \tilde{\Upsilon} \cup \{\psi_m\}$ is $\vdash$-inconsistent and hence $\tilde{\Upsilon} \cup \{\psi_m\}$ is $\vdash$-inconsistent . We then have $\tilde{\Upsilon}$ a maximal $\vdash$-consistent set which contains Υ.

Now let Υ to be a maximal consistent subset of Δ. Using the properties of $\vdash$ we have:

(i) Let $\varphi \in \Delta$, we want to show that either $\Upsilon \cup \{\varphi\}$ or $\Upsilon \cup \{\neg\varphi\}$ is $\vdash$-consistent . Assume that both $\Upsilon \cup \{\varphi\}$ and $\Upsilon \cup \{\neg\varphi\}$ are $\vdash$-inconsistent . Then for all formulas $\xi \in \mathcal{L}$, $\Upsilon \cup \{\varphi\} \vdash \xi$ and $\Upsilon \cup \{\neg\varphi\} \vdash \xi$. Since we are working with classical logic it follows that $\Upsilon \cup \{\varphi \vee \neg\varphi\} \vdash \xi$. But then $\Upsilon \cup \{\varphi \vee \neg\varphi\}$ is $\vdash$-inconsistent and therefore Υ is $\vdash$-inconsistent (because $\varphi \vee \neg\varphi$ is a classical propositional tautology), which is a contradiction.
So $\Upsilon \cup \{\varphi\}$ is $\vdash$-consistent or $\Upsilon \cup \{\neg\varphi\}$ is $\vdash$-consistent . If $\Upsilon \cup \{\varphi\}$ is $\vdash$-consistent , then $\varphi \in \Upsilon$ because Υ is maximal. Similarly, in the other case, $\neg\varphi \in \Upsilon$. Of course, φ and $\neg\varphi$ could not belong both to Υ, for otherwise by property v. of $\vdash$, Υ would not be $\vdash$-consistent .

(ii) Let $\varphi \wedge \psi \in \Delta$.
If $\varphi \wedge \psi \in \Upsilon$, then we must have $\varphi \in \Upsilon$, for otherwise, by (i) $\neg\varphi \in \Upsilon$ and Υ would be $\vdash$-inconsistent . Similarly, $\psi \in \Upsilon$.
Assume now $\varphi, \psi \in \Upsilon$, we must have $\varphi \wedge \psi \in \Upsilon$, for otherwise by (i), $\neg(\varphi \wedge \psi) \in \Upsilon$

and then Υ could be $\vdash$-inconsistent .

(iii) Suppose $\varphi, (\varphi \to \psi) \in \Upsilon$ and assume $\neg\psi \in \Upsilon$.
Consider $\{\varphi, \varphi \to \psi, \neg\psi\} \subseteq \Upsilon$ a subset. We have:
$\neg(\varphi \wedge \varphi \to \psi \wedge \neg\psi) = \neg(\varphi \wedge (\neg\varphi \vee \psi) \wedge \neg\psi)$
$= \neg((\varphi \wedge \neg\varphi \wedge \neg\psi) \vee (\varphi \wedge \psi \wedge \neg\psi)) = (\neg\varphi \vee \varphi \vee \psi) \wedge (\neg\varphi \vee \neg\psi \vee \psi)$
which is provable. So Υ is $\vdash$-inconsistent , which is a contradiction.
By (i) we must have $\psi \in \Upsilon$.

(iv) Suppose φ is provable.
$\Upsilon \cup \{\varphi\}$ is clearly $\vdash$-consistent , but Υ is maximal, so $\varphi \in \Upsilon$. ■

Lemma 2.0.14 *Let $\varphi_1, \ldots, \varphi_m, \varphi \in \mathcal{L}$ be formulas.*
If $\{\varphi_1, \ldots, \varphi_m, \neg\varphi\}$ is $\vdash$-inconsistent then $\vdash \varphi_1 \to (\varphi_2 \to (\ldots \to (\varphi_n \to \varphi) \cdots))$.

Proof: Suppose $\{\varphi_1, \ldots, \varphi_m, \neg\varphi\}$ is $\vdash$-inconsistent . By Definition 2.0.11,

$$\varphi_1, \ldots, \varphi_m, \neg\varphi \vdash \neg(\varphi_1 \wedge \ldots \wedge \varphi_m \wedge \neg\varphi).$$

Since we are working with classical negation we equivalently have

$$\varphi_1, \ldots, \varphi_m, \neg\varphi \vdash \neg\varphi_1 \vee \ldots \vee \neg\varphi_m \vee \varphi.$$

And using i. it follows that

$$\varphi_2, \ldots, \varphi_m, \neg\varphi \vdash \varphi_1 \to (\neg\varphi_1 \vee \ldots \vee \neg\varphi_m \vee \varphi).$$

Using propositional reasoning this is clearly equivalent to

$$\varphi_2, \ldots, \varphi, \neg\varphi \vdash \varphi_1 \to (\neg\varphi_2 \vee \ldots \vee \neg\varphi_m \vee \varphi).$$

By an induction argument we get

$$\neg\varphi \vdash \varphi_1 \to (\varphi_2 \to (\cdots \to (\varphi_m \to \varphi) \cdots)).$$

Therefore $\vdash \neg\varphi \to (\varphi_1 \to (\varphi_2 \to (\cdots \to (\varphi_m \to \varphi) \cdots)))$, which is equivalent to

$$\vdash \varphi_1 \to (\varphi_2 \to (\cdots \to (\varphi_m \to \varphi) \cdots)).$$

■

As we saw, the language is typically defined recursively. In the proofs we will use very often this recursive feature of the language. For this we define the notion of subformula.

Definition 2.0.15 *Let L be a language and consider Φ and C to be, respectively, the set of primitive propositions and the set of constructors used ti define the language.*
We define the set of subformulas of φ as:

- $Sub(p) = \{p\}$, *for* $p \in \Phi$
- $Sub(c(\varphi_1, \ldots, \varphi_n)) = \{c(\varphi_1, \ldots, \varphi_n)\} \cup \bigcup_{i=1}^{n} Sub(\varphi_i)$.

Moreover, we define $\overline{Sub\varphi}$ to be the set of subformulas of φ and their negations,

$$\overline{Sub\varphi} = Sub(\varphi) \cup \{\psi \in \mathcal{L} \mid \neg\psi \in Sub(\varphi)\}.$$

Later we will need the notion of functional completeness. Its reciprocal consists of a simple observation.

Remark 2.0.16 *If we assume the logic to have propositional symbols $p_1, \ldots, p_n$ and to be classical based, then it is straightforward to see that each classical formula φ with n variables, $\varphi(p_1, \ldots, p_n)$, define a Boolean function $f : 2^n \longrightarrow 2$. To define the function f it is sufficient to construct a truth table.*

Example 2.0.1 *To the formula $p_1 \wedge p_2$ corresponds the function $f : 2^2 \longrightarrow 2$ defined by*

$$f(1,1) = 1,\ f(1,0) = 0,\ f(0,1) = 0,\ f(0,0) = 0.$$

Definition 2.0.17 *If every function $f : 2^n \longrightarrow 2$ for $n \geq 1$ can be realized by a formula φ which only uses the connectives on a set C, we say that the set C is functional complete.*

Remark 2.0.18 $\{\wedge, \neg\}$ *is functional complete.*

Chapter 3

Dynamic Probabilistic Epistemic Logic

We are interested in studying dynamical probabilistic epistemic logics. With this purpose we start our study with the epistemic case, then we introduce uncertainty and further we want to be able to reason about a dynamical component.

All of these logics have the particularity of being modal logics. We shall therefore briefly introduce the study of modal logic.

In modal logic, the language has, besides the usual constructors of classical based logics, modal operators $\{\Box_j\}_{j\in J}$ and $\{\Diamond_j\}_{j\in J}$, which represents *necessity* and *possibility*. Assume each modal operator $\Box_j$ (or $\Diamond_j$) has arity m_j.

Convention: We define the possibility operator $\Diamond$ as

$$\Diamond A \leftrightarrow \neg\Box\neg A.$$

The language in modal logic is defined recursively, as usual. We fix Φ to be a set of primitive propositions, then using the constructors and the modal operators the formulas are constructed.

Notation: We define the formula $true$ to be $p \vee \neg p$ for any primitive proposition p. $false$ is defined to be $\neg true$.

The models for modal logic that we use are Kripke structures.

Definition 3.0.19 *A Kripke structure is a tuple $M = (S, \pi, \{R_j\}_{j \in J})$ where S is a set of states, π is an identification function that for each $s \in S$ assigns true or false to the primitive propositions and R_j is a $(m_j + 1)$-ary relation on S, for each $j \in J$.*

For semantics to be fully characterized we define by induction the truth of formulas with the modal operator $\Box$.

Definition 3.0.20 *Let Φ be the set of primitive propositions, M a Kripke structure and $\mathcal{L}$ a language with the modal operator $\Box$ which has arity n. Let $s \in S$ be a state and $\varphi \in \mathcal{L}$ a formula.*
If φ is a primitive proposition, we have $(M, s) \Vdash \varphi$ iff $\pi(s)(\varphi) = true$.
If φ is of the form $\Box(\varphi_1 \ldots, \varphi_n)$ for some formulas $\varphi_1, \ldots, \varphi_n \in \mathcal{L}$, we define

$$(M, s) \Vdash \Box(\varphi_1, \ldots, \varphi_n) \quad \textit{iff for all } v_1, \ldots, v_n \in S \textit{ such that } (s, v_1, \ldots, v_n) \in R, (M, v_i) \Vdash \varphi_i,$$

for all $i = 1, \ldots, n$.

Moreover, when the logic uses connectives, the truth of formulas using that connectives should be defined.

Typically in modal logic we study infinite sets which usually makes the logic not complete in the strong sense. Therefore in this text we will seek to prove soundness and completeness in the weak sense only.

To close this preamble in modal logic we present two basic definitions and a trivial result that are needed in future proofs.

Definition 3.0.21 *Let R be a binary relation on a set S.*
R is said to be an equivalence relation if

- *R is reflexive, i.e, for all $s \in S$, $(s, s) \in R$,*
- *R is symmetric, i.e., whenever $(r, s) \in R$, $(s, r) \in R$ and*
- *R is transitive, i.e., whenever $(r, s), (s, t) \in R$, $(r, t) \in R$.*

Definition 3.0.22 *Let R be a binary relation on a set S.*
R is said to be Euclidean if whenever $(s, t) \in R$ and $(s, u) \in R$ then $(t, u) \in R$, where $s, t, u \in S$.

Lemma 3.0.23 *If R is reflexive and Euclidean, then R is symmetric.*

Proof: Suppose R is reflexive and Euclidean and let $s, t \in S$ be such that $(s,t) \in R$. Since R is reflexive, $(s,s) \in R$. So we have $(s,t), (s,s) \in R$. R is Euclidean, so $(t,s) \in R$ and R is symmetric. ■

3.1 Epistemic Logic

In this section we provide an overview of epistemic logic in [7].

Definition 3.1.1 *Consider n agents $1, \ldots, n$. The epistemic language $\mathcal{L}_n^K(\Phi)$ has the following inductive syntax*

$$\varphi \ ::= \ p \,|\, \neg\varphi \,|\, \varphi \wedge \psi \,|\, K_i\varphi$$

where $p \in \Phi$ and $i \in \{1, \ldots, n\}$.

Notation: Since the set of primitive propositions was fixed at the beginning of the chapter, we will drop the dependence of the language on Φ and we will denote $\mathcal{L}_n^K := \mathcal{L}_n^K(\Phi)$.

The epistemic logic we are presenting contains the modal operators $K_1, \ldots, K_n$ that allow us to reason about the knowledge of each agent.

The expression $K_i\varphi$ should be read as "agent i knows φ".

It should be noted however that there are other approaches to epistemic logic, namely logics that reason about belief.

Definition 3.1.2 *A Kripke structure for knowledge for n agents $1 \ldots, n$ over Φ is a tuple $M = (S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n)$ where S is a nonempty set of states or worlds, π is an interpretation function that for each state $s \in S$ assigns true or $false$ to the primitive propositions $p \in \Phi$, and finally, for each $i \in \{1, \ldots, n\}$ $\mathcal{K}_i$ is an equivalence relation.*

In the context of epistemic logic is intuitive the meaning of the equivalence relation $\mathcal{K}_i$: $(s,t) \in \mathcal{K}_i$ if agent i considers world t possible given his information in world s.

Remark 3.1.3 *It is common to define Kripke structures assuming $\mathcal{K}_i$ to be any binary relation, but in order to model knowledge we require each $\mathcal{K}_i$ to be an equivalence relation. Then it will coincide with our idea that $(s,t) \in \mathcal{K}_i$ if s and t are indistinguishable for agent i, i.e., agent i has the same information in both worlds.*

The assumption that $\mathcal{K}_i$ are equivalence relations traduces in properties that represent the characteristics of a perfect reasoner. It is our assumption throughout this text that the agents are perfect reasoners.

Notation: Let $\mathcal{K}_i(s) := \{t \in S \mid (s,t) \in \mathcal{K}_i\}$ represent the set of all the states indistinguishable from s from the point of view of the agent i.

Definition 3.1.4 *Let $\mathcal{L}_n^K$ be the epistemic language over Φ and $M = (S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n)$ a Kripke structure for knowledge over Φ. Let $s \in S$ be a state and $\varphi \in \mathcal{L}_n^K$ be a formula. If φ is a primitive proposition $p \in \Phi$, we define*

$$(M,s) \Vdash p \quad \text{if and only if} \quad \pi(s)(p) = true. \tag{3.1}$$

If φ is of the form $\neg\psi$, for some formula ψ, we define

$$(M,s) \Vdash \neg\psi \quad \text{if and only if} \quad (M,s) \nVdash \psi \tag{3.2}$$

If φ is of the form $\xi \wedge \psi$, for some formulas ξ and ψ, we define

$$(M,s) \Vdash \xi \wedge \psi \quad \text{if and only if} \quad (M,s) \Vdash \xi \text{ and } (M,s) \Vdash \psi. \tag{3.3}$$

If φ is of the form $K_i\psi$, for some formula ψ we define

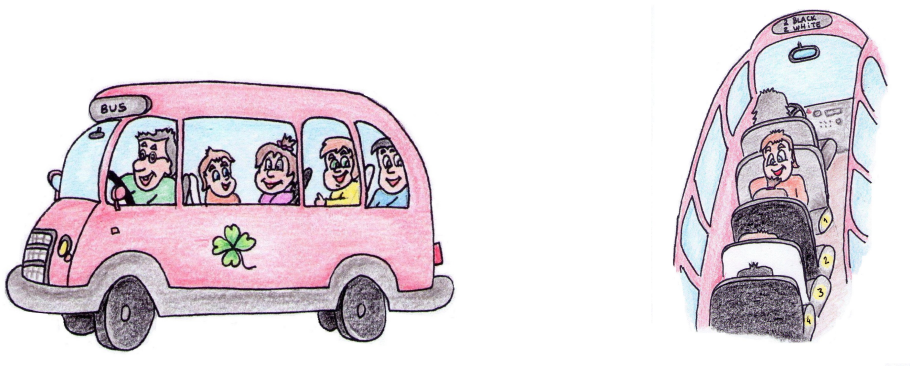
$$(M,s) \Vdash K_i\psi \quad \text{if and only if} \quad \text{for all } t \in S \text{ s.t. } (t,s) \in \mathcal{K}_i,\ (M,t) \Vdash \psi. \tag{3.4}$$

(3.2) and (3.3) tell us we are dealing with classical connectives. Whereas (3.4) expresses the idea that agent i knows ψ at a given world s if ψ holds in all worlds that agent i considers indistinguishable from s.

Notation: Let $\mathcal{M}_n^K$ denote the collection of Kripke structures for knowledge for agents $1, \ldots, n$ over Φ.

Throughout the overview of the dynamic probabilistic epistemic logic we will follow closely an example inspired in my bus trips to the high school. The pictures depict the situation and should be observed while the problem is exposed.

Example 3.1.1 *Consider four passengers traveling in a bus.*
In the beginning of the trip the driver reveals that the bus has four passenger seats, two of them have black back side and the other two have white back sides.
Passengers are arranged in such a way that passenger 1 and passenger 2 do not see any



back side of the other seats, passenger 3 *sees the back side of* 2*'s seat and passenger* 4 *sees the back side of the seats of* 2 *and* 3.

In this bus trip there are 4 *agents. The primitive propositions should express the color of each seat's back side. For each* $i \in \{1,2,3,4\}$ *let us assume* w_i *means "the back side of passenger* i*'s seat is white". Consider* $\Phi = \{w_1, w_2, w_3, w_4\}$ *to be the set of primitive propositions.*
The Kripke structure for knowledge is given by $M = (S, \pi, \mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_3, \mathcal{K}_4)$*, where* $S = \{(x_1, x_2, x_3, x_4) \in \{0,1\}^4 : x_1 + x_2 + x_3 + x_4 = 2\}$ *represents all the possible worlds.*
Denoting the real world by s^* *we have*

$$\pi(s^*)(w_1) = \pi(s^*)(w_3) = true,$$

$$\pi(s^*)(w_2) = \pi(s^*)(w_4) = false.$$

It is straightforward to define π *on all the other worlds of* S.
We should expect that

$$\mathcal{K}_4 = \left\{((s_1, s_2, s_3, s_4), (t_1, t_2, t_3, t_4)) \in S^2 : s_2 = t_2 \text{ and } s_3 = t_3\right\},$$

This means agent 4 *can not distinguish worlds where seats* 2 *and* 3 *has the same color. In particular, this restriction on* $\mathcal{K}_4$ *implies*

$$(M, s^*) \Vdash K_4(\neg w_2) \wedge K_4(w_3),$$

i.e. passenger 4 *knows that the back side of* 2*'s seat is black and the back side of* 3*'s seats is white, as we imposed in the beginning.*
Moreover, $\mathcal{K}_3 = \left\{((s_1, s_2, s_3, s_4), (t_1, t_2, t_3, t_4)) \in S^2 : s_2 = t_2\right\}$ *and* $\mathcal{K}_1 = \mathcal{K}_2 = S^2$. □

Now that we have inspired us, we need to introduce some axioms and inference rules that allow us to reason deductively over the epistemic logic.

Definition 3.1.5 *Let the inference system for knowledge $\mathfrak{H}^K$ be composed by the following axioms and inference rules:*

K1. *All tautologies of the classical propositional calculus*

K2. $(K_i\varphi \wedge K_i(\varphi \to \psi)) \to K_i\psi,\ \ i = 1, \ldots, n$ *[Distribution Axiom]*

K3. $K_i\varphi \to \varphi,\ i = 1 \ldots, n$ *[Knowledge Axiom]*

K4. $K_i\varphi \to K_iK_i\varphi,\ \ i = 1, \ldots, n$ *[Positive Introspection Axiom]*

K5. $\neg K_i\varphi \to K_i\neg K_i\varphi,\ i = 1, \ldots, n$ *[Negative Introspection Axiom]*

R1. *From φ and $\varphi \to \psi$ infer ψ* *[Modus Ponens]*

R2. *From φ infer $K_i\varphi$* *[Knowledge Generalization]*

Notation: Let $\vdash_n^K$ represent the deductive system corresponding to the inference system for knowledge.

This inference system allows us to reason about knowledge. $K2$ represents the idea that agents know all the logical consequences of their knowledge. $K3$ means agents only know valid formulas. Moreover, agents are perfect reasoners and it follows that our logic verifies the additional properties $K4$, agent i recognizes all the things he knows, and $K5$, agent i recognizes what he does not know.

Proposition 3.1.1 *Consider the epistemic deductive system $\vdash_n^K$. We have the theorems*

$$K(A \to B) \to (KA \to KB) \tag{3.5}$$

$$K(A \wedge B) \leftrightarrow (KA \wedge KB) \tag{3.6}$$

$$KA \to K(A \vee B) \tag{3.7}$$

Proof:

(3.5) Is an immediate consequence of $K2$.

(3.6)

$$K(A \wedge B) \quad \textit{iff} \quad K(\neg(A \to \neg B)) \textit{ then } \neg K(A \to \neg B) \textit{ then } \neg(KA \to K\neg B) \textit{ then}$$

$$\neg(\neg KA \vee K\neg B) \textit{ then } \neg(\neg KA \vee \neg KB) \quad \textit{iff} \quad KA \wedge KB.$$

Reciprocally, since $B \to (A \to A \wedge B)$ is a tautology, if $KA \wedge KB$ then $KA \wedge K(A \to A \wedge B)$ and using $K2$, $K(A \wedge B)$.

(3.7) Suppose KA holds.
Since $A \to A \vee B$ is a tautology, applying $R2$ we have $K(A \to A \vee B)$.
Then $KA \wedge K(A \to A \vee B)$ holds and by $K2$ it follows that $K(A \vee B)$. ■

Lemma 3.1.6 *If*

$$\textit{every } \vdash^K\textit{-consistent formula in } \mathcal{L}_n^K \textit{ is satisfiable with respect to } \mathcal{M}_n^K \tag{3.8}$$

then

$$\textit{every formula in } \mathcal{L}_n^K \textit{ that is valid with respect to } \mathcal{M}_n^K \textit{ is provable in } \mathfrak{H}^K.$$

Proof: Suppose that (3.8) holds and let $\varphi \in \mathcal{L}_n^K$ be a formula.
In order to obtain a contradiction let us assume φ is valid with respect to $\mathcal{M}_n^K$ and φ is not provable. Since we are using classical negation this means $\neg\neg\varphi$ is not provable. Then, by Definition 2.0.11, $\neg\varphi$ is $\vdash^K$-consistent . By (3.8), $\neg\varphi$ is satisfiable with respect to $\mathcal{M}_n^K$, which contradicts the assumption that φ is valid. ■

Theorem 3.1.7 $\mathfrak{H}^K$ *is a sound and (weakly) complete axiomatization for the epistemic logic with respect to* $\mathcal{M}_n^K$.

Proof:
Let us begin proving soundness. Consider M to be a Kripke structure for knowledge in $\mathcal{M}_n^K$.
First of all, we will see $K1$ holds. Let A be a propositional tautology. We want to see that $M \Vdash A$.
A being a tautology means A is true in every valuation, with the inductive definition of validity this means that for every state t we have $(\mathcal{M}, t) \Vdash A$, so $M \Vdash A$.

Let us now see $R1$ is a valid in $\mathcal{L}_n^K$. Suppose $M \Vdash \varphi$ and $M \Vdash \varphi \to \psi$.
For all states $s \in S$, $(M, s) \Vdash \varphi$ and $(M, s) \Vdash \varphi \to \psi$. By $K1$, for each state $s, (M, s) \Vdash \psi$, so $M \Vdash \psi$.

For $R2$, suppose $M \Vdash \varphi$. For all states $s \in S$, $(M, s) \Vdash \varphi$. Let $t \in S$ be any state, we have, for all $s \in \mathcal{K}_i(t), (M, s) \Vdash \varphi$, so $(M, t) \Vdash K_i\varphi$. Since $t \in S$ is any state, $M \Vdash K_i\varphi$.

For axiom $K2$, let $i \in \{1, \ldots, n\}$ and $s \in S$ be any state. Suppose that

$$(M, s) \Vdash (K_i\varphi \wedge K_i(\varphi \to \psi)).$$

We have

$$\text{for all state } t \in \mathcal{K}_i(s) \text{ such that } (M, t) \Vdash \varphi \text{ and } (M, t) \Vdash \varphi \to \psi$$

$$\textit{iff} \quad \text{for all state } t \in \mathcal{K}_i(s) \text{ such that } (M, t) \Vdash \varphi \wedge (\varphi \to \psi)$$

By $R1$ we have for all state $t \in \mathcal{K}_i(s)$ such that $(M, t) \Vdash \psi$, so $(M, s) \Vdash K\psi$.
Since s is any state it follows that $M \Vdash K_i\psi$.

For $K3$ assume $M \Vdash K_i\varphi$, then for all $s \in S, (M, s) \Vdash K_i\varphi$. Fix $s \in S$. For all $t \in \mathcal{K}_i(s)$ we have $(M, t) \Vdash \varphi$. $\mathcal{K}_i$ is reflexive so $(s, s) \in \mathcal{K}_i$ and we have $(M, s) \Vdash \varphi$. Now let s range over S and get $M \Vdash \varphi$.

Axiom $K4$ follows from transitivity. Suppose $M \Vdash K_i\varphi$.
For any state $s \in S$, $(M, s) \Vdash K_i\varphi$. Fix $s \in S$. For each state $t \in \mathcal{K}_i(s)$ we have that for all $u \in \mathcal{K}_i(s)$, since K_i is transitive and $(u, t), (t, s) \in \mathcal{K}_i(s)$ then $u \in \mathcal{K}_i(s)$ so $(M, u) \Vdash \varphi$.
Therefore, $(M, s) \Vdash K_i\varphi$ and since t is any state in $\mathcal{K}_i(s)$ it follows that $(M, s) \Vdash K_iK_i\varphi$.
Hence $M \Vdash K_iK_i\varphi$.

Finally, axiom $K5$ follows from symmetry and transitivity. Suppose $M \Vdash \neg K_i\varphi$. Then, for every $w \in S$, $(M, w) \Vdash \neg K_i\varphi$ *iff*
exists $t \in \mathcal{K}_i(s)$ such that $(M, t) \nVdash \varphi$, i.e.,
exists $t \in \mathcal{K}_i(s)$ such that $(M, t) \Vdash \neg\varphi$.
For each $u \in \mathcal{K}_i(s)$, since $\mathcal{K}_i$ is transitive and symmetric, $(t, u) \in \mathcal{K}_i$, so $(M, u) \Vdash \neg K_i\varphi$.
And therefore $(M, w) \Vdash K_i\neg K_i\varphi$.
Since $w \in S$ is any state, it now follows that $M \Vdash K_i\neg K_i\varphi$.

For completeness to be proved we want to show that every formula in $\mathcal{L}_n^K$ that is valid with respect to $\mathcal{M}_n$ is provable. By Lemma 3.1.6, if we prove (3.8) we are done. With

this purpose, consider φ to be a $\vdash^K$-consistent formula and let us construct a *canonical structure* $M^C \in \mathcal{M}_n$ where φ is valid.
Our construction has in mind its subsequent extension to the more complex logics we will define later. It could be done in a more general procedure, like in [7], but want to prepare the ground for further completeness proofs.
Let the canonical structure for φ be defined by $M^C = (S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n)$ where

$S = \{s_V \mid V \text{ is a } \overline{Sub\varphi} \text{ maximal consistent set}\}$

$\pi(s_V)(p) = \begin{cases} true & \text{if } p \in V \\ false & \text{if } p \notin V \end{cases}$ for each state $s_V \in S$ and primitive proposition $p \in \Phi$.

$\mathcal{K}_i = \{(s_V, s_W) \in S^2 \mid V/K_i \subseteq W\}$, where $V/K_i = \{\varphi \in \mathcal{L}_n^K \mid K_i\varphi \in V\}$.

Lemma 3.1.8 *For all $\overline{Sub\varphi}$ maximal consistent set V and epistemic formula $\psi \in \overline{Sub\varphi}$ we have*

$$(M^C, s_V) \Vdash \psi \quad \textit{iff} \quad \psi \in V.$$

Proof of Lemma 3.1.8: Let $\psi \in \overline{Sub\varphi}$ be a formula and $s_V \in S$ be a state.
The proof is done by induction on the structure of formulas. If ψ is a primitive proposition, the result follows from the definition of $\pi(s_V)$.
We proceed assuming it holds for all subformulas of ψ. (IH)
If ψ is of the form $\psi = \neg\xi$,

$$(M, s_V) \Vdash \psi \quad \textit{iff} \quad (M, s_V) \nVdash \xi \quad \textit{iff} \quad \xi \notin V.$$

Since V is a maximal consistent subset of $\overline{Sub\varphi}$, by Lemma 2.0.13, $\psi = \neg\xi \in V$.
If ψ is of the form $\psi = \xi \wedge \chi$,

$$(M, s_V) \Vdash \xi \wedge \chi \quad \textit{iff} \quad (M, s_V) \Vdash \xi \text{ and } (M, s_V) \Vdash \chi \quad \textit{iff} \quad \xi \in V \text{ and } \chi \in V.$$

By Lemma 2.0.13, $\xi \wedge \chi \in V$.
Now let us assume ψ is of the form $K_i\xi$, we want to show that

$$(M^C, s_V) \Vdash K_i\xi \quad \textit{iff} \quad K_i\xi \in V.$$

Suppose $(M^C, s_V) \Vdash K_i\xi$. Note that, by construction of V, either $K_i\xi \in V$ or $\neg K_i\xi \in V$.
Let us see that $(V/K_i) \cup \{\neg\xi\}$ is $\vdash$-inconsistent .

Suppose $(V/K_i) \cup \{\neg\xi\}$ is $\vdash$-consistent , by Lemma 2.0.12 it is contained in some $\overline{Sub\varphi}$ maximal consistent set W. Note that $(s_V, s_W) \in \mathcal{K}_i$. By (IH), since $\neg\xi \in W$ we have $(M^C, s_W) \Vdash \neg\xi$ therefore $(M^C, s_V) \Vdash \neg K_i\xi$ which is a contradiction. So $(V/K_i) \cup \{\neg\xi\}$ is $\vdash$-inconsistent , then it has a finite subset $\{\varphi_1, \ldots, \varphi_k, \neg\xi\}$ which is $\vdash$-inconsistent .
By Lemma 2.0.14,

$$\vdash \varphi_1 \to (\varphi_2 \to (\ldots \to (\varphi_k \to \xi)\cdots)).$$

By the inference rule $R2$ we have

$$\vdash K_i(\varphi_1 \to (\varphi_1 \to (\varphi_2 \to (\ldots \to (\varphi_k \to \xi)\cdots))).$$

By induction on k and using (3.5) we have

$$\vdash K_i\varphi_1 \to (K_i\varphi_2 \to (\ldots \to (K_i\varphi_k \to K_i\xi)\cdots)).$$

By (iv) of Lemma 2.0.13 we have

$$K_i\varphi_1 \to (K_i\varphi_2 \to (\ldots \to (K_i\varphi_k \to K_i\xi)\cdots)) \in V.$$

Since $\varphi_1, \ldots, \varphi_k \in V/K_i$ we have $K_i\varphi_1, \ldots, K_i\varphi_k \in V$ and by (iii) of Lemma 2.0.13 we have $K_i\xi \in V$.

Reciprocally, suppose $K_i\xi \in V$, then $\xi \in V/K_i$. By definition of $\mathcal{K}_i$, for all X such that $(s_V, s_X) \in \mathcal{K}_i$, $\xi \in X$ then, by (IH), we have $(M^C, s_X) \Vdash \xi$. Hence, $(M^C, s_V) \Vdash K_i\xi$, which concludes the proof of Lemma 3.1.8. ■

As a consequence of Lemma 3.1.8 we have that (3.8) holds: let φ be $\vdash$-consistent . Then φ belongs to some $\overline{Sub\varphi}$ maximal consistent set V. From Lemma 3.1.8 we have $(M^C, s_V) \Vdash \varphi$, so φ is satisfiable in M^C. Then we just need to prove $M^C \in \mathcal{M}_n$, i.e., M^C belongs to the class of Kripke structures whose relations $\mathcal{K}_i$ are equivalence relations.

Lemma 3.1.9 $M^C \in \mathcal{M}_n$.

Proof: Clearly every maximal $\vdash$-consistent set V contains every instance of axioms $K3$, $K4$ and $K5$.
We begin proving axiom $K3$ corresponds to reflexivity:
Let V be a maximal $\vdash$-consistent set. Since every instance of axiom $K3$ are true at s_V, we have $V/K_i \subseteq V$, so the relations $\mathcal{K}_i$ are reflexive.

Now we prove $K4$ corresponds to transitivity:
Let $(s_V, s_W), (s_W, s_X) \in \mathcal{K}_i$. Since all instances of $K4$ are true at s_V, we have that if

$K_i\varphi \in V$ then $K_iK_i\varphi \in V$, so $K_i\varphi \in W$ and $\varphi \in X$. Thus $V/K_i \subseteq X$ and therefore $(s_V, s_X) \in \mathcal{K}_i$, so $\mathcal{K}_i$ is a transitive relation.

We see now that axiom $K5$ corresponds to the Euclidean property:
Let $(s_V, s_W), (s_V, s_X) \in \mathcal{K}_i$. We want to prove

$$W/K_i \subseteq X,$$

which is exactly the same as proving $\mathcal{L}_n^K \setminus X \subseteq W/\neg K_i$ where $W/\neg K_i$ is defined in the natural way, $W/\neg K_i = \{\varphi \in \mathcal{L}_n^K : \neg K_i\varphi \in W\}$. Let $\varphi \in \mathcal{L}_n^K \setminus X$ i.e. $\varphi \notin X$. Since $(s_V, s_X) \in \mathcal{K}_i$, we have $V/K_i \subseteq X$, then $K_i\varphi \notin V$ and so $\neg K_i\varphi \in V$. But all instances of $K5$ are contained on V so $K_i\neg K_i\varphi \in V$. Since $(s_V, s_W) \in \mathcal{K}_i$, we have $\neg K_i\varphi \in W$, as we wanted.
We just proved $\mathcal{K}_i$ are reflexive, transitive and Euclidean relations. By Lemma 3.0.23, we have $\mathcal{K}_i$ are equivalence relations and then $M^C \in \mathcal{M}_n$ (recall $\mathcal{M}_n$ is the class of Kripke structures where the relations $\mathcal{K}_i$ are equivalence relations), which ends the proofs of Lemma 3.1.9 and of Theorem 3.1.7. ■■

Definition 3.1.10 *Let $M = (S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n)$ be a Kripke structure for knowledge. We define the size of M, $||M||$ to be the number of states in S.*

Theorem 3.1.11 *If φ is a $\vdash^K$-consistent formula then φ is satisfiable in a Kripke structure for knowledge M with size at most $2^{|Sub\varphi|}$.*

Proof: We just need to show that the canonical structure we constructed on the proof of Theorem 3.1.7 has size at most $2^{|Sub\varphi|}$.
Since a subformula of φ and its negation can not both belong to a maximal consistent subset of $\overline{Sub\varphi}$, the maximum number of elements which are contained in a maximal consistent subset of $\overline{Sub\varphi}$ is $|Sub\varphi|$ and so the number of states in the canonical Kripke structure M^C is at most $2^{|Sub\varphi|}$. ■

3.2 Probabilistic Epistemic Logic

We want to be able to talk about the truth of formulas such as $P_i(\varphi) \geq b$, which is supposed to say that "according to agent i, formula φ holds with probability at least b". We are even interested in analyzing linear formulas such as $a_1P_i(\varphi_1) + \ldots + a_kP_i(\varphi_k) \geq b$, where

$a_1, \ldots, a_k, b \in \mathbb{Q}$ and $k \geq 1$. With this purpose we do now an overview of the probabilistic epistemic logic presented in [5] and [15].

In this study we will not admit formulas such as $P_i(\varphi) - P_j(\varphi) \geq b$. Comparing probabilities of several agents over a given formula would be interesting but it turns decidability a hard task.

For simplicity, we will use some abbreviations with which we are familiar: we will use $P_i(\varphi) \geq P_i(\psi)$ to represent $P_i(\varphi) - P_i(\psi) \geq 0$, $P_i(\varphi) \leq b$ will represent $-P_i(\varphi) \geq -b$, $P_i(\varphi) < b$ is an abbreviation of $\neg(P_i(\varphi) \geq b)$ and $P_i(\varphi) = b$ will be used instead of $(P_i(\varphi) \geq b) \wedge (P_i(\varphi) \leq b)$.

Definition 3.2.1 *Consider n agents $1, \ldots, n$. The probabilistic epistemic language $\mathcal{L}_n^{KP}$ has the following inductive syntax*

$$\varphi \ ::= \ p \mid \neg\varphi \mid \varphi \wedge \psi \mid K_i\varphi \mid a_1 P_i(\varphi_1) + \cdots + a_k P_i(\varphi_k) \geq b$$

where $p \in \Phi$, $i \in \{1, \ldots, n\}$, $a_1, \ldots, a_k, b \in \mathbb{Q}$.

Definition 3.2.2 *A Kripke structure for knowledge and probability for n agents $1, \ldots, n$ over Φ is a tuple $(S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n, \mathcal{P})$ where $(S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n)$ is a Kripke structure for knowledge over Φ and $\mathcal{P}$ is a probability assignment, which assigns to each agent $i \in \{1, \ldots, n\}$ and state $s \in S$ a probability function $\mathcal{P}(i, s) : S_{i,s} \longrightarrow [0, 1]$, where $S_{i,s} := dom(\mathcal{P}(i, s)) \subseteq S$ is countable.*

Notation: Consider $M = (S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n, \mathcal{P})$ to be a Kripke structure for knowledge and probability. We define $\alpha(M)$ to denote the unique Kripke structure for knowledge $(S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n)$ which corresponds to M.

Remark 3.2.3 *In a more general setting $\mathcal{P}(i, s)$ is defined to be a probability space $\mathcal{P}(i, s) = (S_{i,s}, \mathfrak{A}_{i,s}, \mu_{i,s})$, where $S_{i,s} \subseteq S$, $\mathfrak{A}_{i,s}$ is a σ-algebra of subsets of $S_{i,s}$ and $\mu_{i,s}$ is a probability measure defined on the elements of $\mathfrak{A}_{i,s}$.*
In this generalized approach we are able to reason about uncountable sets of states. Being in fact a wider approach, it complexifies the logic, in particular when we proceed to the introduction of the dynamic component, below. Eventually, the generalization will be part of the future work we propose to develop, for the construction of security logics.

Now we extend Definition 3.1.4 to formulas involving probabilities.

Definition 3.2.4 *Let $\mathcal{L}_n^{KP}$ the probabilistic epistemic language and $M = (S, \pi, \mathcal{K}_1 \ldots, \mathcal{K}_n, \mathcal{P})$ a Kripke structure for knowledge and probability over Φ. Let $s \in S$ be a state and $\varphi \in \mathcal{L}_n^{KP}$ be a formula.*
If φ is an epistemic formula, we define

$$(M, s) \Vdash \varphi \quad \text{if and only if} \quad (\alpha(M), s) \Vdash \varphi.$$

If φ is of the form $(a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b)$, for some formulas $\varphi_1, \ldots, \varphi_k$, and rational numbers $a_1, \ldots, a_k, b$, we define

$$\begin{aligned}(M, s) \Vdash a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b \quad &\text{if and only if} \\ a_1 \mathcal{P}(i, s)(\varphi_1) + \ldots + a_k \mathcal{P}(i, s)(\varphi_k) \geq b,&\end{aligned} \tag{3.9}$$

where, for each $l \in \{1, \ldots, n\}$, defining $\Lambda_{i,s}^l = \{u \in dom(\mathcal{P}(i, s)) | (M, u) \Vdash \varphi_l\}$, we consider

$$\mathcal{P}(i, s)(\varphi_l) = \sum_{v \in \Lambda_{i,s}^l} \mathcal{P}(i, s)(v).$$

If φ is of the form $K_i\,(a_1 P_j(\varphi_1) + \ldots + a_k P_j(\varphi_k) \geq b)$, for some formulas $\varphi_1, \ldots, \varphi_k$, rational numbers $a_1, \ldots, a_k, b$ and $j \in \{1, \ldots, n\}$, we define

$$\begin{aligned}(M, s) \Vdash K_i\,(a_1 P_j(\varphi_1) + \ldots + a_k P_j(\varphi_k) \geq b) \quad &\text{if and only if} \\ \text{for all } t \in S \text{ s.t. } (t, s) \in \mathcal{K}_i,\ (M, t) \Vdash a_1 P_j(\varphi_1) + \ldots + a_k P_j(\varphi_k) \geq b.&\end{aligned} \tag{3.10}$$

(3.9) tells that $P_i(\varphi) \geq b$ denotes the probability of φ to be at least b according to agents i's probability function in state s.

Now think for a few seconds about the sets $S_{i,s}$, the domain of the probability function $\mathcal{P}(i, s)$, for a given agent i and state s. It seems reasonable to assume that $S_{i,s} \subseteq \mathcal{K}_i(s)$, recall that $\mathcal{K}_i(s) := \{t \in S : (s, t) \in \mathcal{K}_i\}$. If this condition does not hold we are allowing agent i to place positive probability on a formula he knows to be false.

It thus appears reasonable to assume

C1. For all $i \in \{1, \ldots, n\}$ and $s \in S$, $S_{i,s} \subseteq \mathcal{K}_i(s)$.

The reader may even question himself why do we not assume that $S_{i,s} = \mathcal{K}_i(s)$. In fact we could assume so, but this condition would be too restrictive and even unintuitive. The agent may consider a situation plausible but do not care with assigning to it any probability and can even consider another situation which is not even plausible and so he does not want to assign any probability to it.

There are two other interesting conditions, but since it complexify the logic too much we choose not to assume it, but we do not ignore its existence and gains.

We might well consider that all agents have the same probabilistic assignment at each state

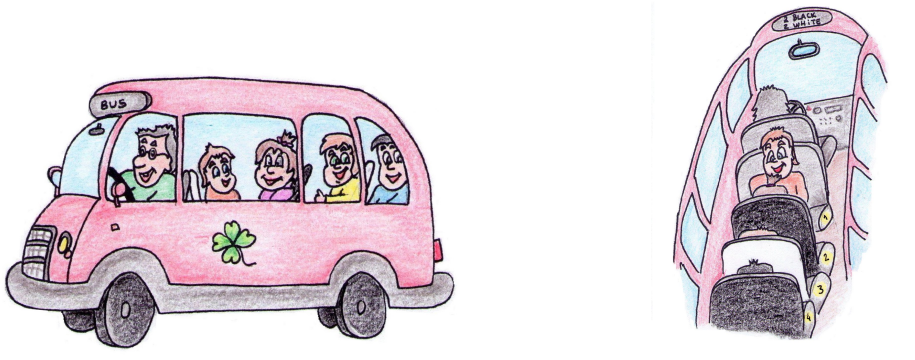
C2. For all $i, j \in \{1, \ldots, n\}$ and $s \in S$, $\mathcal{P}_{i,s} = \mathcal{P}_{j,s}$.

Or even a condition over the agent's probability assignment at different states,

C3. For all $i \in \{1, \ldots, n\}$ and $s, t \in S$ if $t \in S_{i,s}$ then $\mathcal{P}_{i,s} = \mathcal{P}_{i,t}$.

Note that this third condition seems quite reasonable. At condition $C1$ we assumed $S_{i,s}$ to be included on $\mathcal{K}_i(s)$. Moreover, we defined the set $\mathcal{K}_i(s)$ to be the set of worlds indistinguishable from s for agent i. It seems very acceptable to assign the same probabilities for two states which are indistinguishable. Summarizing, the condition $C3$ would help us to clarify the idea of indistinguishability of states.

In this text we will assume $C1$ and will not assume $C2$ nor $C3$. However, depending on the example we can assume some of the latter conditions on the studied model. Let us check the three conditions on our bus trip.



Example 3.2.1 *The bus trip example presented before has a probabilistic component. For each agent $i \in \{1, 2, 3, 4\}$ and state $s \in S$, we define the probability assignment of the*

Kripke structure for knowledge and probability $M = (S, \pi, \mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_3, \mathcal{K}_4, \mathcal{P})$ *as follows:*

$$\begin{array}{rccc} \mathcal{P}(i,s): & \mathcal{K}_i(s) & \longrightarrow & [0,1] \\ & t & \longmapsto & \frac{1}{|\mathcal{K}_i(s)|} \end{array}$$

Since passenger 4 *knows* w_2 *to be false, he does not assign positive probability to worlds where* w_2 *holds, for this reason* $C1$ *holds, moreover we have the equality* $S_{i,s} = \mathcal{K}_i(s)$.
The definition of the probability assignment implies that $C3$ *is also true. However* $C2$ *clearly does not hold: passengers have different information.* □

Now we provide a sound and complete axiomatization for the logic of knowledge and probability.

To the inference system for knowledge we add some axioms that allow us to reason about linear inequalities:

I1. $(a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b) \leftrightarrow (a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) + 0 P_i(\varphi_{k+1}) \geq b)$;

I2. $(a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b) \rightarrow (a_{l_1} P_i(\varphi_{l_1}) + \ldots + a_{l_k} P_i(\varphi_{l_k})) \geq b)$,

for all $(l_1 \cdots l_k)$ permutation of $(1 \cdots k)$;

I3. $(a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b) \wedge (a'_1 P_i(\varphi_1) + \ldots + a'_k P_i(\varphi_k) \geq b') \rightarrow$

$\rightarrow (a_1 + a'_1) P_i(\varphi_i) + \ldots + (a_k + a'_k) P_i(\varphi_k)) \geq (b + b')$;

I4. $(a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b) \leftrightarrow (d a_1 P_i(\varphi_1) + \ldots + d a_k P_i(\varphi_k)) \geq db)$, for all $d > 0$;

I5. $(a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b) \vee (a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k)) \leq b)$;

I6. $(a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b) \rightarrow (a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k)) > c$ if $b > c$

with $k \geq 1$, $i \in \{1, \ldots, n\}$, $a_1, \ldots, a_n, b, c \in \mathbb{Q}$.

Some other axioms that allows us to reason about probability:

P1. $P_i(\varphi) \geq 0$;

P2. $P_i(true) = 1$;

P3. $P_i(\varphi \wedge \psi) + P_i(\varphi \wedge \neg\psi) = P_i(\varphi)$

P4. $P_i(\varphi) = P_i(\psi)$ if $\varphi \leftrightarrow \psi$ is a proposition tautology.

Finally the axiomatization for $C1$, $C2$ and $C3$ are respectively

P5. $K_i\varphi \rightarrow (P_i(\varphi) = 1)$.

P6. $(a_1P_i(\varphi_1) + \ldots + a_kP_i(\varphi_k) \geq b) \rightarrow (a_1P_j(\varphi_1) + \ldots + a_kP_j(\varphi_k) \geq b)$.

P7. $\varphi \rightarrow P_i(\varphi) = 1$, where φ is of the form $a_1P_i(\varphi_1) + \ldots + a_kP_i(\varphi_k) \geq b$ or its negation.

Axioms $I1 - I6$ are quite intuitive if we think about the corresponding expressions on the real numbers.

true was defined as denoting $p \vee \neg p$ for some primitive proposition p. Since we are dealing with a classical based language, we should expect that $P2$ holds. For the same reason, from our intuition of probabilities $P3$ follows. $P4$ is a consequence of the indistinguishability that agent i should assign to equivalent formulas φ and ψ. $P5$ covers our intuition that if an agent knows a formula, he should be able to assign probability 1 to it. Condition $C2$ assumes that different agents have the same probability assignments and $P6$ follows. Axiom $P7$ results from the fact that each formula of the form $a_1P_i(\varphi_1) + \ldots + a_kP_i(\varphi_k) \geq b$ has the same truth value on all states in the domain of each probability function, which is a consequence of condition $C3$.

Remark 3.2.5 *From $P2$ and $P3$, taking $\varphi = \psi = true$ follows that $P_i(false) = 0$.*

Remark 3.2.6 *$P(\varphi \vee \psi) = P(\varphi) + P(\psi) - P(\varphi \wedge \psi)$ is provable from $P3$.*

Recall that we will not assume $C2$ nor $C3$ in this text.

Notation: Let $\mathcal{M}_n^{KP}$ denote the collection of Kripke structures for knowledge and probability for agents $1, \ldots, n$ over Φ satisfying the assumption $C1$.

Definition 3.2.7 *Let $\mathfrak{H}^{KP}$ be the inference system for knowledge and probability obtained by joining $\mathfrak{H}^{K}$ together with axioms I1-I6 and P1-P5 and $\vdash_n^K$ be the corresponding deductive system.*

We present now some results that will enable us to prove completeness of $\mathfrak{H}^{KP}$.

Lemma 3.2.8 *The inference system $\mathfrak{H}^*$ resulting of joining $\mathfrak{H}^{KP}$ together with*

I0′. $x \geq x$

I1′. $(a_1x_1 + \ldots + a_kx_k \geq c) \leftrightarrow (a_1x_1 + \ldots + a_kx_k + 0x_{k+1} \geq c)$

I2′. $(a_1x_1 + \ldots + a_kx_k \geq c) \rightarrow (a_{j_1}x_{j_1} + \ldots + a_{j_k}x_{j_k} \geq c)$,
if $(j_1 \cdots j_k)$ is a permutation of $(1 \cdots k)$

I3′. $(a_1x_1 + \ldots + a_kx_k \geq c) \wedge (a'_1x_1 + \ldots + a'_kx_k \geq c') \rightarrow$
$\rightarrow ((a_1 + a'_1)x_1 + \ldots + (a_k + a'_k)x_k \geq (c + c'))$

I4′. $(a_1x_1 + \ldots + a_kx_k \geq c) \leftrightarrow (da_1x_1 + \ldots + da_kx_k \geq dc)$, *if* $d > 0$

I5′. $(a_1x_1 + \ldots + a_kx_k \geq c) \vee (a_1x_1 + \ldots + a_kx_k \leq c)$

I6′. $(a_1x_1 + \ldots + a_kx_k \geq c) \rightarrow (a_1x_1 + \ldots + a_kx_k > d)$, *if* $c > d$.

is complete.

Afterwards axioms $I1 - I6$ result from axioms $I1' - I6'$ replacing each x_j by $P_i(\varphi_j)$ and $I0'$ is replaced by $P4$.

Sketch of the Proof of Lemma 3.2.8: Soundness results from the extension of the model with an assignment to statements of the form $a_1x_1 + \ldots + a_kx_k \geq c$.

Now we sketch the proof of completeness performed in Theorem 4.3 of Fagin et al. (1990). We will use a general procedure, which will be recalled at Lemma 3.2.18. Consider a $\vdash$-consistent formula φ and reduce it to a canonical form.
Once proved the formula

$$a_1x_1 + a'_1x_1 + a_2x_2 + \ldots + a_nx_n \geq c \leftrightarrow ((a_1 + a'_1)x_1 + a_2x_2 + \ldots + a_nx_n \geq c),$$

we can assume any variable is repeated and proving then that

$$0x_1 + \ldots + 0x_n \geq 0$$

we still assume variables are presented in the same order. Hence, we assume φ to be the conjunction of the following standard formulas

$$\begin{array}{lcl} a_{1,1}x_1 + \ldots + a_{1,n}x_n & \geq & c_1 \\ \vdots & & \\ a_{r,1}x_1 + \ldots + a_{r,n}x_n & \geq & c_r \\ a'_{1,1}x_1 + \ldots + a'_{1,n}x_n & < & c'_1 \\ \vdots & & \\ a'_{t,1}x_1 + \ldots + a'_{t,n} & < & c'_t \end{array}$$

Lemma 3.2.8 follows with some results of linear programming, making a distinction between case $t = 0$ and $t > 0$ and assuming, as usual, the system is unsatisfiable (and so is φ) and achieving a contradiction. ■

Definition 3.2.9 *Consider $\Lambda \subseteq \Phi$ to be a set of primitive propositions and let $m \geq 1$. We define ψ to be a m-atom with respect to (wrt) Λ if ψ is of the from $\psi = A_1 \wedge \ldots \wedge A_m$, where for each $j \in \{1, \ldots, m\}$ either $A_j \in \Lambda$ or $\neg A_j \in \Lambda$. The set of m-atoms wrt Λ will be denoted by At_m^Λ.*
When $\Lambda = \Phi$ we only say ψ is a m-atom.

Remark 3.2.10 $\left|At_m^{\{p_1,\ldots,p_m\}}\right| = 2^m$.

Lemma 3.2.11 *Let $i \in \{1, \ldots, n\}$ be an agent and φ be a propositional formula. Let $\{p_1, \ldots, p_u\}$ include all the primitive propositions that appear in φ. Consider the set*

$$\mathcal{A}_u(\varphi) = \left\{\psi \in At_u^{\{p_1,\ldots,p_u\}} \mid \psi \to \varphi \text{ is a propositional tautology}\right\}.$$

Then $P_i(\varphi) = \sum_{\psi \in \mathcal{A}_u(\varphi)} P_i(\psi)$ is provable in the deductive system $\vdash_n^{KP}$.

Proof: Assume $At_j^{p_1 \cdots p_j} = \{\psi_1, \ldots, \psi_{2^j}\}$ are all the j-atoms wrt $\{p_1 \cdots p_j\}$.
We will prove that

$$P_i(\varphi) = P_i(\varphi \wedge \psi_1) + \ldots + P_i(\varphi \wedge \psi_{2^j})$$

by induction on j.
For $j = 1$, it immediately follows from $P3$, and eventually from $I2$ and propositional reasoning, which enable us to rearrange terms.
Let $j \in \mathbb{N}$. Assume that $P_i(\varphi) = P_i(\varphi \wedge \psi_1) + \ldots + P_i(\varphi \wedge \psi_{2^j})$. (IH)
By $P3$, for each $l \in \{1, \ldots, 2^j\}$, $P_i(\varphi \wedge \psi_l \wedge p_{j+1}) + P_i(\varphi \wedge \psi_l \wedge \neg p_{j+1}) = P_i(\varphi \wedge \psi_l)$ is

provable. Using the same argument as for the case $j = 1$, we can replace each $P_i(\varphi \wedge \psi_l)$ by $P_i(\varphi \wedge \psi_l \wedge p_{j+1}) + P_i(\varphi \wedge \psi_l \wedge \neg p_{j+1})$, which concludes the proof that for each j, $P_i(\varphi) = P_i(\varphi \wedge \psi_1) + \ldots + P_i(\varphi \wedge \psi_{2^j})$.
In particular it follows that

$$P_i(\varphi) = P_i(\varphi \wedge \omega_1) + \ldots + P_i(\varphi \wedge \omega_{2^u}),$$

where $At_u^{\{p_1,\ldots,p_u\}} = \{\omega_1, \ldots, \omega_{2^u}\}$.
Since $\{p_1, \ldots, p_u\}$ includes all primitive propositions that appear in φ, it is now clear that if $\omega_l \in \mathcal{A}_u(\varphi)$ then $\varphi \wedge \omega_l$ is equivalent to ω_l and so the term $P_i(\varphi \wedge \omega_l)$ can be replaced by $P_i(\omega_l)$, if $\omega_l \notin \mathcal{A}_u(\varphi)$ then $\varphi \wedge \omega_l$ is equivalent to $false$ and in this case the term $P_i(\varphi \wedge \omega_l)$ can be replaced by $P_i(false)$ which is provably equal to 0.
Hence, $P_i(\varphi) = \sum_{\psi \in \mathcal{A}_u(\varphi)} P_i(\psi)$ is provable. ■

Theorem 3.2.12 *$\mathfrak{H}^{KP}$ is a sound and (weakly) complete axiomatization for probabilistic epistemic logics with respect to $\mathcal{M}_n^{KP}$.*

Proof: This proof will be done just as [15], but we will prove most of the technical issues which are dropped in [15].

We prove soundness verifying that each axiom in $\mathfrak{H}^{KP}$ is valid in $\mathcal{L}_n^{KP}$. Axioms in $\mathfrak{H}^K$ are already proved to be valid in $\mathcal{L}_n^{KP}$, so let us begin by $I1$.
Let $\varphi_1, \ldots, \varphi_n \in \mathcal{L}_n^{KP}$, we have the following equivalences,

$(M, w) \Vdash a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b$ *iff*
$a_1 \mathcal{P}(i, w)(\varphi_1) + \ldots + a_k \mathcal{P}(i, w)(\varphi_k) \geq b$ *iff*
$a_1 \mathcal{P}(i, w)(\varphi_1) + \ldots + a_k \mathcal{P}(i, w)(\varphi_k) + 0\mathcal{P}(i, w)(\varphi_{k+1}) \geq b$ *iff*
$(M, w) \Vdash a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) + 0 P_i(\varphi_{k+1}) \geq b$

Hence $I1$ follows. Analogously we see axioms $I2 - I6$ are valid in $\mathcal{M}_n^{KP}$. We just need to note that, for any formulas $\varphi_1, \ldots, \varphi_k \in \mathcal{L}_n^{KP}$, agent i and $a_1, \ldots, a_k, b \in \mathbb{Q}$, $a_1 \mathcal{P}(i, s)(\varphi_1) + \ldots + a_k \mathcal{P}(i, s)(\varphi_k) \in \mathbb{R}$, so all the axioms become from the properties of addition and multiplication on the real numbers.

$P1$ is immediate: for every state $w \in S$,

$$(M, w) \Vdash P_i(\varphi) \geq 0 \quad \textit{iff} \quad \mathcal{P}(i, w)(\varphi) \geq 0.$$

Indeed, by definition of $\mathcal{P}(i, w)$, we have $\mathcal{P}(i, w)(\varphi) \geq 0$.

For $P2$, let $w \in S$ be any state,

$(M, w) \Vdash P_i(true) = 1 \quad iff \quad \mathcal{P}(i, w)(true) = 1 \quad iff \quad \sum_{v \in \Lambda^{true}_{i,w}} \mathcal{P}(i, w)(v) = 1,$
where $\Lambda^{true}_{i,w} = \{u \in S_{i,w} \mid (M, u) \Vdash true\} = \{u \in S_{i,w} \mid (M, u) \Vdash p \vee \neg p\} = S_{i,w}$.
So, $\sum_{v \in S_{i,w}} \mathcal{P}(i, w)(v) = 1$, which is true because $\mathcal{P}(i, w)$ is a probability function and $S_{i,w} := dom(\mathcal{P}(i, w))$.

Axiom $P3$ also follows from the fact that for all $w \in S$, $\mathcal{P}(i, w)$ is a probability function, note that
$\mathcal{P}(i, w)(\varphi) = \mathcal{P}(i, w)(\varphi \wedge true) = \mathcal{P}(i, w)(\varphi \wedge (\psi \vee \neg\psi)) = \mathcal{P}(i, w)((\varphi \wedge \psi) \vee (\varphi \wedge \neg\psi))$.

Since the events $\varphi \wedge \psi$ and $\varphi \wedge \neg\psi$ are mutually exclusive we have
$$\mathcal{P}(i, w)((\varphi \wedge \psi) \vee (\varphi \wedge \neg\psi)) = \sum_{v \in \Lambda^{1 \vee 2}_{i,w}} \mathcal{P}(i, w)(v) = \sum_{v \in \Lambda^{1}_{i,w}} \mathcal{P}(i, w)(v) + \sum_{u \in \Lambda^{2}_{i,w}} \mathcal{P}(i, w)(u) =$$
$$= \mathcal{P}(i, w)(\varphi \wedge \psi) + \mathcal{P}(i, w)(\varphi \wedge \neg\psi)$$

where $\Lambda^{1 \vee 2}_{i,w} = \{t \in S_{i,w} \mid (M, t) \Vdash (\varphi \wedge \psi) \vee (\varphi \wedge \neg\psi)\}$, $\Lambda^{1}_{i,w} = \{t \in S_{i,w} \mid (M, t) \Vdash \varphi \wedge \psi\}$ and $\Lambda^{2}_{i,w} = \{t \in S_{i,w} \mid (M, t) \Vdash \varphi \wedge \neg\psi\}$.

So, $(M, w) \Vdash P_i(\varphi) = P_i(\varphi \wedge \psi) + P_i(\varphi \wedge \neg\psi)$.

For $P4$, suppose $\varphi \leftrightarrow \psi$ is a propositional tautology. For all state $w \in S$

$$(M, w) \Vdash P_i(\varphi) = P_i(\psi) \quad iff$$
$$\mathcal{P}(i, w)(\varphi) = \mathcal{P}(i, w)(\psi) \quad iff$$
$$\sum_{v \in \Lambda^{\varphi}_{i,w}} \mathcal{P}(i, w)(v) = \sum_{t \in \Lambda^{\psi}_{i,w}} \mathcal{P}(i, w)(t), \tag{3.11}$$

where $\Lambda^{\varphi}_{i,w} = \{s \in S_{i,w} \mid (M, s) \Vdash \varphi\}$ and $\Lambda^{\psi}_{i,w} = \{s \in S_{i,w} \mid (M, s) \Vdash \psi\}$.
Since $\varphi \leftrightarrow \psi$, it follows that $\Lambda^{\varphi}_{i,w} = \Lambda^{\psi}_{i,w}$ and so (3.11) holds.

For $P5$, suppose $M \Vdash K_i\varphi$.
For all states $s \in S$, $(M, s) \Vdash K_i\varphi$. Fix $s \in S$, for all states $t \in \mathcal{K}_i(s)$, we have $(M, t) \Vdash \varphi$.

$$\mathcal{P}(i, s)(\varphi) = \sum_{t \in S_{i,s},\ (M,t) \Vdash \varphi} \mathcal{P}(i, s)(t).$$

Since $S_{i,s} \subseteq \mathcal{K}_i(s)$, all states $w \in S_{i,s}$ verify $(M, w) \Vdash \varphi$. Then

$$P_i(\varphi) = \sum_{t \in S_{i,s}} \mathcal{P}(i,s)(t) = 1.$$

Since $s \in S$ is any state, it follows that $M \Vdash P_i(\varphi) = 1$.

For completeness, we need to show that if a formula φ is $\vdash^{KP}$-consistent then φ is satisfiable in a Kripke structure for knowledge and probability.

Suppose φ is $\vdash^{KP}$-consistent . We will perform the construction of the canonical model $M^C = (S, \pi, \mathcal{K}_1, \ldots . \mathcal{K}_n, \mathcal{P})$ as we did in the epistemic case:

$S = \{s_V \mid V \text{ is } \overline{Sub\varphi} \text{ maximal consistent}\}$

$\pi(s_V)(p) = \begin{cases} true & \text{if} \quad p \in V \\ false & \text{if} \quad p \notin V \end{cases}$ for each state $s_V \in S$ and primitive proposition $p \in \Phi$

$\mathcal{K}_i = \{(s_V, s_w) \in S^2 \mid V/K_i \subseteq W\}$, for each $i \in \{1, \ldots, n\}$

The probability assignment is a new feature and we have to define it carefully.

Notation: Given a finite set Z define φ_Z to be the conjunction of elements in Z.

Lemma 3.2.13 *Let $s_V, s_W \in S$. If $s_V \neq s_W$ then $\vdash \varphi_V \rightarrow \neg\varphi_W$.*

Proof: Let $s_V, s_W \in S$ with $s_V \neq s_W$ and where $V = \{\psi_1, \ldots, \psi_{|Sub\varphi|}\}$ and $W = \{\xi_1, \ldots, \xi_{|Sub\varphi|}\}$. Since $V \neq W$ and by construction of maximal consistent sets of $\overline{Sub\varphi}$, there is some $i \in \{1, \ldots, |Sub\varphi|\}$ such that $\psi_i \in V$ and $\neg\psi_i \in W$, say $\neg\psi_i = \xi_i$.
Suppose $\vdash \varphi_V$, i.e., $\vdash \psi_1 \wedge \ldots \wedge \psi_{|Sub\varphi|}$. In particular, ψ_i holds. Since $\neg\varphi_W = \neg\xi_1 \vee \cdots \vee \neg\xi_i \vee \cdots \neg\xi_{|Sub\varphi|}$ and $\psi_i = \neg\xi_i$ holds. we have $\neg\varphi_W$ holds. ■

Lemma 3.2.14 $\vdash \psi \leftrightarrow \bigvee_{\{s_V \mid \psi \in V\}} \varphi_V$, *for all $\psi \in \overline{Sub\varphi}$.*

Proof of Lemma 3.2.14: Let $\psi \in \overline{Sub\varphi}$.
Since for every $\overline{Sub\varphi}$ maximal consistent set V and for every subformula φ' of φ, either $\varphi' \in V$ or $\neg\varphi' \in V$, then denoting $Sub\varphi = \{\varphi_1, \ldots, \varphi_{|Sub\varphi|-1}, *\psi\}$ (note that either $\psi \in Sub\varphi$ or $\neg\psi \in Sub\varphi$), we have

$$\bigvee_{\{s_V \in S \mid \psi \in V\}} \varphi_V \leftrightarrow \left(\bigwedge_{i=1}^{|Sub\varphi|-1} (\varphi_i \vee \neg\varphi_i) \right) \wedge \psi \leftrightarrow \psi,$$

as we wanted. ■

The following Lemma is immediate from Lemma 3.2.13, Lemma 3.2.14 and axiom $P4$.

Lemma 3.2.15 *If* $\psi \in \overline{Sub\varphi}$ *then* $P_i(\psi) = \sum_{\{s_V \in S | \psi \in V\}} P_i(\varphi_V)$

Lemma 3.2.16 *A formula* $\left(\sum_{l=1}^{k} a_l P_i(\psi_l) \geq b\right) \in \overline{Sub\varphi}$ *is provably equivalent to a formula*

$$\sum_{s_V \in S} c_V P_i(\varphi_V) \geq b,$$

for some coefficients c_V.

Proof of Lemma 3.2.16: By Lemma 3.2.15 and by axiom **I1**, for each $l \in \{1, \ldots, k\}$.

$$P_i(\psi_l) = \sum_{\{s_V | \psi_l \in V\}} P_i(\varphi_V) = \sum_{\{s_V \in S | \psi_l \in V\}} P_i(\varphi_V) + \sum_{\{s_V \in S | \psi_l \notin V\}} 0 \cdot P_i(\varphi_V) = \sum_{s_V \in S} \gamma_V^l P_i(\varphi_V),$$

with $\gamma_V^l = \begin{cases} 1 & \text{if} \quad \psi_l \in V \\ 0 & \text{if} \quad \psi_l \notin V \end{cases}$.

Therefore,

$$\sum_{l=1}^{k} a_l P_i(\psi_l) \geq b \quad \textit{iff} \quad \sum_{l=1}^{k} \left(a_l \sum_{s_V \in S} \gamma_V^l P_i(\varphi_V) \right) \geq b \quad \textit{iff} \quad \sum_{s_V \in S} \left(\sum_{l=1}^{k} a_l \gamma_V^l \right) P_i(\varphi_V) \geq b.,$$

which ends the proof of Lemma 3.2.16. ■

Lemma 3.2.17 *Let* $s_V, s_{V'} \in S$. *If* $s_{V'} \notin \mathcal{K}_i(s_V)$ *then* $\varphi_V \to (P_i(\varphi_{V'}) = 0)$ *is provable.*

Proof of Lemma 3.2.17: Let $s_V \in S$ and $s_{V'} \notin \mathcal{K}_i(s_V)$.
We begin proving $\varphi_V \to K_i(\neg\varphi_{V'})$.
Since $s_{V'} \notin \mathcal{K}_i(s_V)$, $V/K_i \not\subseteq V'$, which means there is a formula $K_i\omega \in V$ such that $\omega \notin V'$, so $\neg\omega \in V'$.
Since $\neg\varphi_{V'} \leftrightarrow \left(\bigvee_{\psi \in V' \setminus \{\neg\omega\}} \neg\psi\right) \vee \omega$, by property (3.7), it follows that

$$\varphi_V \to K_i \neg\varphi_{V'}.$$

Applying $P5$, $\varphi_V \to (P_i(\neg\varphi_{V'}) = 1)$ is provable.
By $P2$ and $P3$,

$P_i(true \wedge \varphi_{V'}) + P_i(true \wedge \neg\varphi_{V'}) = P_i(true)$ *iff* $P_i(\varphi_{V'}) + P_i(\neg\varphi_{V'}) = 1$.
Then, $\varphi_V \rightarrow (P_i(\varphi_{V'}) = 0)$ is provable, and we are done in the proof of Lemma 3.2.17. ■

Let $i \in \{1, \ldots, n\}$ be an agent and $s_W \in S$ be a state. Let us construct one inequality corresponding to every formula $\psi = \left(\sum_{l=1}^{k} a_l P_i(\varphi_l) \geq b\right) \in \overline{Sub\varphi}$.

Let $\psi = \left(\sum_{l=1}^{k} a_l P_i(\varphi_l) \geq b\right)$ be a formula in $\overline{Sub\varphi}$, which by Lemma 3.2.16 is equivalent to $\sum_{s_{V'} \in S} c_{V'} P_i(\varphi_{V'}) \geq b$. We have either $\psi \in s_W$ or $\neg\psi \in s_W$. If $\psi \in s_W$ then the inequality corresponding to ψ is

$$\sum_{s_{V'} \in S} c_{V'} \mathcal{P}(i, s_W)(s_{V'}) \geq b. \tag{3.12}$$

If $\neg\psi \in s_W$, since $\psi \leftrightarrow \sum_{s_{V'} \in S} c_{V'} P_i(\varphi_{V'}) \geq b$ we have $\neg\psi \leftrightarrow \sum_{s_{V'} \in S} c_{V'} P_i(\varphi_{V'}) < b$ so the corresponding inequality is

$$\sum_{s_{V'} \in S} c_{V'} \mathcal{P}(i, s_W)(s_{V'}) < b. \tag{3.13}$$

On the other side, we have

$$\sum_{s_{V'} \in S} \mathcal{P}(i, s_W)(s_{V'}) = 1. \tag{3.14}$$

Moreover, $\mathcal{P}(i, s_W)(s_{V'}) = 0$ when $s_{V'} \notin \mathcal{K}_i(s_W)$.
Let us associate to agent i and state s_W, $\mathfrak{S}^{i,W}$, the system of equalities and inequalities composed by equality (3.14), (inequalities 3.12) or (3.13) for each $\psi \in \overline{Sub\varphi}$, equations $\mathcal{P}(i, s_W)(s_{V'}) = 0$ for each $s_{V'} \in S \setminus \mathcal{K}_i(s_W)$ and inequalities $\mathcal{P}(i, s_W)(s_{V'}) \geq 0$ for each $s_{V'} \in \mathcal{K}_i(s_W)$.

Observation: Notice that since φ_V's are mutually exclusive, we can indifferently refer to $P_i(s_V)$ or $P_i(\varphi_V)$.

Lemma 3.2.18 *Let $s_W \in S$ be a state and $i \in \{1, \ldots, n\}$ denote an agent. If φ_W is $\vdash$-consistent then the system of linear equalities and inequalities $\mathfrak{S}^{i,W}$ has a solution $\mathcal{P}^*(i, s_W)(s_V)$, for each $s_V \in S$.*

Proof: We begin by reducing φ_W to a canonical form.
φ_W is provably equivalent to a disjunction $\xi_1 \vee \ldots \vee \xi_s$, where each ξ_j is a conjunction

of basic probability formulas such as $a_1P_i(A_1) + \ldots + a_kP_i(A_k) \geq c$ and their negations, where $a_1, \ldots, a_k, c$ are integers, $k \geq 1$ and $A_1, \ldots, A_k$ are propositional formulas. Since φ_W is $\vdash$-consistent , then so is some ξ_j: suppose for all j, $\neg\xi_j$ is provable, then so is $\neg(\xi_1 \vee \ldots \vee \xi_s)$, therefore φ_W is $\vdash$-inconsistent . On the other hand, if ξ_j is satisfied in some Kripke structure, then so is φ_W.

So we reduce our study to the case where φ_W is a conjunction of basic probability formulas and their negations.

Now let $\{p_1, \ldots, p_u\}$ represent all the primitive propositions that appear on φ_W. By Lemma 3.2.11 we can replace in φ_W each term of the form $P_i(A_l)$ by an expression of the form $\sum_{\psi \in \mathcal{A}_u(\varphi)} P_i(\psi) + \sum_{\psi \in At_u^{\{p_1,\ldots,p_u\}} \setminus \mathcal{A}_u(\varphi)} 0P_i(\psi)$. Moreover, replacing each term in φ_W of the form $a_1P_i(A_1) + \ldots + a_kP_i(A_k)$ by the corresponding term $b_1P_i(\psi_1) + \ldots + b_{2^u}P_i(\psi_{2^u})$, where $At_u^{\{p_1,\ldots,p_u\}} = \{\psi_1, \ldots, \psi_{2^u}\}$, we get a provably equivalent formula $\overline{\varphi_W}$.

Let $\overline{\overline{\varphi_W}}$ be a formula which consists on adding by conjunction to $\overline{\varphi_W}$ the following probability formulas:

- $P_i(\psi_j) = 0$ for those n-atoms $\psi_j \in \Upsilon$, where

  $$\Upsilon = \Big\{\psi \in At_u^{\{p_1,\ldots,p_u\}} \mid \begin{array}{l}\text{the set } U \text{ whose conjunction of all elements is } \psi_j \\ \text{is a } \overline{Sub\varphi} \text{ maximal set and does not verify } W/K_i \subseteq U\end{array}\Big\}.$$

  Note that these equations are a consequence of Lemma 3.2.17.

- $P_i(\psi_l) \geq 0$ for each n-atoms $\psi_j \notin \Upsilon$.

- the probability formula $P_i(\psi_1) + \ldots + P_i(\psi_{2^u}) = 1$ which is provable provided Lemma 3.2.11 taking $\varphi = true$, and resumes to the inequalities $P_i(\psi_1) + \ldots P_i(\psi_{2^u}) \geq 1$ and $P_i(\psi_1) + \ldots + P_i(\psi_{2^u}) \leq 1$.

Then we get $\overline{\overline{\varphi_W}}$ provably equivalent to $\overline{\varphi_W}$ and so provably equivalent to φ_W.

Note that $\overline{\overline{\varphi_W}}$ results from the conjunction of the following equalities and inequalities:

$$\begin{array}{lcll}
P_i(\psi_1) + \ldots + P_i(\psi_{2^u}) & \geq & 1 & \\
P_i(\psi_1) + \ldots + P_i(\psi_{2^u}) & \leq & 1 & \\
P_i(\psi_j) & = & 0 & \text{if } \psi_j \in \Upsilon \\
P_i(\psi_k) & \geq & 0 & \text{if } \psi_k \notin \Upsilon \\
b_{1,1}P_i(\psi_1) + \ldots + b_{1,2^u}P_i(\psi_{2^u}) & \geq & d_1 & \\
\vdots & & & \\
b_{r,1}P_i(\psi_1) + \ldots + b_{r,2^u}P_i(\psi_{2^u}) & \geq & d_r & \\
b'_{1,1}P_i(\psi_1) + \ldots + b'_{1,2^u}P_i(\psi_{2^u}) & < & d'_1 & \\
\vdots & & & \\
b'_{t,1}P_i(\psi_1) + \ldots + b'_{t,2^u}P_i(\psi_{2^u}) & < & d'_t &
\end{array}$$

where $b_{l,j}, d_l, b'_{k,j}$ and d'_k are integers.

Since the number of u-atoms wrt $\{p_1, \ldots, p_u\}$ is finite and the probability can be assigned independently to each u-atom wrt $\{p_1 \ldots, p_u\}$, φ_W is satisfiable if and only if the following system of linear equalities and inequalities is satisfiable:

$$\left\{\begin{array}{lcll}
x_1 + \ldots + x_{2^u} & \geq & 1 & \\
x_1 + \ldots + x_{2^u} & \leq & 1 & \\
x_j & = & 0 & \text{if } \psi_j \in \Upsilon \\
x_k & \geq & 0 & \text{if } \psi_k \notin \Upsilon \\
b_{1,1}x_1 + \ldots + b_{1,2^u}x_{2^u} & \geq & d_1 & \\
\vdots & & & \\
b_{r,1}x_1 + \ldots + b_{r,2^u}x_{2^u} & \geq & d_r & \\
b'_{1,1}x_1 + \ldots + b'_{1,2^u}x_{2^u} & < & d'_1 & \\
\vdots & & & \\
b'_{t,1}x_1 + \ldots + b'_{t,2^u}x_{2^u} & < & d'_t &
\end{array}\right. \tag{3.15}$$

If we show (3.15) is satisfiable, for each $s_{V'} \in S$ and the corresponding $\varphi_{V'} \in At_u^{\{p_1,\ldots,p_n\}}$, say $\varphi_{V'} = \psi_l$, we define $\mathcal{P}(i, s_W)(s_{V'}) = \mathcal{P}(i, s_W)(\varphi_{V'}) = x_l$. Then just remains to show 3.15 is satisfiable.

Assume 3.15 is unsatisfiable (which is equivalent to say $\overline{\overline{\varphi_W}}$ is unsatisfiable), then by Lemma 3.2.8, $\neg\overline{\overline{\varphi_W}}$ is provable. Since $\overline{\overline{\varphi_W}}$ is provably equivalent to φ_W, it follows that $\neg\varphi_W$ is

provable, which is a contradiction with the initial assumptions that φ_W is consistent and it ends the proof of Lemma 3.2.18. ■

For each $i \in \{1, \ldots, n\}$ and $s_W \in S$, we solve the set of equalities and inequalities separately and get the solution $\mathcal{P}^*(i, s_W)$ by Lemma 3.2.18. Now, for each $i \in \{1, \ldots, n\}$ and $s_W \in S$, define $\mathcal{P}$ as $\mathcal{P}(i, s_W) : S \longrightarrow [0, 1]$ where

$$\mathcal{P}(i, s_W)(s_V) = \mathcal{P}^*(i, s_W)(s_V).$$

Since $\sum_{s_{V'} \in S} \mathcal{P}^*(i, s_W)(s_{V'}) = 1$, $\mathcal{P}(i, s_W)$ is a probability function.
Now we just need to readjust the domain of our probability function $\mathcal{P}(i, s)$ for each agent i and state s.
For each $i \in \{1, \ldots, n\}$ and $s_W \in S$, the probability function was defined for all values of S. By condition $C1$, it should verify $S_{i,s_W} \subseteq \mathcal{K}_i(s_W)$. Indeed, in our definition of $\mathcal{P}(i, s_W)$, when $s_V \notin \mathcal{K}_i(s_W)$ it follows that $\mathcal{P}(i, s_W)(s_V) = 0$, so we can conclude the construction by considering $S_{i,s_W} = \mathcal{K}_i(s_W)$ for each agent i and state s_W.

Analogously to the proof of Theorem 3.1.7, we now need to prove that given a formula $\psi \in \overline{Sub\varphi}$ and the state $s_V \in S$,

$$(M, s_V) \Vdash \psi \quad \textit{iff} \quad \psi \in V.$$

The proof proceed by induction.
If ψ is a primitive proposition, it follows from definition of $\pi(s_V)$.
Now assume the claim holds for all subformulas of ψ. (IH).
The case where ψ is an epistemic formula was analyzed in Theorem 3.1.7.
Let $\psi = \sum_{l=1}^{k} a_l P_i(\varphi_l) \geq b$ be a probability formula, then
$(M, s_V) \Vdash \psi \quad \textit{iff} \quad (M, s_V) \Vdash \sum_{s_{V'} \in S} c_{V'} P_i(\varphi_{V'}) \geq b \quad \textit{iff} \quad \sum_{s_{V'} \in S} c_{V'} \mathcal{P}(i, s_V)(\varphi_{V'}) \geq b.$
By the arguments used for (3.12), this is equivalent to $\psi \in V$.

If φ is $\vdash^{KP}$-consistent it should belong to one of the maximal consistent subsets of $\overline{Sub\varphi}$. Therefore, if φ is $\vdash^{KP}$-consistent it is satisfiable in the structure M^C, and we are done in the proof of Theorem 3.2.12. ■

Theorem 3.2.19 *If φ is a $\vdash^{KP}$-consistent formula then φ is satisfiable in a Kripke structure for knowledge and probability M with size at most $2^{|Sub\varphi|}$.*

Proof: Since the canonical structure we constructed in Theorem 3.2.12 has the same states of the one we used to prove Theorem 3.1.7, the result is immediate. ■

3.2.1 Single Agent Case

In this subsection we call the reader's attention for relevant results in the single agent case, which results on a huge simplification of our logic under the assumption of some of the conditions $C1$, $C2$ and $C3$.

We are interested in studying problems related to information security, so the single agent case will be important. We will not assume all the conditions $C1$, $C2$ and $C3$ in this text, however depending on the examples it could be quite interesting to assume them. In doing so we may greatly simplify the logic.

Theorem 3.2.20 *$\mathfrak{H}^{KP}$ joint together with axioms $P6$ and $P7$ is a sound and complete axiomatization for the probabilistic epistemic logics with respect to the collection of Kripke structures for knowledge and probability over Φ satisfying the assumptions $C2$ and $C3$.*

Observation: $\mathfrak{H}^{KP}$ already incorporates axiom $P5$. Note that $C1$ is a previous assumption.

Proof: We begin proving soundness by showing validity of $P6$.
Let i, j be any agents and $s \in S$ be a state. Suppose $(M, s) \Vdash a_1P_i(\varphi_1)+\ldots+a_kP_i(\varphi_k) \geq b$ i.e.

$$a_1\mathcal{P}(i, s)(\varphi_1) + \ldots + a_k\mathcal{P}(i, s)(\varphi_k) \geq b.$$

Since condition $C2$ holds we have

$$a_1\mathcal{P}(j, s)(\varphi_1) + \ldots + a_k\mathcal{P}(j, s)(\varphi_k) \geq b$$

then $(M, s) \Vdash a_1P_j(\varphi_1) + \ldots + a_kP_j(\varphi_k) \geq b$.

For $P7$, let ψ be of the form $a_1P_i(\varphi_1) + \ldots + a_kP_i(\varphi_k) \geq b$ or its negation and $s \in S$ be a state.
Suppose $(M, s) \Vdash \psi$.
We want to show $(M, s) \Vdash P_i(\psi) = 1$, i.e.

$$\mathcal{P}(i, s)(\psi) = 1.$$

By definition of probability of a formula,

$$\mathcal{P}(i,s)(\psi) = \sum_{v \in S_{i,s} \; st \; (M,v) \Vdash \psi} \mathcal{P}(i,s)(v).$$

Since condition $C3$ holds and ψ is of the form we referred before, for each state $v \in S_{i,s}$, ψ holds on state v and since $\mathcal{P}(i,s)$ is a probability function it follows that $\mathcal{P}(i,s)(\psi) = 1$ as we wanted.

For completeness we need to adapt the construction in the proof of Theorem 3.2.12 for the new conditions.

Since $P6$ is an axiom of our new inference system it follows immediately that we do not care with the agent that corresponds to each probability assignment. We can consider a new construction of the canonical model assuming $\mathcal{P}(i,s) = \mathcal{P}(j,s)$ for different agents i and j and it follows that condition $C2$ holds.

Consider $T_i(s)$ to be the set of states that contain all the formulas of the form $a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b$, or negations of it, that hold in s.

Lemma 3.2.21 *Assume $P7$ is a valid axiom and let $s_V, s_{V'} \in S$ be any states.*
If $s_{V'} \notin T_i(s_V)$ then

$$\varphi_V \longrightarrow (P_i(\varphi_{V'} = 0)$$

is provable.

Proof: Suppose $s_{V'} \notin T_i(s_V)$.
There is some probability formula $a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b$ that holds in s_V and does not hold in $s_{V'}$,

$$(M, s_V) \Vdash a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b$$

and

$$(M, s_{V'}) \Vdash \neg \left(a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b\right).$$

By $P7$, since $(M, s_V) \Vdash a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b$,

$$(M, s_V) \Vdash P_i(a_1 P_i(\varphi_1) + \ldots + a_k P_i(\varphi_k) \geq b) = 1.$$

Then

$$\mathcal{P}_i(s_V)(\varphi_{V'}) = \sum_{s\in S_{i,s_V} \text{ st } (M,s)\Vdash\varphi_{V'}} \mathcal{P}_i(s_V)(s) \leq \sum_{s\in S_{i,s_V} \text{ st } (M,s)\Vdash\neg(a_1P_i(\varphi_1)+\ldots+a_kP_i(\varphi_k)\geq b} \mathcal{P}_i(s_V)(s) =$$

$$= \mathcal{P}_i(s_V)(\neg(a_1P_i(\varphi_1) + \ldots + a_kP_i(\varphi_k) \geq b)) = 0.$$

It follows then that $\varphi_V \longrightarrow P_i(\varphi_{V'}) = 0$ is provable. ■

Since $P7$ is valid we can construct our model in such a way that $S_{i,s} \subseteq T_i(s)$. With this purpose we should introduce some new equations in the system (3.15): for each agent i consider the equations

$$x_l = 0, \text{ if } \psi_l \notin T_i(s).$$

$P7$ is valid then it is also easy to see that $T_i(s)$ is a subset of $S_{i,s}$ and that whenever $t \in S_{i,s}$ then we should have $T_i(s) = T_i(t)$ (for otherwise, in $P7$ $P_i(\varphi)$ could not sum 1), so we can now take $\mathcal{P}(i,s) = \mathcal{P}(i,t)$ whatever the $t \in T_i(s)$, and so $C3$ holds. ■

Theorem 3.2.22 *Let M^* be a Kripke structure for knowledge and probability in the single-agent case which verifies $C1$ and $C3$ and consider $\varphi \in \mathcal{L}_1^{KP}$ to be a formula. Then φ is satisfiable in a Kripke structure for knowledge and probability in the single-agent case of size polynomial in $|Sub(\varphi)|$.*

Sketch of the proof: Let $M = (S, \pi, \mathcal{K}, \mathcal{P})$ be a structure where φ is satisfiable.
Notice that we are on the single agent case, so, for instance, we denote $\mathcal{P}$ to be defined by $\mathcal{P}(1,s) : S_s \longrightarrow [0,1]$, for each $s \in S$.
Since $C1$ holds, $S_s \subseteq \mathcal{K}(s)$ for each state s.
We then assume without loss of generality that $\mathcal{K}$ is a single equivalent class, i.e. of the form $S \times S$: suppose $(M,s) \Vdash \varphi$, then construct a model $M^0 = (S^0, \pi^0, \mathcal{K}^0, \mathcal{P}^0)$ where S^0 is the equivalence class of $\mathcal{K}$ which includes s and π^0, $\mathcal{K}^0$ and $\mathcal{P}^0$ be the restriction of π, $\mathcal{K}$ and $\mathcal{P}$ to S^0. It is straightforward to conclude that $(M^0, s) \Vdash \varphi$ and indeed, $\mathcal{K}^0$ is a single equivalence class.

Since $C3$ holds it is easy to see that for distinct functions $\mathcal{P}_s$ and $\mathcal{P}_t$, for states $s \neq t$ the domains do not intersect each other: let $\mathcal{P}_s \neq \mathcal{P}_t$ and $v \in S_s \cap S_t$ then, by $C3$, $\mathcal{P}_s = \mathcal{P}_v = \mathcal{P}_t$ which is a contradiction.

We want to construct a model $M' = (S', \pi', \mathcal{K}', \mathcal{P}')$ which satisfies φ and has size polynomial in $|Sub\varphi|$. For this, using some results of linear programming, it is shown the existence of $\mathcal{P}'_s : S'_s \longrightarrow [0,1]$ for each state $s \in S$, where $|S'_s| \leq |Sub\varphi|$.

Now only remains to introduce some more states on S' (note that $S'_s \subseteq S'$). Let $w \in S$ be a state such that $(M, w) \Vdash \varphi$. For each formula $\xi = \neg K\psi \in \overline{Sub\varphi}$ such that $(M, w) \Vdash \xi$, collect on $F \subseteq S$ the state v_ξ where $(M, v_\xi) \Vdash \neg\psi$. To this set F add also the state w.

Notice that $|F| \leq 1 + |Sub\varphi|$.
Finally define S' to be $S' = \bigcup_{s \in F} S'_s$, π' to be the restriction of π to S', $\mathcal{K} = S' \times S'$ and $\mathcal{P}'(1, s) = \mathcal{P}'_s$.
Then it is easy to show M' verifies $C1$ and $C3$, $(M', v) \Vdash \varphi$ and it is obvious that M' has size polynomial in $|Sub\varphi|$. ■

3.3 Dynamic Probabilistic Epistemic Logic

We want our logic to be able to deal with communication between agents or even better, we want our logic to deal with updates of the information available to the agents. With this purpose, it is time to introduce a dynamical component in the logic, which allows us to reason about information changes. This section pretends to make an overview of the work in [3].

We return now to the n agents case.

3.3.1 Public Announcement Model

We begin introducing a kind of deterministic updates. In this subsection the updates are done in terms of *public announcements* of some true proposition A, $!A$. Intuitively, $[!A]\varphi$ means that "φ holds after the announcement that A holds".

Definition 3.3.1 *Consider n agents $1, \ldots, n$. The language for public announcements $\mathcal{L}_n^{KP[!]}$ has the following inductive syntax:*

$$\varphi ::= p \mid \neg\varphi \mid \varphi \wedge \psi \mid K_i\varphi \mid a_1 P_i(\varphi_1) + \cdots + a_n P_i(\varphi_n) \geq b \mid [!\varphi]\psi,$$

where $p \in \Phi$, $i \in \{1, \ldots, n\}$ and $a_1, \ldots, a_n, b \in \mathbb{Q}$.

Definition 3.3.2 *Let $\mathcal{L}_n^{KP[!]}$ the language for public announcements and $M = (S, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n, \mathcal{P})$ a Kripke structure for knowledge and probability over Φ. Let $s \in S$ be a state and $\varphi \in \mathcal{L}_n^{KP[!]}$ a formula.*

If φ is a probabilistic epistemic formula, then $\varphi \in \mathcal{L}_n^{KP}$ and the validity follows from Definition 3.2.4.

If φ is of the form $[!A]\xi$, for some formulas A and ξ, we define

$$(M,s) \Vdash [!A]\xi \quad \textit{if and only if} \quad (M,s) \Vdash A \ \textit{implies} \ (M|A,s) \Vdash \xi, \tag{3.16}$$

where the updated model $M|A = (S^A, \pi^A, \mathcal{K}_1^A, \ldots, \mathcal{K}_n^A, \mathcal{P}^A)$ is defined as follows:

$$\begin{array}{lcl} S^A & = & \{t \in S \mid (M,t) \Vdash A\} \\ \pi^A & = & \pi|_{S^A} \\ \mathcal{K}_j^A & = & \left\{(u,v) \in (S^A)^2 \mid (u,v) \in \mathcal{K}_j\right\} \\ dom(\mathcal{P}^A(j,t)) & = & \{v \in dom(\mathcal{P}(j,t)) \mid (M,v) \Vdash A\} \end{array}$$

$$\mathcal{P}^A(j,t)(v) = \begin{cases} \frac{\mathcal{P}(j,t)(v)}{\mathcal{P}(j,t)(A)} & \text{if } \mathcal{P}(j,t)(A) > 0 \\ \\ 0 & \text{otherwise} \end{cases}$$

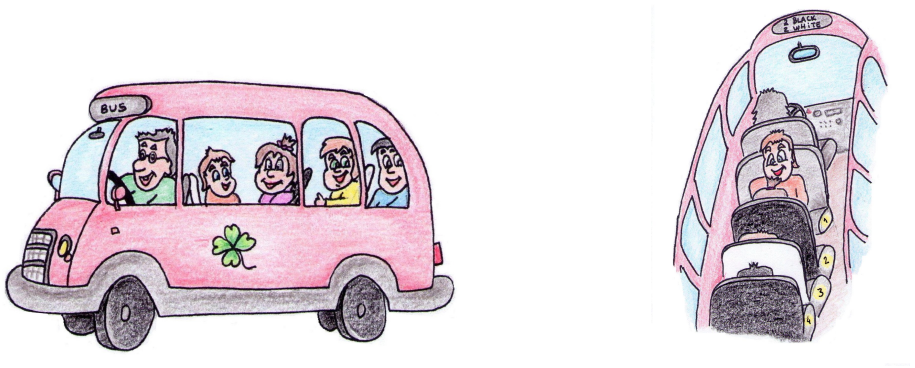
Intuitively, update with a given sentence A, $!A$, results on removing all the worlds where A does not hold. We restrict our attention to these worlds.

Moreover, we should concern ourselves with the possibility of updating with a sentence which has zero probability. In this case we define the probabilities of all the worlds to be equal to zero. There are other ways, no less controversial, to define these probabilities. It is still possible to let it undefined, however in a strictly formal point of view this issue can not be considered a real problem, as can be read in [3] and [2].

Notation: Let $\mathcal{M}_n^{KP[!]}$ denote the collection of Kripke structures for knowledge and probability for agents $1, \ldots, n$ over Φ and with the interpretation of validity for public announcements given by Definition 3.3.2.

Example 3.3.1 *Let us return to the bus trip. In the middle of the journey, the driver asks: "Do you know the color of your seat?".*
Immediately all of them answer "No!". The public announcement of passenger 4 saying he does not know the color of his seat makes passenger 3 immediately update his information and be sure his color is different from 2's color. Therefore, we should have

$$[!(\neg K_4 w_4 \wedge \neg K_4 \neg w_4)](K_3 w_3).$$



Let us see:

Note that when passenger 4 *announces he does not know the color of his seat, all the passengers become to know* 2 *and* 3 *have different colors, so* $\neg K_4 w_4 \wedge \neg K_4 \neg w_4$ *is equivalent to the disjunction of the following conjunctions of primitive propositions and their negations:*

$$\begin{array}{l} w_1 \wedge w_2 \wedge \neg w_3 \wedge \neg w_4 \\ \neg w_1 \wedge w_2 \wedge \neg w_3 \wedge w_4 \\ w_1 \wedge \neg w_2 \wedge w_3 \wedge \neg w_4 \\ \neg w_1 \wedge \neg w_2 \wedge w_3 \wedge w_4 \end{array} \tag{3.17}$$

Since agent 3 *knows* 2*'s color is black, agent* 3 *immediately considers just two worlds possible: the world labeled by* $w_1 \wedge \neg w_2 \wedge w_3 \wedge \neg w_4$ *and the world labeled by* $\neg w_1 \wedge \neg w_2 \wedge w_3 \wedge w_4$*. Then,*

$$\textit{for all } t \in \mathcal{K}_3(s^*), (M,t) \Vdash w_3, \textit{ so } (M,s^*) \Vdash K_3 w_3.$$

On the other hand, besides the fact that passengers 1 *and* 2 *do not become to know their colors, their information also changes: when passenger* 4 *announces he does not know his color, the probability that each passenger* 1 *and* 2 *assigns to the real world* s^* *becomes* $\frac{1}{4}$ *instead of* $\frac{1}{6}$ *as before. Let us present this easy calculation using the probability expression for public announcements:*

Since $\neg K_4 w_4 \wedge \neg K_4 \neg w_4$ *holds in all the worlds in (3.17),*

$$\mathcal{P}(1,s^*)(\neg K_4 w_4 \wedge \neg K_4 \neg w_4) = \sum_{s \in S \text{ st } (M,s) \Vdash \neg K_4 w_4 \wedge \neg K_4 \neg w_4} \mathcal{P}(1,s^*)(s) = \frac{4}{\binom{4}{2}} = \frac{4}{6}.$$

Before the public announcements we still have

$$\mathcal{P}(1, s^*)(s^*) = \frac{1}{6},$$

so we have the following probabilities after the public announcement of $\neg K_4 w_4 \wedge \neg K_4 \neg w_4$*:*

$$\mathcal{P}^{\neg K_4 w_4 \wedge \neg K_4 \neg w_4}(1, s^*)(s^*) = \frac{\frac{1}{6}}{\frac{4}{6}} = \frac{1}{4}.$$

The same way, $\mathcal{P}^{\neg K_4 w_4 \wedge \neg K_4 \neg w_4}(2, s^*)(s^*) = \frac{1}{4}$ *holds.*

Note that passenger 4 *does not change the information he had, he did not learn anything from his public announcement.*
Moreover, all passengers become to know what the other passengers know. □

Remark 3.3.3 *The reader should be aware that when a public announcement* $[!A]$ *is made,* A *must be true. However, it may be the case that after that* A *can turn to be false. A classical example is the public announcement of "you do not know that* p*, but* p *is true", this proposition become false after its public announcement.*

Let us introduce a dynamic component with public announcements in the inference system $\mathfrak{H}^{KP}$.

U1. $[!A]p \leftrightarrow (A \to p)$, where p is a primitive proposition;

U2. $[!A]\neg\varphi \leftrightarrow (A \to \neg[!A]\varphi)$;

U3. $[!A](\varphi \wedge \psi) \leftrightarrow ([!A]\varphi \wedge [!A]\psi)$;

U4. $[!A]K_i\varphi \leftrightarrow (A \to K_i(A \to [!A]\varphi))$;

U5. $P_i(A) > 0 \to ([!A]\left(\sum_{l=1}^{n} a_l P_i(\varphi_l) \geq b\right) \leftrightarrow \left(\sum_{l=1}^{n} a_l P_i(A \wedge [!A]\varphi_l) \geq b P_i(A)\right))$;

U6. $P_i(A) = 0 \to ([!A]\left(\sum_{l=1}^{n} a_l P_i(\varphi_l) \geq b\right) \leftrightarrow 0 \geq b)$.

Definition 3.3.4 *Let* $\mathfrak{H}^{KP[!]}$ *be the inference system obtained by joining* $\mathfrak{H}^{KP}$ *together with axioms* $U1$-$U6$ *and let* $\vdash_n^{KP[!]}$ *be the corresponding deductive system.*

Axioms $U1 - U6$ are recursive, the reader should note that each logical operator is moved from the dynamical language to the outside of the formulas involving $[!A]$.

$U1$ tells that A is a necessary precondition for $!A$ to occur, so we say that p is valid after the public announcement of A if whenever A holds, p holds. $U2$ and $U3$ are quite intuitive and follow from our notion of negation and conjunction. $U4$ is exactly what we expect to occur when after the public announcement of A, agent i knows φ: we should be careful with the precondition A and then ensure agent knows that whenever A holds, the public announcement of A turns φ valid.

$U5$ and $U6$ follows immediately from the expression of probability for public announcements: we restrict our attention to worlds where A is valid and therefore we need to require that A is valid and we must normalize the expression. Whenever $P(A) = 0$, probability 0 is assigned to all worlds.

Proposition 3.3.1 *Consider the deductive system* $\vdash_n^{KP[!]}$. *Then:*

If φ *is a Boolean formula, then*

$$[!A]\varphi \leftrightarrow (A \to \varphi) \tag{3.18}$$

If φ *is an epistemic formula and* B *is a Boolean formula, then*

$$[!A][!B]\varphi \longleftrightarrow [!(A \wedge [!A]B)]\,\varphi \tag{3.19}$$

$$\textit{If } A \textit{ is a Boolean formula, then } [!A]K_iA \tag{3.20}$$

$$\textit{If } A \textit{ and } B \textit{ are Boolean formulas then } [!(A \wedge B)]K_iA \tag{3.21}$$

Proof:

(3.18) The proof is done recursively on the structure of φ.
If φ is a primitive proposition it resumes to $U1$.

Suppose (3.18) holds for any subformula of φ. (IH)
Let $\varphi = \neg\psi$.
Using $U2$, $[!A](\neg\psi)$ *iff* $(A \to \neg[!A]\psi)$. By (IH) this is equivalent to

$(A \to \neg(A \to \psi))$ *iff* $(A \to \neg(\neg A \vee \psi))$ *iff* $(A \to A \wedge \neg\psi)$ *iff*

$(\neg A \vee (A \wedge \neg\psi))$ *iff* $(\neg A \vee A) \wedge (\neg A \vee \neg\psi)$ *iff* $\neg A \vee \neg\psi$ *iff* $(A \to \neg\psi))$.

Now consider $\varphi = \psi \wedge \chi$,

By $U3$ $[!A](\psi \wedge \chi) \quad \textit{iff} \quad ([!A]\psi \wedge [!A]\chi)$.
Using again (IH), we equivalently have
$(A \to \psi) \wedge (A \to \chi) \quad \textit{iff} \quad (\neg A \vee \psi) \wedge (\neg A \vee \chi) \quad \textit{iff} \quad \neg A \vee (\psi \wedge \chi) \quad \textit{iff} \quad A \to \psi \wedge \chi.$

(3.19) If φ is a Boolean formula, using (3.18) we have:
$[!A][!B]\varphi \quad \textit{iff} \quad [!A](B \to \varphi) \quad \textit{iff} \quad (A \to (B \to \varphi)) \quad \textit{iff} \quad \neg A \vee (B \to \varphi) \quad \textit{iff}$

$\neg A \vee (\neg B \vee \varphi) \quad \textit{iff} \quad \neg A \vee \neg B \vee \varphi.$

On the other hand we have
$[!(A \wedge [!A]B)]\varphi \quad \textit{iff} \quad ((A \wedge [!A]B) \to \varphi) \quad \textit{iff} \quad ((A \wedge (A \to B)) \to \varphi) \quad \textit{iff}$

$((A \wedge (\neg A \vee B)) \to \varphi) \quad \textit{iff} \quad (((A \wedge \neg A) \vee (A \wedge B)) \to \varphi) \quad \textit{iff} \quad ((A \wedge B) \to \varphi) \quad \textit{iff}$

$\neg(A \wedge B) \vee \varphi \quad \textit{iff} \quad \neg A \vee \neg B \vee \varphi$

If $\varphi = K\psi$ we use induction and obtain the following equivalences:
$[!A][!B]K\psi$
$\textit{iff} \quad [!A]([!B]K\psi)$
$\textit{iff} \quad [!A](B \to K(B \to [!B]\psi))$
$\textit{iff} \quad [!A](B \to K(B \to \psi)$
$\textit{iff} \quad [!A](\neg B \vee K(B \to \psi))$
$\textit{iff} \quad [!A]\neg(B \wedge \neg K(B \to \psi))$
$\textit{iff} \quad A \to \neg[!A](B \wedge \neg K(B \to \psi))$
$\textit{iff} \quad A \to \neg((A \to B) \wedge (A \to \neg[!A]K(B \to \psi)))$
$\textit{iff} \quad A \to (\neg(A \to B) \vee \neg(A \to \neg(A \to K(A \to (B \to \psi)))))$
$\textit{iff} \quad \neg A \vee \neg(A \to B) \vee (A \wedge (A \to K(A \to (B \to \psi))))$
$\textit{iff} \quad \neg A \vee \neg(A \to B) \vee (A \wedge K(A \to (B \to \psi)))$
On the other side we have
$\textit{iff} \quad [!(A \wedge [!A]B)]K\psi)$
$\textit{iff} \quad [!(A \wedge (A \to B))]K\psi)$
$\textit{iff} \quad (A \wedge (A \to B)) \to K((A \wedge (A \to B)) \to \psi)$
$\textit{iff} \quad (A \wedge (A \to B)) \to A \wedge K((A \wedge (A \to B)) \to \psi)$
$\textit{iff} \quad (A \wedge (A \to B)) \to A \wedge K(\neg A \vee \neg(A \to B) \vee \psi)$
$\textit{iff} \quad (A \wedge (A \to B)) \to A \wedge K(\neg A \vee (A \wedge \neg B) \vee \psi)$
$\textit{iff} \quad (A \wedge (A \to B)) \to A \wedge K(\neg A \vee \neg B \vee \psi)$

(3.20) From $U4$ we have

$$[!A]K_iA \quad \textit{iff} \quad (A \to K_i(A \to [!A]A) \quad \textit{iff} \quad A \to K_i(A \to A) \quad \textit{iff} \quad A \to K_i(true) \quad \textit{iff} \quad true.$$

So $[!A]K_iA$ holds.

(3.21) The equivalences follow easily:

$$[!(A \wedge B)]K_iA \quad \textit{iff} \quad (A \wedge B \to K_i[!(A \wedge B)]A) \quad \textit{iff} \quad (A \wedge B \to K_i(A \wedge B \to A) \quad \textit{iff}$$
$$(A \wedge B \to K_i\, true) \quad \textit{iff} \quad true \qquad \blacksquare$$

Theorem 3.3.5 *$\mathfrak{H}^{KP[!]}$ is a sound axiomatization for the dynamic probabilistic epistemic logic for public announcements with respect to $\mathcal{M}_n^{KP[!]}$.*

Proof: We begin proving the validity of $U1$. Let p be a primitive proposition, we have the following equivalent steps:
$(M, w) \Vdash [!A]p \quad \textit{iff} \quad (M, w) \Vdash A$ implies $(M \mid A, w) \Vdash p$.
Denoting the interpretation function of $M \mid A$ as π^A as in Definition 3.3.2, since $\pi^A = \pi$, we have $(M \mid A, w) \Vdash p \quad \textit{iff} \quad (M, w) \Vdash p$ and it follows that

$$(M, w) \Vdash A \text{ implies } (M, w) \Vdash p, \text{i.e.,}$$

$$(M, w) \Vdash (A \to p).$$

Let us go on with $U2$,
$(M, w) \Vdash (A \to \neg[!A]\varphi) \quad \textit{iff}$
$(M, w) \Vdash A$ implies $(M, w) \Vdash \neg[!A]\varphi \quad \textit{iff}$
$(M, w) \Vdash A$ implies $(M, w) \nVdash [!A]\varphi \quad \textit{iff}$
$(M, w) \Vdash A$ implies $((M, w) \Vdash A$ and $(M \mid A, w) \nVdash \varphi)$
From propositional calculus, it can easily be shown the expression $(a \to a \wedge b) \leftrightarrow (a \to b)$ is valid, so we have
$(M, w) \Vdash A$ implies $(M \mid A, w) \nVdash \varphi \quad \textit{iff}$
$(M, w) \Vdash A$ implies $(M \mid A, w) \Vdash \neg\varphi \quad \textit{iff}$
$(M, w) \Vdash [!A]\neg\varphi$.

Axiom $U3$ also follows from the propositional calculus,
$(M, w) \Vdash [!A](\varphi \wedge \psi) \quad \textit{iff}$

$(M,w) \Vdash A$ implies $(M \mid A, w) \Vdash \varphi \wedge \psi$ *iff*
$(M,w) \Vdash A$ implies $((M \mid A, w) \Vdash \varphi$ and $(M \mid A, w) \Vdash \psi)$
From propositional calculus we can still prove the following expression is valid: $(a \rightarrow b \wedge c) \leftrightarrow (a \rightarrow b \wedge a \rightarrow c)$, so we have
$((M,w) \Vdash A$ implies $(M \mid A, w) \Vdash \varphi)$ and $((M,w) \Vdash A$ implies $(M \mid A, w) \Vdash \psi)$ *iff*
$(M,w) \Vdash [!A]\varphi \wedge [!A]\psi$.

Let us now verify validity of $U4$,
$(M,w) \Vdash A \rightarrow K_i(A \rightarrow [!A]\varphi)$ *iff*
$(M,w) \Vdash A$ implies $(M,w) \Vdash K_i(A \rightarrow [!A]\varphi)$ *iff*
$(M,w) \Vdash A$ implies for all state t such that $(w,t) \in \mathcal{K}_i, (M,t) \Vdash A$ implies $(M,t) \Vdash [!A]\varphi$
$(M,w) \Vdash A$ implies for all state t such that $(w,t) \in \mathcal{K}_i, (M,t) \Vdash A$ implies $((M,t) \Vdash A$ implies $(M \mid A, t) \Vdash \varphi)$ *iff*
$(M,w) \Vdash A$ implies for all state t st $(w,t) \in \mathcal{K}_i, (M,t) \Vdash A$ implies $(M \mid A, t) \Vdash \varphi$ *iff*
$(M,w) \Vdash A$ implies for all state t such that $(w,t) \in \mathcal{K}_i^A, (M \mid A, t) \Vdash \varphi$ *iff*
$(M,w) \Vdash [!A]K_i\varphi$.

For $U5$, let $s \in S$ be a state. Suppose $(M,s) \Vdash P_i(A) > 0$ i.e. $\mathcal{P}(i,s)(A) > 0$, then, for each formula φ, we have
$\mathcal{P}^A(i,s)(\varphi) = \sum_{v \in dom(\mathcal{P}^A(i,s)) \text{ st } (M|A,v) \Vdash \varphi} \mathcal{P}^A(i,s)(v) =$

$= \frac{\sum_{v \in dom(\mathcal{P}^A(i,s)) \text{ st } (M|A,v) \Vdash \varphi} \mathcal{P}(i,s)(v)}{\mathcal{P}(i,s)(A)} = \frac{\sum_{v \in dom(\mathcal{P}(i,s)) \text{ st } (M,v) \Vdash A \text{ and } (M,v) \Vdash [!A]\varphi} \mathcal{P}(i,s)(v)}{\mathcal{P}(i,s)(A)} =$
$= \frac{\mathcal{P}(i,s)(A \wedge [!A]\varphi)}{\mathcal{P}(i,s)(A)}$

It follows that

$(M,s) \Vdash [!A]\,(\sum_{l=1}^n a_l P_i(\varphi_l) \geq b)$ *iff* $(M,s) \Vdash (\sum_{l=1}^n a_l P_i(A \wedge [!A]\varphi_l) \geq b P_i(A))$.

For $U6$, let $s \in S$ be a state and suppose $(M,s) \Vdash P_i(A) = 0$ i.e. $\mathcal{P}(i,s)(A) = 0$, then for each formula φ,

$\mathcal{P}^A(i,s)(\varphi) = \sum_{u \in dom(\mathcal{P}^A(i,s)) \text{ st } (M|A,u) \Vdash \varphi} \mathcal{P}^A(i,s)(v) = \sum_{u \in dom(\mathcal{P}^A(i,s)) \text{ st } (M|A,u) \Vdash \varphi} 0 = 0.$
So we have
$(M,s) \Vdash [!A]\,(\sum_{l=1}^n a_l P_i(\varphi_l) \geq b)$ *iff* $(M,s) \Vdash 0 \geq b$. ■

To prove completeness we need to move a formula from the dynamic system for the static one. Let us define a *translation* function which will take us from dynamic probabilistic epistemic logic to probabilistic epistemic logic. Since $\mathfrak{H}^{KP}$ is complete for the probabilistic epistemic logic, we just need to prove that a formula is provably equivalent in $\mathfrak{H}^{KP[!]}$ to its translation.

Definition 3.3.6 *Let Φ be the set of primitive propositions and $\mathcal{L}_n^{KP[!]}$ and $\mathcal{L}_n^{KP}$ denote the language for public announcements and probabilistic epistemic language, respectively. We define the translation function $\tau : \mathcal{L}_n^{KP[!]} \longrightarrow \mathcal{L}_n^{KP}$ recursively as follows:*

i. $\tau(p) = p$

ii. $\tau(\neg\varphi) = \neg\tau(\varphi)$

iii. $\tau(\varphi \wedge \psi) = \tau(\varphi) \wedge \tau(\psi)$

iv. $\tau(K_i\varphi) = K_i\tau(\varphi)$

v. $\tau\left(\sum_{l=1}^{n} a_l P_i(\varphi_l) \geq b\right) = \left(\sum_{l=1}^{n} a_l P_i(\tau(\varphi_l)) \geq b\right)$

vi. $\tau([!A]p) = (\tau(A) \rightarrow p)$

vii. $\tau([!A]\neg\varphi) = (\tau(A) \rightarrow \neg\tau([!A]\varphi))$

viii. $\tau([!A](\varphi \wedge \psi)) = \tau([!A]\varphi) \wedge \tau([!A]\psi)$

ix. $\tau([!A]K_i\varphi) = (\tau(A) \rightarrow K_i(\tau(A) \rightarrow \tau([!A]\varphi)))$

x. $\tau\left([!A]\sum_{l=1}^{n} a_l P_i(\varphi_l) \geq b\right) = (P_i(\tau(A)) > 0 \wedge (\sum_{l=1}^{n} a_l P_i(\tau(A) \wedge \tau([!A]\varphi_l)) \geq bP_i(\tau(A))) \vee$

$$\vee\, (P_i(\tau(A)) = 0 \wedge 0 \geq b))$$

Lemma 3.3.7 *For every formula $\xi \in \mathcal{L}_n^{KP[!]}$, ξ is provably equivalent in $\vdash_n^{KP[!]}$ to the sentence $\tau(\xi) \in \mathcal{L}_n^{KP}$.*

Proof: The proof is done by induction.
If ξ is a primitive proposition, obviously ξ is provably equivalent to $\tau(\xi)$.
Now assume the claim holds for all subformulas of ξ. (IH)
If ξ is of the form $\xi = \neg\varphi$, by (IH), φ is provably equivalent to $\tau(\varphi)$, then ξ is provably equivalent to

$$\neg\tau(\varphi).$$

The proofs for iii.,iv. and v. are analogous.
Now suppose $\xi = [!A]p$. By $U1$, $[!A]p \leftrightarrow A \rightarrow p$, therefore $[!A]p$ is provably equivalent to $\tau(A) \rightarrow p$ if and only if $A \rightarrow p$ is provably equivalent to $\tau(A) \rightarrow p$, which is provided by (IH).
The proofs for vii, viii, ix and x result from the same arguments. Note that all of them are the instance of an axiom. ■

Theorem 3.3.8 *$\mathfrak{H}^{KP[!]}$ is a weakly complete axiomatization for the dynamic probabilistic epistemic logic for public announcements with respect to $\mathcal{M}_n^{KP[!]}$.*

Proof: We already saw $\mathfrak{H}^{KP}$ is a complete axiomatization with respect to the semantics of probabilistic epistemic language. By Lemma 3.3.7, every sentence $\varphi \in \mathcal{L}_n^{KP[!]}$ is provably equivalent to $\tau(\varphi) \in \mathcal{L}_n^{KP}$ in $\mathfrak{H}^{KP[!]}$. Since any sentence $\psi \in \mathcal{L}_n^{KP}$ can be proved using the inference system $\mathfrak{H}^{KP}$, we have $\mathfrak{H}^{KP[!]}$ is a complete axiomatization for the dynamic probabilistic epistemic logic with respect to $\mathcal{M}_n^{KP[!]}$.
The weakness follows from the weak completeness of $\mathfrak{H}^{KP}$. ■

Corollary 3.3.9 *The language for public announcements is just as expressive as the probabilistic epistemic language.*

3.3.2 Product Update Logic

In the logic with public announcements the updates are deterministic. Now we improve the logic for updates that have an associated uncertainty. Now the updates are represented by the occurrence of events. See the next definition.

Definition 3.3.10 *A probabilistic event model for n agents $1, \ldots, n$ is defined to be a structure $\mathbb{E} = (E, \Psi, Pre, \mathcal{P}^{\mathbb{E}})$, where E is a non-empty set of events, Ψ is a set of pairwise inconsistent sentences, the function $Pre : \Psi \times E \longrightarrow [0,1]$ is such that for each fixed $\psi \in \Psi$, $Pre(\psi, \cdot)$ is a probability function and $\mathcal{P}^{\mathbb{E}}$ is a probability assignment which assigns to each agent $i \in \{1, \ldots, n\}$ and event $e \in E$ a probability function $\mathcal{P}^{\mathbb{E}}(i, e) : E \longrightarrow [0,1]$.*

A probabilistic event model contains information about the allowed updates. There is a set of possible events E, a set Ψ which includes the preconditions for each event to occur and we associate to each $\psi \in \Psi$ the probability $Pre(\psi, e)$ of ψ to be a condition for e to occur, for any event $e \in E$.

Finally, since there is a chance of being unable to distinguish events, we associate a probabilistic assignment $\mathcal{P}^{\mathbb{E}}$ that for every agent i and event e assigns a probability function $\mathcal{P}^{\mathbb{E}}(i,e)$ that for each $e' \in E$ represents the probability $\mathcal{P}^{\mathbb{E}}(i,e)(e')$ that agent i assigns to event e' to occur given that actually e is the occurred event.

Notation: Let M be a probabilistic epistemic model and $s \in S$ be a state, we denote by $Pre(s,e)$ the value of $Pre(\varphi,e)$, where φ is the unique element of Ψ which is true at the state s. If no such φ exists, we assume $Pre(s,e) = 0$.

Definition 3.3.11 *Let E a set of events and consider n agents $1,\ldots,n$. The language for product update $\mathcal{L}_n^{KP[\,]}$ has the following inductive syntax:*

$$\varphi ::= p \mid \neg\varphi \mid \varphi \wedge \psi \mid K_i\varphi \mid a_1P_i(\varphi_1) + \cdots + a_nP_i(\varphi_n) \geq b \mid [e]\varphi \ ,$$

where $p \in \Phi$, $i \in \{1,\ldots,n\}$, $a_1,\ldots,a_n,b \in \mathbb{Q}$ and $e \in E$ is an event.

Definition 3.3.12 *Let $\mathcal{L}_n^{KP[\,]}$ the language for product update, $M = (S,\pi,\mathcal{K}_1,\ldots,\mathcal{K}_n,\mathcal{P})$ a Kripke structure for knowledge and probability over Φ and $\mathbb{E} = (E,\Psi,Pre,\mathcal{P}^{\mathbb{E}})$ a probabilistic event model. Let $s \in S$ be a state and $\varphi \in \mathcal{L}_n^{KP[\,]}$ a formula.*

If φ is a probabilistic epistemic formula, then $\varphi \in \mathcal{L}_n^{KP}$ and the validity follows from Definition 3.2.4.

If φ is of the form $[e]\psi$, for some formula ψ and event e, we define

$$(M,s) \Vdash [e]\psi \text{ if and only if for all } \xi \in \Psi, (M,s) \Vdash \xi \quad \text{implies} \quad (M \times \mathbb{E},(s,e)) \Vdash \psi, \tag{3.22}$$

where the product update model $M \times \mathbb{E}$ is defined by $M \times \mathbb{E} = (S',\pi',\mathcal{K}_1',\ldots,\mathcal{K}_n',\mathcal{P}')$ with

$$\begin{aligned}
S' &= \{(s,e) \in S \times E \mid Pre(s,e) > 0\} \\
\pi'(s,e) &= \pi(s), \quad \text{for all } (s,e) \in S' \\
\mathcal{K}_i' &= \left\{((s,e),(s',e)) \in (S')^2 \mid (s,s') \in \mathcal{K}_i\right\}
\end{aligned}$$

$$dom(\mathcal{P}'(i,(s,e))) = \{(s',e') \in dom(\mathcal{P}(i,s)) \times E \mid Pre(s',e') > 0\}$$

$$\mathcal{P}'(i,(s,e))(s',e') = \begin{cases} \frac{Pre(s',e')\mathcal{P}(i,s)(s')\mathcal{P}^{\mathbb{E}}(i,e)(e')}{\sum_{s'' \in S, e'' \in E} Pre(s'',e'')\mathcal{P}(i,s)(s'')\mathcal{P}^{\mathbb{E}}(i,e)(e'')} & \text{if } \textit{denominator} > 0 \\ 0 & \text{otherwise} \end{cases}$$

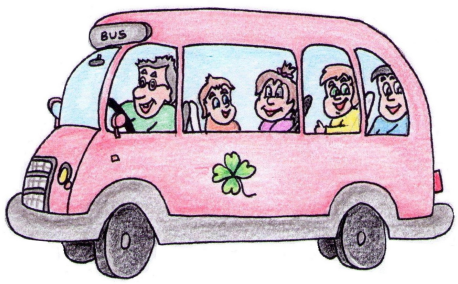
The states of the product update model are pairs (s,e) where the event e occurs at state s with positive probability. Since the events are non-deterministic, the expression of prob-

ability is now the product of all the probabilistic components involved in our model: the probability that agent i assigns for s' to occur given his information at state s, the chance of e' to occur at state s' and finally the probability of agent i to observe e' instead of e. To get a probability function in the end, we normalize the expression.

The degenerated case, i.e. when *denominator* $= 0$, is a problem similar to that mentioned for the public announcements case. And again in a strictly formal point of view this is not actually a real problem. We refer the reader to [3] and [2].

Remark 3.3.13 *Note that, except for the degenerated case, this product model is a probabilistic model and therefore we can take the same assumption as in the static case, for instance the condition* $C1$.

Notation: Let $\mathcal{M}_n^{KP[\,]}$ denote the collection of Kripke structures for knowledge and probability for agents $1, \ldots, n$ over Φ and with the interpretation of validity for updates with events given by Definition 3.3.12.



Example 3.3.2 *Suppose that the driver, instead of asking if any of the passengers know the color of their own seat, asked the passengers to name the color of any seat they could see.*

Let us analyze the behavior of passenger 4.

The action of passenger 4 *is not deterministic. He can possibly answer he knows* w_3 *or either he knows* $\neg w_2$.

First of all, we need to clarify what the probabilistic event model is for this case. Let $\mathbb{E} = (E, \Psi, Pre, \mathcal{P}^{\mathbb{E}})$, *where*

$\{!K_4 w_3, !K_4 w_2, !K_4 \neg w_2, !K_4 \neg w_3\} \subseteq E$.

Since we just worry with the case of agent 4, *we let the other events undefined. Notice that*

"!" here means again the act of publicly announce, but now this public announcement is probabilistic.
We abuse of notation and do not distinguish Ψ from the set of states S. Note that we usually denote the states by the values of its primitive propositions.
We define $Pre : \Psi \times E \longrightarrow [0,1]$ as

$$Pre(\varphi, !K_4 w_k) = \begin{cases} \frac{1}{2} & \text{if } \varphi \to w_k \\ 0 & \text{otherwise} \end{cases}$$

$$Pre(\varphi, !K_4 \neg w_k) = \begin{cases} \frac{1}{2} & \text{if } \varphi \to \neg w_k \\ 0 & \text{otherwise} \end{cases},$$

for $k \in \{1,2\}$.
And finally, since there is no chance of confusion about the event which takes place, $\mathcal{P}^{\mathbb{E}}$ is defined trivially,

$$\mathcal{P}^{\mathbb{E}}(i,e)(e') = \begin{cases} 1 & \text{if } e = e' \\ 0 & \text{otherwise} \end{cases}$$

Assume passenger 4 choose to answer he knows that w_3 holds. We should expect that, after that, the probability that agent 3 assigns to w_3 should be 1, as we will see right now.

Recall that at the beginning the set $\mathcal{K}_3(s^*) = dom(\mathcal{P}(3,s^*))$ has 3 states, i.e. passenger 3 at the beginning consider 3 possible states: he just know that $(M,s^*) \Vdash \neg w_2$. Moreover, note that $\mathcal{P}^{\mathbb{E}}$ being degenerated implies a huge simplification on the expression of product probability.

$$\mathcal{P}'(3,(s^*,!K_4w_3))(w_3) = \sum_{(s',!K_4w_3)\in\Gamma_{3,w_3}} \frac{\mathcal{P}'(3,(s^*,!K_4w_3))(s',K_4w_3)}{\sum_{s''\in S} Pre(s'',!K_4w_3)\mathcal{P}(3,s^*)(s'')} =$$

$$= \frac{\sum_{(s',!K_4w_3)\in\Gamma_{3,w_3}} Pre(s',!K_4w_3)\cdot\mathcal{P}(3,s^*)(s')}{2\cdot\frac{1}{2}\cdot\frac{1}{3}} = \frac{2\cdot\frac{1}{2}\cdot\frac{1}{3}}{2\cdot\frac{1}{2}\cdot\frac{1}{3}} = 1,$$

where $\Gamma_{k,\varphi} = \{(s,!K_4w_3) \mid s \in dom(\mathcal{P}'(k,(s^*,!K_4w_3)))and\ (M,(s,!K_4w_3)) \Vdash \varphi\}$, which means

$$(M,s^*) \Vdash [!K_4w_3]\,(P_3(w_3) = 1)\,.$$

Moreover, the probability that agent 2 assigns to $\neg w_2$ changes with the statement of passenger 4.

$$\mathcal{P}'(2,(s^*,!K_4w_3))(\neg w_2) = \sum_{(s',!K_4w_3)\in\Gamma_{2,\neg w_2}} \frac{\mathcal{P}'(2,(s^*,!K_4w_3))(s',!K_4w_3)}{\sum_{s''\in S} Pre(s'',!K_4w_3)\mathcal{P}(2,s^*)(s'')} = 2\frac{\frac{1}{2}\cdot\frac{1}{6}}{3\cdot\frac{1}{2}\frac{1}{6}} = \frac{2}{3},$$

i.e. $(M,s^*) \Vdash [!K_4w_3]\left(P_2(\neg w_2) = \frac{2}{3}\right)$. □

Notation: Let $\mathbb{E}$ be a probabilistic event model, and $e \in E$ an event. We say

$$(M,(s,e)) \Vdash P^{\mathbb{E}}(i,e)(e') = a \quad \textit{iff} \quad \mathcal{P}^{\mathbb{E}}(i,e)(e') = a.$$

To the inference system $\mathfrak{H}^{KP}$ we add some axioms that allow us to reason about product update.

PM1. $[e]p \;\leftrightarrow\; (\bigvee_{\xi\in\Psi, Pre(\xi,e)>0} \xi \to p)$, where p is a primitive proposition;

PM2. $[e]\neg\varphi \;\leftrightarrow\; (\bigvee_{\xi\in\Psi, Pre(\xi,e)>0} \xi \to \neg[e]\varphi)$;

PM3. $[e](\varphi\wedge\psi) \;\leftrightarrow\; ([e]\varphi \wedge [e]\psi)$;

PM4. $[e]K_i\varphi \;\leftrightarrow\; (\bigvee_{\xi\in\Psi, Pre(\xi,e)>0} \xi \to K_i(\bigvee_{\xi\in\Psi, Pre(\xi,e)>0} \xi \to [e]\varphi))$;

PM5. $\sum_{\xi\in\Psi,e'\in E} Pre(\xi,e')P_i(\xi)P^{\mathbb{E}}(i,e)(e') > 0 \to \Big([e]\sum_{l=1}^{k} a_l P_i(\varphi_l) \geq b \leftrightarrow$

$$\leftrightarrow \left(\sum_{\substack{\xi\in\Psi,e'\in E\\ 1\leq l\leq k}} a_l Pre(\xi,e')P_i(\xi\wedge[e']\varphi_l)P^{\mathbb{E}}(i,e)(e') \geq b\sum_{\substack{\xi\in\Psi\\ e'\in E}} Pre(\xi,e')P_i(\xi)P^{\mathbb{E}}(i,e)(e')\right)\Big)$$

PM6. $\sum_{\xi\in\Psi,e'\in E} Pre(\xi,e')P_i(\xi)P^{\mathbb{E}}(i,e)(e') = 0 \to \left([e]\sum_{l=1}^{k} a_l P_i(\varphi_l) \geq b \leftrightarrow 0 \geq b\right)$

Definition 3.3.14 *Let $\mathfrak{H}^{KP[\,]}$ be the inference system obtained by joining $\mathfrak{H}^{KP}$ together with axioms $PM1-PM6$ and let $\vdash_n^{KP[\,]}$ be the corresponding deductive system.*

Remark 3.3.15 *The public announcement approach is a particular case of the product update approach. Note that in the dynamical model with public announcements the disjunction $\bigvee_{\xi\in\Psi,Pre(\xi,!A)>0}\xi$ reduces to A and $\mathcal{P}^{\mathbb{E}}$ is degenerated.*

The motivation for axioms $PM1-PM6$ is a kind of generalization of the one we gave for $U1-U6$. As remarked before, we just need to keep in mind what the preconditions are on each approach.

Theorem 3.3.16 *$\mathfrak{H}^{KP[\,]}$ is a sound axiomatization for the dynamic probabilistic epistemic logic with product update with respect to $\mathcal{M}_n^{KP[\,]}$.*

Proof: The proof of soundness for product update is very similar to the one with public announcements, we just need to rename "A" just as the Remark 3.3.15 tells us.
Let us begin proving validity of $PM1$. Let p be a primitive proposition and $w \in S$ be any state. By definition of semantics,

$$(M,w) \Vdash [e]p \quad \textit{iff} \quad \text{for all } \xi \in \Psi \ (M,w) \Vdash \xi \text{ implies } (M \times \mathbb{E}, (w,e)) \Vdash p.$$

Denoting the interpretation function of $M \times \mathbb{E}$ as π', we have $\pi'(w,e) = \pi(w)$. Moreover, $(w,e) \in S'$ only if $Pre(\xi, e) > 0$ where ξ is the unique element of Ψ such that $(M,w) \Vdash \xi$. Then we can write equivalently

$$(M,w) \Vdash [e]p \quad \textit{iff} \quad \text{for all } \xi \in \Psi \ st \ Pre(\xi,e) > 0 \text{ if } (M,w) \Vdash \xi \text{ implies } (M,w) \Vdash p, \text{ i.e.}$$

$$(M,w) \Vdash [e]p \quad \textit{iff} \quad (M,w) \Vdash \left(\bigvee_{\xi \in \Psi, Pre(\xi,e)>0} \xi \to p \right).$$

For $PM2$, $PM3$ and $PM4$ the trick is the same.

Now let us prove validity of $PM5$: let $s \in S$ be a state.
Suppose $(M,s) \Vdash \sum_{\xi \in \Psi, e' \in E} Pre(\xi, e') P_i(\xi) P^{\mathbb{E}}(i,e)(e') > 0$, i.e.,

$$\sum_{\xi \in \Psi, e' \in E} Pre(\xi, e') \mathcal{P}(i,s)(\xi) \mathcal{P}^{\mathbb{E}}(i,e)(e') > 0,$$

then for each formula φ and denoting the probability assignment of $M \times \mathbb{E}$ to be $\mathcal{P}'$, we have

$$\mathcal{P}'(i,(s,e))(\varphi) = \sum_{(v,e') \in dom(\mathcal{P}'(i,(s,e)))\ st\ (M \times \mathbb{E}, (v,e')) \Vdash \varphi} \mathcal{P}'(i,(s,e))(v,e') =$$

$$= \frac{\displaystyle\sum_{(v,e') \in dom(\mathcal{P}'(i,(s,e)))\ st\ (M \times \mathbb{E}, (v,e')) \Vdash \varphi} Pre(v,e') \mathcal{P}(i,s)(v) \mathcal{P}^{\mathbb{E}}(i,e)(e')}{\displaystyle\sum_{s'' \in S, e'' \in E} Pre(s'',e'') \mathcal{P}(i,s)(s'') \mathcal{P}^{\mathbb{E}}(i,e)(e'')} =$$

$$= \frac{\displaystyle\sum_{e' \in E, v \in dom(\mathcal{P}(i,s))\ st\ Pre(v,e')>0, (M \times \mathbb{E}, (v,e')) \Vdash \varphi} Pre(v,e') \mathcal{P}(i,s)(v) \mathcal{P}^{\mathbb{E}}(i,e)(e')}{\displaystyle\sum_{s'' \in S, e'' \in E} Pre(s'',e'') \mathcal{P}(i,s)(s'') \mathcal{P}^{\mathbb{E}}(i,e)(e'')} =$$

Since $Pre(v,e') > 0$, by the Notation introduced in the beginning of this section, there is some $\xi \in \Psi$ such that $(M,v) \Vdash \xi$ and $Pre(\xi,e') =: Pre(v,e') > 0$, so we still have

$$\frac{\sum_{\substack{e'\in E, v\in dom(\mathcal{P}(i,s)) \text{ st } (M\times\mathbb{E},(v,e'))\Vdash\varphi \text{ and} \\ \text{for all } \xi\in\Psi \text{ if },(M,v)\Vdash\xi \text{ then } Pre(\xi,e')>0}} Pre(\xi,e')\mathcal{P}(i,s)(v)\mathcal{P}^{\mathbb{E}}(i,e)(e')}{\sum_{s''\in S,e''\in E} Pre(s'',e'')\mathcal{P}(i,s)(s'')\mathcal{P}^{\mathbb{E}}(i,e)(e'')} =$$

$$= \frac{\sum_{e'\in E,\xi\in\Psi} Pre(\xi,e')\mathcal{P}(i,s)(\xi\wedge[e']\varphi)\mathcal{P}^{\mathbb{E}}(i,e)(e')}{\sum_{s''\in S,e''\in E} Pre(s'',e'')\mathcal{P}(i,s)(s'')\mathcal{P}^{\mathbb{E}}(i,e)(e'')}.$$

It follows that

$$(M,s) \Vdash [e]\left(\sum_{l=1}^{n} a_l P_i(\varphi_l) \geq b\right) \quad \textit{iff}$$

$$(M,s) \Vdash \sum_{\substack{e'\in E,\xi\in\Psi \\ 1\geq l\geq n}} a_l Pre(\xi,e') P_i(\xi\wedge[e']\varphi) P^{\mathbb{E}}(i,e)(e') \geq b \sum_{\substack{\xi''\in\Psi \\ e''\in E}} Pre(\xi,e'') P_i(\xi) P^{\mathbb{E}}(i,e)(e'').$$

$PM6$ is immediate from the definition of the probability assignment for the product update. ■

For this product update approach, completeness also results from the completeness of the static model. So let us construct our translation function in the same way as we did for public announcements.

Definition 3.3.17 *Let Φ be the set of primitive propositions, $\mathbb{E}$ a probabilistic event model and $\mathcal{L}_n^{KP[\,]}$ and $\mathcal{L}_n^{KP}$ denote the language for product update and probabilistic epistemic language, respectively. We define the translation function $\tau : \mathcal{L}_n^{KP[\,]} \longrightarrow \mathcal{L}_n^{KP}$ recursively as follows:*

i. $\tau(p) = p$

ii. $\tau(\neg\varphi) = \neg\tau(\varphi)$

iii. $\tau(\varphi\wedge\psi) = \tau(\varphi)\wedge\tau(\psi)$

iv. $\tau(K_i\varphi) = K_i\tau(\varphi)$

v. $\tau\left(\sum_{l=1}^{n} a_l P_i(\varphi_l) \geq b\right) = \left(\sum_{l=1}^{n} a_l P_i(\tau(\varphi_l)) \geq b\right)$

vi. $\tau([e]p) = (\tau(\bigvee_{\varphi\in\Psi, Pre(\varphi,e)>0} \varphi) \to p)$

vii. $\tau([e]\neg\varphi) = (\tau(\bigvee_{\varphi\in\Psi, Pre(\varphi,e)>0} \varphi) \to \neg\tau([e]\varphi))$

viii. $\tau([e](\varphi \wedge \psi)) = \tau([e]\varphi) \wedge \tau([e]\psi)$

ix. $\tau([e]K_i\varphi) = (\tau(\bigvee_{\varphi\in\Psi, Pre(\varphi,e)>0} \varphi) \to K_i(\tau(\bigvee_{\varphi\in\Psi, Pre(\varphi,e)>0} \varphi) \to \tau([e]\varphi)))$

x. $$\tau\left([e]\sum_{l=1}^{n} a_l P_i(\varphi_l) \geq b\right) = \Bigg(\Big(\textstyle\sum_{\xi\in\Psi, e'\in E} Pre(\xi,e')P_i(\tau(\xi))\mathcal{P}^{\mathbb{E}}(i,e)(e') > 0\Big) \wedge$$

$$\wedge \left(\sum_{\substack{\xi\in\Psi, e'\in E \\ 1\leq l\leq k}} a_l Pre(\xi,e')P_i(\tau(\xi)\wedge\tau([e']\varphi))\mathcal{P}^{\mathbb{E}}(i,e)(e') \geq b \sum_{\substack{\xi\in\Psi \\ e'\in E}} Pre(\xi,e')P_i(\tau(\xi))\mathcal{P}^{\mathbb{E}}(i,e)(e')\right)\Bigg) \vee$$

$$\vee \left(\left(\sum\nolimits_{\substack{\xi\in\Psi \\ e'\in E}} Pre(\xi,e')P_i(\tau(\xi))\mathcal{P}^{\mathbb{E}}(i,e)(e') = 0\right) \wedge (0 \geq b)\right)$$

Lemma 3.3.18 *For every formula $\xi \in \mathcal{L}_n^{KP[\,]}$, ξ is provably equivalent in $\vdash_n^{KP[\,]}$ to the sentence $\tau(\xi) \in \mathcal{L}_n^{KP}$.*

Proof: Similar to Lemma 3.3.7.

Now completeness is immediate.

Theorem 3.3.19 *$\mathfrak{H}^{KP[\,]}$ is a weakly complete axiomatization for the dynamic probabilistic epistemic logic for product update with respect to $\mathcal{M}_n^{KP[\,]}$.*

Corollary 3.3.20 *The language for product update is just as expressive as the probabilistic epistemic language.*

Chapter 4

Applications

We present two applications that represent important aspects of the information security logics we wish to develop in the future. The first depicts a simplified approach of a typical problem toward cryptanalysis. The second is developed around the notion of computational indistinguishability.

4.1 Mastermind

In the first situation, we apply our logic to a problem which is similar to the usual problems associated with cryptanalysis in information security - the Mastermind game.

Briefly, the game of Mastermind is developed with the aim of a player discover a secret. This is a known game, but we decided to simplify it, here we do not allow the secret to be any word but rather a binary word.

In the cryptanalytic point of view, most of the times, when there is a secret to discover and an attacker who interacts with a system, we assume that we are in the presence of a single-agent case because we rely on the analysis of the attacker's behavior. This particularization of such a cryptanalytic problem to a game will also take only one agent into account.

Let $m = (m_1, \ldots, m_a)$ be the secret to save. To discover the secret the attacker is allowed to make some bets on potential secrets. Bets are placed sequentially and for each bet $p_1, \cdots p_a$ the attacker gets an answer $s \in \{1, \ldots, a\}$ representing the number of bits of the

bet that match with the secret, $s = \#\{i \mid p_i = m_i, i \in \{1, \ldots, a\}\}$. Note that if the answer is a the player actually guessed the secret. We assume that the answer is obtained by the agent through some mechanism of dealing with the secret message he can not access, but from which he can obtain his answer.

Let us try to model this problem.

The set of primitive propositions of our model is $\Phi = \{m_n\}_{n\in\mathbb{N}}$. Nevertheless, for a secret with length a we just care with $\{m_1, \ldots, m_a\}$, where a is the length of the secret and $m_i \in \{0, 1\}$ is the i^{th} bit of the secret. We pretend to construct a model $M = (S, \pi, \mathcal{K}, \mathcal{P})$ that represents this game, and we make it as follows.

The set of states S should represent all possible combinations of bits of the secret, i.e. all the combinations that the agent can consider to be possible

$$S = \{0, 1\}^a.$$

Since we label the states with the values of the primitive propositions on each state, defining the identification function π is straightforward.

In the beginning, our attacking agent is supposed not to know any bit of the secret, so he should not be able to distinguish any two states. Thus the knowledge relation should be defined by $\mathcal{K} = S^2$.

Observation: Defining the binary relation $\mathcal{K} = S^2$ implies that at the beginning we have

$$\bigwedge_{i=1}^{a} (\neg K m_i \wedge \neg K \neg m_i).$$

At the beginning, the attacker should assign the same probability to all worlds, so, for each $s \in S$ we define

$$\begin{array}{rccc} \mathcal{P}(s): & S & \longrightarrow & [0,1] \\ & s' & \mapsto & \frac{1}{2^a} \end{array}$$

As a consequence of this construction we have, for each state $s \in S$ and $i \in \{1, \ldots, a\}$,

$$(M, s) \Vdash \left(P(m_i) = \frac{1}{2}\right) \wedge \left(P(\neg m_i) = \frac{1}{2}\right). \tag{4.1}$$

The reader just need to note, for instance that

$$\mathcal{P}(s)(m_i) = \sum_{s' \in S \text{ st } (M,s') \Vdash m_i} \mathcal{P}(s)(s') = 2^{a-1} \cdot \frac{1}{2^a} = \frac{1}{2}.$$

Notation: In the single agent case, instead of writing $\mathcal{P}(1, s)$ as denoted for the n agents case, we write $\mathcal{P}(s)$.

Since we often are going to use the primitive propositions and their negations, let us define a function D which helps us to represent the negation of a bit. If x is a Boolean formula, $D_\bullet(x)$ is defined as

$$\begin{cases} D_1(x) &= \neg x \\ D_0(x) &= x \end{cases} \tag{4.2}$$

Each state s of our set of states S has a corresponding combination $D_{r_1^s}(m_1) \cdots D_{r_n^s}(m_a)$ of primitive propositions and their negations that characterizes the state uniquely. Let us label each state s by such combination.

4.1.1 Smart Strategy

To guess the secret, the player must place bets. We model these bets as actions and denote the bet of the sequence $p_1 \cdots p_a$ by $[p_1 \cdots p_a]$.

There are several ways of attacking the problem. In this subsection we assume that the intruder is clever and will assimilate all the answers that arises from his bets.

So, whenever he makes a bet, the attacker should have autonomy to eliminate all the states whose combination of bits does not match with the answer he got.

To the inference system presented for the dynamic probabilistic epistemic logic with public announcements for the single-agent case we add an axiom that allows us to model the transitions between states in this specific strategy.

M1. $A_s^{p_1,\ldots,p_a} \longrightarrow ([p_1 \cdots p_a]\,\varphi \leftrightarrow [!A_s^{p_1,\ldots,p_a}]\,\varphi)$, $s = 0, 1, \ldots, a$

where $A_s^{p_1,\ldots,p_a}$ characterizes exactly the states where the answer to $p_1, \ldots, p_a$ is s:

$$A_s^{p_1,\ldots,p_a} = \bigvee_{j_1,\ldots,j_s \in \{1,\ldots,a\}} \left(\left(\bigwedge_{k=1}^{s} \neg D_{p_{j_k}}(m_{j_k}) \right) \wedge \left(\bigwedge_{l \neq j_1,\ldots,j_s} D_{p_l}(m_l) \right) \right). \tag{4.3}$$

In particular,

$$A_0^{p_1,\ldots,p_a} = D_{p_1}(m_1) \wedge \ldots D_{p_a}(m_n)$$

and

$$A_a^{p_1,\ldots,p_a} = \neg D_{p_1}(m_1) \wedge \ldots \wedge \neg D_{p_a}(m_a).$$

Note that the last one represents the case where the bet $p_1, \ldots, p_a$ coincides exactly with the secret: the answer s is equal to a.

Intuitively $M1$ tells us that betting $p_1, \ldots, p_n$ is the same as performing a public announcement (defined just like in subsection 3.3.1) of the slice of states which coincides with the bet s bits.

Using (3.20) the following Lemma is immediate.

Lemma 4.1.1 *Axiom $M1$ implies that* $[p_1, \ldots, p_a]\left(\bigvee_{s\in\{0,1,\ldots,a\}} K A_s^{p_1,\ldots,p_a}\right)$*, i.e. when the agent makes a bet and gets answer s he immediately becomes to know the slice of the states corresponding to the answer s.*

Remark 4.1.2 *The result for the composition of bets follows easily from a simple induction argument:*

$$A_{u_1}^{p_1^1,\ldots,p_a^1} \wedge \ldots \wedge A_{u_l}^{p_1^l,\ldots,p_a^l} \longrightarrow \left([p_1^1, \ldots, p_a^1] \cdots [p_1^l, \ldots, p_a^l]\varphi \leftrightarrow [!A_{u_1}^{p_1^1,\ldots,p_a^1}] \cdots [!A_{u_l}^{p_1^l,\ldots,p_a^l}]\varphi\right)$$

For instance, let $l = 2$ and suppose $A_{u_1}^{p_1^1,\ldots,p_a^1} \wedge A_{u_2}^{p_1^2,\ldots,p_a^2}$. We have:

$$[p_1^1, \ldots, p_a^1][p_1^2, \ldots, p_a^2]\varphi \quad \textit{iff} \quad [p_1^1, \ldots, p_a^1]\left(\left[!A_{u_2}^{p_1^2,\ldots,p_a^2}\right]\varphi\right) \quad \textit{iff} \quad [!A_{u_1}^{p_1^1,\ldots,p_a^1}][!A_{u_2}^{p_1^2,\ldots,p_a^2}]\varphi.$$

We need now to define some standard bets.

Notation: For each $i, k \in \{1, \ldots, a\}$, define $(e_0)_i = 1$ and $(e_k)_i = \delta_i^k$.

The reader should recognize that when the agent bets e_0, the answer he gets is the number of elements of the set $\{i \in \{1, \ldots, a\} \mid m_i \text{ holds } \}$, intuitively this is the number of ones in the secret.

Now we prepare some results that we will use on a special strategy - the *smart strategy* - that we will present later.

Lemma 4.1.3 $A_u^{e_0} \longleftrightarrow A_{a-u+1}^{e_k} \vee A_{a-u-1}^{e_k}$

Proof:

$$A_u^{e_0} = \neg D_{e_0^k}(m_k) \wedge \Big(\bigvee_{j_1,\ldots,j_{u-1} \in \{1\ldots n\}\setminus\{k\}} \Big(\Big(\bigwedge_{j_r = j_1,\ldots,j_{u-1}} \neg D_{e_0^{j_r}}(m_{j_r}) \Big) \wedge \Big(\bigwedge_{j_l \neq j_1\ldots,j_{u-1}} D_{e_0^{j_l}}(m_{j_l}) \Big) \Big) \Big)$$

$$\vee D_{e_0^k}(m_k) \wedge \Big(\bigvee_{i_1,\ldots,i_u \in \{1,\ldots,n\}\setminus\{k\}} \Big(\Big(\bigwedge_{i_r = i_1,\ldots,i_u} \neg D_{e_0^i}(m_{i_r}) \Big) \wedge \Big(\bigwedge_{i_l \neq i_1,\ldots,i_u} D_{e_0^{i_l}}(m_{i_l}) \Big) \Big) \Big)$$

$$\longleftrightarrow \neg D_{e_k^k}(m_k) \wedge \Big(\bigvee_{j_1,\ldots,j_{u-1} \in \{1,\ldots,n\}\setminus\{k\}} \Big(\Big(\bigwedge_{j_r = j_1,\ldots j_{u-1}} D_{e_k^{j_r}}(m_{j_r}) \Big) \wedge \Big(\bigwedge_{j_l \neq j_1,\ldots,j_{u-1}} \neg D_{e_k^{i_l}}(m_{i_l}) \Big) \Big) \Big)$$

$$\vee D_{e_k^k}(m_k) \wedge \Big(\bigvee_{i_1,\ldots,i_u \in \{1,\ldots,n\}\setminus\{k\}} \Big(\Big(\bigwedge_{i_r = i_1,\ldots i_u} D_{e_k^{i_r}}(m_{i_r}) \Big) \wedge \Big(\bigwedge_{i_l \neq i_1,\ldots,i_u} \neg D_{e_k^{i_l}}(m_{i_l}) \Big) \Big) \Big)$$

$$\longleftrightarrow A^{e_k}_{(a-1)-(u-1)+1} \vee A^{e_k}_{(a-1)-u} \qquad \longleftrightarrow \qquad A^{e_k}_{a-u+1} \vee A^{e_k}_{a-u-1} \qquad \blacksquare$$

Since $e_k^k = 1$, from the previous proof we have $\neg D_{e_k^k}(m_k) = m_k$ and $D_{e_k^k}(m_k) = \neg m_k$. Therefore,

$$m_k \longleftrightarrow (A_u^{e_0} \leftrightarrow A^{e_k}_{a-u+1}) \tag{4.4}$$

$$\neg m_k \longleftrightarrow (A_u^{e_0} \leftrightarrow A^{e_k}_{a-u-1}) \tag{4.5}$$

Remark 4.1.4 *Under the assumptions of our Mastermind game, the semantics for the actions is defined as:*

$$(M,s) \Vdash [p_1,\ldots,p_a]\varphi \qquad \textit{if and only if} \qquad (M,s) \Vdash A_u^{p_1,\ldots,p_a} \ \textit{implies} \ (M|A_u^{p_1,\ldots,p_a}) \Vdash \varphi,$$

where $s \in S$ is a state, $\varphi \in \mathcal{L}^{KP[!]}$ is a formula, M is a Kripke structure for knowledge and probability and $A_u^{p_1,\ldots,p_a}$ is defined by (4.3).

After we have modeled the problem and we have shown some basic preliminary results, we now present a *smart strategy*, which is very particular but efficient. Then we prove if the attacker chooses the *smart strategy*, he will discover the secret with a finite number of bets.

Definition 4.1.5 *We define the smart strategy to be the following sequence of actions:* $[e_0][e_1]\ldots[e_a]$.

We want to prove that if the agent adopts this smart strategy, he will discover the secret. With this purpose, we will prove the following Lemma using both semantics and a formal proof.

Lemma 4.1.6 *For each $k \in \{1,\ldots,n\}$ we have $[e_0][e_k](Km_k \vee K\neg m_k)$.*

Semantic Proof of Lemma 4.1.6: Let $s \in S$ be a state and suppose $(M,s) \Vdash A_u^{e_0}$.
By Lemma 4.1.3, only two cases can occur:

$$(M,s) \Vdash A_u^{e_0} \wedge A^{e_k}_{a-u+1}$$

or

$$(M,s) \Vdash A_u^{e_0} \wedge A^{e_k}_{a-u-1}.$$

Suppose $(M,s) \Vdash A_u^{e_0} \wedge A_{a-u+1}^{e_k}$.

We have $(M \mid A_u^{e_0} \wedge A_{a-u+1}^{e_k}, s) \Vdash Km_k$ if and only if for all state t such that $(t,s) \in \mathcal{K}_i^{A_u^{e_0} \wedge A_{a-u+1}^{e_k}}$ we have

$$(M \mid A_u^{e_0} \wedge A_{a-u+1}^{e_k}, t) \Vdash m_k \tag{4.6}$$

By (4.4) $A_u^{e_0} \wedge A_{a-u+1}^{e_k} \rightarrow m_k$. Since $(M,t) \Vdash A_u^{e_0} \wedge A_{a-u+1}^{e_k}$ we have $(M,t) \Vdash m_k$.

By the definition of the updated model $M \mid A_u^{e_0} \wedge A_{a-u+1}^{e_k}$,

$$\pi^{A_u^{e_0} \wedge A_{a-u+1}^{e_k}} = \pi$$

therefore (4.6) holds.

And so $(M \mid A_u^{e_0} \wedge A_{a-u+1}^{e_k}, s) \Vdash Km_k$, then $(M \mid A_u^{e_0} \wedge A_{a-u+1}^{e_k}, s) \Vdash (Km_k \vee K\neg m_k)$

Analogously, $(M \mid A_u^{e_0} \wedge A_{a-u-1}^{e_k}, s) \Vdash (Km_k \vee K\neg m_k)$.

By Remark 4.1.4 we have $[e_0][e_k](Km_k \vee K\neg m_k)$, which ends the semantic proof. ■

Formal Proof of Lemma 4.1.6:
The following equivalences are valid

$$\text{By Remark 4.1.2} \quad A_u^{e_0} \wedge A_s^{e_k} \longrightarrow ([e_0][e_k]\phi \leftrightarrow [!A_u^{e_0}]\,[!A_s^{e_k}]\,\varphi) \quad \textit{iff} \tag{I}$$

$$\text{(using (3.19))} \quad A_u^{e_0} \wedge A_s^{e_k} \longrightarrow ([e_0][e_k]\phi \leftrightarrow [!\,(A_u^{e_0} \wedge [!A_u^{e_0}]\,A_s^{e_k})]\,\varphi) \quad \textit{iff}$$

$$\text{(using (3.18))} \quad A_u^{e_0} \wedge A_s^{e_k} \longrightarrow ([e_0][e_k]\phi \leftrightarrow [!\,(A_u^{e_0} \wedge (A_u^{e_0} \rightarrow A_s^{e_k}))]\,\varphi)\,.$$

Lemma 4.1.6 follows immediately from the following lemmas:

Lemma 4.1.7 $A_u^{e_0} \wedge A_{a-u+1}^{e_k} \longrightarrow [e_0][e_k]Km_k$

Proof of Lemma 4.1.7: Suppose $A_u^{e_0} \wedge A_{a-u+1}^{e_k}$.

(using (3.21)) $\left[\,!\,\left(A_u^{e_0} \wedge \left(A_u^{e_0} \to A_{a-u+1}^{e_k}\right)\right)\right] KA_u^{e_0} \wedge$

$\wedge\ \left[\left[\,!\,\left(A_u^{e_0} \wedge \left(A_u^{e_0} \to A_{a-u+1}^{e_k}\right)\right)\right] K\left(A_u^{e_0} \to A_{a-u+1}^{e_k}\right)\right.$ *iff*

(using $U3$) $\left[\,!\,\left(A_u^{e_0} \wedge\ A_u^{e_0} \to A_{a-u+1}^{e_k}\right)\right]\left(KA_u^{e_0} \wedge K\left(A_u^{e_0} \to A_{a-u+1}^{e_k}\right)\right)$ *then*

(using $K2$) $\left[\,!\,\left(A_u^{e_0} \wedge\ A_u^{e_0} \to A_{a-u+1}^{e_k}\right)\right]\left(KA_u^{e_0} \wedge KA_{a-u+1}^{e_k}\right)$ *iff*

(using (3.18)) $\left[\,!\,\left(A_u^{e_0} \wedge\ [!A_u^{e_0}]\, A_{a-u+1}^{e_k}\right)\right]\left(KA_u^{e_0} \wedge KA_{a-u+1}^{e_k}\right)$ *iff*

(using (3.19)) $[!A_u^{e_0}]\left[!A_{a-u+1}^{e_k}\right]\left(KA_u^{e_0} \wedge KA_{a-u+1}^{e_k}\right)$ *iff*

(using (3.6)) $[!A_u^{e_0}]\left[!A_{a-u+1}^{e_k}\right] K\left(A_u^{e_0} \wedge A_{a-u+1}^{e_k}\right)$ *then*

(using (4.4)) $[!A_u^{e_0}]\left[A_{a-u+1}^{e_k}\right] Km_k$ *iff*

(using (I)) $[e_0][e_k]Km_k,$

which ends the proof of Lemma 4.1.7. ■

Similarly we can prove

Lemma 4.1.8 $A_u^{e_0} \wedge A_{a-u-1}^{e_k} \longrightarrow [e_0][e_k]K\neg m_k$

From Lemmas 4.1.7 and 4.1.8, we still have

$$A_u^{e_0} \wedge A_{a-u+1}^{e_k} \to [e_0][e_k](Km_k \vee \neg Km_k)$$

and

$$A_u^{e_0} \wedge A_{a-u-1}^{e_k} \to [e_0][e_k](Km_k \vee \neg Km_k).$$

Since by Lemma 4.1.3, $A_u^{e_0} \longleftrightarrow A_{a-u+1}^{e_k} \vee A_{a-u-1}^{e_k}$ we get

$$\left(A_u^{e_0} \wedge A_{a-u+1}^{e_k}\right) \vee \left(A_u^{e_0} \wedge A_{a-u-1}^{e_k}\right) \longrightarrow [e_0][e_k]\left(Km_k \vee K\neg m_k\right)$$

which concludes the formal proof of Lemma 4.1.6. ■

The following theorem will also be proved with both the semantic and the formal approaches and tells us that is a *smart* strategy.

Theorem 4.1.9 *Performing the smart strategy the agent should discover the secret,*

$$[\,e_0\,]\,[\,e_1\,]\,\ldots\,[\,e_a\,]\bigwedge_{i=1}^{a}(Km_i \vee K\neg m_i).$$

Semantic Proof of 4.1.9:

To make this semantic proof, we need the following

Lemma 4.1.10 *Let φ and ψ be epistemic formulas.*
If

$$(M,s) \Vdash A \quad \textit{implies} \quad (M|A,s) \Vdash \varphi$$

and

$$(M,s) \Vdash B \quad \textit{implies} \quad (M|B,s) \Vdash \psi,$$

then $(M,s) \Vdash A \wedge B \quad \textit{implies} \quad (M \mid A \wedge B, s) \Vdash \varphi \wedge \psi$.

Proof: Suppose $(M,s) \Vdash A \wedge B$. We just need to prove for φ.

If φ is a primitive proposition, it follows from the definition of updated model that $\pi^{A\wedge B}(s)(\varphi) = \pi^{A}(s)(\varphi)$ and so we are done in this case.

Assume that $(M \mid A, s) \Vdash \xi \quad \textit{iff} \quad (M \mid (A \wedge B), s) \Vdash \xi$ for all subformulas ξ of φ. (IH)

If $\varphi = \neg\varphi'$, $(M \mid A \wedge B, s) \Vdash \neg\varphi' \quad \textit{iff} \quad (M \mid A \wedge B, s) \nVdash \varphi'$.

Since $(M \mid A, s) \Vdash \neg\varphi'$ i.e. $(M \mid A, s) \nVdash \varphi'$, the result follows applying (IH).

For $\varphi = \varphi_1 \wedge \varphi_2$ it is similar.

Now let φ be of the form $K_i\varphi'$ we have

$$(M \mid A \wedge B, s) \Vdash K_i\varphi' \quad \textit{iff} \quad \text{for all } t \in \mathcal{K}_i^{A\wedge B}(s), \ (M \mid A \wedge B, t) \Vdash \varphi' \tag{4.7}$$

We know that $(M \mid A, s) \Vdash K_i\varphi'$ so, for all $t \in \mathcal{K}_i^{A}(s)$, $(M \mid A, t) \Vdash \varphi'$.

Since $\mathcal{K}_i^{A\wedge B}(s) \subseteq \mathcal{K}_i^{A}(s)$, from (IH), (4.7) holds.

We proved that if φ is an epistemic formula, we have $(M \mid A \wedge B, s) \Vdash \varphi$. Similarly we can prove that $(M \mid A \wedge B, s) \Vdash \psi$.

By (3.3) we have $(M \mid A \wedge B, s) \Vdash \varphi \wedge \psi$, which ends the proof of Lemma 4.1.10. ■

Now let us prove we have $[e_0][e_1]\cdots[e_a]\bigwedge_{i=1}^{n}(Km_i \vee K\neg m_i)$.

By Remark 4.1.4, we want to prove that

$$(M,s) \Vdash \bigwedge_{i=1}^{a}(A_u^{e_0} \wedge A_{F_{m_i}(u)}^{e_i}) \quad \text{implies} \quad \left(M \mid \bigwedge_{i=1}^{a}\left(A_u^{e_0} \wedge A_{F_{m_i}(u)}^{e_i}\right), s\right) \Vdash \bigwedge_{i=1}^{a}(Km_i \vee K\neg m_i),$$

where $F_.(u)$ is defined as

$$\begin{cases} F_1(u) &= n-u+1 \\ F_0(u) &= n-u-1 \end{cases} \tag{4.8}$$

Suppose $(M,s) \Vdash \bigwedge_{i=1}^{a}(A_u^{e_0} \wedge A_{F_{m_i}(u)}^{e_i})$.

Indeed, by Lemmas 4.1.6 and 4.1.10 and using an inductive argument,

$$\left(M \mid \bigwedge_{i=1}^{a}(A_u^{e_0} \wedge A_{F_{m_i}(u)}^{e_i}), s\right) \Vdash \bigwedge_{i=1}^{a}(Km_i \vee K\neg m_i),$$

which concludes the semantic proof of Lemma 4.1.9. ■

Formal Proof of 4.1.9:

Let $\{A_n\}_{n\in\mathbb{N}}$ be Boolean formulas, we define formulas Δ_n recursively as:

$$\begin{aligned} &\Delta_1 := A_1 \\ &\Delta_n := \Delta_{n-1} \wedge \ (\Delta_{n-1} \to A_n) \quad \text{for } n > 1 \end{aligned}$$

Observation: Note that $\Delta_n \to \Delta_m$ for $m \leq n$.

Lemma 4.1.11 *If $A_1 \ldots, A_n$ are Boolean formulas, then $\Delta_n \longleftrightarrow A_1 \wedge \ldots \wedge A_n$*

Proof: Since $A \wedge B \longleftrightarrow A \wedge (A \to B)$ is a tautology, the proof is immediate. ■

Lemma 4.1.12 *If $A_1, \ldots, A_m$ are Boolean formulas then*

$$[!A_1] \ldots [!A_m]\,\varphi \quad \textit{iff} \quad (\Delta_m \to \varphi)$$

Proof: The proof is done by induction on m.
Let $m = 1$: $[!A_1]\varphi \quad \textit{iff} \quad A_1 \longrightarrow \varphi$.
Let $m = 2$:

$$\begin{aligned} [!A_1][!A_2]\varphi \quad & \textit{iff} \quad [!(A_1 \wedge [!A_1]A_2)]\varphi \\ & \textit{iff} \quad (A_1 \wedge [!A_1]A_2) \to \varphi \\ & \textit{iff} \quad (A_1 \wedge (A_1 \to A_2)) \to \varphi \\ & \textit{iff} \quad \Delta_2 \to \varphi. \end{aligned}$$

Now let $m \in \mathbb{N}$ and suppose that

$$[!A_1] \cdots [!A_m]\varphi \quad \textit{iff} \quad \Delta_m \to \varphi. \quad (IH)$$

We have

$$[!A_1] \cdots [!A_m][!A_{m+1}]\varphi \quad \textit{iff} \quad ([!A_1] \cdots [!A_m])\,[!A_{m+1}]\varphi.$$

By (IH), equivalently we get

$\Delta_m \to [!A_{m+1}]\varphi$
iff $[!\Delta_m][!A_{m+1}]\varphi$
iff $[!(\Delta_m \wedge [!\Delta_m]A_{m+1})]\varphi$
iff $(\Delta_m \wedge \Delta_m \to A_{m+1}) \to \varphi$
iff $\Delta_{m+1} \to \varphi$. ■

Lemma 4.1.13 *Let $A_1 \ldots, A_m$ be Boolean formulas. Then $\Delta_m \longrightarrow (A_1 \wedge \ A_1 \to A_m\ )$.*

Proof of Lemma 4.1.13:
Suppose Δ_m holds.
By Lemma 4.1.11, it implies $A_1 \wedge \ldots \wedge A_m$ is valid and it follows that:

$(A_1 \wedge \ldots \wedge A_m)$ *then* $(A_1 \wedge A_m)$ *iff* $A_1 \wedge (\ A_1 \wedge A_1 \to A_m)$ *iff*
iff $(A_1 \wedge A_1) \wedge A_1 \to A_m$ *iff* $A_1 \wedge A_1 \to A_m$ ■

Now is time to proof that the bets are commutative in this Mastermind game.

Lemma 4.1.14 *Let $A^{e_0}_{l_0}$ and $A^{e_k}_{l_k}$ be defined by (4.3). Then*

$$[!A^{e_0}_{l_0}][!A^{e_k}_{l_k}]\varphi \leftrightarrow [!A^{e_k}_{l_k}][!A^{e_0}_{l_0}]\varphi.$$

Proof: Let Δ_2^{0k} denote the formula Δ_2 defined recursively above adapted to $A^{e_0}_{l_0}$ and $A^{e_k}_{l_k}$ instead of A_1 and A_2, and Δ_2^{k0} defined the same way but this time with $A^{e_k}_{l_k}$ and $A^{e_0}_{l_0}$ instead of A_1 and A_2. By the previous results the equivalences follow:

$[!A^{e_0}_{l_0}][!A^{e_k}_{l_k}]\varphi$ *iff* $[!(A^{e_0}_{l_0} \wedge [!A^{e_0}_{l_0}]A^{e_k}_{l_k})]\varphi$ *iff* $[!(A^{e_0}_{l_0} \wedge A^{e_0}_{l_0} \to A^{e_k}_{l_k})]\varphi$ *iff* $[!\Delta_2^{0k}]\varphi$ *iff*

$[!(A^{e_0}_{l_0} \wedge A^{e_k}_{l_k})]\varphi$ *iff* $[!(A^{e_k}_{l_k} \wedge A^{e_0}_{l_0})]\varphi$ *iff* $[!\Delta_2^{k0}]\varphi$ *iff*

$[!(A^{e_k}_{l_k} \wedge A^{e_k}_{l_k} \to A^{e_0}_{l_0})]\varphi$ *iff* $[!A^{e_k}_{l_k}][!A^{e_0}_{l_0}]\varphi$. ■.

Lemma 4.1.15 *Let $A_1, \ldots, A_m$ be Boolean formulas and ψ be any formula, then*

$$[!A_1][!A_m]\psi \to [!A_1] \ldots [!A_m]\psi$$

Proof of Lemma 4.1.15: Suppose $[!A_1][\,!A_m]\ \psi$. By (3.18) this is equivalent to

$$(A_1 \wedge \ A_1 \to A_m) \to \psi.$$

Finally, by Lemma 4.1.13, Δ_m implies $(A_1 \wedge \ A_1 \to A_m)$, so $\Delta_m \to \psi$. ■

Assume $A_{l_0}^{e_0} \wedge A_{l_1}^{e_1} \wedge \ldots \wedge A_{l_a}^{e_a}$ holds. Then we get:

$$
\begin{array}{ll}
 & [e_0][e_1]\ldots[e_a]\bigwedge_{i=1}^{a}(Km_i \vee K\neg m_i) \qquad \text{(by Remark 4.1.2)} \\
\textit{iff} & [!A_{l_0}^{e_0}][!A_{l_1}^{e_1}]\ldots[!A_{l_a}^{e_a}]\bigwedge_{i=1}^{a}(Km_i \vee K\neg m_i) \qquad \text{(by } U3\text{)} \\
\textit{iff} & \bigwedge_{i=1}^{a}[!A_{l_0}^{e_0}][!A_{l_1}^{e_1}]\cdots[!A_{l_a}^{e_a}](Km_i \vee K\neg m_i) \qquad \text{(by Lemma 4.1.15)} \\
\text{if} & \bigwedge_{i=1}^{a}[!A_{l_0}^{e_0}][!A_{l_i}^{e_i}](Km_i \vee K\neg m_i) \qquad \text{(by Remark 4.1.2)} \\
\textit{iff} & \bigwedge_{i=1}^{a}[e_0][e_i](Km_i \vee K\neg m_i)
\end{array}
$$

By Lemma 4.1.6, $[e_0][e_i](Km_i \vee K\neg m_i)$ holds for each $i \in \{1, \ldots, a\}$, so

$$[e_0][e_1]\cdots[e_a]\bigwedge_{i=1}^{a}(Km_i \vee K\neg m_i)$$

which concludes the formal proof of Theorem 4.1.9. ■

4.1.2 Dumb strategy

Contrasting to the situation presented in the previous subsection, if the player is *dumb* and choose to play a strategy completely random and *blind* then *probably* he will not find out the secret in a polynomial number of bets.

The dumb strategy that the agent may be tempted to use consists of choosing a random combination of a bits and betting. After that he is just concerned with the fact that the bet coincides with the secret or not. If it does not match, being a blind strategy, the agent ignores completely the answer he gets from the bet and proceed as before, choosing again a combination of a bits randomly.

The previous strategy was a very well defined strategy in the sense that it was a fixed sequence of some specific bets that bring the attacker to the discovery of the secret. Nevertheless, in this approach of the game the actions are not deterministic so we need to use the product update logic to model it.

Define the probabilistic event model $\mathbb{E}$ to be $\mathbb{E} = (E, \Psi, Pre, \mathcal{P}^{\mathbb{E}})$, where E denote all the relevant bets $E = \{\textit{right bet}, \textit{wrong bet}\}$, where the $\textit{right bet} = D_{r_1^{s^*}}(m_1)\cdots D_{r_a^{s^*}}(m_a)$ with s^* denoting the real worlds and *wrong bet* represents the bet of any combination of primitive propositions and their negations other than the secret.

We would think that E should be the set of all possible bets, but the idea should be to distinguish the types of events that affect the system differently. Whenever the attacker makes a bet that is not the secret he should take the same information, regardless of the specific bet he does at each moment. However if he bets the secret, the behavior of the model should distinguish itself from the other situations.

$\Psi \equiv S$ is the set S. As we referred at Subsection 3.3.2 we will consider indifferently the state or its corresponding formula on the set Ψ. Since the strategy is blind, we do not restrict any bet with any precondition, hence Pre is defined uniformly and independent of $s \in \Psi$ by

$Pre(\textit{right bet}) := Pre(s, \textit{right bet}) = \frac{1}{2^a}$,

$Pre(\textit{wrong bet}) := Pre(s, \textit{wrong bet}) = \frac{2^a-1}{2^a}$, with $s \in \Psi$.

This means Pre is uniform over each state and realizes the idea that our strategy is completely random and blind. Moreover captures the assumption that the agent makes a bet randomly chosen from the set of all states, every time.

And finally, the probability function $\mathcal{P}^{\mathbb{E}}$ is degenerated, i.e., .

$$\mathcal{P}^{\mathbb{E}}(i,e)(e') = \begin{cases} 1 & \text{if } e = e' \\ \\ 0 & \text{otherwise} \end{cases},$$

which means that there is no confusion about what event (bet) takes place each time. Whenever the attacker makes a bet, it is well-defined to be the *right bet* or a *wrong bet*.

The epistemic model $M = (S, \pi, \mathcal{K}, \mathcal{P})$ was defined at the beginning of this section.

The way we defined the precondition function Pre results on an immediate corollary.

Corollary 4.1.16 *At the first bet agent discovers the secret with probability* $\frac{1}{2^a}$,

$$Pre(\textit{right bet}) = \frac{1}{2^a}.$$

The reader should note that whenever we make a public announcement of a formula it must be true. However, in the more general situation of the product model that is not necessarily true. The attacker can bet a combination of bits that does not occur in the world where the attacker supposes to be. Nevertheless note that when the attacker bets the combination corresponding to the secret he is in the situation of a public announcement: he is betting a formula that is true. Moreover when the attacker bets the secret, he should immediately forget all the other worlds and be sure that the real world is s^* and the secret is $(m_1, \ldots, m_a)$. Our idea is that the attacker should eliminate all the other worlds of his account and with this purpose, beyond the axioms for the product update model we should also consider the axiom

M2. $[right\ bet]\varphi \longleftrightarrow \left[!\left(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a)\right)\right]\varphi$

On the other hand our model should cover the idea that when the bet is a wrong combination, the attacker should not learn anything and should remain strictly in the product update model.

Remark 4.1.17 *With this model, when the attacker makes a wrong bet he do not learn anything,*

$$[wrong\ bet]K\varphi \longleftrightarrow K\varphi.$$

Actually when he makes a wrong bet the system stands on the product update model, so we have

$$((s', wrong\ bet), (s, wrong\ bet)) \in \mathcal{K}' \quad iff \quad (s, s') \in \mathcal{K},$$

which implies

$$[wrong\ bet]K\varphi \longleftrightarrow K\varphi.$$

Remark 4.1.18 *On the other side, from the axiom M2 is immediate that when the attacker bets the secret, he becomes to know it,*

$$[right\ bet\ ]K(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a)).$$

From the definition of the knowledge relation $\mathcal{K}$ for the public announcement is immediate that

$$\mathcal{K}'(s^*, right\ bet) = \{(s^*, right\ bet)\},$$

following that $(M, (s^*, right\ bet)) \Vdash K(D_{r_1^{s^*}}(m_1) \wedge D_{r_a^{s^*}}(m_a))$. So,

for all $(s, right\ bet) \in \mathcal{K}'(s^*, right\ bet) = \{(s^*,\ right\ bet)\}, (M, s) \Vdash D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a)$.

Theorem 4.1.19 *After a polynomial number of bets, the attacker discovers the secret with a negligible probability, i.e.*

$$[bet\ 1] \cdots [bet\ q(a)]\, P\left(K\left(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a)\right)\right) < \frac{1}{p(a)},$$

for any polynomial p and for a large enough length a.

Semantic Proof:

$$(M, s^*) \Vdash [bet\ 1] \cdots [bet\ q(a)]\, P\left(K\left(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a)\right)\right) < \frac{1}{p(a)} \quad iff$$

$$\sum_{\substack{((s,e_1)\ldots,e_{q(a)})\in S\times E\times\ldots\times E \text{ st} \\ (M\times\mathbb{E}\times\ldots\times\mathbb{E},((s,e_1)\ldots,e_{q(a)}))\Vdash K(D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a))}} \mathcal{P}((s^*, bet\ 1)\ldots, bet\ q(a))((s,e_1)\ldots,e_{q(a)}) < \frac{1}{p(a)}$$

Since

$dom(\mathcal{P}((s^*, bet\ 1)\ldots, bet\ q(a))) \subseteq \mathcal{K}((s^*, bet\ 1)\ldots, bet\ q(a)) = \{((s, bet\ 1)\ldots, bet\ q(a)) \mid s \in S\}$,

$$\sum_{\substack{((s,e_1)\ldots,e_{q(a)})\times E\times\ldots\times E \text{ st} \\ (M\times\mathbb{E}\times\ldots\times\mathbb{E},((s,e_1)\ldots,e_{q(a)}))\Vdash K(D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a))}} \mathcal{P}((s^*, bet\ 1)\ldots, bet\ q(a))((s, e_1)\ldots, e_{q(a)}) =$$

$$= \sum_{\substack{((s,bet\ 1)\ldots,bet\ q(a))\ \text{st}\ (M\times\mathbb{E}\times\ldots\times\mathbb{E}, \\ ((s,bet\ 1)\ldots,bet\ q(a)))\Vdash K(D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a))}} \mathcal{P}((s^*, bet\ 1)\ldots, bet\ q(a))((s, bet\ 1)\ldots, bet\ q(a)).$$

But by Remark 4.1.17,

$$(M', s') \Vdash [bet]K(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a)) \quad \textit{iff} \quad \text{“}bet\text{”} = \text{“}\textit{right bet}\text{”}.$$

Moreover,

$$[\textit{wrong bet}]K\varphi \longleftrightarrow K\varphi.$$

So when the intruder makes a sequence of $q(a)$ bets and ends up discovering the secret, there must be an $i \in \{1, \ldots, q(a)\}$ such that *bet* $i =$ “*right bet*”, i.e. either the first bet is the right one, or the second, or the third, ... , or the last one.

Suppose the i^{th} bet is the *right bet*.

Let us compute $\mathcal{P}(((s^*, bet\ 1)\ldots, right\ bet)\ldots, bet\ q(a))(((s, bet\ 1)\ldots, right\ bet)\ldots, bet\ q(a))$:

$$\mathcal{P}(((s^*, bet\ 1)\ldots, right\ bet)\ldots, bet\ q(a))(((s, bet\ 1)\ldots, right\ bet)\ldots, bet\ q(a)) =$$

$$= \frac{Pre(bet\ q(a))\mathcal{P}((s^*, bet\ 1)\ldots, bet\ q(a)-1)((s, bet\ 1)\ldots, bet\ q(a)-1)\mathcal{P}^{\mathbb{E}}(bet\ q(a))(bet\ q(a))}{\sum_{\substack{s'\in S \\ e'\in E}} Pre(e')\mathcal{P}((s^*, bet\ 1)\ldots, bet\ q(a)-1)((s', bet\ 1)\ldots, bet\ q(a)-1)\mathcal{P}^{\mathbb{E}}(bet\ q(a))(e')} =$$

$$= \frac{Pre(bet\ q(a))\mathcal{P}((s^*, bet\ 1)\ldots, bet\ q(a)-1)((s, bet\ 1)\ldots, bet\ q(a)-1)}{Pre(bet\ q(a)))\sum_{s'\in S}\mathcal{P}((s^*, bet\ 1)\ldots, bet\ q(a)-1)((s', bet\ 1)\ldots, bet\ q(a)-1)} =$$

$$= \mathcal{P}((s^*, bet\ 1)\ldots, bet\ q(a)-1)((s, bet\ 1)\ldots, bet\ q(a)-1).$$

Going on inductively, after $q(a) - i$ steps we get

$$\mathcal{P}(((s^*, bet\ 1)\ldots, right\ bet)\ldots, bet\ q(a))(((s, bet\ 1)\ldots, right\ bet)\ldots, bet\ q(a)) =$$

$$= \mathcal{P}((s^*, bet\ 1)\ldots, right\ bet)((s, bet\ 1)\ldots, right\ bet).$$

Notice that this should be expected to occur: the attacker does not gain any information when he bets a *wrong bet*.

So we have

$$\sum_{\substack{((s,bet\ 1)\ldots,bet\ q(a))\ \text{st}\ (M\times\mathbb{E}\times\ldots\times\mathbb{E}, \\ ((s,bet\ 1)\ldots,bet\ q(a)))\Vdash K(D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a))}} \mathcal{P}((s^*, bet\ 1)\ldots, bet\ q(a))((s, bet\ 1)\ldots, bet\ q(a)) =$$

$$= \sum_{\substack{((s,bet\ 1)\ldots,right\ bet)\ \text{st}\ (M\times\mathbb{E}\times\ldots\times\mathbb{E},\\ ((s,bet\ 1)\ldots,right\ bet))\Vdash K(D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a))}} \mathcal{P}((s^*,bet\ 1)\ldots,right\ bet)((s,bet\ 1)\ldots,right\ bet)$$

Now we need to use the formula for probabilities with public announcements.

$$\sum_{\substack{((s,bet\ 1)\ldots,right\ bet)\ \text{st}\ (M\times\mathbb{E}\times\ldots\times\mathbb{E},\\ ((s,bet\ 1)\ldots,right\ bet))\Vdash K(D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a))}} \mathcal{P}((s^*,bet\ 1)\ldots,right\ bet)((s,bet\ 1)\ldots,right\ bet) =$$

$$\sum_{\substack{((s,bet\ 1)\ldots,bet\ i-1)\ \text{st}\ (M\times\mathbb{E}\times\ldots\times\mathbb{E},\\ ((s,bet\ 1)\ldots,bet\ i-1))\Vdash[right\ bet]K(D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a))}} \mathcal{P}^{right\ bet}((s^*,bet\ 1)\ldots,bet\ i{-}1)((s,bet\ 1)\ldots,bet\ i{-}1) =$$

$$\sum_{\substack{((s,bet\ 1)\ldots,bet\ i-1)\ \text{st}\ (M\times\mathbb{E}\times\ldots\times\mathbb{E},\\ ((s,bet\ 1)\ldots,bet\ i-1))\Vdash[right\ bet]K(D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a))}} \frac{\mathcal{P}((s^*,bet\ 1)\ldots,bet\ i-1)((s,bet\ 1)\ldots,bet\ i-1)}{\mathcal{P}((s^*,bet\ 1)\ldots,bet\ i-1)(D_{r_1^{s^*}}(m_1)\wedge\cdots\wedge D_{r_a^{s^*}}(m_a))}$$

The denominator is equal to

$$\sum_{\substack{((s,bet\ 1)\ldots,bet\ i-1)\ \text{st}\\ (M\times\mathbb{E}\times\ldots\times\mathbb{E},((s,bet\ 1)\ldots,bet\ i-1))\Vdash D_{r_1^{s^*}}(m_1)\wedge\cdots\wedge D_{r_a^{s^*}}(m_a)}} \mathcal{P}((s^*,bet\ 1)\ldots,bet\ i-1)((s,bet\ 1)\ldots,bet\ i-1),$$

But $D_{r_1^{s^*}}(m_1)\wedge\cdots\wedge D_{r_a^{s^*}}(m_a)$ is a Boolean formula so

$(M\times\mathbb{E}\times\ldots\times\mathbb{E},((s,bet\ 1)\ldots,bet\ i-1))\Vdash D_{r_1^{s^*}}(m_1)\wedge\cdots\wedge D_{r_a^{s^*}}(m_a)$ *iff*

$$(M,s)\Vdash D_{r_1^{s^*}}(m_1)\wedge\cdots\wedge D_{r_a^{s^*}}(m_a).$$

So s must be equal to s^* and we get

$$\sum_{\substack{((s,bet\ 1)\ldots,bet\ i-1)\ \text{st}\ (M\times\mathbb{E}\times\ldots\times\mathbb{E},\\ ((s,bet\ 1)\ldots,bet\ i-1))\Vdash D_{r_1^{s^*}}(m_1)\wedge\cdots\wedge D_{r_a^{s^*}}(m_a)}} \mathcal{P}((s^*,bet\ 1)\ldots,bet\ i-1)((s,bet\ 1)\ldots,bet\ i-1) =$$

$$= \mathcal{P}((s^*,bet\ 1)\ldots,bet\ i-1)((s^*,bet\ 1)\ldots,bet\ i-1).$$

Then we should compute both the denominator and the numerator just as in the beginning, using the formula for probability in the product model repetitively. In the end we should get

$$\mathcal{P}((s^*,bet\ 1)\ldots,bet\ i-1)((s,bet\ 1)\ldots,bet\ i-1) = \mathcal{P}(s^*)(s),\ \text{for each } s\in S.$$

Observation: Note that, if some other bet was also the *right bet*, the quotient given by the formula for public announcements had denominator equal 1: the probability of $D_{r_1^{s^*}}(m_1)\wedge\cdots\wedge D_{r_a^{s^*}}(m_a)$ should be 1 in the already updated model with that announcement.

Finally we get

$$\sum_{\substack{((s,bet\ 1)\ldots,bet\ i-1)\ \text{st}\ (M\times\mathbb{E}\times\ldots\times\mathbb{E},\\ ((s,bet\ 1)\ldots,bet\ i-1))\Vdash[right\ bet]K(D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a))}} \frac{\mathcal{P}((s^*,bet\ 1)\ldots,bet\ i-1)((s,bet\ 1)\ldots,bet\ i-1)}{\mathcal{P}((s^*,bet\ 1)\ldots,bet\ i-1)(D_{r_1^{s^*}}(m_1)\wedge\cdots\wedge D_{r_a^{s^*}}(m_a))} =$$

$$= \sum_{s\in S\ \text{st}\ (M,s)\Vdash[right\ bet]K(D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a))} \frac{\mathcal{P}(s^*)(s)}{\mathcal{P}(s^*)(s^*)}.$$

But

$$[right\ bet]\varphi \longleftrightarrow [!D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a)]\varphi,$$

so in particular $(M,s)\Vdash D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a)$. And effectively s^* is the only state that satisfies the condition over the sum, so

$$\sum_{s\in S\ \text{st}\ (M,s)\Vdash[right\ bet]K(D_{r_1^{s^*}}(m_1)\wedge\cdots\wedge D_{r_a^{s^*}}(m_a))} \frac{\mathcal{P}(s^*)(s)}{\mathcal{P}(s^*)(s^*)} = \frac{\mathcal{P}(s^*)(s^*)}{\mathcal{P}(s^*)(s^*)} = 1.$$

So:

$$[bet\ 1]\cdots[bet\ q(a)]\,P\left(K\left(D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a)\right)\right) =$$

$$Pre(right\ bet)\sum_{\substack{((s,right\ bet)\ldots,bet\ q(a))\ \text{st}\\ (M\times\mathbb{E}\times\ldots\times\mathbb{E},((s,right\ bet)\ldots,bet\ q(a)))\Vdash\\ \Vdash K(D_{r_1^{s^*}}(m_1)\cdots D_{r_a^{s^*}}(m_a))}} \mathcal{P}((s^*,right\ bet)\ldots,bet\ q(a))((s,right\ bet)\ldots bet\ q(a))+$$

$$+\ldots+Pre(right\ bet)\sum_{\substack{((s,bet\ 1)\ldots,right\ bet)\ \text{st}\\ (M\times\mathbb{E}\times\ldots\times\mathbb{E},((s,bet\ 1)\ldots,right\ bet))\Vdash\\ \Vdash K(D_{r_1^{s^*}}(m_1)\cdots D_{r_a^{s^*}}(m_a))}} \mathcal{P}((s^*,bet\ 1)\ldots,right\ bet)((s,bet\ 1)\ldots right\ bet) =$$

$$= q(a)\cdot Pre(right\ bet) = \frac{q(a)}{2^a}.$$

So, asymptotically, for any polynomial p,

$$[bet\ 1]\cdots[bet\ q(a)]\,P\left(K\left(D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a)\right)\right) = \frac{q(a)}{2^a} < \frac{1}{p(a)}.$$

■

Formal Proof:

We pretend to prove formally that $[bet\ 1]\ldots[bet\ q(a)]P(K(D_{r_1^{s^*}}(m_1)\wedge\ldots\wedge D_{r_a^{s^*}}(m_a)))$ is negligible we will analyse several cases.

1^{st} **case:**
Suppose any bet is the *right bet*. We pretend to prove

$$[wrong\ bet]\dots[wrong\ bet]P(K(D_{r_1^{s*}}(m_1)\wedge\dots\wedge D_{r_a^{s*}}(m_a)))=0.$$

Applying repetitively $PM5$ we get

$$[wrong\ bet]\dots[wrong\ bet]P(K(D_{r_1^{s*}}(m_1)\wedge\dots\wedge D_{r_a^{s*}}(m_a)))=0\quad iff$$

$$Pre(wrong\ bet)\dots Pre(wrong\ bet)P([wrong\ bet]\dots[wrong\ bet]K(D_{r_1^{s*}}(m_1)\wedge\dots\wedge D_{r_a^{s*}}(m_a))=$$

$$=0\cdot Pre(wrong\ bet)\dots Pre(wrong\ bet)\quad iff$$

$$P([wrong\ bet]\dots[wrong\ bet]K(D_{r_1^{s*}}(m_1)\wedge\dots\wedge D_{r_a^{s*}}(m_a))=0.$$

Applying repetitively the property of Remark 4.1.17 we get equivalently

$$P(K(D_{r_1^{s*}}(m_1)\wedge\dots\wedge D_{r_a^{s*}}(m_a)))=0.$$

But no state s on the static model verifies $(M,s)\Vdash K(D_{r_1^{s*}}(m_1)\wedge\dots\wedge D_{r_a^{s*}}(m_a))$ so we get a final equivalence with

$$0=0.$$

i^{th} **case:**
Then we should concern with the possibility of at least one of the bets be the right one. Let *bet* $i=$ *right bet*. We want to prove that

$$[bet\ 1]\dots[right\ bet]\dots[bet\ q(a)]P(K(D_{r_1^{s*}}(m_1)\wedge\dots\wedge D_{r_a^{s*}}(m_a)))=1$$

is provable.

Applying repetitively $PM5$ we get

$$[bet\ 1]\dots[right\ bet]\dots[bet\ q(a)]P(K(D_{r_1^{s*}}(m_1)\wedge\dots\wedge D_{r_a^{s*}}(m_a)))=1\quad iff$$

$$Pre(bet\ i{+}1)\dots Pre(bet\ q(a))[bet\ 1]\dots[right\ bet]P([bet\ i{+}1]\dots[bet\ q(a)]K(D_{r_1^{s*}}(m_1)\wedge\dots\wedge D_{r_a^{s*}}(m_a)))=$$
$$=Pre(bet\ i+1)\dots Pre(bet\ q(a)).$$

Using the property of Remark 4.1.17 we get equivalently

$$[bet\ 1]\dots[right\ bet]P(K(D_{r_1^{s*}}(m_1)\wedge\dots\wedge D_{r_a^{s*}}(m_a)))=1.$$

Using $U5$ this is equivalent to
$[bet\ 1]\dots[bet\ i-1]P(D_{r_1^{s*}}(m_1)\wedge\dots\wedge D_{r_a^{s*}}(m_a)\wedge[right\ bet]K(D_{r_1^{s*}}(m_1)\wedge\dots\wedge D_{r_a^{s*}}(m_a)))=$

$$=P(D_{r_1^{s*}}(m_1)\wedge\dots\wedge D_{r_a^{s*}}(m_a)).$$

Now we proceed assuming without loss of generality that *bet 1* $= \cdots =$ *bet* $i-1 =$ "*wrong bet*". However note that if this is not the case $P(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a)) = 1$ in the updated model.

Applying now repetitively $PM5$ we get equivalently

$$Pre(bet\ 1) \ldots Pre(bet\ i-1) P(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a) \wedge$$

$$\wedge [bet\ 1] \ldots [bet\ i-1][right\ bet] K(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a)) =$$

$$= P(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a)) Pre(bet\ 1) \ldots Pre(bet\ i-1).$$

Using the property of Remark 4.1.18 we know that $[right\ bet] K(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a)) = true$ so equivalently comes

$$P(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a)) = P(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a)).$$

Which proves that

$$[bet\ 1] \ldots [right\ bet] \ldots [bet\ q(a)] P(K(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a))) = 1.$$

Now using $I4$ we have Using $I4$,

$$Pre(right\ bet)[bet\ 1] \ldots [right\ bet] \ldots [bet\ q(a)] P(K(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a^{s^*}}(m_a))) = Pre(right\ bet) = \frac{1}{2^a}$$

is provable.

Covering all the possibilities we finally get

$$[bet\ 1] \ldots [bet\ q(a)] P(K(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a{}^{s^*}}(m_a))) = 0 + Pre(right\ bet) + \ldots + Pre(right\ bet) = \frac{q(a)}{2^a}.$$

So, asymptotically, for any polynomial p,

$$[bet\ 1] \cdots [bet\ q(a)]\ P\left(K\left(D_{r_1^{s^*}}(m_1) \wedge \ldots \wedge D_{r_a{}^{s^*}}(m_a)\right)\right) = \frac{q(a)}{2^a} < \frac{1}{p(a)}.$$

■

4.2 Computational Indistinguishability

In this subsection we dedicate ourselves on applying the dynamic probabilistic epistemic logic to computational indistinguishability. Computational indistinguishability is the base of many relevant notions in information security, like in the semantic characterizations of asymmetric encryption schemes such as chosen-plaintext attack or chosen-ciphertext attack.

Definition 4.2.1 *Let I be a countable set. A collection of random variables indexed by I, $\{X_i\}_{i\in I}$, is said to be a distribution ensemble.*

Definition 4.2.2 *Let $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ be distribution ensembles indexed by a security parameter n. $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ are computationally indistinguishable if for any probabilistic polynomial time algorithm A and any positive polynomial p there is some m such that for all $n > m$,*

$$|P(A(X_n) = 1) - P(A(Y_n) = 1)| < \frac{1}{p(n)},$$

where $P(A(X_n) = 1) = \sum_{p\in X_n} P(X_n = p) \cdot P(A(p) = 1)$.

Basically, we define two distribution ensembles to be computationally indistinguishable if there is no efficient procedure to distinguish them. More specifically, if two distribution ensembles are computationally indistinguishable, any efficient probabilistic algorithm should accept both of them with probabilities whose difference is negligible.

The usual definition in literature for computational indistinguishability is the definition 4.2.2. If the algorithmt is uniform we do not really know how to model it with our logic. Whereas if the algorithm is non-uniform we can try to model it using the epistemic component of the logic, so this is what we will assume.

As mentioned, it seems interesting to explore the approach that assumes the algorithm is non-uniform. The variation of this definition with the non-uniform case is in fact much investigated.

In order to use the dynamical probabilistic epistemic logic to characterize computational indistinguishability of distribution ensembles we should begin by finding a way to rewrite this definition with *well defined objects* in our logic. We are not able to compute the probability of an algorithm to answer 1 or 0, so we use functional completeness to reduce it to the study of the probability of a formula.

By functional completeness, for each Boolean function $f : 2^n \longrightarrow 2$ exists a Boolean formula φ such that

$$\varphi(p_1, \ldots, p_n) = true \quad \textit{iff} \quad f(p_1, \ldots, p_n) = 1.$$

The algorithm that is described in Definition 4.2.2 is probabilistic, i.e. from time to time, before getting the answer, the algorithm tosses a coin and the answer depends on the coin tosses, of course. So let us readjust the input, making this include already the sequence of (say k) coin tosses the algorithm will call. Now the inputs are of the form $p_1, \ldots, p_n, e_1, \ldots, e_k$ and we do not care anymore about the non-determinism of the algorithm.

Remark 4.2.3 *Note that, to each algorithm corresponds an unknown distribution ensemble on the coin tosses.*

We can now use functional completeness to give a new look to the Definition 4.2.2.

Definition 4.2.4 *Let $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ be distribution ensembles indexed by a security parameter n. $\{X_n\}_n$ and $\{Y_n\}_n$ are computationally indistinguishable if for all Boolean formulas φ with polynomial length and its corresponding distribution ensemble of coin tosses $\{E_k\}_{k\in\mathbb{N}}$, for any positive polynomial p there is some m such that for all $n > m$,*

$$\left|[e_1 \cdots e_k]P^{X_n}(\varphi) - [e'_1 \cdots e'_k]P^{Y_n}(\varphi)\right| < \frac{1}{p(n)},$$

where $e_1, \ldots, e_k$ and $e'_1, \ldots, e'_k$ are samples of E_k.

$(M, s) \Vdash [e_1 \cdots e_k]P^{X_n}(\varphi)$ has the value of the probability that after generated a sequence of coin tosses $e_1 \cdots e_k$, the Boolean circuit φ evaluated in $(s, e_1 \cdots e_k)$ holds. Further we will analyse this definition in detail.

Now that we already approached this important notion of computational indistinguishability to the dynamical probabilistic epistemic logic, we check the equivalence of the two variations, in the non-uniform case

Proposition 4.2.1 *Two distribution ensembles $\{X_n\}_n$ and $\{Y_n\}_n$ are computationally indistinguishable in the sense of Definition 4.2.2 for non-uniform algorithms if and only if they are computationally indistinguishable in the sense of Definition 4.2.4.*

Proof: A non-uniform algorithm is a Boolean function. Functional completeness implies then that computational indistinguishability in the sense of Definition 4.2.2 implies the approach of Definition 4.2.4.
Reciprocally, $\wedge, \vee, \neg$ are computable functions, so (just as we saw in Remark 2.0.16) we can get all the Boolean functions $f : 2^n \longrightarrow 2$, from all the Boolean formulas with n inputs, for $n \geq 1$, and the equivalence follows. ■

Remark 4.2.5 *P/poly is the complexity class of languages decidable by deterministic circuits of polynomial size. Whereas P is the complexity class of languages decidable by a deterministic Turing machine using polynomial time.*

In fact these are not the complexity classes associated with the problem we are studying. The algorithm that the Definition 4.2.2 refers is not a function, i.e. being probabilistic, the algorithm can return 1 *or* 0 *to each input with a given probability distribution. Moreover, being non deterministic, the algorithm does not necessarily answer the same to a given input in different tests. We should then analyze the complexity classes of distributions in this sense.*

The classes P *and* $P/poly$ *actually correspond to complexity classes analogous to the definitions 4.2.2 and 4.2.4 (respectively) in a deterministic approach. The complexity classes that we should consider would be analogous to* P *and* $P/poly$ *for the case of distributions rather than functions.*

Maybe we can dare to postulate a relationship between such complexity classes by analyzing the deterministic case.

$$P \subseteq P/poly$$

Since we opted for the variation of the Definition 4.2.2 that adopts the non-uniformity of the algorithm, it seems credible to believe that if we restrict ourselves to this case, these classes should coincide.

This is an important issue associated with this problem and constitutes one of the proposals for future work.

Example 4.2.1 *Let* $\{U_n\}_n$ *be the uniform distribution ensemble and* $\{\mathbb{1}_n\}_n$ *be the constant distribution ensemble,* $\mathbb{1}_n = 1 \cdots 1$*, for all* $n \in \mathbb{N}$*.*
We should be able to distinguish these two distribution ensembles.
Let $p_1 \cdots p_n$ *be a sample of* U_n *and* $1 \cdots 1$ *be the sample of* $\mathbb{1}_n$*.*
Consider $\varphi(\xi_1, \ldots, \xi_n) = \xi_1 \wedge \ldots \wedge \xi_n$ *a Boolean circuit (without random inputs).*
In this example we have no random component, so we simply ignore it from the definition and get

$$\left|P^{X_n}(\varphi) - P^{Y_n}(\varphi)\right| < \frac{1}{p(n)}.$$

For any polynomial p *exists* $m \in \mathbb{N}$ *such that, for all* $n > m$*,*

$$2^n > p(n) > 2.$$

So it follows that $1 - \frac{1}{2^n} > 1 - \frac{1}{p(n)}$*. Since* $p(n) > 2$*, we have,* $1 - \frac{1}{2^n} > 1 - \frac{1}{p(n)} > \frac{1}{p(n)}$*. Hence,*

$$\left(1 - \frac{1}{2^n}\right) > \frac{1}{p(n)}.$$

Since

$$\left|P^{X_n}(\varphi) - P^{Y_n}(\varphi)\right| = \left| \sum_{\substack{p_1 \cdots p_n \text{ sample of } U_n \text{ st} \\ p_1 \wedge \ldots \wedge p_n \text{ holds}}} \mathcal{P}^{U_n}(p_1 \cdots p_n) - \sum_{\substack{p_1 \cdots p_n \text{ sample of } \mathbb{1}_n \text{ st} \\ p_1 \wedge \ldots \wedge p_n \text{ holds}}} \mathcal{P}^{\mathbb{1}_n}(p_1 \cdots p_n) \right| =$$

$$= \left|\mathcal{P}^{U_n}(1\cdots 1) - \mathcal{P}^{\mathbb{1}_n}(1\cdots 1)\right| = \left|\frac{1}{2^n} - 1\right| > \frac{1}{p(n)},$$

the distribution ensembles $\{U_n\}_n$ *and* $\{\mathbb{1}_n\}_n$ *are computationally distinguishable.* □

Now we dedicate on the construction of the model to reason about computational indistinguishability.

Let $\{X_n\}_n$ and $\{Y_n\}_n$ be the distribution ensembles we want to (in)distinguish computationally. Before we go on, we should emphasize that, in fact, the notion of indistinguishability analyzes two ensembles simultaneously. Essentially, we want, say, in each iteration of indistinguishability to test two samples simultaneously. Well, therefore we aim at modeling the joint distribution of X_n and Y_n.

We begin by constructing a model for each of the random variables. The probabilistic epistemic model for X_n, $M^{X_n} = (S^{X_n}, \pi^{X_n}, \mathcal{K}^{X_n}, \mathcal{P}^{X_n})$ is defined as follows:
The space of states should contain all the samples of the random variable,

$$S^{X_n} = \{(p_1, \ldots, p_n) \mid p_1, \ldots, p_n \text{ is a sample of } X_n\}.$$

Since we confuse a label of a state with the values of the primitive propositions, the identification function is defined straightforward. Moreover all the samples should be equally plausible,

$$\mathcal{K}^{X_n} = \left(S^{X_n}\right)^2.$$

$\mathcal{P}^{X_n}$ is defined according to the probabilities of the distribution X_n and should be independent of the world where the attacker thinks to be, i.e. $\mathcal{P}^{X_n}(s) =: \mathcal{P}^{X_n} : S \longrightarrow [0,1]$.

Similarly we can construct the probabilistic epistemic model for Y_n.

For each Boolean formula φ in Definition 4.2.4 with k random inputs sampled from a random variable E_k, we can consider a probabilistic event model $\mathbb{E} = (E, \Psi, Pre, \mathcal{P}^{\mathbb{E}})$ which, of course, depends on the Boolean circuit one considers. E should be defined as the set of all the samples of E_k,

$$E^{E_k} = \{(e_1, \ldots, e_k) \mid e_1, \ldots, e_k \text{ is a sample of } E_k\}.$$

The set Ψ and the probability function $Pre : \Psi \times E \longrightarrow [0,1]$ should depend on the case in study, nevertheless there are some typical assumptions such as taking the functions $Pre : \Psi \times E \longrightarrow [0,1]$ not depending on the parameter $\psi \in \Psi$, i.e. $Pre : E \longrightarrow [0,1]$.

Moreover, we assume from now that $\mathcal{P}^{\mathbb{E}}(e) : E \longrightarrow [0,1]$ is a probability function defined without depending on e: $\mathcal{P}^{\mathbb{E}}(e) =: \mathcal{P}^{\mathbb{E}} : E \longrightarrow [0,1]$. In fact, the event e that appears in the Definition 4.2.4 is absolutely outside the control of the intruder. And, of course, this probabilistic function should be defined according to the random variable E_k. Since it does not depend on the events $e_1 \cdots e_k$, $[e_1 \cdots e_k]P^{X_n}(\varphi)$ could be written as

$$[\varphi]P^{X_n}(\varphi),$$

where $[\varphi]P^{X_n}(\varphi)$ would be interpreted in the model exactly the same way as $[e_1 \cdots e_k]P^{X_n}(\varphi)$. However, this alternative notion lose the uniformity introduced in the product update model, with the events.

This construction is very intuitive for each of the random variables. But recall that in this environment of computational indistinguishability, we intend to test two samples simultaneously, so this is not our final model. Alternatively, we must construct a model for the joint distributions of both X_n, Y_n and E_k with itself.

So consider $M^{X_n,Y_n} = (S, \pi, \mathcal{K}, \mathcal{P})$, the model for the joint distribution. So:

$$\begin{array}{lcl} S & = & S^{X_n} \times S^{Y_n} = \{(p,q) \mid p \text{ is a sample of } X_n \text{ and } q \text{ is a sample of } Y_n\}, \\ \pi(p,q) & = & true \quad iff \quad \pi(p) = true \text{ and } \pi(q) = true \\ \mathcal{K} & = & S^2, \\ \mathcal{P} & = & \mathcal{P}^{X_n,Y_n}, \text{ is the joint probability distribution of } X_n \text{ and } Y_n \end{array}$$

Note that, despite the fact that we need to refer the joint probability distribution, we will not explicitly use it. We are interested in using strictly the marginal distributions, is what indeed arises in the definition of indistinguishability. We then use the properties of the joint probability distribution to reduce to the marginal probability distribution.

We can now define the event model of the joint distribution of E_k with itself essentially the same way,

$$\mathbb{E}^{(E_k),(E_k)} = (E, \Psi, Pre, \mathcal{P}^{\mathbb{E}}) \text{ can be defined as}$$

$$\begin{array}{lcl} E & = & E^{E_k} \times E^{E_k}, \\ \Psi & = & \left(\Psi^{E_k}\right)^2, \\ Pre & = & Pre^{E_k,E_k} \text{ is the joint probability distribution,} \\ \mathcal{P}^{\mathbb{E}} & = & \mathcal{P}^{\mathbb{E}^{E_k,E_k}} \text{ is the joint probability distribution.} \end{array}$$

Finally we have a model for knowledge and probability and a probabilistic event model, so we are able to define the product model as we did at subsection 3.3.2,

$$M = M^{X_n,Y_n} \times \mathbb{E}^{(E_k),(E_k)}.$$

The expression which appears in the Definition 4.2.4 of computational indistinguishability should be adapted formally to our model as

$$(M, (p^*, q^*)) \Vdash \left|[\bar{e_1}]P^{X_n}(\varphi) - [\bar{e_2}]P^{Y_n}(\varphi)\right| < \frac{1}{p(n)} \quad iff$$

$$(M, (p^*, q^*)) \Vdash \left|[\bar{e_1}, \bar{e_2}]\left(P^{X_n} - P^{Y_n}\right)(\varphi)\right| < \frac{1}{p(n)}. \tag{4.9}$$

Indeed, we now deal with pairs of samples and pairs of events, however symbolically we will keep the notation of Definition 4.2.4 because it is more intuitive and more consistent with the original definition of computational indistinguishability, however (4.9) is the correct formal expression and should be interpreted as follows

$$\left| \sum_{\substack{((p,q),(e_1,e_2))\in S\times E \text{ st} \\ (M\times\mathbb{E},((p,q),(e_1,e_2)))\Vdash\varphi}} \left(\frac{Pre(p,e_1)\mathcal{P}^{X_n}(p)\mathcal{P}^{\mathbb{E}}(e_1)}{\sum_{\substack{(p',q')\in S \\ (e_1',e_2')\in E}} Pre(p',e_1')\mathcal{P}^{X_n}(p')\mathcal{P}^{\mathbb{E}}(e_1')} - \frac{Pre(q,e_2)\mathcal{P}^{Y_n}(q)\mathcal{P}^{\mathbb{E}}(e_2)}{\sum_{\substack{(p',q')\in S \\ (e_1',e_2')\in E}} Pre(q',e_2')\mathcal{P}^{X_n}(q')\mathcal{P}^{\mathbb{E}}(e_2')} \right) \right| < \frac{1}{p(n)}$$

Remark 4.2.6 *Notice the subtlety that exists in the joint probability distribution, $\mathcal{P}^{X_n,Y_n}$, of two random variables X_n and Y_n,*

$$\sum_{\xi\in\Psi_0^{X_n}} \sum_{\xi'\in\Psi^{Y_n}} \mathcal{P}^{X_n,Y_n}(\xi,\xi') = \sum_{\xi\in\Psi_0^{X_n}} \mathcal{P}^{X_n}(\xi), \text{ where } \Psi_0^{X_n} \subseteq \Psi^{X_n}.$$

This is a basic property that we will use whenever we invoke axiom $PM5$ in this approach of computational indistinguishability.

Example 4.2.2 *Let $\{X_n\}_n = \{Y_n\}$ be the same distribution ensemble.*
We should trivially prove they are computationally indistinguishable.
Indeed in

$$\sum_{\substack{((p,q),(e_1,e_2))\in S\times E \text{ st} \\ (M\times\mathbb{E},((p,q),(e_1,e_2)))\Vdash\varphi}} \left(\frac{Pre(p,e_1)\mathcal{P}^{X_n}(p)\mathcal{P}^{\mathbb{E}}(e_1)}{\sum_{\substack{(p',q')\in S \\ (e_1',e_2')\in E}} Pre(p',e_1')\mathcal{P}^{X_n}(p')\mathcal{P}^{\mathbb{E}}(e_1')} - \frac{Pre(q,e_2)\mathcal{P}^{X_n}(q)\mathcal{P}^{\mathbb{E}}(e_2)}{\sum_{\substack{(p',q')\in S \\ (e_1',e_2')\in E}} Pre(q',e_2')\mathcal{P}^{X_n}(q')\mathcal{P}^{\mathbb{E}}(e_2')} \right)$$

the terms will cancel with each other, hence

$$\left|[e_1\cdots e_k]P^{X_n}(\varphi) - [e_1'\cdots e_k']P^{X_n}(\varphi)\right| = 0 < \frac{1}{p(n)},$$

for any polynomial p. Therefore, $\{X_n\}$ and $\{X_n\}$ are computationally indistinguishable. □

Example 4.2.3 *Consider we now sample not the sequence but the bits and then join it together to construct the sequence. So, consider $\{U_n\}_n$ is a uniform distribution ensemble, i.e. a sample $p = p_1\cdots p_n$ results from sampling each of p_i from the uniform distribution. At the end, of course, $P^{U_n}(p_1,\ldots,p_n) = \frac{1}{2^n}$.*
And let $\{Y_n\}_n$ be a distribution ensemble which is almost uniform, in the following sense: we construct a sample $q = q_1\cdots q_n$ of Y_n, sampling all the $q_1,\ldots,q_{n-1}$ from an uniform distribution and q_n from another distribution, where $P(q_n = 1) = \delta$ and δ presents a negligible deviation from $\frac{1}{2}$, i.e.

$$\left|\delta - \frac{1}{2}\right| \sim \mathcal{O}\left(\frac{1}{2^n}\right).$$

Summarizing, we have a uniform distribution ensemble and a quasi uniform distribution ensemble

and so we should expect that we could not be able to distinguish them.
Moreover let us assume we define $Pre(p_1 \cdots p_n, e_1 \cdots e_k)$ in such a way we get a fair coin. To get a fair coin, actually $Pre(p_1 \cdots p_n, e_1 \cdots e_k) =: Pre(e_1 \cdots e_k)$ should not depend on $p_1 \cdots p_n$.

We pretend to prove that

$$\left|[\overline{e_1}, \overline{e_2}]\left(\mathcal{P}^{U_n} - \mathcal{P}^{Y_n}\right)(\varphi)\right| \leq C\frac{1}{2^n},$$

for some constant C.

$\left|[\overline{e_1}, \overline{e_2}]\left(\mathcal{P}^{U_n} - \mathcal{P}^{Y_n}\right)(\varphi)\right| \leq C\frac{1}{2^n}$ *(using Remark 4.2.6 and $PM5$)*

$$\left|\sum_{\substack{(e_1,e_2)\in E \\ \xi\in\Psi^{U_n}}} Pre(e_1,e_2)\mathcal{P}^{U_n}(\xi \wedge [e_1]\varphi)\mathcal{P}^{\mathbb{E}}(e_1,e_2) - \sum_{\substack{(e_1,e_2)\in E \\ \xi\in\Psi^{Y_n}}} Pre(e_1,e_2)\mathcal{P}^{Y_n}(\xi \wedge [e_2]\varphi)\mathcal{P}^{\mathbb{E}}(e_1,e_2)\right| \leq$$

$$\leq C\frac{1}{2^n}\sum\nolimits_{\substack{\xi\in\Psi \\ (e_1,e_2)\in E}} Pre(e_1,e_2)\mathcal{P}(\xi)\mathcal{P}^{\mathbb{E}}(e_1,e_2)$$

$$\left|\sum_{(e_1,e_2)\in E} Pre(e_1,e_2)\mathcal{P}^{U_n}\left(\left(\bigvee_{\xi\in\Psi^{U_n}}\xi\right)\wedge[e_1]\varphi\right)\mathcal{P}^{\mathbb{E}}(e_1,e_2) - \sum_{(e_1,e_2)\in E} Pre(e_1,e_2)\mathcal{P}^{Y_n}\left(\left(\bigvee_{\xi\in\Psi^{Y_n}}\xi\right)\wedge[e_2]\varphi\right)\mathcal{P}^{\mathbb{E}}(e_1,e_2)\right| \leq$$

$$\leq C\frac{1}{2^n}\sum\nolimits_{(e_1,e_2)\in E} Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2)$$

$$\left|\sum_{(e_1,e_2)\in E} Pre(e_1,e_2)\mathcal{P}^{U_n}\left([e_1]\varphi\right)\mathcal{P}^{\mathbb{E}}(e_1,e_2) - \sum_{(e_1,e_2)\in E} Pre(e_1,e_2)\mathcal{P}^{Y_n}\left([e_2]\varphi\right)\mathcal{P}^{\mathbb{E}}(e_1,e_2)\right| \leq$$

$$\leq C\frac{1}{2^n}\sum\nolimits_{(e_1,e_2)\in E} Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2)$$

$$\left|\sum_{(e_1,e_2)\in E} Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2)\left(\sum_{\substack{p\in S^{U_n} \\ (M\times\mathbb{E},(p,e_1))\vdash\varphi}}\mathcal{P}^{U_n}(p)\right) - \sum_{(e_1,e_2)\in E} Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2)\left(\sum_{\substack{p\in S^{Y_n} \\ (M\times\mathbb{E},(q,e_2))\vdash\varphi}}\mathcal{P}^{Y_n}(q)\right)\right| \leq$$

$$\leq C\frac{1}{2^n}\sum_{(e_1,e_2)\in E} Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2) \tag{4.10}$$

But note that, since the set of sequences sampled coincide in both U_n and Y_n (the distinction is just in the probability of the sequences in each random variable),

$$\frac{1}{2^{n-1}}\left(\sum_{(e_1,e_2)\in E} Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2)\left(\sum_{\substack{p\in S^{U_n}\\(M\times\mathbb{E},(p,e_1))\vdash\varphi}}\frac{1}{2}\right)-\sum_{(e_1,e_2)\in E} Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2)\left(\sum_{\substack{q\in S^{Y_n}\\(M\times\mathbb{E},(q,e_2))\vdash\varphi}}\delta q_n+(1-\delta)(1-q_n)\right)\right)=$$

$$=\frac{1}{2^{n-1}}\sum_{\substack{p\in S^{U_n},e_1\in E\\(M\times\mathbb{E},(p,e_1))\vdash\varphi}}\left(\sum_{e_2\in E} Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2)\frac{1}{2}-\sum_{e_2\in E} Pre(e_2,e_1)\mathcal{P}^{\mathbb{E}}(e_2,e_1)(\delta q_n+(1-\delta)(1-q_n))\right).$$

Moreover, since Pre and $\mathcal{P}^{\mathbb{E}}$ represent the joint probability distribution of a random variable with itself,

$$Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2)=Pre(e_2,e_1)\mathcal{P}^{\mathbb{E}}(e_2,e_1),\ \textit{so}$$

$$\frac{1}{2^{n-1}}\sum_{\substack{p\in S^{U_n},e_1\in E\\(M\times\mathbb{E},(p,e_1))\vdash\varphi}}\left(\sum_{e_2\in E} Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2)\frac{1}{2}-\sum_{e_2\in E} Pre(e_2,e_1)\mathcal{P}^{\mathbb{E}}(e_2,e_1)(\delta q_n+(1-\delta)(1-q_n))\right)=$$

$$\frac{1}{2^{n-1}}\sum_{\substack{p\in S^{U_n},e_1\in E\\(M\times\mathbb{E},(p,e_1))\vdash\varphi}}\left(\sum_{e_2\in E} Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2)\right)(\frac{1}{2}-(\delta p_n+(1-\delta)(1-p_n))).$$

And

$$\left|\frac{1}{2^{n-1}}\sum_{\substack{p\in S^{U_n},e_1\in E\\(M\times\mathbb{E},(p,e_1))\vdash\varphi}}\left(\sum_{e_2\in E} Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2)\right)\left(\frac{1}{2}-(\delta p_n+(1-\delta)(1-p_n))\right)\right|\leq$$

$$\leq\frac{1}{2^{n-1}}\sum_{\substack{p\in S^{U_n},e_1\in E\\(M\times\mathbb{E},(p,e_1))\vdash\varphi}}\left(\sum_{e_2\in E} Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2)\right)\left|\frac{1}{2}-\delta\right|$$

Recalling that $\left|\frac{1}{2}-\delta\right|$ has order of $\frac{1}{2^n}$ we have

$$\frac{1}{2^{n-1}}\sum_{(e_1,e_2)\in E}\left(Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2)\sum_{\substack{p\in S^{U_n}\\(M\times\mathbb{E},(p,e_1))\vdash\varphi}}\left|\frac{1}{2}-\delta\right|\right)\leq\frac{1}{2^n}\ C\sum_{(e_1,e_2)\in E} Pre(e_1,e_2)\mathcal{P}^{\mathbb{E}}(e_1,e_2),$$

for some constant C. Indeed this proves assertion (4.10).

Hence, U_n and Y_n are computationally indistinguishable. □

Chapter 5

Conclusion

We were looking for a logic in the literature with potentialities that allowed us to reason about relevant aspects in information security. The dynamic probabilistic epistemic model allows us to reason about knowledge and uncertainty and even allows updating of information, so it seemed to be promising. We made an overview of dynamic probabilistic epistemic logic and tested it in applications that seemed pertinent from the perspective of information security. It turns out that this logic was expressive enough to model these simple, but meaningful, situations. Therefore, the hope we placed in this logic was credible.

In the future we want to analyze alternative variations of this logic and one of the future ideas is to make an approach of this logic with an equational base rather than propositional. That step will allow us to express the properties of ciphers on top of an algebra of messages, a scenario much closer to the usual security models. After we get an axiomatization and prove completeness we intend to prove the correctness, even if bounded, of security protocols. Already Halpern, Pass and Raman (in [Zero Knowledge]) used epistemic logic for the modeling zero-knowledge systems and establish their correctness.

During the overview of the logic, namely in Definition 3.2.2, we opted for considering the probabilistic assignments to be probability functions instead of probability spaces. Actually we lost some expressiveness but we simplified significantly the logic and indeed this was all we needed for the applications of the last chapter.

Throughout the text, a formal question has emerged with respect to the rigor with which we deal with updates of events with probability 0. In fact, these particular cases should not be relevant in practice, but is recommended further reading of the literature, namely [3] and [2].

The very last application of this work, the problem of computational indistinguishability, could have

been modeled using a modal logic with algorithmic knowledge. As we saw, our logic fits perfectly in this example. However the approach which follows from the work of Halpern and Pucella [14] is an interesting alternative. This latter approach consists on defining algorithmic knowledge and joining this together with the probabilistic epistemic logic by introducing a new modal operator that represents the algorithmic knowledge and framing it in the probabilistic component. In fact, such a logic distinguishes explicit knowledge from implicit knowledge and, indeed, in computational indistinguishability we want to model explicit knowledge. However, the logic with algorithmic knowledge is far from being axiomatizable and, at once, our approach using dynamic probabilistic epistemic logic appeared to be much more suitable and versatile. Still exist two alternative approaches to explore in this context, [16] and [17].

This text proved that it is worth to devote closer attention to the dynamic probabilistic epistemic logic in the context of information security.

Bibliography

[1] Abadi, M., Rogaway, P., 2002 'Reconciling two views of Cryptography', *Journal of Cryptography*, 103-127.

[2] Bacchus, F., 1990, *Representing and reasoning with probabilistic knowledge*, MIT Press.

[3] van Benthem, J., Gerbrandy, J., Kooi, B., 2008, 'Dynamic update with probabilities', *Studia Logica* 93: 67-96.

[4] Enderton, H., 2001, *A mathematical introduction to logic, Second edition*, Harcourt / Academic Press.

[5] Fagin, R. and Halpern, J., 1994, 'Reasoning about knowledge and probability', *Journal of the Association for Computing Machinery* **41**, 340-367.

[6] Fagin, R., Halpern, J. and Megiddo, N., 1990, 'A logic for reasoning about probabilities', *Information and Computation* 87, 78-128.

[7] Fagin, R., Halpern, J., Moses, Y. and Vardi, M., 1995, *Reasoning about knowledge*, Cambridge, MA: MIT Press.

[8] Gerbrandy, J., 1999, 'Bissinulations on Planet Kripke', ILLC Dissertation Series, Amsterdam: ILLC.

[9] Goldreich, O., 2008, *Computational complexity - A conceptual perspective*, Cambridge University Press.

[10] Goldreich, O., 2001, *Foundations of cryptography: Volume I, Basic tools*, Cambridge University Press.

[11] Goldreich, O., 2004, *Foundations of cryptography: Volume II, Basic applications*, Cambridge University Press.

[12] Goldreich, O., Meyer, B., 1996, 'Computational indistinguishability: algorithms vs. circuits'.

[13] Halpern, J., Pass, R. and Raman, V., 2009, 'An epistemic characterization of zero knowledge'.

[14] Halpern, J. and Pucella, R., 2003, 'Probabilistic algorithmic knowledge', *Proceedings of the Ninth Conference on Theoretical Aspects of Rationality and Knowledge*, 118-130.

[15] Kooi, B., 2003, 'Probabilistic dynamic epistemic logic', *Journal of Logic, Language and Information* **12**: 381-408.

[16] den Hartog, J., 2008, 'Towards mechanized correctness proofs for cryptographic algorithms: Axiomatization of a probabilistic Hoare style logic', *Sci. Comput. Program.*, 74(1-2): 52-63.

[17] Chadha, R., Cruz-Filipe, L., Mateus, P. and Sernadas, A., 2007, 'Reasoning about probabilistic sequential programs', *Theoretical Computer Science*, 379(1-2):142-165.