Epistemic reasoning in Artificial Intelligence (HdR)

François Schwarzentruber

January 7, 2019
# Contents

## 1 Introduction
- 1.1 Applications
  - 1.1.1 Human-aware robots
  - 1.1.2 Distributed systems
  - 1.1.3 Multi-robot systems
  - 1.1.4 AI and games
  - 1.1.5 Video games
  - 1.1.6 Psychology
- 1.2 Outline of the book

## 1 Modeling

### 2 Dynamic epistemic logic
- 2.1 Epistemic models
- 2.2 Epistemic logic
  - 2.2.1 Syntax
  - 2.2.2 Semantics
  - 2.2.3 Common knowledge
- 2.3 Event models
- 2.4 Update products
- 2.5 Dynamic language
- 2.6 Bisimulation and equivalence
  - 2.6.1 Bisimulations for epistemic models
  - 2.6.2 Equivalence of event models
- 2.7 Action tokens VS action types
- 2.8 Related work
  - 2.8.1 Variant of epistemic models
  - 2.8.2 Interpreted systems
  - 2.8.3 Action language VS transition systems
  - 2.8.4 Learning models
  - 2.8.5 Variant of event models

### 3 Succinct representation
- 3.1 Accessibility programs
- 3.2 Succinct Kripke models
  - 3.2.1 Definition
  - 3.2.2 From succinct Kripke models to Kripke models
CONTENTS

3.2.3 From Kripke models to succinct models ........................................... 33
3.2.4 Succinctness of succinct Kripke models .......................................... 34
3.3 Succinct event models ........................................................................... 34
   3.3.1 Definition ..................................................................................... 34
   3.3.2 From succinct event models to event models ................................. 34
   3.3.3 From event models to succinct event models ................................. 34
   3.3.4 Succinctness of succinct event models .......................................... 35
3.4 Language of succinct DEL ..................................................................... 37

II Decision problems ................................................................................. 39

4 Model checking .......................................................................................... 41
   4.1 Motivation ......................................................................................... 41
   4.2 A first algorithm ................................................................................ 41
   4.3 PSPACE-membership ........................................................................ 42
   4.4 Other results ..................................................................................... 46
      4.4.1 Explicit models .......................................................................... 46
      4.4.2 Succinct models ......................................................................... 46
   4.5 Implementation .................................................................................. 47

5 Satisfiability problem ................................................................................ 49
   5.1 Motivation ......................................................................................... 49
   5.2 Tableau method ................................................................................ 49
      5.2.1 Principle .................................................................................... 49
      5.2.2 Tableau rules ............................................................................. 50
   5.3 The common knowledge free fragment .............................................. 51
   5.4 Common knowledge .......................................................................... 52
      5.4.1 Upper bound .............................................................................. 52
      5.4.2 Reduction ................................................................................... 56
   5.5 Arbitrary events ................................................................................ 59
   5.6 Implementation .................................................................................. 59

6 Epistemic planning ..................................................................................... 61
   6.1 Undecidability proof .......................................................................... 61
      6.1.1 Universal 1D cellular automata .................................................. 62
      6.1.2 Finite linear states ...................................................................... 63
      6.1.3 Simulating cellular automata in DEL ......................................... 63
   6.2 Undecidability frontier ....................................................................... 65
   6.3 Decidable restrictions ......................................................................... 65
      6.3.1 Public actions ............................................................................. 65
      6.3.2 Purely epistemic actions .............................................................. 66

7 Propositional Epistemic planning ............................................................. 67
   7.1 Introduction ....................................................................................... 67
   7.2 Preliminaries on automatic structures and decidable theories .......... 69
      7.2.1 Structures and logics .................................................................. 69
      7.2.2 Automatic presentations ............................................................ 70
   7.3 Model checking against cMSO over regular automatic trees .............. 72
      7.3.1 The logic cMSO over trees ......................................................... 72
Chapter 1

Introduction

My work is about technical results about autonomous agents (robots, humans, UAVs, etc.) that can reason about high-order knowledge properties (e.g. agent $a$ knows that agent $b$ knows...) and their dynamics. This document is based on a software I developed since 2015, called Hin- tikka’s world and presented as a demonstration at IJCAI-ECAI 2018 [Sch18]. The tool is available at the following address:

http://hintikkasworld.irisa.fr/

Reasoning about knowledge is important for autonomous agents for taking decisions. For instance, if $a$ knows that $b$ knows whether there is fire in the building or not, and $a$ requires to know it, then $a$ may ask $b$. Morally, we consider several agents that have different views on the global state of the world and may have different goals. In other terms, our setting falls within the scope of several research subfields of computer science:

- multi-agent systems [Woo09] and artificial intelligence [MV04];
- distributed systems (amazingly, the number of occurrences of ‘know...’ in Michel Raynal’s book is 364 [Ray13]);
- game theory, in which, as Aumann pointed out [Aum99], higher-order knowledge is important.

We use the adjective epistemic ($\epsilonπιστηµη$ in Greek) reasoning for referring to reasoning about knowledge. In 1983, in their IJCAI tutorial [DM83], Ernest Davis and Leora Morgenstern interestingly mentioned epistemic planning (see Chapter 6) whereas it was not settled yet. In the rest of the introduction, we review some applications of epistemic reasoning.
1.1 Applications

1.1.1 Human-aware robots

An important challenge is to conceive robots that are able to assist humans in everyday life.

Towards socially intelligent robots

To this aim, robots need to be socially intelligent, that is to understand others and how to interact properly with others. This task is challenging and the use of robots that do not incorporate social intelligence can be quite embarrassing and awkward as reported by Barras, in *New Scientist*, vol. 204 in 2009 [Bar09]:

TUG was a hospital worker, and its colleagues expected it to have some social smarts, the absence of which led to frustration—for example, when it always spoke in the same way in both quiet and busy situations.

That is why, in order the interaction between a robot and humans being more natural, the robot needs to reason about higher-order knowledge, that is to have beliefs about beliefs of others ([Sca02], [BGB07], [DA16]).

Example 1 Let us consider a situation inspired by the Sally and Anne test [WP83]. A robot is assisting Anne and Sally at home. They are all the three in the living room. The robot sees the entire room. Anne puts the key in the drawer and goes in the kitchen for a while. Sally takes the key, uses it and put it in the box. When Anne comes back and open the drawer, the robot tells Anne that the key are now in the box. This was possible because the robot believes that Anne believes that the key are in drawer whereas it is in the box.

In general, robots should be able to handle false-beliefs, that is, they should understand that a human or other agents may have false information about the current world [Bol14].

Explanations

Also, we aim at developing artificial agents that can be trusted by humans. For that, these agents should be able to explain their decisions (see the notion of explainable agency, [LMSC17]). We advocate the use of formal methods and reasoning about knowledge in order to produce coherent explanations. The formal representation of knowledge is useful in several aspects:

- the robot can only explain facts it knows, and from which it can extract some reasonable proof;
- the robot should not explain a fact it believes the human already know, as pointed out by Miller ([Mii19], p. 29);
- explanations could be given with an interaction with other agents (e.g., humans), and therefore the robot should be able to keep track of updates of knowledge of itself, knowledge of the other agents and in general higher-order epistemic properties.
1.1. APPLICATIONS

1.1.2 Distributed systems

Fagin and Halpern [HF89] advocate for the use of knowledge-based programs (e.g., ‘if a knows that b does not know \( x = 2 \) then ...’) for designing distributed systems. Also Moses claims that a necessary condition for an agent \( a \) to perform an action should be epistemic and of the form ‘\( a \) knows that...’ [Mos15].

Example 2 (computing the maximum) Let us consider some agents holding integers. The goal is that a given agent \( a \) has to print the maximum of these integers. Agent \( a \) having received the maximal value is not a condition to print it. Actually, agent \( a \) should know that he actually has the maximum value in order to print it.

The computation of knowledge could be implemented by extra local variables. For instance, a developer could proceed manually and introduce some low-level Boolean variables, e.g. \( b \text{ knows } p \) for storing the Boolean value of the fact ‘\( b \) knows \( p \)’, \( a \text{ knows } b \text{ knows } q \) for storing the Boolean value of the fact ‘\( a \) knows that\( b \) knows \( q \)’, etc. Nevertheless, proceeding manually would require to face some issues.

- Verification issue. How could we guarantee that the program always update the Boolean variables \( (b \text{ knows } p, a \text{ knows } b \text{ knows } q, \text{ etc.}) \) correctly?
- Design issue. What about the cost of extending the software with new features? Especially, what would be the cost of introducing new variables (e.g. a variable \( \text{not } c \text{ knows } p \) for ‘\( c \) does not know \( p \)’ in the system)?
- Readability issue. What is the cost of understanding the program code made up of many low-level variables to capture reasoning about knowledge?

Knowledge-base programs sit at the adequate abstract level for designing distributed systems: the mechanism of acquisition of knowledge (perception, communication, etc.) is then developed independently from the decision making part. The idea is then that the real executed program is automatically generated from the knowledge-base program specification.

Concerning knowledge acquisition, gossip protocols [HHL88] are designed to spreading information among a group of agents. For instance, agents may have their time availability for a meeting and the goal is that all agents have the time availability of all agents. Another example, in a video game, is that each agent has its own information about their personal virtual character and the goal is that all agents have the information of all virtual characters.

Recently, gossip has been investigated with epistemic goals ([HM15], [CHM+16]): for instance, at the end, all agents knows that all agents have all the secrets, all agents knows that all agents knows that all agents have all the secrets, etc. A variety of epistemic gossip protocols are studied in [vdEp+17].

1.1.3 Multi-robot systems

Multi-robot systems are in many applications more robust that a single-robot:

- monitoring buildings;
- decontaminating component parts in a nuclear installation;
- evaluating defects in different types of constructions (buildings, bridges, etc.);
- measuring pollution, noise, etc.
• automated fertilizing (especially in permaculture for which environment is complex).

In such systems, robots have imperfect information about the real state, but still need to cooperate to perform complex tasks. They need to reason about strategies in an imperfect information setting. These strategies are called uniform (see \[vdHW03\]). Recently, a framework with knowledge-based programs that centrally synthesized but decentralized executed has been proposed \[SSZ18\]. The main advantages are the readability of programs: they are more succinct that reactive policies.

1.1.4 AI and games

AI computer programs now master humans in many perfect information games, such as Chess and Go. For instance, the technique used for Go is a combination of tree search and deep neural networks \[SHM+16\]. Imperfect information games is even more challenging. More recently, an efficient dedicated algorithm for poker has been created \[BFJT14\].

More interestingly, a big challenge in AI is to design a computer program that can play to arbitrary games \[CLP05\], without any bench of examples, but only with a description of rules (see for instance, the program Woodstock \[KLPTT17\]). The language used by the community of General Game Playing to describe game rules has recently extended for capturing epistemic features (\[Thi16\], \[JZPZ16\]).

Higher-order knowledge plays an important role in games, especially in card games, such as Cluedo \[vD02\], e.g. a player a may know that player b knows that a knows that the murderer is not Colonel Mustard and thus, play accordingly. Therefore, we claim that Dynamic Epistemic Logic can provide a suitable and rich framework to represent knowledge and actions of players.

1.1.5 Video games

Video games are typical examples of applications where artificial agents may take decisions. In order scenarios to be realistic, especially in role-playing games/strategic games, it is relevant to model higher-order knowledge in that context (see \[KWZ09\] and \[WZK08\] for preliminary attempts for scripting video games with higher-order knowledge-based programs). Realistic scenarios also require to model emotions of artificial agents. Knowledge/belief is a key ingredient of some emotions, such as counterfactual emotions \[LS11\] (e.g. agent a regrets p if a knows she could have prevented p and a desires p to be false) and higher-order knowledge is relevant for reasoning about emotions of other agents (e.g. agent b knows that agent a regrets p).

Also, from a theoretical perspective, models that incorporate epistemic features, help to measure the intrinsic difficulty of games. For instance, Coulombe and Lynch prove some undecidability results of the existence of winning strategies in video games \[CL18\], meaning it is impossible to design a program that plays perfectly to some video games.

1.1.6 Psychology

Sally and Anne is a psychological test developed in \[WP83\] to measure the ability to imagine that others have false beliefs. The test was experimented for real \[BCLF85\] and autistic children seem to have difficulties, if this claim is contradicted \[TF07\]. To some extent, we claim that Dynamic Epistemic Logic can help to model psychological tests, implement them in tools such as Hintikka’s world, predict and explain behaviors. Interestingly, Arslan et al. (\[AVTH15\], \[AVTH18\]) develop new methods for children to improve the learning of higher-order knowledge.
1.2 Outline of the book

Part 1: Modeling

- Chapter 2 presents Dynamic epistemic logic with the software Hintikka’s world. DEL provides a logical language for expressing high-order knowledge properties (e.g. agent $a$ knows that agent $b$ knows...) and models for representing epistemic states and epistemic actions. Typically, artificial agents reason by means of an epistemic state and check properties. It corresponds to the model checking approach, promoted by Halpern and Vardi [HV91].

- Chapter 3 introduces succinct models for Dynamic epistemic logic. In particular, we show how to represent succinctly epistemic states and epistemic actions.

Part 2: Decision problems

- Chapter 4 presents algorithms and complexity results for the model checking problem in DEL. Model checking could be used for bounded epistemic planning when the initial state is described by means of a Kripke model. It somehow corresponds to the “situated automata” approach ([Ros85], [RK86]).

- Chapter 5 focuses on the opposite approach: theorem proving. It corresponds to the standard approach in AI to knowledge representation [McC59]: an agent possesses a set of formulas, called a knowledge base, and she knows $\varphi$ if $\varphi$ is provable from the knowledge base. Rosenschein [Ros85] called this approach the “interpreted symbolic structures”. The main advantage is that a formula can embrace a set of epistemic states and not only one as in the model checking approach. Theorem proving could be used for bounded epistemic planning from any initial state satisfying a given formula.

- Chapter 6 presents an overview of (unbounded) epistemic planning. Planning is the following reachability problem: can we reach an epistemic state that satisfies a given epistemic goal? We show that it is undecidable in general and exhibits some decidable fragments.

- Chapter 7 focuses on a large decidable fragment of epistemic planning. In this case, more involved properties that just reachability, are decidable.

Part 3: Applicability in AI

The last part presents how models for epistemic states and epistemic actions may be inferred automatically in the following practical cases. In all cases, agents share common knowledge about assumptions about the system.

- Chapter 8 focuses on how epistemic states could be inferred from locations of physical agents, assuming common knowledge on visual abilities ([BGST13], [GGS15]).

- Chapter 9 depicts how epistemic states could be inferred in an asynchronous systems, assuming common knowledge about the behavior of message passing mechanism [KMS17].
Part I

Modeling
Chapter 2

Dynamic epistemic logic

In this chapter, we recall basics of Dynamic epistemic logic (DEL), a logical framework for reasoning about knowledge, factual and information change. We stick to the modern presentation of DEL, that is by means of so called event models (sometimes also called action models in the literature) to model information change ([BMS98b], [vvK08], [vBvEK06]).

We will use the muddy children puzzle [vDK15] as a running example. As shown in Figure 2.1, two children are looking at each others. They know that they know that... (i.e. it is common-knowledge) that each does not know whether her forehead is muddy or not and that each knows the state of the forehead of the other.

Let $AP$ be a countably infinite set of atomic propositions, whose typical members are denoted by $p$, $q$, etc. Atomic propositions are atomic facts in worlds, for instance ‘child a forehead is muddy’. and let $AGT$ be a countably infinite set of agents, whose typical members are denoted by $a$, $b$, etc. In the muddy children example, there are two agents that are the two children.

2.1 Epistemic models

In order to model an epistemic situation as shown in Figure 2.1, Saul Kripke ([Kri63], [Hin86]) introduced graphs of possible worlds, called epistemic models. It is the underlying structure used by the software Hintikka’s world. Actually, by clicking on agents in the software, it shows the unraveling of a epistemic model (see Figure 2.2 that shows the example of two muddy children [McC87]) by means of thought bubbles.

Definition 1 An epistemic model $M = (W, (Ra)_{a \in AGT}, V)$ is a tuple where:

- $W$ is a non-empty finite set of possible worlds,
- $Ra \subseteq W \times W$ is an accessibility relation for agent $a$,
- $V : W \rightarrow 2^{AP}$ is a valuation function.

The intended meaning of $wRaU$ is that in world $w$ agent $a$ considers that $u$ might be the actual world. The function $V$ maps each world $w$ to the subset of atomic propositions $V(w) \subseteq AP$ that hold in $w$. A pair $(M, w)$ is called a pointed epistemic model or simply a state. In a state $(M, w)$, $w$ is called the real world. In Hintikka’s world, the real world is the single world shown outside any thought bubbles. We also use the notation $S$ to denote a state.
Possible worlds for agent $a$ in one of the possible world of agent $b$ in one of the possible world of agent $a$

Possible worlds for agent $b$ in one of the world of agent $a$

Possible worlds for agent $a$

Real world

Figure 2.1: Muddy children with two children in Hintikka’s world.

Example 3 (Two muddy children) Figure 2.2 shows the Kripke model defined by $M = (W, (R_a)_{a \in AGT}, V)$ with

- $W = \{w_{00}, w_{01}, w_{10}, w_{11}\}$,
- $R_a = \{(w_{00}, w_{00}), (w_{01}, w_{01}), (w_{10}, w_{10}), (w_{11}, w_{11}), (w_{00}, w_{10}), (w_{10}, w_{00}), (w_{01}, w_{11}), (w_{11}, w_{01})\}$,
- $R_b = \{(w_{00}, w_{00}), (w_{01}, w_{01}), (w_{10}, w_{10}), (w_{11}, w_{11}), (w_{00}, w_{01}), (w_{01}, w_{00}), (w_{10}, w_{11}), (w_{11}, w_{10})\}$,
- $V(w_{00}) = \emptyset, V(w_{01}) = \{m_b\}, V(w_{10}) = \{m_a\}, V(w_{11}) = \{m_a, m_b\}$.

The atomic propositions $m_a$ and $m_b$ are read as `agent $a$ (resp. $b$) is muddy'. The set $W$ contain the four possible configurations. The relation $R_a$ contains the pairs of worlds of the form
(w_i, w_i), that is pairs of worlds in which the forehead state i of agent b is the same. The relation R_b is defined symmetrically. The valuation function V informs which agents are muddy or not in a given world. Figure 2.1 depicts the state M, w_{11}. The real world is w_{11}, the world in which both agents a and b are muddy. The possible worlds for agent a are w_{11} and w_{01}.

The two muddy children puzzle generalizes to n children. In the following example, a world is represented by the subset of agents that are the muddy ones.

**Example 4 (n muddy children)** The Kripke model is \( M = (W, (R_a)_{a \in AGT}, V) \) with

- W is the set of subsets of AGT;
- for all agents a, \( R_a = \{ (w, u) \in W \times W \mid w \setminus \{a\} = u \setminus \{a\} \} \);
- \( V(w) = \{ p_a \mid a \in w \} \).

The relation \( R_a \) contains pairs \((w, u)\) such that in both \( w \) and \( u \), all forehead states for all agents except a are the same. The valuation \( V(w) \) paraphrases the fact that muddy children in \( w \) are exactly those who belong to the subset \( w \).

**Example 5 (Belote)** In the card game Belote, the initial configuration of the game is a possible distribution of 8 cards per players, among 4 players as shown in Figure 2.3.

Let AGT a set of 4 players. Let \( C \) be the set of 32 cards. Such an initial configuration is a partition \( \vec{H} = (H_a)_{a \in AGT} \) of \( C \) such that for all \( a \in AGT \), \( |H_a| = 8 \). The initial epistemic state corresponding to the initial configuration for the game Belote is defined by \( M = (W, (R_a)_{a \in AGT}, V) \) where:

- W is the set of possible initial configurations \( \vec{H} \);
- for all \( a \in AGT \), \( R_a = \{ (\vec{H}, \vec{H}') \in W \mid H_a = H'_a \} \);
- \( V(\vec{H}) = \{ p_{ac} \mid c \in H_a \} \).

The relation \( R_a \) is defined so that agent a considers another world \( \vec{H}' \) in \( \vec{H} \) iff she owns the same cards in \( \vec{H} \) and \( \vec{H}' \). The valuation simply introduces propositions \( p_{ac} \) for ‘agent a owns card c’.
Example 6 (Hanabi)  Contrary to classical games, such as Belote, interestingly, in the card game Hanabi, a player sees the cards of the other players but her own cards.

\[ \text{Figure 2.4: A possible initial configuration of the game Hanabi.} \]

The initial configuration of the game is a possible distribution of 5 cards per player, among 4 players as shown in Figure 2.4. Let AGT a set of 4 players. Let C be the set of 32 cards. Such an initial configuration is a partition \( \vec{H} = (H_a)_{a \in AGT} \) of a subset of C such that for all \( a \in AGT, |H_a| = 5 \). The initial epistemic state corresponding to the initial configuration for the game Belote is defined by \( M = (W, (R_a)_{a \in AGT}, V) \) where:

- \( W \) is the set of possible initial configurations \( \vec{H} \);
- for all \( a \in AGT, R_a = \{ (\vec{H}, \vec{H}') \in W \mid \text{for all } a' \in AGT \setminus \{a\}, H_a = H'_{a'} \} \);
- \( V(\vec{H}) = \{ p_{ac} \mid c \in H_a \} \).

For Hanabi, the relation \( R_a \) is defined so that agent \( a \) considers another world \( \vec{H}' \) in \( \vec{H} \) iff she sees the same cards in \( \vec{H} \) and \( \vec{H}' \) for the other players.

An epistemic model is said to be S5 if the accessibility relations were equivalence relations.

<table>
<thead>
<tr>
<th></th>
<th>Agent a always consider the real world as possible</th>
<th>Reflexivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>wRa w</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>Agent a always consider a world as possible</td>
<td>Seriality</td>
</tr>
<tr>
<td></td>
<td>there is u such that wRa u</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Agent a is positively introspective</td>
<td>Transitivity</td>
</tr>
<tr>
<td></td>
<td>wRa u and uRa v implies wRa v</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Agent a is negatively introspective</td>
<td>Euclideanity</td>
</tr>
<tr>
<td></td>
<td>wRa u and u Ra v implies wRa v</td>
<td></td>
</tr>
</tbody>
</table>

Table 2.1: Relevant properties of epistemic models.

Our setting also captures belief, that is epistemic models that said to be KD45 and that satisfy properties D, 4, 5 of Table 2.1. Whereas possible worlds for an agent \( a \) form an equivalence class in S5 models, KD45 models just exclude the real world from the set of possible worlds as shown in Figure 2.5.
2.2. EPISTEMIC LOGIC

By generality, our setting also captures weak notion of belief/knowledge for which $D$, 4 or 5 may be dropped.

Example 7 Figure 2.6 shows a state made up of two worlds $w$ and $u$. World $w$ is the real world in which all propositions are false. Agent $a$ imagines a sole possible world $u$ in which proposition $p$ is true.

![Figure 2.6: Epistemic model for an agent $a$ believing $p$ whereas $p$ is false.](image)

2.2 Epistemic logic

The language of epistemic logic, $\mathcal{L}_{EL}$, is the language of propositional logic extended with one knowledge modality for each agent. Intuitively, $K_a\varphi$ reads as “agent $a$ knows/believes that $\varphi$ holds”.

2.2.1 Syntax

The syntax of $\mathcal{L}_{EL}$ is given by the following grammar:

$$\varphi ::= p \mid \neg \varphi \mid (\varphi \lor \varphi) \mid K_a \varphi$$

where $p$ ranges over $AP$ and $a$ ranges over $AGT$. We define the usual abbreviations $(\varphi_1 \land \varphi_2)$ for $\neg(\neg \varphi_1 \lor \neg \varphi_2)$ and $K_a \varphi$ for $\neg K_a \neg \varphi$. The size of $\varphi$ is the number of operators needed to write $\varphi$. There are three possible epistemic attitudes for agent $a$ w.r.t a formula $\varphi$:

- $K_a \varphi$: agent $a$ knows $\varphi$;
- $K_a \neg \varphi$: agent $a$ knows that $\varphi$ is false;
- $\neg K_a \varphi \land \neg K_a \neg \varphi$: agent $a$ is ignorant about the truth value of $\varphi$. 

Figure 2.5: Differences between S5 and KD45 models

![Figure 2.5: Differences between S5 and KD45 models](image)
Example 8 Let us consider atomic propositions $m_a$ and $m_b$ that are respectively read ‘agent $a$ is muddy’ and ‘agent $b$ is muddy’. The formula $(K_a m_b \lor K_a \neg m_b)$ is in $\mathcal{L}_{\text{EL}}$, and is read ‘either agent $a$ knows that $b$ is muddy or agent $a$ knows that $b$ is not muddy’ or better ‘agent $a$ knows whether $b$ is muddy or not’. Formula $(\neg K_a m_a \land \neg K_a \neg m_a)$ is read ‘agent $a$ does not know whether $a$ is muddy or not’.

Formula $K_a K_b ((K_a m_b \lor K_a \neg m_b) \land (\neg K_a m_a \land \neg K_a \neg m_a))$ is read ‘agent $a$ knows that agent $b$ knows that agent $a$ knows whether $b$ is muddy or not but agent $a$ does not know whether $a$ is muddy or not’.

2.2.2 Semantics

The semantics of $\mathcal{L}_{\text{EL}}$ is given in terms of pointed epistemic models. We define the truth condition relation $\mathcal{M}, w \models \varphi$, read as ‘formula $\varphi$ holds in the pointed epistemic model $(\mathcal{M}, w)$.

**Definition 2** $\mathcal{M}, w \models \varphi$ is defined by induction on $\varphi$:

- $\mathcal{M}, w \models p$ if $p \in V(w)$;
- $\mathcal{M}, w \models \neg \varphi$ if it is not the case that $\mathcal{M}, w \models \varphi$;
- $\mathcal{M}, w \models (\varphi \lor \psi)$ if $\mathcal{M}, w \models \varphi$ or $\mathcal{M}, w \models \psi$;
- $\mathcal{M}, w \models K_a \varphi$ if for all $u$ such that $wR_a u$, $\mathcal{M}, u \models \varphi$.

Example 9 In the model depicted in Figure 2.2, we have:

$\mathcal{M}, w_{11} \models K_a K_b ((K_a m_b \lor K_a \neg m_b) \land \neg K_a m_a \land \neg K_a \neg m_a)$.

A formula $\varphi$ is satisfiable if there exists a pointed Kripke model $\mathcal{M}, w$ such that $\mathcal{M}, w \models \varphi$. A formula $\varphi$ is valid if for all pointed Kripke models $\mathcal{M}, w$, we have $\mathcal{M}, w \models \varphi$.

2.2.3 Common knowledge

Common knowledge $[\text{HM90a}]$ is a condition for agents to act simultaneously. Common knowledge of $\varphi$ among agents in group $G \subseteq \text{AGT}$ is the fact all agents in $G$ knows that agents in $G$ knows that ... agents in $G$ knows that $\varphi$. We augment the language $\mathcal{L}_{\text{EL}}$ with the common knowledge construction $C_{G}\varphi$ read as ‘property $\varphi$ is commonly known by the group $G$’. The obtained language is $\mathcal{L}_{\text{ELCK}}$, and is defined by the following grammar:

$$\varphi ::= p \mid \neg \varphi \mid (\varphi \lor \psi) \mid K_a \varphi \mid C_G \varphi$$

where $p$ ranges over $\text{AP}$, $a$ ranges over $\text{AGT}$, and $G$ ranges over $2^{\text{AGT}}$.

The semantics of $\mathcal{L}_{\text{ELCK}}$ extended by the following clause:

- $\mathcal{M}, w \models C_G \varphi$ if for all $u \in W, wR_G u$ implies $\mathcal{M}, u \models \varphi$ where $R_G$ is the transitive closure of $\bigcup_{a \in G} R_a$.

Example 10 This example just shows the relevance of common knowledge in game theory, for the so-called iterated deletion of strictly dominated strategies. Let assume that the following normal form game is common knowledge among players $a$ and $b$. The following table gives the payoffs of the agents. For instance, if $a$ plays action $A$ and $b$ plays $\beta$, then agent $a$ receives a payoff of $4$ and agent $b$ receives a payoff of $1$. 
We also assume that there is common knowledge that $a$ and $b$ are rational. In that case, player $a$ will actually never play action $B$: indeed, whatever $b$ plays, $a$ will always get a better payoff by playing $A$. In the same way, player $b$ will never play $\beta$ (do you see why?). Actually, as it is common knowledge that players are rational, it is common knowledge that $B$ and $\beta$ will never be played and we are left with the following new game:

<table>
<thead>
<tr>
<th></th>
<th>$a : A$</th>
<th>$a : B$</th>
<th>$a : C$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b : \alpha$</td>
<td>$a : 5, b : 2$</td>
<td>$a : 2, b : 7$</td>
<td>$a : 4, b : 0$</td>
</tr>
<tr>
<td>$b : \beta$</td>
<td>$a : 4, b : 1$</td>
<td>$a : 3, b : 4$</td>
<td>$a : 9, b : 6$</td>
</tr>
<tr>
<td>$b : \gamma$</td>
<td>$a : 6, b : 3$</td>
<td>$a : 2, b : 6$</td>
<td>$a : 3, b : 8$</td>
</tr>
</tbody>
</table>

Now in the same way, we see that $a$ will not play $C$ since it is always better to play $A$. For $b$ it is always better to play $\gamma$. We finally end up with the following game:

<table>
<thead>
<tr>
<th></th>
<th>$a : A$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b : \gamma$</td>
<td>$a : 6, b : 3$</td>
</tr>
</tbody>
</table>

Unfortunately, Halpern and Moses [HM90b] showed that common knowledge cannot be attained when communication may fail. To see that, they considered the so-called coordinated attack problem [MV04, p. 64]. Clark explains the role of common knowledge via the consecutive number game [Cla02]. Interestingly, the concept of common knowledge has been generalized for agents to act in different point in time: timely common knowledge [GM13]. Common knowledge is impossible to

2.3 Event models

In some mathematical models in the literature, such as epistemic temporal models [vBGP07], transition systems, concurrent game structures, decPOMDP (decentralized Partially Observable Markov Decision Processes) [BGIZ02], interpreted systems [FMHV03], the dynamics of systems is set in stone: the executability of an action $A$ is directly indicated in the model – let say by the presence of an outgoing edge labelled by $A$ from state $s$ to $s'$. The effect of an action is also directly indicated by the state $s'$.

However, it is often challenging to model complex actions, in a transition system e.g. the public announcement $A$ of a true formula $K_a p$. Indeed, adding an edge from $s$ to $s'$ by $A$ would require:

1. to actually know at the design of the model whether formula $K_a p$ holds in $s$;
2. to guarantee that the accessibility relations for the knowledge in state $s'$ indeed correspond to the very knowledge of agents after the announcement of $K_a p$.

Dynamic epistemic logic (DEL) takes another perspective: describing actions for generating epistemic temporal structures. In DEL, actions are represented by event models as proposed by Baltag et al. [BMS98b]. This very description indicates in which states the action is executable.
and the effects of an action. In general DEL events can bring information and modify the world, and such events are called *ontic events* \[\text{vDK06}\]. Let us know give the definition of event models.

In this sense, DEL extends the approach taken in planning, where actions are also described. Finally, DEL extends epistemic logic with modalities that represent the occurrence of actions.

**Definition 3** An event model $\mathcal{E} = (E, (R_a^{E})_{a \in \text{AGT}}, \text{pre}, \text{post})$ is a tuple where:

- $E$ is a non-empty finite set of possible events,
- $R_a^{E} \subseteq E \times E$ is an accessibility relation on $E$ for agent $a$,
- $\text{pre} : E \rightarrow \mathcal{LELC}$ is a precondition function,
- $\text{post} : E \times \text{AP} \rightarrow \mathcal{LELC}$ is a postcondition function.

A pair $(E, e)$ is called a pointed event model, where $e$ represents the actual event. A pair $(\mathcal{E}, E_0)$ with $E_0 \subseteq E$ is called a multi-pointed event model, where $E_0$ represents the set of possible actual events. Pointed event models correspond to deterministic actions and multi-pointed event models correspond non-deterministic actions. We may confuse $(\mathcal{E}, e)$ and $(\mathcal{E}, \{e\})$. Sometimes, especially in Chapter 6, a pointed event model is called an action and is denoted by $A$.

Interestingly, we can define intuitive restrictions on the shape of event models that correspond to different types of actions.

**Definition 4** We say that $\mathcal{E}$ is purely epistemic, or is without postconditions, or has no postconditions if the postcondition function is trivial in the following sense: for all event $e$, for all atomic propositions $p$,

$$\text{post}(e, p) = p.$$ 

**Definition 5** We say that $\mathcal{E}, e$ is a public action if for all agents $a$, $(e, e)R_a^{E}$ and for all events $e'$, $(e, e')R_a^{E}$ implies $e' = e$.

**Definition 6** We say that $\mathcal{E}, e$ is a public announcement of $\varphi$ if it is a public action, $\text{pre}(e) = \varphi$ and if for all event $e$, for all atomic propositions $p$, $\text{post}(e, p) = p$. In picture:

In words, the public announcement of $\varphi$ corresponds to an event where it is common knowledge that a true message $\varphi$ is received by all agents. The public announcement of $\varphi$ is modelled by a pointed event model made up of a single possible event, with reflexive loops for each agent, whose precondition is $\varphi$ and whose postcondition is trivial (truth values of atomic propositions are unchanged). In picture:

```
 a, b
 ========
     \cap
       \uparrow
a, b
  \downarrow
\text{pre} : \varphi
\text{post} : / 
```

The logic containing only public announcements was originally studied on its own and was proposed by [Pla07] earlier than the development of event models.

**Example 11 (private announcement)** The private announcement of the message $A$ to agent $a$  

\footnote{We use the word *action* although according to \texttt{aud15}, an action should always have an author.}
is modelled by the following pointed event model

Example 12 (Sally and Anne) Sally and Anne (agent \( a \)) moves the marble from the basket into the box while Sally (agent \( b \)) is outside. Proposition \( p \) stands for ‘the marble is in the basket’. This event is modelled by the following pointed event model:

In the real event \( e \), the marble is actually removed from the basket (\( p \leftarrow \bot \)) whereas the marble is not moved in the event \( f \) imagined by agent \( b \).

Example 13 (Learn publicly the value of \( p \)) It is modelled by the following multi-pointed event model:

Example 14 (Learning semi-privately the value of \( p \)) The fact that \( a \) is learning the value of \( p \) but and \( b \) knows that is modelled by the following multi-pointed event model:

Example 15 (Received or lost (example of Thomas Bolander)) The fact that \( a \) sends the message \( p \) to \( b \) or that the message may be lost is:

Example 16 (child getting muddy (example of Andreas Herzig)) The fact that child \( a \) is getting muddy while not knowing it, but agent \( b \) is noticing it is modelled by the following pointed event model
where \( m_a \) is an atomic proposition read as ‘agent a is muddy’.

**Example 17 (semi-private announcement)**

The semi-private announcement of the message A to agent a where agent b knows that the message is either A or B, while agent a not being aware that agent b knows it is modelled by the following pointed event model:

2.4 **Update products**

In this section, we describe how to compute the updated epistemic model resulting from the execution of an action in a given epistemic model. An event \( e \) can occur in a world \( w \) of an epistemic model \( \mathcal{M} \) if, and only if, its precondition is verified, i.e. \( \mathcal{M}, w \vDash pre(e) \), which leads to the following definition:

**Definition 7** Let \( \mathcal{M} = (W, (R_a)_{a \in AGT}, V) \) be a Kripke model. Let \( \mathcal{E} = (E, (R^E_a)_{a \in AGT}, pre, post) \) be an event model. The product of \( \mathcal{M} \) and \( \mathcal{E} \) is \( \mathcal{M} \otimes \mathcal{E} = (W', (R'_a), V') \) where:

1. \( W' = \{(w, e) \in W \times E \mid \mathcal{M}, w \vDash pre(e)\} \);
2. \((w, e)R'_a(w', e')\) iff \( wR_a w' \) and \( eR^E_a e' \);
3. \( V'((w, e)) = \{p \in AP \mid \mathcal{M}, w \vDash post(e, p)\} \).
2.5 Dynamic language

The language $\mathcal{L}_{DELCK}$ extends $\mathcal{L}_{ELCK}$ with dynamic modalities and is defined by the following BNF:

$$
\phi ::= \top \mid p \mid \neg \phi \mid (\phi \lor \psi) \mid K_a \phi \mid C_G \phi \mid (\langle E, E_0 \rangle) \phi
$$

with $p \in AP$, $a \in AGT$. Formula $\langle E, E_0 \rangle \phi$ reads as “There is an executable event in $E_0$ and $\phi$ holds after having executed it”. We define the dual construction $[E, E_0]! \neg \phi$ for $\neg (\langle E, E_0 \rangle \neg \phi)$, that is read as “For all executable events in $E_0$, $\phi$ holds after having executed it”.

Definition 8 We extend the definition $M, w \models \phi$ to $\mathcal{L}_{DELCK}$ with the following clause:

- $M, w \models (\langle E, E_0 \rangle) \phi$ if there exists $e \in E_0$ s.th. $M, w \models pre(e)$ and $M \otimes E, (w, e) \models \phi$. 

The product of a pointed epistemic model $(M, w)$ with a pointed event model $(E, e)$ is defined as $(M \otimes E, (w, e))$ if $M, w \models pre(e)$, otherwise it is undefined.

An event is $e$ is said executable in a world $w$ if its precondition $pre(e)$ holds in $w$.

The update product helps to define epistemic temporal structures that correspond to the application of several update products from an initial state. They are called DEL structures but are defined later (see Definition 44). Let us point out two implicit assumptions made up in DEL:

- **synchronicity**: the set of possible worlds in $M \otimes E$ are all pairs; it is common knowledge that exactly one event occurred when an action is executed (see item 1 of Definition 7);

- **perfect recall** (also known as no forgetting): if $w$ and $w'$ are distinguished by agent $a$, $(w, e)$ and $(w', e')$ are distinguished by agent $a$ too (see item 2 of Definition 7); it is impossible to model an action that makes an agent forgetting what she learned.
CHAPTER 2. DYNAMIC EPISTEMIC LOGIC

Example 18 Figure [2.7] shows an example of an epistemic model $\mathcal{M}$, an event model $\mathcal{E}$ and its product $\mathcal{M} \otimes \mathcal{E}$.

Definition 9 (public announcement logic) When $\mathcal{E}, e$ is the public announcement of $\varphi$, we write $\langle \varphi! \rangle$ instead of $\langle \mathcal{E}, e \rangle$. The language with dynamic operators that are public announcements and without common knowledge by $\mathcal{L}_{ELPA}$. The language with dynamic operators that are public announcements and with common knowledge by $\mathcal{L}_{ELCKPA}$.

Table 2.2 sums up the different languages considered in this book.

<table>
<thead>
<tr>
<th>Knowledge operators $K_a$</th>
<th>$\mathcal{L}_{EL}$</th>
<th>$\mathcal{L}_{ELCK}$</th>
<th>$\mathcal{L}_{ELPA}$</th>
<th>$\mathcal{L}_{DEL}$</th>
<th>$\mathcal{L}_{DELCK}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common knowledge $C_G$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Public announcement</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>dynamic operators $\langle \varphi! \rangle$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>General dynamic operators $\langle \mathcal{E}, e \rangle$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 2.2: Logical languages of epistemic logic.

2.6 Bisimulation and equivalence

We define notions of equivalence for models. The main motivation for bisimulation is, given an epistemic model for a given situation, to compute an equivalent model that is smaller. Figure 2.8 shows two pointed epistemic model that are actually equivalent (as we will see) and the model on the right is smaller that the one on the left.

2.6.1 Bisimulations for epistemic models

The usual notion of equivalence for epistemic models is bisimulation.

Definition 10 Let $AP$ be a finite set of atomic propositions, $\mathcal{M} = (W, (R_a)_{a \in AGT}, V)$ and $\mathcal{M}' = (W', (R'_a)_{a \in AGT}, V')$ be two Kripke models, $w \in W$ and $w' \in W'$. A relation $B \subseteq W \times W'$ is an $AP$-bisimulation between $\mathcal{M}$ and $\mathcal{M}'$ iff for all $w \in W, w' \in W'$ such that $wBw'$.
2.6. BISIMULATION AND EQUIVALENCE

- **Invariance:** \( V(w)|_{AP} = V'(w')|_{AP} \);
- **Zig:** for all \( u \in W \) such that \( wRu \) there exists \( u' \in W' \) such that \( w'R_u u' \) and \( Buu' \);
- **Zag:** for all \( u' \in W' \) such that \( w'R_u u' \) there exists \( u \in W \) such that \( wRu_u uBu' \).

We say that two pointed Kripke models \((M, w)\) and \((M', w')\) are \(AP\)-bisimilar if there is a \(AP\)-bisimulation \(B\) between \(M\) and \(M'\) with \(wBw'\). \((M, w)\) and \((M', w')\) are \(AP\)-bisimilar iff \((M, w) \models \varphi\) iff \((M', w') \models \varphi\) for all formulas \(\varphi\) of \(\mathcal{L}_{\text{DEL}}\), whose propositions are in \(AP\). When \(AP\) is clear from the context, we say bisimilar instead of \(AP\)-bisimilar. Two Kripke models \(M\) and \(M'\) are bisimilar if there exists \(w \in W\) and \(w' \in W'\) such that \((M, w)\) and \((M', w')\) are bisimilar.

**Example 19** Figure 2.8 shows two bisimilar pointed Kripke models. A bisimulation \(B\) is

\[ \{ (w_0, w'_0), (w, w_0), (u, u') \}. \]

2.6.2 Equivalence of event models

For event models, the equivalence is defined as follows.

**Definition 11** Let \((E, e)\) and \((E', e')\) be two pointed event models. They are equivalent if for all pointed Kripke models \((M, w)\), \((M \otimes E, (w, e))\) and \((M \otimes E', (w, e'))\) are bisimilar.

Equivalence of event models without postconditions is characterized by action emulations \((\mathcal{E}_{\text{ERS12}})\) defined as follows.

**Definition 12** Let \(E = (E, (\to_a)_{a \in \text{AGT}}, \pre)\) and \(E' = (E', (\to_a')_{a \in \text{AGT}}, \pre')\) be two event models without postconditions. Let \(\Sigma\) be the set of preconditions appearing in \(E\) and \(E'\). Let \(\hat{\Sigma}\) be the set of formulas containing \(\Sigma\) and closed under sub-formulas and negation (see [ERS12] for more details). Let \(CS(\hat{\Sigma})\) be the set of maximal consistent subsets of \(\hat{\Sigma}\). An action emulation \(AE\) is a set of relations \(\{ AE_{\Gamma} \}_{\Gamma \in CS(\hat{\Sigma})} \subseteq E \times E'\) such that whenever \(eAE_{\Gamma} e'\):

- **Invariance:** \(\pre(e) \in \Gamma\) and \(\pre(e') \in \Gamma\);
- **Zig:** For all \(f \in E\) and \(\Gamma' \in CS(\hat{\Sigma})\), if \(e \vdash_{\Gamma} f\), \(\pre(f) \in \Gamma'\) and the formula \((\bigwedge_{\psi \in \Gamma} \psi \land \bigwedge_{\psi' \in \Gamma'} \psi')\) is consistent then there exists \(f' \in E'\) such that \(e' \vdash_{\Gamma'} f'\) and \(fAE_{\Gamma'} f'\);
- **Zag:** symmetric of Zig for \(E'\).

Action emulation is similar to bisimulation in the sense that the types of rules are the same, except that instead of imposing equivalence for preconditions, we just ask here that they are in a same maximal consistent subset of \(\hat{\Sigma}\).

Action emulation characterizes equivalence: \((E, e)\) and \((E', e')\) are equivalent if there is an action emulation \(AE\) between \(E\) and \(E'\) such that for all and \(\Gamma \in CS(\hat{\Sigma})\) such that \(\pre(e) \in \Gamma\), we have \(eAE_{\Gamma} e'\).
2.7 Action tokens VS action types

Several logics for reasoning about the existence of an action have been developed. Instead of reasoning about a particular action token described by an action model, we reason about the existence of an action of a given type. Arbitrary public announcement logic \([FvD08]\) provides a construction \(\Diamond \psi\) read as ‘there exists a (\(\Diamond\)-free) formula \(\varphi\) that is true and such that \(\psi\) after announcing \(\varphi\)’. Group announcement logic is a variant of arbitrary public announcement logic \([ABvDS10]\), that provides constructions \(\Diamond_G \psi\) where \(G\) is a group of agents, for which the announced formula \(\varphi\) is of the form \(\bigwedge_{a \in G} K_a \varphi_a\).

Refinement modal logic \([BvDF^{+}14]\) corresponds to the logic for reasoning about arbitrary action models with trivial postconditions (the correspondance is treated by Prop. 14 in \([BvDF^{+}14]\), and Prop 4, 5 in \([vDF08]\)).

Aucher proposed a language to describe a class of action models by a formula over a similar language than epistemic logic \([Auc11]\).

2.8 Related work

2.8.1 Variant of epistemic models

The model used in robotics by Devin and Alami \([DA16]\) corresponds to Kripke structures where epistemic relations are functional. In other terms, any agent \(a\) has a single possible world that she imagines to be the real one. The same approach was used in \([BGB07]\). Although this restriction is reasonable for Sally and Anne, it is not relevant more complex cases, e.g. card games.

Dynamic epistemic logic, as presented in this chapter does not capture belief revision \([AGM85]\): an announcement of \(\varphi\) while an agent believing \(\neg \varphi\) will delete all possible worlds for that agent. Baltag and Smets extends DEL models for capturing belief revision \([BS06]\). Some authors distinguish implicit and explicit beliefs \([Lev84], [FH87], [Vel14]\). Lorini proposed models for implicit and explicit beliefs that are hybrid: they involves Kripke semantics and syntactic sets of formulas \([Lor18]\).

2.8.2 Interpreted systems

Interpreted systems \([FMHV03b]\) are an alternative to model distributed systems. Possible worlds are runs of the system and two runs are undistinguishable for agent \(a\) iff agent \(a\) has the same local state in both runs. Contrary to DEL, the setting of interpreted systems also capture asynchronous systems. However, the semantics is grounded: epistemic relations are not given but inferred, and are equivalence relations. Furthermore, it is not unclear how to model complex actions such as public/private announcements of modal formulas.

2.8.3 Action language VS transition systems

In the planning community, the description of actions is central. That is why, specification languages, as STRIPS \([FN71]\) and PDDL, enables to describe a collection of actions. Dynamic epistemic logic follows this very same tradition. However, the fact that epistemic situations and actions are both described by graphs is neat and powerful in terms of expressivity: higher-order updates are made very precise by event models. Also the description of actions is independent from the states they are applied in. Only the semantics of an action is dependent of the current state: the behavior of the announcement of \(\varphi\) depends on the truth values of \(\varphi\) in each possible world. The language mAL proposed in \([HGPS13]\) is a dynamic extension of epistemic logic with
2.8. RELATED WORK

constructions to express observability, awareness, communication, aimed at solved the so-called ramification problem. Thielscher proposed an epistemic extension of Game Description Language (Thi16, Thi17) by adding epistemic and perception constructions to the language.

On the contrary, in the verification community, they also tackle imperfect information, but actions themselves are not central and the system (or each part of the system) is described globally by a transition system. It is the case in concurrent game structures or in decPOMDPs (decentralized Partially Observable Markov Decision Processes) [BGIZ02]. Typically, a transition is labeled by a joint action of agents and observations. The observations are atomic; at first glance higher-order knowledge seems not important. However, even for these kind of models, higher-order knowledge plays a role for conciseness, as shown in [SSZ18]. It makes the framework less flexible: there is no description of actions; they are directly hard-coded in the transition system. For instance, it is unclear how to model a public announcement of a given formula $\phi$: it would require to compute the truth value of $\phi$ and to add the corresponding transitions. Interestingly, DEL and ETL (epistemic temporal logic) are compared in [vBGP07].

Importantly, we insist on the fact that having actions described in the logical languages enables to figure out syntactic fragments on the type of actions: public announcements, public actions, restrictions on the modal depth of preconditions, ontic actions, etc.

2.8.4 Learning models

Gerasimczuk proposes algorithms for learning event models from samples [Gie09].

2.8.5 Variant of event models

Similar alternatives to event models exist: arrow update [KR11], edge-conditioned event models [Bo14]. Analogously to the decomposition of integers as a product of prime numbers, an event model can decomposed. First, an event model (without postconditions) is equivalent up to modal depth $n$ to a program made up of instances of so-called test event model, non-determinism, sequence and a learning operation [FHT14]. Similarly, an event model can decomposed in terms of so-called copy and remove operators [AvDFS17].

Interestingly, Aucher studies the logical properties when epistemic models are multi-pointed, in order to capture internal perspective of agents [Auc12].
Chapter 3

Succinct representation

In classical DEL, Kripke models and event models are represented explicitly. It faces some practical limits when models become so large they cannot be stored in the memory of a computer.

Example 20 (Belote) The initial Kripke model for Belote (see Example 3) contains
\[
\binom{32}{8} \binom{24}{8} \binom{16}{8} = 9.95 \times 10^{16} \text{ worlds.}
\]

Example 21 (Hanabi) The initial Kripke model for Hanabi (see Example 6) contains
\[
\binom{50}{5} \binom{45}{5} \binom{40}{5} \binom{35}{5} = 5.5 \times 10^{23} \text{ worlds.}
\]

Also it may be exponential in the number of atomic propositions and/or the number of agents.

Example 22 (muddy children) The initial Kripke model for muddy children contains \(2^n\) worlds, where \(n\) is the number of agents.

In order to be able to automatically reason about such large models, we propose to define succinct models for DEL, i.e. succinct Kripke models and event models. Such models were originally introduced in [CS15] and [CS17], but we present the simplification of the definitions proposed in [CS18] compared to their original definitions. In particular, the presentation of the new definitions of succinct Kripke models and succinct event models are neater: their sets of atomic propositions and not mixed as in [CS17].

3.1 Accessibility programs

Instead of describing the epistemic relations \(R^a_A\) and \(R^e_E\) respectively in Kripke models and event models in extension, we describe them in intention by using accessibility programs. Technically, we use Dynamic Logic with Propositional Assignments proposed by Herzig et al. ([BHST14], [BHT13]). The use of them will become clear when succinct Kripke models are presented. First, let us recall the syntax and semantics of accessibility programs.

Definition 13 The syntax for accessibility programs is defined by the BNF
\[
\pi ::= p \leftarrow \beta \mid \beta ? \mid (\pi ; \pi) \mid (\pi \cup \pi)
\]
where \(p \in \text{AP}, \beta\) is a Boolean formula.
Program $p \leftarrow \beta$ reads as “assign atomic proposition $p$ to the truth value of $\beta$”. Program $\beta ?$ reads as “test $\beta$”. Program $\pi_1; \pi_2$ reads as “execute $\pi_1$ then $\pi_2$”. Program $(\pi_1 \cup \pi_2)$ reads as “either execute $\pi_1$ or $\pi_2$”. We write $\text{assign}(p_1, \ldots, p_n) = (p_1 \leftarrow \perp \cup p_1 \leftarrow \top); \ldots; (p_n \leftarrow \perp \cup p_n \leftarrow \top)$ for the program setting arbitrary values to $p_1, \ldots, p_n$.

**Definition 14** The semantics of $\pi$ is the binary relation over valuations defined by induction on $\pi$ as follows, where $w$ and $u$ are valuations:

- $w \xrightarrow{p \leftarrow \beta} u$ if $(u = w \setminus \{p\}$ and $w \not\models \beta$) or $(u = w \cup \{p\}$ and $w \models \beta$);
- $w \xrightarrow{\beta ?} u$ if $w = u$ and $w \models \beta ?$;
- $w \xrightarrow{\pi_1; \pi_2} u$ if there exists a valuation $v$ such that $w \xrightarrow{\pi_1} v$ and $v \xrightarrow{\pi_2} u$;
- $w \xrightarrow{\pi_1 \cup \pi_2} u$ if $w \xrightarrow{\pi_1} u$ or $w \xrightarrow{\pi_2} u$;

We distinguish a particular program $\text{assign}(p_1, \ldots, p_n)$ that allows to reach all worlds which may differ from the current one only on the valuation of propositions $p_1, \ldots, p_n$. This program non-deterministically assigns values to $p_1, \ldots, p_n$, namely:

$$\text{assign}(p_1, \ldots, p_n) = (p_1 \leftarrow \perp \cup p_1 \leftarrow \top); \ldots; (p_n \leftarrow \perp \cup p_n \leftarrow \top)$$

We now give examples of programs.

**Example 23 (Programs for muddy children)** Since child $a$ sees the forehead of $b$ but not her own, the program for $a$ amounts to modifying the truth value of $p_a$. That is, $\pi_a = \text{assign}(p_a)$, and symmetrically $\pi_b = \text{assign}(p_b)$.

**Example 24 (Program for an omniscient agent)** The program $\top ?$ represents an omniscient agent since the only reachable valuation with $\top ?$ is the actual valuation, the only possible world is the current one. For instance in the muddy children, the program of the father is $\pi_f = \top ?$.

**Example 25 (Program for an agent believing $p$)** Let $AP = \{p, q\}$. The program $\pi = p \leftarrow \top; \text{assign}(q)$ represents an agent $a$ that believes $p$ but is uncertain of $q$.

The size of an accessibility program corresponds to the number of operators needed to write the program. For instance, the mental program $(p \leftarrow \top) \cup (q?; p \leftarrow \perp)$ has size 10. The models are succinctly described by means of mental programs. We are interested here in describing Kripke models, event models and the product update.

### 3.2 Succinct Kripke models

From now on, we suppose that we have a set $AP$ to define the formulas. We now give the definition of succinct Kripke models.

#### 3.2.1 Definition

**Definition 15** A succinct Kripke model is a tuple $M = \langle AP_M, \beta_M, (\pi_a)_{a \in \text{AGT}} \rangle$ where $AP_M \supset AP$ is a finite set of atomic propositions, $\beta_M$ is a Boolean formula over $AP_M$, and $\pi_a$ is a program over $AP_M$ for each agent $a$.

The Boolean formula $\beta_M$ succinctly describes the set of epistemic states. Intuitively, each $\pi_a$ succinctly describes the accessibility relation $\rightarrow_a$ for an agent $a$. A pointed succinct Kripke model is a pair $M, w$ where $M = \langle AP_M, \beta_M, (\pi_a)_{a \in \text{AGT}} \rangle$ is a succinct Kripke model and $w$ is a valuation satisfying $\beta_M$. 
3.2. SUCCINCT KRIPKE MODELS

3.2.2 From succinct Kripke models to Kripke models

Definition 16 Given a succinct Kripke model $\mathfrak{M} = \langle AP, \beta, (\pi_a)_{a \in AGT} \rangle$, the Kripke model represented by $\mathfrak{M}$, noted $\mathcal{M}(\mathfrak{M})$ is the model $\mathcal{M} = (W, (R_a)_{a \in AGT}, V)$ where $W = \{w \in V(AP_{\mathcal{M}}) \mid w \models \beta \mathcal{M}\}; R_a = \{(w, u) \in W^2 \mid w \overset{a}{\rightarrow} u\}; V(w) = w$.

Example 26 In the muddy children example [McC87], each child does not know whether she is muddy or not, but knows the muddiness of the other children. If $m_a$ is a proposition for “child $a$ is muddy”, a succinct Kripke model is $\mathfrak{M} = \langle AP_{\mathcal{M}}, \beta_{\mathcal{M}}, (\pi_a)_{a \in AGT} \rangle$ with $AP_{\mathcal{M}} = \{m_a, a \in AGT\}$, $\beta_{\mathcal{M}} = T$ and $\pi_a = assign(m_a)$. This representation is polynomial in the number of agents $|AGT|$ whereas the non-succinct Kripke model has exponential size in $|AGT|$. Figure 3.1 shows $\mathcal{M}(\mathfrak{M})$ for two agents $a$ and $b$.

3.2.3 From Kripke models to succinct models

Any Kripke model can be represented as a succinct Kripke model of polynomial size in the worst case. To do so, we define a succinct Kripke model $\mathfrak{M}_{\mathcal{M}}$ representing the Kripke model $\mathcal{M}$ with respect to a set of propositions $AP$.

Definition 17 Let $\mathcal{M} = (W, (R_a)_{a \in AGT}, V)$ be a Kripke model. We define the succinct Kripke model $\mathfrak{M}_{\mathcal{M}} = \langle AP_{\mathcal{M}}, \beta_{\mathcal{M}}, (\pi_a)_{a \in AGT} \rangle$ where: $AP_{\mathcal{M}} = AP \cup \{p_w \mid w \in W\}; \beta_{\mathcal{M}} = \exists!\{(p_w \mid w \in W\} \land \bigwedge_{w \in W} p_w \Rightarrow desc(V(w)); \pi_a = \bigcup_{w R_a u} p_w; assign(AP_{\mathcal{M}}); p_u$.

The intended meaning of the fresh atomic propositions $p_w$ is to designate the world $w$ (as nominals in hybrid logic [Bla00]). Formula $\beta_{\mathcal{M}}$ describes the set $W$ and the valuation $V$. Program $\pi_a$ performs a non-deterministic choice over edges $w \rightarrow_a u$ and then simulate the transition $w \rightarrow_a u$. The following proposition states that $\mathfrak{M}_{\mathcal{M}}$ indeed represents $\mathcal{M}$.

Proposition 1 $\mathcal{M}(\mathfrak{M}_{\mathcal{M}}), \{p_u\} \cup V(w)$ and $\mathcal{M}, w$ are AP-bisimilar.

Proof.
We note $\mathcal{M} = (W, (\rightarrow_a)_{a \in AGT}, V)$ and $\mathcal{M}(\mathfrak{M}_{\mathcal{M}}) = (W', (\rightarrow_a')_{a \in AGT}, V')$. We define $B := \{(u, p_u \cup V(u)) \mid u \in W\}$. Let us prove that $B$ is a $AP$-bisimulation. Invariance of $B$ is routine. For Zig, consider $w \in W$. For all $u \in W$, if $w \rightarrow_a u$ then we can verify that $\mathcal{M}(\mathfrak{M}_{\mathcal{M}}), u \cup V(u) \models \beta_{\mathcal{M}}$ and that $p_u \cup V(w) \overset{a}{\rightarrow} p_u \cup V(u)$ so we have $w \rightarrow_a u$. The Zag property is symmetrical. $\blacksquare$

Example 27 The Kripke model $\mathcal{M}$ from Figure 2.7 is modeled by the succinct Kripke model $\mathfrak{M}_{\mathcal{M}} = \langle AP_{\mathcal{M}}, \beta_{\mathcal{M}}, (\pi_a)_{a \in AGT} \rangle$ with $AP_{\mathcal{M}} = \{p, p_{w_1}, p_u\}$, $\beta_{\mathcal{M}} = \exists!\{(p_u, p_w)\} \land (p_w \rightarrow p) \land (p_u \rightarrow \neg p)$ and $\pi_a = \bigcup_{w_1, w_2 \in W} p_{w_1}$. $assign(AP_{\mathcal{M}}); p_{w_2}$.
### 3.2.4 Succinctness of succinct Kripke models

To show the succinctness of succinct Kripke models, we describe a family of Kripke models having exponentially more compact representations with succinct Kripke models.

**Example 28** We consider the extension of the classical muddy children puzzle \cite{vDK15} where children may pay attention to the father or not (as in \cite{BoD16}). We introduce atomic proposition $m_a$ meaning that $a$ is muddy and atomic proposition $h_a$ meaning that agent $a$ hears (i.e. pays attention to) the announcements of the father. We consider the model $M = (W, (\rightarrow_a)_{a \in AGT}, V)$ where $W = \{m_a, h_a \mid a \in AGT\}$, $w \rightarrow_a u$ if $(w \models h_a) \iff (u \models h_a)$ and for all $b \neq a$ $(u \models m_b)$ and $V(w) = w$ for all $w \in W$.

In $M$, an agent $a$ will not distinguish two worlds $w$ from $u$ as long he sees the same forehead states for the other agents and his pay attention status is the same in both worlds.

Let us consider the family of models $M$ given in Example 28 for all number of agents $n$. The Kripke model $M$ is succinctly represented by the succinct Kripke model $\mathfrak{M} = (AP_M, \beta_M, (\pi_a)_{a \in AGT})$ defined by $\beta_M = \top$, $AP_M = \{h_a, m_a \mid a \in AGT\}$ and $\pi_a = \text{assign}(\{m_a\} \cup \{h_b \mid b \neq a\})$.

Formula $\beta_M = \top$ means that the set of possible worlds is the set of all valuations. Program $\pi_a$ changes propositions agent $a$ is uncertain of ($m_a$ and $h_b$ for all $b \neq a$) while the truth values of other propositions remain unchanged. Pointed Kripke models $M, w$ and $M(\mathfrak{M}), w$ are bisimilar. The number of worlds in $M$ is $2^{2^n}$ while the size of $\mathfrak{M}$ is $O(n^2)$ (each program $\pi_a$ is of size $O(n)$).

Furthermore, there is no bisimilar Kripke model $M'$ with less worlds than $M$ since all valuations appear exactly once in $M$.

### 3.3 Succinct event models

We adopt a similar method for succinct event models.

#### 3.3.1 Definition

**Definition 18** A succinct event model is a tuple $\mathcal{E} = (AP_{\mathcal{E}}, \chi_{\mathcal{E}}, (\pi_a, \mathcal{E})_{a \in AGT}, \text{pre}, \text{post})$ where $AP_{\mathcal{E}}$ is a set of atomic propositions disjoint from $AP$; $\chi_{\mathcal{E}}$ is a propositional formula over $AP_{\mathcal{E}}$ characterizing the set of events; $\pi_a, \mathcal{E}$ is a program over $AP_{\mathcal{E}}$ for all $a \in AGT$; $\text{pre}$ is a propositional formula over $AP_{\mathcal{E}} \cup L_{EL}(AP)$ (meaning that any atom from $AP_{\mathcal{E}}$ cannot be under the scope of a $C$ or a $\mathcal{E}$ operator); For all $p \in AP$, $\text{post}(p)$ is a propositional formula over $AP_{\mathcal{E}} \cup L_{EL}(AP)$.

#### 3.3.2 From succinct event models to event models

**Definition 19** Given a succinct event model $\mathcal{E} = (AP_{\mathcal{E}}, \chi_{\mathcal{E}}, (\pi_a, \mathcal{E})_{a \in AGT}, \text{pre}, \text{post})$, the event model represented by $\mathcal{E}$, noted $\hat{E}(\mathcal{E})$ is the model $(E, (R^E_a)_{a \in AGT}, \text{pre}, \text{post})$ on $AP$ where $E = \{v_e \in V(AP_{\mathcal{E}}) \mid v_e \models \chi\}; R^E_a = \{(v_e, v_{e'}) \mid v_e \xrightarrow{\pi_a, \mathcal{E}} v_{e'}\}; pre(v_e) = \text{pre} \land \text{desc}(v_e); post(v_e, p) = \text{post}(p) \land \text{desc}(v_e)$.

#### 3.3.3 From event models to succinct event models

We define a succinct event model $\mathcal{E}_{\mathcal{E}}$ representing the event model $\mathcal{E}$.
3.3. **SUCCINCT EVENT MODELS**

**Definition 20** Let \( \mathcal{E} = (E, (R^E_a)_{a \in \text{AGT}}, \text{pre}, \text{post}) \) be an event model on \( AP \). We define the succinct event model \( \mathcal{E}_E = (AP_E, \chi_E, (\pi_a)_a \in \text{AGT}, \text{pre}, \text{post}) \) where \( AP_E = \{p_e \mid e \in E\}; \chi_E = \exists! (AP_E); \pi_a,E = \bigcup_{e \in E} p_e e \); \( \text{pre} = \bigwedge_{e \in E} (p_e \rightarrow \text{pre}(e)); \text{post}(p) = \bigwedge_{e \in E} (p_e \rightarrow \text{post}(e,p)) \).

The fresh atomic proposition \( p_e \) designates event \( e \). Formula \( \chi_E \) describes the set \( E \) and the precondition \( \text{pre} \). Program \( \pi_a,E \) performs a non-deterministic choice in the same spirit of \( \pi_a \) in Definition 17. Program \( \text{post} \) non-deterministically chooses the current event \( e \) and applies the postcondition assignments in parallel. The following proposition states that \( \mathcal{E}_E \) indeed represents \( \mathcal{E} \).

**Example 29** The event model \( \mathcal{E} \) of Figure 3.2 is modeled by the succinct event model \( \mathcal{E}_E \) with \( AP_E = \{p_{e1}, p_{f}\}, \chi_E = \exists! (AP_E) \land (p_{e1} \rightarrow p) \land (p_f \rightarrow T) \), \( \pi_a,E = \bigcup_{e \in E} p_e a \); \( \text{assign}(AP_M \cup AP_E); p_{e1} \); and \( \text{post} = (p_{e1} ; p \leftarrow \bot) \lor (p_f ?) \) (trivial postcondition counterpart in \( \text{post} \) has been omitted).

**Proposition 2** \( \mathcal{E}(\mathcal{E}_E) \) and \( \mathcal{E} \) are equivalent.

### 3.3.4 Succinctness of succinct event models

As for succinct Kripke models, we provide a family of event models having exponentially more compact representations with succinct event models.

**Example 30** We focus on the notion of attention-based announcement of \( p \) as shown in [BvDH+10]. In addition to classic atomic propositions, we add propositions \( h_a \) for “agent \( a \) is listening to the announcement”. The attention-based announcement of \( p \) can be then represented by the event model \( \mathcal{E} = (E, (\rightarrow^E_a)_{a \in \text{AGT}}, \text{pre}) \) where:

- \( E = \mathcal{V}(\{p\} \cup \{h_a \mid a \in \text{AGT}\}) \cup \{\text{idle}\} \);
- for all \( a, e \rightarrow^E_a f \) if \( e \neq \text{idle}, f \neq \text{idle}, e \models h_a \) and \( f \models p \);
- for all \( a, e \rightarrow^E_a \text{idle} \) if \( e \neq \text{idle} \) and \( e \not\models h_a \);
- for all \( a, \text{idle} \rightarrow^E_a \text{idle} \);  
- \( \text{pre}(e) = \begin{cases} \text{desc}(e) & \text{if } e \neq \text{idle} \\ T & \text{otherwise.} \end{cases} \)

**Figure 3.3** shows the event model of the attention-based announcement of \( p \) for two agents \( a_1 \) and \( a_2 \). Event idle is the event where nothing happens. The relation \( \rightarrow^E_a \) is defined as follows: if \( a \) is listening (\( e \models h_a \)) then \( a \) believes that \( p \) has been announced (\( f \models p \)). If \( a \) is not listening (\( e \not\models h_a \)) then \( a \) believes nothing happens. The precondition is defined to match the fact that...
attentive agents listen to the announcement of $p$ (thus leading to events where $p$ holds) and that other agents believe that nothing happened (thus the $\top$ precondition on $\text{idle}$). The announcement is purely epistemic so the postcondition function is trivial.

Let us consider the family of models $(\mathcal{E}_n)_{n \in \mathbb{N}}$ given in Example 30 for all number of agents $n$. The event model $\mathcal{E}$ is succinctly represented by the succinct event model $\mathcal{E} = (\mathcal{E}_n)_{n \in \mathbb{N}}$ defined by

- $\chi_E = \top$;
- $\pi_{a,E} = (\lnot \text{idle} ?; (\text{idle} ; p \leftarrow \top; \text{assign} \{ (h_a, b \in AGT) \}) \cup (\lnot h_a ?; \text{assign} (AP_M); p_{\text{idle} \leftarrow \top})) \cup (p_{\text{idle} ?}; \text{assign} (AP_M))$;
- $\text{post} = \top ?$.

Atomic proposition $p_{\text{idle}}$ intuitively means that the event $\text{idle}$ is occurring (at the bottom in Figure 3.3). Formula $\chi_E = \top$ means that the set of possible events is unconstrained. Program $\pi_{a,E}$ works as follows: If $p_{\text{idle}}$ is false, if $h_a$ is true, assign $\top$ to $p$ and arbitrarily change $h_b$ for all $b \neq a$; if $h_a$ is false, change valuations of propositions in $AP_M$ and set $p_{\text{idle}}$ to true; otherwise if $p_{\text{idle}}$ is true, change all truth values of propositions in $AP_M$. The number of worlds in $\mathcal{E}$ is $2^{n+1} + 1$ while the size of $\mathcal{E}$ is $O(n^2)$ (each program $\pi_{a,E}$ is of size $O(n)$).

Now we prove that standard event models cannot represent $\mathcal{E}_n$ as succinctly as succinct event models.

**Theorem 1** There is no propositional event model $\mathcal{E'}_n$ equivalent to $\mathcal{E}_n$ with less than $2^n$ events.

**Proof.**

We use the characterization of equivalent models with action emulations (Definition 12). We suppose that there is an action emulation $AE$ between $(\mathcal{E}_n, e)$ and $(\mathcal{E'}_n, e')$ for some $e \in \mathcal{E}_n$ and $e' \in \mathcal{E'}_n$. Let $\Sigma$ be the set of preconditions of $\mathcal{E}_n$ and $\mathcal{E'}_n$. Note that $\Sigma$ (defined as in Definition 12) is a set of propositional formulas. Let $\mathbf{e}_1$ and $\mathbf{e}_2$ be two valuations in $\mathcal{V}(\{p\} \cup \{h_a \mid a \in AGT\})$.
such that \( e_1 \models p \) and \( e_2 \models p \) and \( e_1 \neq e_2 \).

Suppose that there is \( e' \) of \( E' \) such that \( e_1 \models \neg h_a \) and \( e_2 \models h_a \) (we swap \( e_1 \) and \( e_2 \) if \( e_1 \models h_a \) and \( e_2 \models \neg h_a \)). Then \( e_1 \rightarrow \xi_a \) idle. We consider the maximal consistent subset \( \Gamma' = \{ \phi \in \hat{\Sigma} | \{ h_a, a \in AGT \} \models \phi \} \). We have \( \text{pre}(idle) \in \Gamma' \) and the formula \( \left( \bigwedge_{\psi \in \Gamma_1} \psi \land \hat{K}_a \land \bigwedge_{\psi' \in \Gamma'} \psi' \right) \) is consistent (because \( \Gamma_1 \) and \( \Gamma' \) are propositional). By Zig, there exists \( f' \in E' \) such that \( e' \rightarrow \xi_a f' \) with \( idle \models AE_{\Gamma'} f' \). By Zag, as \( e_2 \models AE_{\Gamma_2} e' \) and the formula \( \left( \bigwedge_{\psi \in E_{\Gamma_2}} \psi \land \hat{K}_a \land \bigwedge_{\psi' \in \Gamma'} \psi' \right) \) is consistent, there exists \( f \in E \) such that \( e \rightarrow \xi_a f \) and \( f \models AE_{\Gamma'} f' \). By invariance we obtain \( \text{pre}(f) \in \Gamma' \). However \( \text{pre}(f) = \text{desc}(f) \) and \( p \in f \) so \( \{ h_a, a \in AGT \} \not\models \text{pre}(f) \). Therefore we derive a contradiction.

This proves that there are at least \( 2^n \) events. ■

3.4 Language of succinct DEL

We define the language \( \mathcal{L}_{\text{succDEL}} \):

\[
\phi ::= \top \mid p \mid \neg \phi \mid (\phi \lor \phi) \mid K_a \phi \mid \langle E, \beta_0 \rangle \phi
\]

where \( E \) is a succinct event model over \((AP_M, AP_E)\) and \( \beta_0 \) is a Boolean formula over \( AP_M \cup AP_E \).

The syntax of succinct DEL is similar to the syntax of DEL itself except that operators \( \langle E, \beta_0 \rangle \) (where \( E, \beta_0 \) is a multi-pointed event model) are replaced by \( \langle E, \beta_0 \rangle \) where \( \beta_0 \) is a Boolean formula that succinctly represents a set of events \( E_0 \). The semantics of \( \langle E, \beta_0 \rangle \) is:

- \( M, w \models \langle E, \beta_0 \rangle \phi \) iff there exists \( e \in \hat{E}(E) \) such that \( e \models \beta_0 \), \( M, w \models \text{pre}(e) \) and \( M \otimes \hat{E}(E), (w, e) \models \phi \) where \( \text{pre}(e) \) is the precondition of \( e \) in \( \hat{E}(E) \).

We write \( M \otimes \hat{E}, w \models \phi \) for \( M \otimes \hat{E}, w \models \phi \).
Part II

Decision problems
Chapter 4

Model checking

In this chapter, we will discuss the following model checking problem.

**Definition 21** The model checking of DEL is defined as follows:

- **Input:** a pointed epistemic model \( M, w \) and a formula \( \varphi \in L_{DEL CK} \);
- **Output:** yes if \( M, w \models \varphi \), no otherwise.

### 4.1 Motivation

In 1991, Halpern and Vardi wrote a manifesto published at KR [HV91], in favor of using model checking in applications where agents have knowledge, opposed to using theorem proving. Typically, in model checking, a pointed epistemic model completely describe the current state of affairs and is given as an input, together with a formula to check.

For instance, let us consider a centralized application: offline video games. In an offline video game, all the data are stored in a single computer and the real world \( w \) is stored. A pointed epistemic model \( M, w \) may represent the epistemic situation of all virtual agents in a given scene. Virtual agents may be programmed with knowledge-based programs where conditions in if-statements are epistemic properties. We then require to evaluate the truth value of a given if-statement condition \( \varphi \) in the current state of affairs \( M, w \).

In a decentralized application such as a system of autonomous robots that do not share memory, we may imagine that each robot \( a \) is equipped with an epistemic model \( M \) and a set of possible worlds she considers as possible (see [Auc10]). In that case, each robot may evaluate formulas of the form \( K_a \varphi \), whose semantics does not depend on the chosen possible world she considers as possible. Therefore, in the decentralized case, we can still use a model checker that solves the model checking problem of Definition 21.

### 4.2 A first algorithm

Figure 4.1 shows an algorithm that takes a model \( M \) and property \( \varphi \) and returns the set of \( \varphi \)-worlds. The presentation is equivalent to algorithms with marking [BS99].

However, the bottleneck is the computations of the product \( M \otimes E \) leading in Kripke models of exponential size in the size of the input. However, in practise, this form is suitable for an implementation since sets of worlds can be represented efficiently with BDDs ([Boo76], [Ake78].

41
**CHAPTER 4. MODEL CHECKING**

```
function mc(M, ϕ)
  match ϕ do
    case p :
      return {w | p holds in M, w}
    case ¬ψ :
      return mc(M, ψ)
    case (ψ1 ∨ ψ2) :
      return mc(M, ψ1) ∪ mc(M, ψ2)
    case Kaψ :
      return {w | Ra(w) ⊆ mc(M, ψ)}
    case ⟨E, e⟩ψ :
      return mc(M, pre(e)) ∩ {w | (w, f) ∈ mc(M ⊗ E, ψ)}
  endMatch
endFunction
```

Figure 4.1: Model checking algorithm.

It has recently been applied to DEL [vBvEGS15]. We will see in Section 4.3 an algorithm for model checking that runs in polynomial space and that never computes products explicitly.

However, the algorithm given in Figure 4.1 is suitable in terms of complexity for \( L_{EL} \) (epistemic logic without actions) and for public announcement logic.

The model checking of \( L_{EL} \) is \( P \)-complete. The \( P \)-hard proof can be found in [Sch02]. The \( P \)-membership is folklore: the algorithm in Figure 4.1 without the \( ⟨E, e⟩ψ \)-case can be implemented in polynomial-time.

In public announcement logic, all event models \( E \) are reflexive single-event models, therefore all models in the subcall in the algorithm 4.1 are submodels of the initial model \( M \). Therefore all operators performed in a node of the computer tree of \( mc(M, ϕ) \) is polynomial in the size of the input. To sum up, the model checking of public announcement logic is also in \( P \) [Ben11].

### 4.3 PSPACE-membership

In this section, we prove the following theorem, given in [CS18], and that subsumes the upper bound given [ASI13] for the model checking problem for \( L_{DEL} \).

**Theorem 2** The model checking problem for \( DEL^{CK} \) is \( Pspace \)-complete.

Hardness comes directly from the \( Pspace \)-hardness of the model checking of \( DEL \) without common knowledge [ASI13] (actually, it is already \( Pspace \)-hard for single-pointed event models [BJS15a], but actually even when the Kripke model is \( S5 \) and event models are \( S5 \) and single-pointed [vdpvRS15]). For the \( Pspace \)-membership, Figure 4.3 provides the pseudo-code of an alternating Turing machine that decides the model checking problem for \( DEL^{CK} \) in polynomial time. In the pseudo-code in Figure 4.3, existential (\( ∃ \)) and keyword **or** (resp. universal (\( ∀ \)) choices and keyword **and** corresponding to existential (resp. universal) states. Keyword **not** corresponds to a negated state. The upper bound is proven since \( Pspace = Aptime \). The machine starts by calling \( mc(M, w, Φ) \). Figure 4.2 gives an example: it shows a portion of the computation tree of the call \( mc(M, w, ⟨E, E_0⟩¬C_{gp}) \).

\(^1\)Epistemic logic is an extension of the fragment of CTL with only the next operators \( AX \) and \( EX \), proven to
4.3. PSPACE-MEMBERSHIP

The specifications of the procedures \(mc\), \(inval\), \(in\), \(rel\) and \(rel^*\) (see Figure 4.3) are given in the following proposition:

**Proposition 3** For all formulas \(\varphi\), for all Kripke models \(\mathcal{M}\), for all sequences of event models \(\mathcal{E}\), for all worlds \(w, v\) of \(\mathcal{M}\), for all agents \(a\), for all groups of agents \(G\), for integers \(i\) that are powers of two,

- configuration \(mc(\mathcal{M}, w, \mathcal{E}, \varphi)\) is accepting if \(\mathcal{M}\), \(w, \mathcal{E} \models \varphi\),
- configuration \(inval(p, \mathcal{E}, \mathcal{E}, \varphi)\) is accepting if \(p \in V(w, \mathcal{E})\),
- configuration \(in(v, \mathcal{E}, \varphi)\) is accepting if \(v \in \mathcal{M}\),
- configuration \(rel(w, v, a, \mathcal{E}, \varphi)\) is accepting if \((w, v, a) \in \mathcal{E}\),
- and configuration \(rel^*(w, v, \mathcal{E}, \varphi)\) is accepting if \((w, v, \mathcal{E}) \in \bigcup_{j \leq i} \left( \bigcup_{a \in G} R_a \right)^j\).

**Proof.**

The proposition is straightforwardly proven by induction since the pseudo-code directly reflects the semantics of \(\text{DELCK}\). The only difficulties are:

- The induction works on the quantities given in Figure 4.3 and thanks to the following Lemma 1,
- \(\bigcup_{j \leq B_{\mathcal{M}, \Phi}} \left( \bigcup_{a \in G} R_a \right)^j = \left( \bigcup_{a \in G} R_a \right)^*\) since the number of worlds in \(\mathcal{M}\) in bounded by \(B_{\mathcal{M}, \Phi}\).

---

\(\text{P}\)-hard.

\(^2\)The beginning of a procedure call is indeed a special configuration of the alternating Turing machine of Figure 4.3.
The design of Procedure \( \text{rel} \) relies on the divide and conquer paradigm. For checking that \( u \vec{f} \) is reachable by at most \( i \bigcup_{a \in G} R_a \)-steps from \( w \vec{c} \), we guess an intermediate world \( v \vec{g} \in \mathcal{M} \vec{E} \) and check that \( v \vec{g} \) is reachable by at most \( \frac{i}{2} \bigcup_{a \in G} R_a \)-steps from \( w \vec{c} \) and that \( u \vec{f} \) is reachable by at most \( i/2 \bigcup_{a \in G} R_a \)-steps from \( v \vec{g} \) (see for instance node \( \text{rel}^*(w,e,f,G,B,M,A,\mathcal{M} \vec{E}) \) in Figure 4.2).
Better than giving a tedious and straightforward proof of Proposition 4.1, let us explain the algorithm on the example of mc(\(M, w, (E, E_0 \neg C_{GP})\)) depicted in Figure 4.2. The procedure starts by choosing \(e \in E_0\). Then, we check that both pre\((e)\) holds in \(w\) and that \(\neg C_{GP}\) holds in \(w\). Checking that \(\neg C_{GP}\) holds in \(w\) leads to a negated configuration; we negate the fact that \(C_{GP}\) holds in \(w\). It is followed by a universal choice of \(u f \in M \tilde{E}\). For each choice of \(uf \in M \tilde{E}\), we progress in an existential configuration that checks that either \(uf \) is not a world of \(M \tilde{E}\), either \(wf \) is not reachable from \(w\) by at most \(B_{M, \Phi} \bigcup_{\alpha \in G} R_{\alpha}^{M \tilde{E}}\)-steps or that \(p\) in \(uf\). Checking that \(p\) holds in \(uf\) is performed by the call of invalid\((p, uf, M \tilde{E})\), which itself check that the postcondition post\((e, p)\) holds in \(u\).

The quantities associated to each procedure call used for the proofs by induction require a careful definition. They depend on the input \((M, w, \Phi)\) of the model checking problem. Let \(B_{M, \Phi}\) be the smallest power of two that is greater than the number of worlds in Kripke model \(M\) where \(\Phi\) holds.

\textbf{Definition 22} \(|M|, |E|\) and \(|\varphi|\) are defined by mutual induction. First, \(|M|\) (resp. \(|E|\)) are the number of bits to encode Kripke model \(M\) (resp. event model \(E\)). In particular, \(|E|\) takes into account the memory needed to store the precondition and the postcondition functions. Then, \(|M \tilde{E}|\) denotes \(|M| + \sum_{i=1}^{n} |E_i|\). Second \(|\varphi|\) denotes the length of \(\varphi\), defined by induction as usual except for the two following cases:

- \(|(E, E_0)\varphi| := |E| + 1 + |\varphi|\);
- \(|CG\varphi| := \log_2 B_{M, \Phi} + 1 + |\varphi|\).

\textbf{Lemma 1} The quantities given in gray in Figure 4.3 are strictly decreasing along a branch of the computation tree (see for instance Figure 4.2 of \(M, w, \Phi\)). \textbf{Proof.}

Let us discuss the following cases (the other ones are left to the reader):

- The quantity for \(mc(M \tilde{E}, w \tilde{e}, CG\varphi)\) is \(|M \tilde{E}| + |CG\varphi| + 1 = |M \tilde{E}| + \log_2 B_{M, \Phi} + |\varphi| + 1\) and is strictly greater than the quantity for \(rel^*(w \tilde{e}, u \tilde{f}, G, B_{M, \Phi}, M \tilde{E})\), which is \(|M \tilde{E}| + \log_2 B_{M, \Phi}\).

- The quantity for \(mc(M \tilde{E}, w \tilde{e}, (E, E_0)\varphi)\) is \(|M \tilde{E}| + |E| + |\varphi| + 1\) and is strictly greater than the quantity for \(mc(M \tilde{E}, w \tilde{e}, pre\((e)\))\), which is \(|M \tilde{E}| + |pre\((e)\)| < \(|M \tilde{E}| + |E|\).

- The quantity for \(invalid(p, w \tilde{e}, M \tilde{E})\) is \(|M \tilde{E}\cdot E| = |M \tilde{E}| + |E|\) and is strictly greater than the quantity for \(mc(M \tilde{E}', w \tilde{e}', post\((e, p)\))\) which \(|M \tilde{E}'| + |post\((e, p)\)|.

\textbf{Proposition 4} \(mc(M, w, \Phi)\) is executed in polynomial time in the size of the input \((M, w, \Phi)\).

\textbf{Proof.} The time is bounded the height of the computation tree rooted in \(mc(M, w, \Phi)\). Thanks to Lemma 1, the height of the computation tree (as shown in Figure 4.2) is bounded by the quantity associated to \(mc(M \tilde{E}, w \tilde{e}, \varphi)\), that is \(|M| + |\varphi|\). This quantity is not the size of the input \((M, w, \Phi)\); for instance the weight of \(C_{G}\)-modalities is \(\log_2 B_{M, \Phi}\). However this quantity is polynomial in the size of the input \((M, w, \Phi)\).

At each node of the computation tree (as depicted in Figure 4.2), the computation performed in a single node is polynomial. For instance, the instruction \(\{\forall\}\) choose \(u \tilde{f} \in M \tilde{E}\) consists in choosing each bit of \(u \tilde{f}\); thus is polynomial in the size of the input.

To conclude, the execution time on each branch in the computation tree is polynomial. ■
4.4 Other results

In this section, we discuss these results and other more anecdotic results shown in the literature.

4.4.1 Explicit models

Aucher et al. \[AS13\] prove that the model checking with that $\cup$ operator is $PSPACE$-hard. Van de Pol et al. (see Theorem 1 in \[vdPvRS15\]) and Bolander et al. (see Theorem 6.1 in \[BJS15\]) independently prove that the model checking is $PSPACE$-hard even without that $\cup$-operator.

The complexity of model checking of attention-based public announcement logic is not given in \[BvDH+16\]: it is in $PSPACE$ but the exact complexity is unknown. In the special case of no propositional preconditions and no postconditions, action models commute \[LPW11\]. Charrier et al. exploit this property to show that the model checking of formulas containing operators of the $\langle (E, e)^i \rangle$ where $i$ is an integer written in binary is in $PSPACE$ (Proposition 1 in \[CMS16\]). Their algorithm is a deterministic algorithm that runs in polynomial space. A tuple $(w, e_1, \ldots, e_k)$ is represented by $(w, (j_e)_{e \in E})$ where $E$ is the set of events and $j_e$ is the number of occurrences of $e$ in the tuple $e_1, \ldots, e_k$. The space required to represent $(w, (j_e)_{e \in E})$ is polynomial in the size of the input, therefore the algorithm runs in polynomial space.

The model checking problems of both arbitrary public announcement logic and group announcement logic are $PSPACE$-complete \[˚ABvDS10\].

4.4.2 Succinct models

When the Kripke model is described succinctly, the model checking of a formula without dynamic operator is already $PSPACE$-hard \[BHT13\].

When the Kripke model and event models are described succinctly by means of accessibility programs, the model checking for $L_{DELCK}$ is in $PSPACE$ \([CS17], [CS18]\). The idea is to use a similar algorithm similar to the one of Figure 4.3 but that manipulates succinct models instead.

Actually, when the Kripke model is succinctly described by means of accessibility programs, the model checking for arbitrary public announcement is $A_{pol}EXPTIME$-complete \[CS15\]. The $A_{pol}EXPTIME$-upper bound is shown as follows. The main difference in the algorithm is that we now store the subset of surviving worlds explicitly as a set of valuations. The time of an operation performs in a node is exponential. Checking that $\Diamond \psi$ holds at a given world consists in search for the existence of a subset of valuations being the next surviving set of worlds for which $\psi$ holds. We model it as an exponential number of atomic non-deterministic existential choices. Dually, checking that $\neg \Diamond \psi$ holds leads to an exponential number of atomic universal choices. As the depth of the tree is linear the size of $\varphi$, the number of alternation over a branch of the computation tree is linear in the size of $\varphi$. 

Table 4.1: Complexity of the model checking problem.

<table>
<thead>
<tr>
<th>Model Class</th>
<th>Explicit Models</th>
<th>Symbolic Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L_{EL}, L_{ELCK}$</td>
<td>$P$-complete</td>
<td>$PSPACE$-complete</td>
</tr>
<tr>
<td>$L_{ELPA}, L_{ELCKPA}$</td>
<td>$P$-complete</td>
<td>$PSPACE$-complete</td>
</tr>
<tr>
<td>$L_{DEL}, L_{DELCK}$ with arbitrary public announcements</td>
<td>$PSPACE$-complete</td>
<td>$PSPACE$-complete</td>
</tr>
<tr>
<td>$A_{pol}EXPTIME$-complete</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.5 Implementation

The main complexity results for model checking are summed up in Table 4.1 and gives an insight on the implementability of the model checking of DEL. Model checking on explicit models is implemented in Hintikka’s world. Model checking on succinct models is implemented in a tool called DEMO ([vBvEGS15], [vBvEGS18]). Model checking on succinct models for arbitrary public announcement logic is implemented by reduction to a first-order prover iprover [CPS17].
Chapter 5

Satisfiability problem

In this chapter, we will discuss the following satisfiability problem.

**Definition 23** The satisfiability problem of DEL is defined as follows:

- **Input:** a formula $\varphi \in \mathcal{L}_{\text{DELCK}}$;
- **Output:** yes if there exists a pointed epistemic model $M, w$ such that $M, w \models \varphi$, no otherwise.

5.1 Motivation

The model checking methodology relies on the fact the full Kripke model of the epistemic state has to be described. As pointed by Sergei Artemov [Art16], a full description is problematic for mainly two reasons.

1. From an applicative point of view, we often actually do not have a complete description of a situation, but a partial description.
2. From a conceptual point of view, having a single Kripke model means that this very model is common knowledge among all agents.

That is why, in this chapter, we focus on the satisfiability problem. It can be used to generate an epistemic state that respects a given property $\varphi$ holds. Hintikka’s World enables to perform this task (build a custom example). Also the satisfiability problem can be seen as the dual problem of validity checking / theorem proving. As an application, we can check a property $\psi$ in a system described textually with $\chi$. The idea is then to check that the formula $\chi \rightarrow \psi$ is valid $(\chi \land \neg \psi)$ is unsatisfiable.

5.2 Tableau method

5.2.1 Principle

The general idea is to try to analyze a given formula and to create an epistemic model $(M, w)$ that satisfies that formula. Let $\mathcal{Lab}$ be a countable set of labels designed to represent possible worlds of the epistemic model $(M, w)$ in creation. Our tableau method manipulates terms that we call tableau terms and they are of the following kind:
• \((\sigma \overset{\vec{e}}{\rightarrow} \varphi)\) where \(\sigma \in \text{Lab}\) is a node (that represents a world in the epistemic model) and \(\vec{e}\) is a finite sequence of events (without loss of generality, we suppose that all dynamic operators refer to the same event model \(\mathcal{E}\) so it is not necessary to mention it). This term means that formula \(\varphi\) is true in the world denoted by \(\sigma\) after the execution of the sequence \(\vec{e}\) and that the sequence is executable in the world denoted by \(\sigma\);

• \((\sigma \overset{\vec{e}}{\rightarrow} \checkmark)\) means that the sequence \(\vec{e}\) is executable in the world denoted by \(\sigma\);

• \((\sigma \overset{\vec{e}}{\rightarrow} \otimes)\) means that the sequence \(\vec{e}\) is not executable in the world denoted by \(\sigma\);

• \((\sigma R_a \sigma_1)\) means that the world denoted by \(\sigma\) is linked by \(R_a\) to the world denoted by \(\sigma_1\);

• \(\bot\) denotes an inconsistency.

A tableau rule is represented by a numerator \(N\) above a line and a finite list of denominators \(D_1, \ldots, D_k\) below this line, separated by vertical bars:

\[
\begin{array}{c|c|c}
N \\
\hline
D_1 & \ldots & D_k \\
\end{array}
\]

The numerator and the denominators are finite sets of tableau terms.

A tableau tree is a finite tree with a set of tableau terms at each node. A rule with numerator \(N\) and denominator \(D\) is applicable to a node carrying a set \(\Gamma\) if \(\Gamma\) contains an instance of \(N\) but not the instance of its denominator \(D\). If no rule is applicable, \(\Gamma\) is said to be saturated. We call a node \(\sigma\) an end node if the set of formulas \(\Gamma\) it carries is saturated, or if \(\bot \in \Gamma\). The tableau tree is extended as follows:

1. Choose a leaf node \(n\) carrying \(\Gamma\) where \(n\) is not an end node, and choose a rule \(\rho\) applicable to \(n\).

2. (a) If \(\rho\) has only one denominator, add the appropriate instantiation to \(\Gamma\).

(b) If \(\rho\) has multiple denominators, choose one of them and add to \(\Gamma\) the appropriate instantiation of this denominator.

A branch in a tableau tree is a path from the root to an end node. A branch is closed if its end node contains \(\bot\), otherwise it is open. A tableau tree is closed if all its branches are closed, otherwise it is open. The tableau tree for a formula \(\varphi\) is the tableau tree obtained from the root \(\{\sigma_0 \epsilon \varphi\}\) when all leafs are end nodes.

### 5.2.2 Tableau rules

The tableau rules of our tableau method are represented in Figure 5.1. In these rules, \(\epsilon\) is the empty sequence of events. The tableau method contains the classical Boolean rules \((\land), (\neg\neg), (\neg\land)\). The rules \((\leftarrow p)\) and \((\leftarrow \neg p)\) handle atomic propositions. The rule \((\bot)\) makes the current execution fail. The rule for \((K_a)\) is applied if \(\vec{e}\) and \(\vec{f}\) are such that the lengths of \(\vec{e}\) and \(\vec{f}\) are equal and for all \(j\), \(e_j = f_j\). Similarly, the rule for \((\hat{K}_a)\) is applied by choosing non-deterministically some \(\vec{f}\) of the same length than \(\vec{e}\) such that \(e_j R_a^e f_j\) and creating a new fresh label \(\sigma_{\text{new}}\). The rules \((\checkmark), (\otimes), (\text{clash}, \checkmark, \otimes)\) and \((\epsilon)\) handle the preconditions.

Rule \(\left[\epsilon\right]\) is the rule for the dynamic operator for single-pointed event models. It says that if \(\left[\epsilon\right]\varphi\) holds in \(\sigma\) after the sequence of actions \(\vec{e}\), then:

• either event \(e\) is not executable;
5.3. THE COMMON KNOWLEDGE FREE FRAGMENT

The satisfiability problem for the language $L_{\text{DEL}}$ is $\text{NExptime}$-complete and the tableau method given in Figure 5.1 is optimal [AS93].

The $\text{NExptime}$ upper bound is explained as follows. First, the tableau method is a non-deterministic algorithm. The depth of the computation tree corresponding to the tableau is polynomial in the input $\varphi$ but the number of tableau terms corresponding to a given a node $\sigma \in \text{Lab}$ is at most exponential in the input $\varphi$. So the non-deterministic algorithm runs in exponential time.

Figure 5.1: Tableau rules.

- of it and $\varphi$ holds after the sequence $\overrightarrow{e}::x$ in $\sigma$.

Rules $([E_0 \cup \{e\}])$ and $([E_0 \cup \{e\}])$ decompose the multi-point set of multi-point event models. Rule $([E_0 \cup \{e\}])$ says that both $[E_0]\varphi$ and $[e]\varphi$ holds in $\sigma$ after $\overrightarrow{e}$. On the contrary, rule $([E_0 \cup \{e\}])$ is non-deterministic:

- Either $\langle E_0 \rangle \varphi$ holds in $\sigma$ after $\overrightarrow{e}$ (one of the events in $E_0$ is executable);

- or $\langle e \rangle \varphi$ holds in $\sigma$ after $\overrightarrow{e}$.

Rule $([\emptyset])$ says that any multi-point event models with an empty designated set of events is not executable.

### 5.3 The common knowledge free fragment

The satisfiability problem for the language $L_{\text{DEL}}$ is $\text{NExptime}$-complete and the tableau method given in Figure 5.1 is optimal [AS93].

The $\text{NExptime}$ upper bound is explained as follows. First, the tableau method is a non-deterministic algorithm. The depth of the computation tree corresponding to the tableau is polynomial in the input $\varphi$ but the number of tableau terms corresponding to a given a node $\sigma \in \text{Lab}$ is at most exponential in the input $\varphi$. So the non-deterministic algorithm runs in exponential time.
The NEXPTIME-lower bound is proven by reduction from a tiling problem but needs the \( \cup \)-operator \[AS13\]. We do not know whether the satisfiability problem for the language without the \( \cup \)-operator is NEXPTIME-hard.

The satisfiability problem of public announcement logic is PSPACE-complete \[Lut06\]. An optimal tableau method is given in \[BvDHL10\] and can be seen as a restriction to the tableau method given in Section 5.2: the possible sequences \( \vec{e} \) correspond to sequences of nested announcements.

**Example 31** By checking the satisfiability of \( [\varphi](p \land [\psi]q) \land [\chi]r \), the set of possible sequences \( \vec{e} \) are \( \epsilon \), \( e_\varphi \), \( e_\psi \) and \( e_\chi \) where \( e_\varphi \), \( e_\psi \) and \( e_\chi \) are respectively the events corresponding to the public announcements of \( \varphi \), \( \psi \) and \( \chi \).

The satisfiability problem of attention-based announcement logic is also PSPACE-complete \[BvDH+16\]. The satisfiability problem of non-normal modal logic variants of public announcement logic have been proven to be NP-complete \[MSSV15\].

### 5.4 Common knowledge

The complexity of the satisfiability of \( L_{ELCK} \) is EXPTIME-complete. It remains EXPTIME-complete when extended with public announcement operators \[Lut06\]. The idea is to reduce the satisfiability with relativized common knowledge.

Reduction axioms for common knowledge uses relativized common knowledge also exist for event models \[WA15\]: we can transform a formula containing pointed event models in a formula without any occurrence of a pointed event model but that contains relativized common knowledge. The translation is non-elementary. Actually, the tableau method can be extended by the following rules \[CS18\]:

\[
\begin{align*}
\frac{(\sigma \; \vec{e} \; C_G \varphi)}{(\sigma \; \vec{e} \; \varphi)} & \quad \frac{(\sigma \; \vec{e} \; C_G \varphi)}{(\sigma_1 \; f \; \varphi)} \quad \frac{(\sigma \; \vec{e} \; C_G \varphi)}{(\sigma_1 \; f \; \varphi)} \\
\frac{(C_G \varphi)}{\varphi} & \quad \frac{(C_G \varphi)}{\varphi} & \quad \frac{(C_G \varphi)}{\varphi}
\end{align*}
\]

**5.4.1 Upper bound**

The satisfiability problem for \( DELCK \), given a \( DELCK \)-formula \( \Phi \), asks to decide \( \Phi \) is satisfiable. In this section, we prove the following upper bound result:

**Theorem 3** The satisfiability problem of \( DELCK \) is in 2-EXPTIME.
5.4. COMMON KNOWLEDGE

**Definition 24** The closure of formula $\Phi$ is the set $Cl(\Phi)$ that contains elements in $\pi$ and ($\overrightarrow{\varphi}$ $\psi$) where $\overrightarrow{\varphi}$ is a sequence of events in $E$ of length at most $\text{dmd}(\Phi)$, and $\psi$ is a subformula (or negation) of $\Phi$ or a subformula (or negation) of a precondition or postcondition in $E$, under the condition that $\text{dmd}(\varphi) + |\overrightarrow{\varphi}| \leq \text{dmd}(\Phi)$.

The intended meaning of ($\overrightarrow{\varphi}$ $\psi$) is that the current world survives the sequence of events $\overrightarrow{\varphi}$. The intended meaning of ($\overrightarrow{\varphi}$ $\neg$ $\psi$) is that formula $\varphi$ is true after having executed the sequence of events $\overrightarrow{\varphi}$.

**Example 32** Let us take the event model $E$ of Figure 2.7 and formula $\Phi := [e]K_a[f]q$. The closure $Cl(\Phi)$ is the set $\{in_e, in_e, in_e, in_e, (e \varphi),(e K_a[f]q),(e K_a[f]q), \ldots\}$.

**Proposition 5** The size of the closure of $\Phi$ is exponential in $|\Phi|$.

**Proof.**

There is a direct correspondence between a subformula of $\Phi$ and a node in the syntactic tree of $\Phi$. Therefore, the number of subformulas of $\Phi$ is in $O(|\Phi|)$. The number of possible $\psi$ is then bounded by $O(|\Phi|)$ (the size of $\Phi$ is the number of memory cells needed to write down $\Phi$, all the information of the event model $E$ included). The number of possible sequences $\overrightarrow{\varphi}$ is $|E|^{dmd(\Phi)}$, thus exponential in $|\Phi|$.

A Hintikka set (see Definition 25) is a maximal subset of $Cl(\Phi)$ that is consistent with respect to propositional logic (points 2-4), common knowledge reflexivity (point 5), dynamic operators (point 6-7), executability of events (points 8-9) and postconditions (point 10).

**Definition 25** A Hintikka set $h$ over $Cl(\Phi)$ is a subset of $Cl(\Phi)$ that satisfies:

1. If ($\overrightarrow{\varphi}$ $\varphi$) $\in h$ then $\text{in}_{\pi} \in h$;
2. If ($\overrightarrow{\varphi} \varphi \wedge \psi$) $\in h$ then ($\overrightarrow{\varphi} \varphi$) $\in h$ and ($\overrightarrow{\varphi} \psi$) $\in h$;
3. If ($\overrightarrow{\varphi} \varphi \lor \psi$) $\in h$ then ($\overrightarrow{\varphi} \varphi$) $\in h$ or ($\overrightarrow{\varphi} \psi$) $\in h$;
4. If $\text{in}_{\pi} \in h$ then ($\overrightarrow{\varphi} \varphi$) $\in h$ xor ($\overrightarrow{\varphi} \neg \varphi$) $\in h$;
5. If ($\overrightarrow{\varphi} C_G \varphi$) $\in h$ then ($\overrightarrow{\varphi} \varphi$) $\in h$;
6. If ($\overrightarrow{\varphi} (E_0)\varphi$) $\in h$ then there exists $e \in E_0$ s.t. $\text{in}_{\pi} \in h$ and ($\overrightarrow{\varphi} : e \varphi$) $\in h$.
7. ($\overrightarrow{\varphi} [E_0] \varphi$) $\in h$ iff for all $e \in E_0$, we have $\text{in}_{\pi} \in h$ implies ($\overrightarrow{\varphi} : e \varphi$) $\in h$;
8. $\text{in}_e \in h$;
9. $\text{in}_{\pi} : e \in h$ iff $\text{in}_{\pi} \in h$ and ($\overrightarrow{\varphi} \text{pre}(e)$) $\in h$;
10. ($\overrightarrow{\varphi} : e \varphi$) $\in h$ iff ($\overrightarrow{\varphi} \text{post}(e)(p)$) $\in h$.

Point (1) means that a Hintikka set contains ($\overrightarrow{\varphi}$ $\varphi$), then it means that $\overrightarrow{\varphi}$ should be executable (in the intuitive world represented by the Hintikka set). Point (4) means that Hintikka sets are consistent. Point (5) says that if $\varphi$ is common knowledge then $\varphi$ is true. Points (6) and (7) mimics the truth condition given in Definition 8. Point (8) means the empty sequence of events $e$ is always executable. Point (9) means that $\overrightarrow{\varphi} : e$ is executable iff $\overrightarrow{\varphi}$ is executable and the precondition of $e$ holds after having executed $\overrightarrow{\varphi}$. Point (10) means that the truth of atomic proposition $p$ after a non-empty sequence $\overrightarrow{\varphi} : e$ of events is given by the truth of its postcondition before the last event $e$.

Now, we define the following structure that takes care about the consistency of the box modalities $K_a, C_G$.

---

1The definition given here contains ‘too many’ formulas. We could have given a much more thorough definition, but the definition would have been more complicated to understand and the closure would have had the same asymptotic size.

2Formula $\neg \varphi$ is the negation of $\varphi$ in the following sense: the negative normal obtained by negating all connectives in $\varphi$.

3We explicitly mentioned $\text{in}_{\pi} : e \in h$ for uniformity with the semantics. However, note that it is implied by point (1).
Definition 26 The Hintikka structure for $\varphi$ is $H := (H, (R_a)_{a \in AGT})$ where:

- $H$ is the set of all possible Hintikka sets over $Cl(\varphi)$;
- $hR_a h'$ if the two following conditions holds:
  
  - $(K_a)$ for all $(\overrightarrow{\tau}, K_a \varphi) \in h$ we have $(\overrightarrow{\tau}^\prime, \varphi) \in h'$ for all $\overrightarrow{\tau}^\prime$ such that $\overrightarrow{\tau} \rightarrow a \overrightarrow{\tau}^\prime$ and $in_{\overrightarrow{\tau}^\prime} \in h'$;
  
  - $(C_G)$ for all $(\overrightarrow{\tau}, C_G \varphi) \in h$ we have $(\overrightarrow{\tau}^\prime, C_G \varphi) \in h'$ for all $\overrightarrow{\tau}^\prime$ such that $\overrightarrow{\tau} \rightarrow a \overrightarrow{\tau}^\prime$ with $a \in G$ and $in_{\overrightarrow{\tau}^\prime} \in h'$.

The size of the Hintikka structure is double-exponential in $|\varphi|$, since there are a double-exponential number of different Hintikka sets. We finish by giving the algorithm isDELCK-sat? (see Figure 5.2) whose repeat...until loop takes care about the consistency of diamond modalities, $K_a, C_a$. The algorithm starts with the full Hintikka structure. Points $(K_a), (C_a)$ remove worlds where $K_a \psi$ and $C_a \psi$ have no appropriate $\psi$-successor. We write $\overrightarrow{\tau} \rightarrow a \overrightarrow{\tau}^\prime$ if for all $(\overrightarrow{\tau^i}, \overrightarrow{\tau^i'}) \in R_a^{\overrightarrow{\tau'}}$.

Proposition 6 Algorithm isDELCK-sat? of Figure 5.2 runs in double-exponential time in $|\Phi|$.

Proof.

The computation of $H$ can be performed by brute-force: enumerate all subsets of $Cl(\varphi)$ and discard those which does not satisfy all conditions (1)-(10) of Definition 26. Compute $R_a$ according to Definition 26. The loop is repeated at most the number of Hintikka sets in $H$, that is $O(2^{2^{|\varphi|}})$ times, since at least one Hintikka set is removed or we exit the loop. Both tests $(K_a)$ and $(C_G)$ can be performed by depth-first search algorithm running in polynomial time in the size of the graph, that is of size double-exponential in $|\Phi|$.

Proposition 7 $\Phi$ is DELCK-satisfiable iff isDELCK-sat? accepts $\Phi$.

Proof.

($\Rightarrow$) Let $M, w$ such that $M, w \models \Phi$. Given a world $u$, we note $h(u)$ the Hintikka set obtained by taking $in_{\overrightarrow{\tau}}$ if $\overrightarrow{\tau}$ is executable in $u$ and $(\overrightarrow{\tau}, \psi)$ if $\psi$ holds in $u, \overrightarrow{\tau}$. We show that no Hintikka
set $h(u)$ is removed from $\mathcal{H}$. In particular, $h(w)$ is not removed, and contains $(e \Phi)$ so the algorithm is DELCK-sat? accepts $\Phi$.

$(\Leftarrow)$ Suppose is DELCK-sat? accepts $\Phi$. We construct a model $\mathcal{M} = (W, (R_a)_{a \in AGT}, V)$ as follows:

- $W$ is the set of Hintikka sets that remain in the structure at the end of the algorithm;
- $R_a$ is the relation for agent $a$ at the end of the algorithm;
- $V(h) = \{ p \in AP \mid (e \ p) \in h \}$.

The proof finishes by proving the following lemma:

**Lemma 2** *(truth lemma)* The properties $\mathcal{P}(in_{\vec{c}})$ and $\mathcal{P}((\vec{c} \varphi))$ defined below hold:

- $\mathcal{P}(in_{\vec{c}})$: for all $h \in W$, $in_{\vec{c}} \in h$ iff $c$ is executable in $\mathcal{M}$, $h$;
- $\mathcal{P}((\vec{c} \varphi))$: for all $h \in W$, $(\vec{c} \varphi) \in h$ iff $M \otimes E |\vec{c}|, (h, \vec{c}) \models \varphi$.

**Proof.**

The proof is performed by induction by assigning the following quantities: the quantity for $in_{\vec{c}}$ is $n|\vec{c}|$; the quantity for $(\vec{c} \varphi)$ is $n|\vec{c}| + |\varphi|$ where $n$ is the length of $\vec{c}$, $|\varphi|$ and $|\varphi|$ are defined as in Definition 22 except that now we use the traditional clause $|C_G \varphi| := |\varphi| + 1$. Let us just present the following induction cases.

- Suppose that for all $e$, $e \in E_0$ s.t. $\mathcal{P}(in_{\vec{c}}) \land \mathcal{P}((\vec{c} :: e \varphi))$. Let us prove that $\mathcal{P}(in_{\vec{c}})$.
  
  $(\vec{c} :: E_0 \varphi) \in h$ if there exists $e \in E_0$ s.t. $in_{\vec{c}} :: e \in h$ and $(\vec{c} :: e \varphi) \in h$.

  - $(\vec{c} :: E_0 \varphi) \in h$ if $\vec{c} :: e$ is executable in $h$ and $M \otimes E |\vec{c} :: e|, (h, \vec{c} :: e) \models \varphi$.
  - $(\vec{c} :: E_0 \varphi) \in h$ if $M \otimes E |\vec{c}|, (h, \vec{c}) \models \varphi$.

- Suppose that for all $\vec{c}'$ of length $n$, we have $\mathcal{P}(in_{\vec{c}'}) \land \mathcal{P}((\vec{c}' \psi))$. Let $\vec{c}$ be of length $n$ and let us prove that $\mathcal{P}(\vec{c} \ C_G \psi)$.

  $(\Rightarrow)$ Suppose $(\vec{c} \ C_G \psi) \in h$. It implies that for all paths $h = h_0 \rightarrow a_1 h_1 \ldots h_k$ and for all paths $\vec{c}(0) \rightarrow a_1 \vec{c}(1) \ldots \rightarrow a_k \vec{c}(k)$ such that $a_1, \ldots, a_k \in G$ and $in_{\vec{c}(i)} \in h_i$, we have $(\vec{c}(k) \ C_G \psi) \in h_k$ by iterating point $(C_G)$ of Definition 26. By 25 we have $(\vec{c}(k) \ C_G \psi) \in h_k$.

  - $(\vec{c} \ C_G \psi) \in h$ if $\mathcal{P}(in_{\vec{c}(k)})$ and $\mathcal{P}((\vec{c}(k) \ C_G \psi))$.
  - $\mathcal{P}(in_{\vec{c}(k)})$ and $\mathcal{P}((\vec{c}(k) \ C_G \psi))$, we have that $M \otimes E |\vec{c}(k)|, (h_k, \vec{c}(k)) \models \psi$. Thus $M \otimes E |\vec{c}|, h \models C_G \psi$.

  $(\Leftarrow)$ Suppose $(\vec{c} \ C_G \psi) \notin h$. By Definition 25 we have $(\vec{c} \ C_G \chi) \notin h$, where $C_G \chi$ is the negation of $C_G \psi$. Step $G$ in the Algorithm of Figure 5 guarantees the existence of a path $h = h_0 \rightarrow a_1 h_1 \ldots h_k$ and a path $\vec{c}(0) \rightarrow a_1 \vec{c}(1) \ldots \rightarrow a_k \vec{c}(k)$ such that $a_1, \ldots, a_k \in G$ with $in_{\vec{c}(i)} \in h_i$ and $(\vec{c}(k) \ C_G \chi) \notin h_k$. In other words, $(\vec{c}(k) \ C_G \chi) \notin h_k$ By $\mathcal{P}((\vec{c}(k) \ C_G \psi))$, $M \otimes E |\vec{c}(k)|, (h_k, \vec{c}(k)) \models \psi$. Properties $\mathcal{P}(in_{\vec{c}'})$ ensure the path is indeed in the product model $M \otimes E |\vec{c}|$, thus $M \otimes E |\vec{c}|, (h, \vec{c}) \notin C_G \psi$.

We conclude by applying the truth lemma (Lemma 2) to the Hintikka set $h$ that contains $(e \ C_G \psi)$ and we obtain that $M, h \models \Phi$.}


Remark 1 The 2EXPTIME upper bound also holds for the satisfiability problem of \textsc{DELCK} in S5 Kripke models. We proceed as in [HM92] (p. 358). We add the following clauses to definition 25:

\[(5') \text{If } \left( \vdash \phi \right) K a \text{ then } \left( \vdash \phi \right) \in h; \]

We add the following clause in the definition of $R_a$ in Definition 26:

\[
\text{for all } \vdash \rightarrow^a \vdash' \text{, if } \text{in } \rightarrow \in h \text{ and } \text{in } \rightarrow' \in h' \text{ then } \left( \vdash \rightarrow^a \right) K a \phi \in h \text{ iff } \left( \vdash \rightarrow' \right) K a \phi \in h'.
\]

5.4.2 Reduction

The aim of this section is to prove the following theorem.

**Theorem 4** The satisfiability problem of \textsc{DELCK} is 2-Exptime-hard.

Let us consider any 2-Exptime decision problem $L$. As $\text{AEXPSPACE} = 2\text{-Exptime}$ [CS76], it is decided by an alternating Turing machine $M$ that runs in exponential space. W.l.o.g we suppose that all executions halt\(^4\) and no state is a negated state. We will define a polynomial reduction $tr$ from $L$ to the satisfiability problem of \textsc{DELCK}, that is $tr$ will be computable in polynomial time, and $\omega$ is a positive instance of $L$ if and only if $tr(\omega)$ is a satisfiable \textsc{DELCK}-formula.

The idea of $tr(\omega)$ is to enforce an expected form of a Kripke model as shown in Figure 5.3 that represents the computation tree of $M$ starting with $\omega$ on the tape. The cursor of the machine remains in the $N$-first cell portion of the tape, where $N$ is exponential in $|\omega|$. We define $N_0 = \log_2(N)$ for the rest of the section. $N_0$ is polynomial in $|\omega|$.

We introduce two agents: agent $ex$ for the transitions in the computation tree and agent $t$ for the linear structure of tapes. A configuration of the Turing machine is represented by a sequence of worlds linked by agent $t$: one so-called control world followed by cell worlds.

\(^4\)If not, we add a double exponential counter to the machine and we abort the execution after a double exponential number of steps.
5.4. COMMON KNOWLEDGE

- The control world contains the type of the configuration: existential (resp. universal) if \( p_\exists \) (resp. \( p_\forall \)) is true. A special atomic proposition \( p_{\text{win}} \) tags control worlds that correspond to winning configurations for player \( \exists \).

- Cell worlds represent the cells of the tape and form a linear structure. They are indexed by \( x \) from \( x = 0 \) (left-most cell) to \( x = N \) (right-most cell). In each cell world, \( p_a \) is true means that the corresponding cell contains letter \( a \in \Gamma \). A proposition of the form \( p_q \) being true means that the cursor is at that cell and the current state is \( q \in Q \).

Besides atomic propositions \( p_\exists, p_\forall, p_a, a \in \Gamma \) and \( p_q, q \in Q \), we also consider the list of atomic propositions for the bits of the cell index \( v \): \( x_1, \ldots, x_N \). We also consider another such list for another cell index \( v \): \( v_1, \ldots, v_N \). The index \( v \) will be used to compare cell worlds of tapes of a configuration and a successor configuration different tapes during transitions.

The definition of \( \text{tr}(\omega) \) needs multi-pointed event models \( (\mathcal{E}^i, \mathcal{E}_0^i) \) given in Figure 5.4 non-deterministically and publicly choose the \( i^{th} \) bit of value \( v \). We also consider Boolean formulas \( x \leq v \), \( x = v \), \( x = v - 1 \) and finally \( K_i x = x + 1 \) (the value of \( K_i x_0 \ldots K_i x_N \) is equal to \( x + 1 \)). All the formal definitions are given in [CS18]. We define the abbreviation \( [\text{choose}\, v] = [\mathcal{E}^0, \mathcal{E}_0^0] \ldots [\mathcal{E}^N, \mathcal{E}_0^N] \).

Technically, it corresponds to non-deterministically choosing and publicly announcing a value for \( v \).

**Definition 27** Formula \( \text{tr}(\omega) \) is the conjunction of the formulas shown in Table 5.7.

In formulas of Table 5.1 common knowledge operators \( C_{ex} \) and \( \check{C}_{ex} \) are used to talk about any control world, while \( C_i \) and \( \check{C}_i \) talk about any cell world.

Importantly, notice that with \textsc{Delck}, it is impossible to force the each world to have exactly one successor. Thus in general, the expected Kripke model is not as depicted in Figure 5.3. Instead, we ensure that cell worlds of depth \( k \) have the value \( x = k \). We use formula (9) that imposes the value of \( x \) to be the same in all successor cell worlds, and formula (10) saying that everywhere, \( K_i x = x + 1 \). Formula (11) states that only one \( p_a \) is true in each cell world, formula (12) states that only one \( p_q \) is true in some cell world, and formula (13) states that if \( p_a \) is true in a cell world, then no \( p_q \) is true in all the \( i \)-successors. Formulas (17), (18) and (19) define the initial tape. Transitions are ensured by formulas (14) to (16). These formulas automatically ensure that several cell worlds with the same index \( x \) have the same valuation over \( x, p_a, a \in \Gamma, p_q, q \in Q \).

Formulas that handle transitions use integer \( v \) to pinpoint a cell index in the tape. It is used in formula (14) to tell that when the cursor is not in a cell world, then the letter remains the same during any transition. It is also used in formula (15) to check the existence of all compatible transitions and in formula (16) to check that all successor control worlds and their tapes correspond to a transition.

**Proposition 8** \( \text{tr}(\omega) \) is satisfiable if and only if \( \omega \) is a positive instance of \( L \).

**Proof.**

(\( \Rightarrow \)) Suppose \( \text{tr}(\omega) \) is satisfiable. There is a pointed Kripke model \( \mathcal{M}, w \) that satisfies \( \text{tr}(\omega) \). The model is not exactly as in Figure 5.3 for instance, a cell world can have several successors but that have all the same valuation. We extract the computation tree of \( \mathcal{M} \) on the

![Figure 5.4: Multi-pointed event models \((\mathcal{E}^i, \mathcal{E}_0^i)\).](image-url)
CHAPTER 5. SATISFIABILITY PROBLEM

Valuations for control worlds

1. \( C_{ex}(x = 0) \)
\[ x = 0 \text{ holds in all control worlds.} \]
2. \( C_{ex}(p_x \leftrightarrow \bigvee_{q \in \mathcal{Q}}(\neg q_x \lor q_{x+1})) \)
3. \( C_{ex}(\bigwedge_{a \in \Gamma} \neg p_a \land \bigwedge_{q \in \mathcal{Q}} \neg p_q) \)

Winning condition

4. \( C_{ex}(\hat{C}_t p_{accept} \rightarrow p_{win}) \)
5. \( C_{ex}(\hat{C}_t p_{rej} \rightarrow \neg p_{win}) \)
6. \( C_{ex}(p_q \land (\hat{C}_t \neg p_{accept})) \rightarrow (p_{win} \leftrightarrow K_{ex}p_{win}) \)
7. \( C_{ex}(p_{\neg} \land (\hat{C}_t \neg p_{accept})) \rightarrow (p_{win} \leftrightarrow K_{ex}p_{win}) \)

Tape

8. \( C_{ex}K_1(x = 0) \)
9. \( C_{ex}K_1C_t(\bigwedge_{i=0}^N (K_1x_i \lor K_t \neg x_i)) \)
10. \( C_{ex}K_1C_t(K_1x = x + 1) \)
11. \( C_{ex}K_1C_t(\bigoplus_{a \in \Gamma} p_a) \)
12. \( C_{ex}C_t(\bigoplus_{q \in \mathcal{Q}} p_q) \)
13. \( C_{ex}C_t(\bigwedge_{q \in \mathcal{Q}} (p_q \rightarrow C_t \bigwedge_{q \in \mathcal{Q}} \neg p_q)) \)

Transitions

- We define here \( \varphi(q,a,q',b,d) = C_t((x = v \rightarrow p_0 \land \neg p_q) \land (x = v + d \rightarrow p_{q'})) \)
- On the tape, if no \( p_q \) is true and \( p_{\neg} \) is true, then at the same position on the successors’ tapes, \( p_{a} \) is true.
- If there is a transition it must be present on the model.
- In every world, any \( ex \)-successor must correspond to a transition.

Initial configuration

- The letters of the initial word are on the initial tape.
- Cells of index \( |\omega| \) are blank.
- Head in the left-most cell. Initially in the initial state.
- The initial control world is winning.

Table 5.1: Clauses of \textbf{DELCK}-formula \( tr(\omega) \).
initial configuration on input $\omega$. We prove by induction that $p_{\text{win}}$ tags a control world iff its corresponding configuration is winning. Thus, as the initial configuration is tagged by $p_{\text{win}}$, the input $\omega$ is accepted by $M$.

($\Leftarrow$) Suppose that $\omega$ is a positive instance of $L$. We construct the model $M, w$ that represent the computation tree of $M$ on input $\omega$ as shown in Figure 5.3. By construction, formula $M, w \models tr(\omega)$. ■

The lower bound given in Theorem 3 still holds for the variant of the satisfiability problem where we require the model to be $\textsf{S}5$, that is, epistemic relations, to be equivalence relations (see [CS18] for details).

5.5 Arbitrary events

The satisfiability problem of arbitrary public announcement and variants are undecidable ([FvD08], [AvDF14], [AvDF16], [vDvdHK16]). Interestingly, the existential fragment of arbitrary public announcement is decidable [vDFH].

Surprisingly, the satisfiability problem of refinement modal logic (it corresponds to epistemic logic extended with a ‘arbitrary event model operator’) is decidable and proven to be non-elementary [BvDF14].

5.6 Implementation

The satisfiability problem for $\textsf{ELCK}$ is implemented in Hintikka’s world and is based on the tableau prover Mettel2 [TSK12].
Chapter 6

Epistemic planning

In artificial intelligence, classical planning consists in generating a finite sequence of actions for achieving a given goal. The so-called epistemic planning (introduced in [BA11], nicely explained in [Bel17]) generalizes classical planning with epistemic goal (agent $a$ knows that...) and complex actions (public announcements, private announcements, etc.). Epistemic planning based on Dynamic epistemic logic ([BMS98a], [Van07]) is undecidable in the general case [BA11] as we will see in this chapter. Formally, we consider the following decision problem:

**Definition 28 (Epistemic planning)**

- **input:** a state $S$, a finite set of actions $A$ and a formula $\varphi \in L_{ELCK}$;
- **output:** yes if there exists a sequence of actions (a plan) $A_1, \ldots, A_m \in A$ such that $S \otimes A_1, \ldots, A_m = \varphi$; no otherwise.

### 6.1 Undecidability proof

We have:

**Theorem 5** Epistemic planning is undecidable.

The idea for proving the undecidability of epistemic planning is to reduce the halting problem of Turing-complete machines. The reduction works according to the following correspondence table:

<table>
<thead>
<tr>
<th>For the halting problem</th>
<th>For the epistemic planning problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial configuration</td>
<td>Initial epistemic model</td>
</tr>
<tr>
<td>Configuration</td>
<td>Epistemic model</td>
</tr>
<tr>
<td>Machine transition specification</td>
<td>Repertoire of actions</td>
</tr>
<tr>
<td>Transition application</td>
<td>Update product</td>
</tr>
<tr>
<td>Halting configuration</td>
<td>Specified by the goal</td>
</tr>
</tbody>
</table>

In this section, we give the simplest proof we know of Theorem 5 inspired from [CPS18] based on cellular automata. Actually, we show the undecidability of epistemic planning problem, where $A$ is fixed and no longer part of the input. For this, we rely on a universal cellular automaton. From now on throughout this section, $AGT = \{a, b\}$; recall that all models (i.e. states and actions) are $S5$ (epistemic relations are equivalence relations).
6.1.1 Universal 1D cellular automata

In this section, we only consider one-dimensional three-neighbor cellular automata. An infinite sequence of cells are settled on a line; each cell is in a state represented by a symbol of a finite alphabet \( \Sigma \). Given a cell, a transition function \( f \) maps a three-neighbor (left-cell symbol, current symbol, right-cell symbol) to the new symbol of the cell.

**Definition 29** A cellular automaton is a pair \( A = (\Sigma, f) \) where \( \Sigma \) is a finite alphabet and \( f : \Sigma^3 \rightarrow \Sigma \) is a transition function.

**Example 33 (Rule 110 [Wol02])** The Rule 110 cellular automaton is the two-symbol cellular automaton \( A_{110} = (\{0, 1\}, f_{110}) \) where \( f_{110} \) is defined by the Boolean formula

\[
f_{110}(x, y, z) := (x \land y \land \neg z) \lor (x \land \neg y \land z) \lor (\neg x \land y \land z) \lor (\neg x \land \neg y \land \neg z).
\]

A configuration, that is the symbols of cells on an infinite line, is modeled by an infinite word \( c \in \Sigma^\mathbb{Z} \), that is, a map that assigns a symbol \( c[i] \) to any integer \( i \in \mathbb{Z} \). A computation step is performed by the following rule.

**Definition 30** Given a cellular automaton \( A \), given an infinite word \( c \in \Sigma^\mathbb{Z} \), we define the successor of \( c \) by \( A \) to be the infinite word \( c' \) defined by \( c'[i] := f(c[i-1], c[i], c[i+1]) \). We write \( c \rightarrow_A c' \).

Figure 6.1 shows the transition function \( f_{110} \) graphically and some successive configurations.

A cellular automaton is deemed universal if it can simulate any Turing machine; the quest for finding such small universal cellular automata started in the 1960s. A common hypothesis is to assume a blank background: we consider that alphabets always contain a special symbol \( \_ \) and that transition functions map \( \_ \_ \_ \) to \( \_ \). Furthermore, we assume that configurations are finite, in the sense that almost all cell symbols are \( \_ \) except a finite number – configurations are of the form \( \_ \alpha \_ \omega \) where \( \alpha \) is a finite word, called the support of the configurations. Starting from a finite configuration only leads to finite configurations.

Smith proved that any \( m \)-symbol \( n \)-state Turing machine can be simulated by a one-dimensional \( (m + 2n) \)-symbol 3-neighbor cellular automaton with a blank background (see Theorem 4 in [Smi68]). As Minsky constructed a 4-symbol 7-state universal Turing machine \( M_{\text{Minsky}} \) [Min67], there exists a \( 4 + 2 \times 7 = 18 \)-symbol universal cellular automaton \( A_{\text{Smith}} = (\Sigma_{\text{Smith}}, f_{\text{Smith}}) \), that simulates \( M_{\text{Minsky}} \).

As a consequence, we obtain the following undecidability result for the reachability problem for \( A_{\text{Smith}} \) with blank background.

---

1 We use ‘symbol’ instead of ‘cell state’, to avoid confusion with a knowledge state.

2 Referred to as \((m + 2n)\)-state in [Smi68].
Theorem 6 There exists a finite word \( h_{\text{Smith}} \) such that it is undecidable to determine, given a finite word \( \alpha \), whether \( \omega \cdot \alpha \cdot \omega \rightarrow^{*} A_{\text{Smith}} \) where the configuration \( c \) contains the pattern \( h_{\text{Smith}} \).

6.1.2 Finite linear states

The main result of this section is Corollary 1 which provides bounds to the parameters of the epistemic planning problem. This is achieved by simulating executions of cellular automata with blank background. First of all, we introduce sufficiently many propositions to encode symbols of the alphabet. Typically, for alphabet \( \Sigma_{\text{Smith}} \) with 18 symbols that we respectively write \( \ell_0, \ell_1, \ldots, \ell_{17} \), only 5 propositions \( p_1, \ldots, p_5 \) suffice. Given a symbol \( \ell \), we note \( \text{enc}(\ell) \) the encoding of \( \ell \): \( \text{enc}(\ell_0) = \neg p_1 \land \ldots \land \neg p_5 \), \( \text{enc}(\ell_1) = p_1 \land \neg p_2 \ldots \land \neg p_5 \), etc. W.l.o.g., we suppose that symbol \( \omega \) is \( \ell_0 \) and is encoded by the valuation making all \( p_i \)'s false. In the rest, \( \bar{p} \) denotes the sequence of propositions \( p_i \)'s.

Now, we encode the finite supports of configurations by means of finite linear states – such states appear in real epistemic puzzles such as the consecutive number puzzle \( [vdk15] \). They are states of the form \( I_n = \{ \neg n, \ldots, -1, 0, 1, \ldots, n \} \), \( (R_a)_{a \in AGT} \), \( w(0) \) with odd \( n \) and:

1. \( R_a = \{ (k, k) \mid k \in [1; n] \} \cup \{(2k, 2k + 1), (2k + 1, 2k) \mid \frac{-n+1}{2} \leq k \leq \frac{n-1}{2} \} \);
2. \( R_b = \{ (k, k) \mid k \in [1; n] \} \cup \{(2k, 2k - 1), (2k - 1, 2k) \mid \frac{-n+1}{2} \leq k \leq \frac{n-1}{2} \} \);
3. \( \wp \in w(k) \) iff \( k \) is even;
4. for all \( i, p_i \notin w(n), w(-n + 1), w(n - 1), w(n) \).

A finite linear state \( I_n \) encodes a finite configuration \( c \) whose support is of length smaller than \( 2n - 3 \) when \( V(k) \) makes \( \text{enc}(\ell_i) \) true iff \( c[k] = \ell_i \); we require that the two terminal \( (-n \) and \( n) \) and the two pre-terminal \((n - 1, -n + 1) \) worlds encode \( \omega \) (Condition 4). For instance, the \( A_{\text{Smith}} \) configuration \( \omega \cdot \omega \cdot \omega \cdot \omega \cdot \omega \cdot \omega \cdot \omega \cdot \omega \) where \( c[-1] = 9 \) can be represented by:

\[
\begin{array}{ccccccccc}
-3 & b & -2 & a & -1 & b & 0 & a & 1 & b & 2 & a & 3 \\
\wp & p_1, p_4 & \wp & p_1, p_3 & \wp & p_2 & \wp & \end{array}
\]

Given a finite word \( \alpha \), let us set once and for all what finite linear state \( S_\alpha \) will encode \( \alpha \): substituting \( \alpha^m \) for \( \alpha \) with \( m \in \{ 0, 1, 2, 3 \} \) so that \( |\alpha| \) be congruent to 3 modulo 4, we set \( S_\alpha = (I_n)_{n \in AGT}, (R_a)_{a \in AGT}, w(0) \) where \( V(k - \frac{|\alpha| - 1}{2}) \) makes \( \text{enc}(\ell_i) \) true iff \( \alpha[k] = \ell_i \) for \( 0 \leq k \leq |\alpha| - 1 \), and makes \( \text{enc}(\omega) \) true outside of this range. These are only technicalities ensuring a sufficiently large odd index for the interval state to respect constraints with a pseudo-centered word.

6.1.3 Simulating cellular automata in DEL

We define action \( F \) mimicking one computation step of the cellular automaton: if \( S \) is a finite linear state encoding a configuration \( c \), then \( S \otimes F \) is (isomorphic to) a finite linear state encoding the successor of \( c \).

Action \( F \) is partially given by Figure 6.2. Intuitively, the actual event \( e_0 \) copies every non-territorial world; event \( e_{-1} \) keeps the left-tip world, while \( e_{-2} \) and \( e_{-3} \) clone it to append two new worlds to the left. Events \( e_1, e_2, e_3 \) play a similar part. In the end, action \( F \) adds two new worlds on each side, while preserving the canonical knowledge state structure that we aim for, including the tips' asymmetry relatively to the agents.

\(^3\)According to the notation of Table 14.8-1 p. 279 in \( [\text{Min67}] \), word \( h_{\text{Smith}} \) is \( q_30 \).
We finish the definition of $\mathbf{F}$ by adding postconditions for $p_j$’s, corresponding to the application of a transition function $f$. Suppose w.l.o.g. that $\Diamond$ holds in a given world $k \in \{-n+1, \ldots, n-1\}$. Bits of $c[k-1]$ are obtained by taking the $b$-transition from the $\neg \Diamond$-world of world $k$. They are: $(\dot{K}_b(\neg \Diamond \land p_i))_i$. In the same way, the values of $\bar{p}$ in world $k+1$ are given by the vector $(K_b(\neg \Diamond \land p_i))_i$. The case where $\Diamond$ does not hold in the current world is symmetric.

We model $f$ by the vector $\langle f \rangle$ of world $\{−64\}$ that an overall set of 6 propositions suffices. We enclose $\mathbf{F}$ by Boolean formulas $f_j(\bar{p}^-, \bar{p}, \bar{p}^+)$ over three sequences of atomic propositions $\bar{p}^-$ (left cell symbol), $\bar{p}$ (middle cell symbol), $\bar{p}^+$ (right cell symbol) that return the value of the $j$th bit of the new symbol at the middle cell. Bits of the new symbol are: $(f_j(\bar{p}^-, \bar{p}, \bar{p}^+))_j$.

The postconditions for $p_j$’s in $\mathbf{F}$ is thus defined as follows. First, $\text{post}(e_0)(p_j) = \perp$ for all $k \neq 0$. Only $e_0$ effectively applies $f$ and $\text{post}(e_0)(p_j)$ is formula $(\Diamond \rightarrow f_j((\dot{K}_b(\neg \Diamond \land p_i))_i, \bar{p}, (\dot{K}_b(\neg \Diamond \land p_i))_i) \land (\neg \Diamond \rightarrow f_j((\dot{K}_b(\neg \Diamond \land p_i))_i, \bar{p}, (\dot{K}_b(\neg \Diamond \land p_i))_i))$. We will refer to $\mathbf{F}_{\text{Smith}}$ for the action model that corresponds to the transition function $f_{\text{Smith}}$ of the cellular automaton $A_{\text{Smith}}$.

On top of proposition $\Diamond$, when considering the particular cellular automaton $A_{\text{Smith}}$, we need no more than 5 extra propositions to encode all symbols of alphabet $\Sigma_{\text{Smith}}$ of cardinal 18, so that an overall set of 6 propositions suffices.

Now, we define formulas encoding the occurrence of a pattern $h$ in the configuration. We first define the formula $\text{wenc}(h) := \text{wenc}_{\Diamond}(h) \lor \text{wenc}_{\neg \Diamond}(h)$ where formulas $\text{wenc}_{\Diamond}(h)$ and $\text{wenc}_{\neg \Diamond}(h)$ are inductively defined by:

- $\text{wenc}_{\Diamond}(e) = \Diamond$ and $\text{wenc}_{\neg \Diamond}(e) = \neg \Diamond$;
- for all letters $t$, $\text{wenc}_{\Diamond}(th) := \Diamond \land \text{enc}(t) \land \dot{K}_b \text{wenc}_{\Diamond}(h)$;
- for all letters $t$, $\text{wenc}_{\neg \Diamond}(th) := \neg \Diamond \land \text{enc}(t) \land \dot{K}_b \text{wenc}_{\Diamond}(h)$.

We can now state the following theorem that derives from our ability to simulate the behavior of the cellular automaton $A_{\text{Smith}}$ and the use of the dual of the common knowledge operator $\dot{C}_{\text{AGT}}$ to search over a finite linear state for the pattern $\text{wenc}(h_{\text{Smith}})$.

**Theorem 7** Given a finite linear state $S$ over 6 propositions, it is undecidable to determine whether or not a state satisfying $\dot{C}_{\text{AGT}} \text{wenc}(h_{\text{Smith}})$ is reachable from $S$ by executing a finite sequence of actions $\mathbf{F}_{\text{Smith}}$.

**Proof.**

By reduction from the undecidable reachability problem of Theorem 6. An instance $a$ of the latter is translated into $S_a$. ■

**Corollary 1** The epistemic planning problem over 2-agent 55 finite models is undecidable, even if the repertoire is $\{\mathbf{F}_{\text{Smith}}\}$, the goal is $\dot{C}_{\text{AGT}} \text{wenc}(h_{\text{Smith}})$ and we only use at most 6 different propositions.

The interested reader can run simulations in DEL of cellular automata using the online software Hintikka’s world. Figure 6.3 shows a screenshot of Hintikka’s World depicting a finite linear state.
6.2 Undecidability frontier

Epistemic planning is undecidable even when we assume these conditions on event models:

- preconditions and postconditions (even up to modal depth 1) and no common knowledge in the goal formula [BA11, CPS18];
- preconditions up to modal depth 2, no postconditions and no common knowledge in the goal formula [CMS16];
- arbitrary preconditions, no postconditions [AB13] and no common knowledge in the goal formula;
- automatic (potentially infinite) initial state but only one public actions [CPS18];

**Conjecture 1** Epistemic planning when actions are purely epistemic and all preconditions are of modal depth at most 1 is decidable.

6.3 Decidable restrictions

6.3.1 Public actions

**Theorem 8** Epistemic planning with public actions is in PSPACE.

**Proof.**
We give a non-deterministic algorithm for deciding epistemic planning with public actions in polynomial space. We start with the initial Kripke model as the current model. At each step, we check whether the goal is satisfied. If yes, we accept the input. If not, we non-deterministically
choose an action and we compute the product of the current model and the selected action. As actions are public, the current model remains of polynomial size in the input. ■

6.3.2 Purely epistemic actions

As public announcement of propositional facts commute and are idempotent, we have:

**Theorem 9** Epistemic planning with propositional public announcements is NP-complete [BJS15b].

As purely epistemic propositional event models commute and an event model \( \mathcal{E} \) stabilize at iteration \( |\mathcal{E}|^d \) with respect to bisimulation up to modal depth \( d \) (see [CMS16]). Therefore, we guess a plan by:

- guessing how many times (at most \( |\mathcal{E}|^d \) ) each event is executed, where \( d \) is the modal depth of the goal formula;
- using the model checking algorithm over the language with iterated event models where numbers are written in binary and that runs in polynomial space.

As this algorithm runs in polynomial space, we get:

**Theorem 10** Epistemic planning with purely epistemic propositional event models is PSPACE-complete ([BJS15b], [CMS16]).
Chapter 7

Propositional Epistemic planning

This chapter is adapted from [DTPS18].

7.1 Introduction

When event preconditions and postconditions are propositional (Boolean) only (intuitively, announcements are Boolean formulas and uncertainty is only about the content of the messages and physical changes), epistemic planning has been shown to be decidable ([YWL13], [Mau14]).

Regrettably, epistemic planning as considered so far concerns finite plans, and is in essence a reachability problem. However, real-life applications may challenge infinite plans. We give three examples of planning goals that require an infinite plan.

1. safety properties, e.g. ‘invariantly, an intruder $a$ does not know the location of the piece of jewelry more than 3 consecutive steps’.

2. recurring bounded properties, e.g. ‘all drones know that the region is safe every 20 steps’;

3. strategic reasoning, e.g. ‘with the current plan, the drone $a$ never knows the region is safe but every 10 steps, there is a(nother) plan to let the drone $a$ eventually know the region is safe’.

Nevertheless, infinite plans have been considered in [Mau14] in the DEL (Dynamic Epistemic Logic) setting. In this approach, DEL structures, those arising from iterating ad infinitum the triggering of events, are seen as infinite relational structures. Maubert has shown that, when all event preconditions and postconditions are propositional, DEL structures are automatic structures (over strings) [BG00, Rub08]. Automatic structures are relational structures which have a presentation by means of a finite family of finite-state automata. As noticed by Maubert, the decidability result of epistemic planning (for epistemic goals) relies on the fact that model checking against first-order logic is decidable over automatic structures: in a DEL structure, the skeleton is a tree whose nodes (or equivalently finite branches) are finite plans, i.e. sequences of triggered events, and this tree structure is augmented with “transverse” binary relations between nodes in possibly different branches. These extra relations denote epistemic relations between histories. In DEL structures, the existence of a plan reduces to the existence of a point in this automatic (tree) structure where the epistemic planning goal (hence expressible in FO) holds. After all, the whole epistemic planning problem can be expressed in FO whose outermost
CHAPTER 7. PROPOSITIONAL EPISTEMIC PLANNING

quantifier is existential. Additionally, automata constructions that answer the query of an FO-formula on an automatic structure allow to synthesize an automaton that recognizes the set of all (finite) plans achieving the goal. Regarding infinite plans, Maubert relies on the involved theory of uniform strategies he has developed [Man14]. This theory enables him to deal with epistemic planning instances whose goals are expressed in the branching-time epistemic logic CTL^K, the extension of temporal logic CTL^* [HT87] with epistemic modalities. The setting does lead to synthesizing infinite plans, but the synthesis relies on a bottom-up technique over the goal formula that prevents the setting from being extended to logics featuring fix-points; while statements (ii) and (iii) above cannot be expressed in CTL^*K, a well-tuned logic with fix-point or monadic with second-order quantifiers would suffice.

In an attempt to enlarge the specification language for epistemic planning goals, that goes beyond CTL^*K while remaining decidable, one should observe that using the full monadic second-order logic (MSO) is hopeless: by [Tho90], model checking against MSO over the binary tree equipped with the transverse binary relation “equal level” is undecidable. Relation “equal level” is an instance of an agent epistemic relation where the agent does not observe anything from the current finite sequence of triggered events but its length. However, there are variants of MSO, where second-order quantifications are constrained enough to yield a decidable model checking problem over infinite trees of the kind of DEL structures. For example, relying on [HT87], and as depicted in Figure 7.1 there exist mainly three interpretations of the second-order quantifiers, yielding full MSO, path-MSO, and chain-MSO. The full MSO logic can be interpreted over arbitrary relational structures and the second-order quantifiers range over all subsets of the structure domain. On the contrary, the path-MSO logic is interpreted on (possibly infinite) trees and the quantifiers range over paths/branches of the tree. Finally, chain-MSO, also interpreted on trees only, requires the second-order quantifier to range over chains, that are subsets of paths [HT87]. It is known that the expressive power of chain-MSO strictly subsumes the one of path-MSO, the former allowing to describe arbitrary ω-regular properties of branches, while the latter captures only star-free properties, see [HT87].

In this paper, we extend chain-MSO of [Tho87, HT87] with relations in the tree, e.g. interpreting epistemic modalities, making statements (ii) and (iii) expressible. This extension is written cMSO. We introduce regular automatic trees, a strict but large subclass of automatic structures that encompass DEL structures with propositional events. We then show that model checking against cMSO is decidable over regular automatic trees. Our decidability result is strongly inspired from the proof technique in [Tho92, Th. 5.2] to show that chain-MSO with the “equal level” predicate is decidable over n-ary trees. Our proof yields automata constructions that can be exploited to achieve the synthesis of plans in epistemic planning.

Noticeably, the logic cMSO captures the linear-time mu-calculus ([BKP86], [?]) enriched with path quantifiers and epistemic modalities, here written BLlin^µK (the acronym stands for ‘Branching Logic of the linear-time µ-calculus with Knowledge). In essence, the logic BLlin^µK is an epistemic extension of the logic ECTL^*, for “extended CTL^*”, of [HT87], but in a nu-calculus style rather than with the use of automata modalities, in the sense of [Wol83]. Since CTL^*K can easily be embedded into BLlin^µK (the hard-coded linear-time temporal operators of CTL^* are based on fix-points expressible in the linear-time mu-calculus), our result significantly exceeds the one of [Ma13] whose proof technique does not allow for considering arbitrary fix-point formulas.

The presented contribution is derived from the preliminary work available in [?]. In Section 7.2, we recall the notion of automatic structures and results on model checking against FO-formulas and MSO-formulas. In Section 7.3, we present the logic cMSO, as well as the subclass of so-called regular automatic trees. We prove that model checking against cMSO is decidable

---

2The difference between paths and branches is irrelevant by [HT87].
7.2 Preliminaries on automatic structures and decidable theories

In this section we recall seminal results on automatic structures: namely that first-order logic FO is decidable over these structures while monadic second-order logic MSO is not. The interested reader may refer to [BG00, Rub08] for further details.

7.2.1 Structures and logics

Logics FO and MSO are interpreted over relation structures.

Definition 31 A relational structure is a structure of the form \( A = \langle D, R_1 \ldots R_p \rangle \) where:

- \( D \) is a non-empty set called the domain;
- \( R_1 \ldots R_p \) are relations over \( D \) of arity \( r_1 \ldots r_p \), respectively; namely \( R_i \subseteq D^{r_i} \).

The set of symbols \( \{ R_1 \ldots R_p \} \) is called the signature of \( A \). We take the convention to write \( R_i(d_1, \ldots, d_{r_i}) \) for \( (d_1, \ldots, d_{r_i}) \in R_i \). We distinguish the particular class of structures that are infinite trees of fixed finite degree \( n \), called \( n \)-ary trees, that are central in our contribution. These structures represent computation trees (with a root of address \( \epsilon \), \( i \)-successor relations, and prefix binary relation between addresses) augmented with additional relations, such as epistemic relations.

Definition 32 Given a finite set \( E := \{1, \ldots, n\} \) of directions, we call \( n \)-ary tree a structure \( T = \langle D, r, S_1, \ldots, S_n, R_1, \ldots, R_p \rangle \) where:

- \( D \) is a prefix-closed subset of \( E^* \) (the addresses of the nodes);
- \( r \) is a unary relation that holds only for \( \epsilon \), the root address of the tree;
- \( S_e(x, xe) \) whenever \( xe \in D \);
• \(R_1, \ldots, R_p\) are additional relations on \(D\).

In the particular case of a tree, elements of \(D\) are nodes. Notice that no condition was imposed on the relations \(R_1 \ldots R_p\) in Definition 32 of a tree. They may therefore correspond to transversal links between nodes just as epistemic relations would do, e.g. the “equal level” binary relation.

Example 34 The structure \(\mathcal{T}_2 = (E^*, S_1, S_2)\) is a 2-ary tree called the infinite full binary tree. Also the structure \(\mathcal{T}'_2 = (E^*, S_1, S_2, \mathfrak{e})\) obtained by augmenting \(\mathcal{T}_2\) with the binary relation “at equal level in the tree” \((\mathfrak{e}(x,y))\) holds if, and only if, \(|x| = |y|\) is another example of a 2-ary tree.

First-order logic (FO) over relational structures \(\mathcal{A} = (D, R_1 \ldots R_p)\) concerns formulas that conform to the following syntax: 
\[
\varphi : = R_i(x_1 \ldots x_r) \mid \neg \varphi \mid (\varphi \land \varphi) \mid \exists x \varphi, \text{ where } x, x_1, x_r \text{ are first-order variables whose interpretation ranges over the domain of relational structures.}
\]

When turning to the more expressive monadic second-order logic (MSO), one allows for second-order variables that range over subsets of the domain of relational structures. Formally, the syntax of MSO is given by: 
\[
\varphi : = R_i(x_1 \ldots x_r) \mid x \in X \mid \neg \varphi \mid (\varphi \land \varphi) \mid \exists x \varphi \mid \exists X \varphi, \text{ where } x \text{ is a first-order variable, while } X, X_1, \ldots, X_m \text{ are second-order variables whose interpretation ranges over subsets of the domain.}
\]

In the following, we let \(V_1\) and \(V_2\) denote respectively the set of first-order variables and second-order variables.

As usual, in a formula, a variable \(x \in V_1\) (resp. \(X \in V_2\)) is free if it is not under the scope of a quantifier, namely some \(Qx\) (resp. \(QX\)) with \(Q \in \{\forall, \exists\}\). A formula is closed if it contains no free variables.

An assignment in domain \(D\) is a function \(\sigma\) that maps a variable of \(V_1\) onto an element of \(D\) and a variable of \(V_2\) onto a subset of \(D\). Given an assignment \(\sigma\) in \(D\), a variable \(x \in V_1\) and \(d \in D\), we let \(\sigma[x \mapsto d]\) be the assignment on \(D\) that coincides with \(\sigma\) but maps \(x\) onto \(d\). Similarly, we define \(\sigma[X \mapsto D']\) where \(D' \subseteq D\) for the second-order variables.

Due to limited space, we do not provide the semantics of MSO, see for example [?].

7.2.2 Automatic presentations

We now describe how some relational structures can be encoded using formal languages, following the presentation of [Rub08]. By alphabet we mean a finite set of symbols, named letters. A word over \(\Sigma\) is a finite sequence of letters. We denote by \(\Sigma^*\) the set of such sequences. For \(\alpha \in \Sigma^*\) and \(n \geq 0\), let \(\alpha[n]\) be the \(n+1\)-th letter of \(\alpha\) (when defined). We assume familiarity with the basic definitions of automata theory and the properties of regular languages.

Let \(\square\) be a fresh padding symbol. If \(\Sigma\) is an alphabet, we define \(\Sigma_{\square}\) as \(\Sigma \cup \{\square\}\). The following definition describes an encoding for \(k\)-tuples of words as a word on the product alphabet \(\Sigma_{\square}^*\); since words of the tuple may have different length, the padding symbol \(\square\) is used to align the words.

Definition 33 If \(u, v \in \Sigma^*\), their convolution \(u \otimes v\) is the word of \((\Sigma_{\square} \times \Sigma_{\square})^*\) of length 
\[
\max(|u|, |v|) \text{ such that } (u \otimes v)[n] = (u[n], v[n]) \text{ if } n < \min(|u|, |v|); (u \otimes v)[n] = (u[n], \square) \text{ if } |v| \leq n < |u|; \text{ and } (u \otimes v)[n] = (\square, v[n]) \text{ if } |u| \leq n < |v|. \text{ Convolution is defined similarly for } k\text{-tuples of words.}
\]

Example 35 The convolution of \(aaba, b\) and \(ba\) over alphabet \(\Sigma = \{a, b\}\) is the four-letter word 
\[
\left(\text{a} \square \text{a} \square \text{b} \square \right) \text{ over alphabet } \Sigma_{\square}^2.
\]

Definition 34 Let \(\mathcal{A} = (D, R_1 \ldots R_p)\) be a relational structure. An automatic presentation of \(\mathcal{A}\) is a tuple of regular languages \((L_D, L_1, \ldots, L_n)\) meeting the following conditions:

that there exists a one-to-one encoding function $\text{enc}: D \to L_D$;

- for all $R_i$ (arity $r_i$), $L_i = \{\alpha_1 \otimes \cdots \otimes \alpha_{r_i} | \forall j, \alpha_j \in L_D \text{ and } (\text{enc}^{-1}(\alpha_1), \ldots, \text{enc}^{-1}(\alpha_{r_i})) \in R_i\}$.

The alphabet $\Sigma$ of $L_D$ is called the encoding alphabet. The inverse $\text{enc}^{-1}$ of the encoding function is the decoding function. We write $\text{enc}(D)$ for $L_D$, and more generally, $\text{enc}(R)$ for the set $\{(\text{enc}(d_1), \ldots, \text{enc}(d_{r_i})) | (d_1, \ldots, d_{r_i}) \in R_i\}$, for an arbitrary relation $R \subseteq D^r$.

A structure is automatic if it has (at least) an automatic presentation. A presentation can effectively be described by a tuple of finite automata $(M_D, M_1, \ldots, M_n)$ recognizing $(L_D, L_1, \ldots, L_n)$.

**Remark 2** We may assume that equality is among the relations $R_i$, represented by the regular language $\{\alpha \otimes \alpha | \alpha \in L_D\}$. In the literature, the standard definition of automatic presentations allows an element to have several encodings, whenever equality can be presented by some regular language. However, both definitions enable to present the same structures [BG00].

**Example 36**

1. Finite structures are automatic, since finite languages are regular.

2. $\langle \mathbb{N}, \leq \rangle$ is automatic, with an automatic presentation over a unary alphabet $\{1\}$ by letting $\text{enc}(n)$ be the unary representation of $n$, that is the word $1^n$. Automaton $M_{\leq}$ depicted in Figure 7.2 verifies there are less $1$’s in the first component than in the second component.

   \[ \begin{array}{ccc}
   \text{start} & \xrightarrow{\{\}} & \text{state0} \\
   & \xrightarrow{\{\}} & \text{state1}
   \end{array} \]

   Figure 7.2: The finite-state automaton $M_{\leq}$ of Example 36 (ii).

3. Both trees $T_2$ and $T_2^d$ are automatic.

   We recall the known fundamental theorem of [Rub08, Th. 3.1] regarding the model checking problem against FO over automatic structures.

**Definition 35** \textbf{Model checking against FO}

- \textbf{Input}: A presentation $(M_D, M_1, \ldots, M_n)$ of a relational structure $\mathcal{A}$ and a closed FO-formula $\varphi$ over the corresponding signature.
- \textbf{Output}: Yes if $\mathcal{A} \models \varphi$, no otherwise.

**Theorem 11** [Rub08, Th. 3.1] Model checking against FO is decidable.

The main ingredient of the proof of Theorem 11 relies on the construction of Proposition 9 which heavily relies on the closure of regular languages by intersection, negation and projection over components.

Let $\varphi(x_1 \ldots x_n) \in \text{FO}$ where $x_1 \ldots x_n \in \mathcal{V}_1$ are the only free variables, and let $\mathcal{A}$ be a relational structure. We write $\varphi^A := \{(d_1 \ldots d_n) \in D^n \mid \mathcal{A} \models [x_i \mapsto d_i]_{1 \leq i \leq n} \models \varphi[x_1 \ldots x_n]\}$ for the set of tuples that satisfy $\varphi$.

**Proposition 9** There is an algorithm that given an automatic presentation of a relation structure $\mathcal{A}$ with encoding function $\text{enc}$, and a first-order formula $\varphi(x_1, \ldots, x_n)$, outputs an automaton that recognizes $\text{enc}(\varphi^A)$. 

Theorem 11 can sometimes be extended to MSO. For example, there are very specific cases where MSO can be decided, among which the typical example of the automatic structure \((\mathbb{N}, <)\).

**Proposition 10** [Bar07] The MSO-theory of a structure having an automatic presentation based on a unary encoding alphabet is decidable.

Also, by Rabin’s Theorem [Rab69], MSO is decidable over the full binary tree with signature \(r, S_1, S_2\). However, MSO becomes undecidable over the full binary relation augmented with the “equal level” relation \(el\) (see Example 34), although the obtained structure is automatic.

**Theorem 12** [Tho90] Model checking against MSO over the binary tree \(T_{2^d}\) is undecidable.

We now focus on a subclass of automatic structures where the undecidability frontier can be pushed back.

### 7.3 Model checking against cMSO over regular automatic trees

We consider the variant of MSO stemming from “chain MSO”, written cMSO in this paper, which contrary to FO and MSO, can only be interpreted over infinite trees. The second-order quantifiers range over chains, namely subsets of nodes along a branch, as depicted in Figure 7.1(c). The logic cMSO has already been defined in [Tho87, HT87, Tho92] for \(n\)-ary trees and with a signature restricted to the successor relations \(S_1, \ldots, S_n\); the main results concern the decidability of the model checking of chain-MSO over the full binary tree, and its expressivity. In our setting, the signature of cMSO can be arbitrary, so that properties involving e.g. knowledge and time can be expressed.

We also exhibit a subclass of automatic structures called regular automatic trees that are automatic trees where the encoding of a node is its address in the tree. This subclass is large and encompasses infinite models arising from the unfolding of finite-state systems but also in dynamic epistemic logic. We establish that model checking against cMSO is decidable over regular automatic trees (Theorem 13).

#### 7.3.1 The logic cMSO over trees

We recall the notion of tree structure \(T = \langle D, r, S_1, \ldots, S_n, R_1, \ldots, R_p \rangle\) over a finite set \(E = \{1, \ldots, n\}\) of directions (Definition 32), where \(D\) is a prefix-closed subset of \(E^*\) describing the nodes through their addresses in the tree. In the following, we let \(S^*\) be the reflexive and transitive closure of the generalized successor relation \(S := \bigcup_{i=1}^{n} S_i\).

**Definition 36** In a tree structure \(T\) of domain \(D \subseteq E^*,\) a subset \(C \subseteq D\) is a chain if it is totally ordered with respect to \(S^*,\) i.e. for all \(d, d' \in C,\) either \(S^*(d, d')\) or \(S^*(d', d)\) holds. We denote by \(Ch(T)\) the set of chains of the tree \(T.\)

**Example 37** In the full binary tree \(T_2,\) the set \(\{1^{2n} \mid n \in \mathbb{N}\}\) is a chain, whereas \(\{1, 2\}\) is not.

The notion of chains enables one to consider an interpretation of MSO formulas in trees, named cMSO, where the second-order quantifiers are restricted to chains.

**Definition 37** The logic cMSO is interpreted in a tree \(T = \langle D, r, S_1, \ldots, S_n, R_1, \ldots, R_p \rangle\) with an assignment \(\sigma\) in \(D\) for free variables as follows.
7.3. MODEL CHECKING AGAINST CMSO OVER REGULAR AUTOMATIC TREES

\[ T, \sigma \models R_i(x_1 \ldots x_r) \text{ iff } \langle \sigma(x_1) \ldots \sigma(x_r) \rangle \in R_i; \]
\[ T, \sigma \models x \in X \text{ iff } \sigma(x) \in \sigma(X); \]
\[ T, \sigma \models \neg \varphi \text{ iff } T, \sigma \not\models \varphi; \]
\[ T, \sigma \models \exists x \varphi \text{ iff there exists } d \in D \text{ such that } T, \sigma[x \mapsto d] \models \varphi; \]
\[ T, \sigma \models \exists X \varphi \text{ iff there exists a chain } C \in Ch(T) \text{ such that } T, \sigma[x \mapsto C] \models \varphi. \]

For a close formula \( \varphi \), we simply write \( T \models \varphi \) without specifying the assignment.

The logic \( \text{cCMSO} \) is close to the logic \( \text{path-MSO} \) \cite{Tho87, HT87} which restricts second-order quantification to maximal branches only. Actually the latter is a subsystem of the former: the \( \text{cCMSO} \)-formula

\[ \text{pathfrom}[X,x_0] := x_0 \in X \land \forall x \{ x \in X \rightarrow [\exists y S(x,y) \rightarrow \exists y (S(x,y) \land y \in X)] \land \neg S(x,x_0) \} \]

expresses that chain \( X \) is a maximal path starting at note \( x_0 \), which corresponds to the very quantifier in \( \text{path-MSO} \). This translation has already been noticed many times in the literature.

### 7.3.2 Regular automatic trees

We now turn to a particular class of trees, called regular automatic trees, which are automatic trees for the most intuitive encoding of nodes, that is by their address in the tree. Since the domain is required to be regular, such trees arise from the unfolding of some finite-state transition systems, hence the terminology of regular trees.

**Definition 38** A tree \( T = \langle D, r, S_1, \ldots, S_n, R_1, \ldots, R_p \rangle \) on the set of directions \( E = \{1, \ldots, n\} \) is a regular automatic tree if the identity function \( \text{enc}: D \rightarrow E^* \) describes an automatic presentation of \( T \) over the encoding alphabet \( E \). This presentation is called the canonical presentation of \( T \).

Since the encoding function of a regular automatic tree is the identity function, the regularity of \( S_1, \ldots, S_n \) and \( \leq \) directly follows from that of \( D \). Thus, a tree is a regular automatic tree if, and only if, \( D \subseteq E^* \) is regular, and for all \( R_i \) (of arity \( r_i \)), \( L_i = \{d_1 \otimes \cdots \otimes d_{r_i} \mid (d_1, \ldots, d_{r_i}) \in R_i \} \) is regular.

**Example 38** The tree \( T_{2^1}^\text{el} \) of Example 34 is a regular automatic tree.

As stated in the following proposition, regular automatic trees form a strict subclass of automatic trees.

**Proposition 11** There are automatic trees that are not regular automatic trees.

**Proof.**
Let \( E = \{1, 2\} \) we consider the binary tree \( T_{\text{notreg}}^\text{auto} = \langle D, r, S_1, S_2, \text{el} \rangle \) of Figure 7.3(a) where \( D = \{1^m2^k \mid 0 \leq k \leq m \} \) and \( \text{el} \) is the “equal level” relation of Example 34. As \( D \) is not a regular language, \( T_{\text{notreg}}^\text{auto} \) is not a regular automatic tree; it is automatic: consider the encoding alphabet \( \Sigma = \{0, 1\}^\omega \) and let \( \text{enc}(1^m2^k) = \text{bin}(m) \otimes \text{bin}(k) \) be the encoding function, as presented in Figure 7.3(b) where \( \text{bin}(m) \) (resp. \( \text{bin}(k) \)) the binary representation of \( m \) (resp. \( k \)) with least significant digit first. For example, \( \text{enc}(112) = \text{enc}(1^22^1) = \text{bin}(2) \otimes \text{bin}(1) = (\frac{1}{3}) (\frac{1}{3}) \). The reader should easily get convinced that \( \text{enc}(D), \text{enc}(S_1), \text{enc}(S_2) \) and \( \text{enc}(\text{el}) \) are regular languages.

\[ \blacksquare \]
CHAPTER 7. PROPOSITIONAL EPISTEMIC PLANNING

Figure 7.3: An automatic tree that is not regular.

When restricting to regular automatic trees, some usual relations over trees can be easily captured by automata over the canonical encoding of nodes. We recall the following additional binary relations over trees.

- The reflexive and transitive closure $S^*$ of the generalized successor binary relation $S$;
- The binary relation $(d,d') \in <$ whenever node $d$ is not deeper than node $d'$ in $T$;
- The binary relation $el$, where $(d,d') \in el$ whenever nodes $d$ and $d'$ are at the same depth in the tree.
- The binary equality relation $=$.

**Lemma 3** Let $\langle D, r, S_1, \ldots, S_n, R_1, \ldots, R_p \rangle$ be a regular automatic tree. Then the relational structure $\langle D, r, S_1, \ldots, S_n, R_1 \ldots R_p, S^*, \leq, el, = \rangle$ is also a regular automatic tree.

**Proof.**

Let $\langle M_D, M_r, (M'_i)_{1 \leq i \leq n}, (M'i)_{1 \leq i \leq p} \rangle$ be a presentation of $T$. It is enough to describe automata $M_{S^*}, M_{\leq}, M_{el}$, and $M_=$ that run over the canonical encodings of nodes and that capture relations $S^*, \leq, el,$ and $=$, respectively.

- The automaton $M_{S^*}$ for $S^*$ accepts a pair of words $(\alpha, \alpha')$ whenever each of them is accepted by $M_D$ and $\alpha$ is prefix of $\alpha'$.
- The automaton $M_{\leq}$ for $\leq$ accepts a pair of words $(\alpha, \alpha')$ whenever each of them is accepted by $M_D$ and the length of $\alpha$ is less than or equal to the length of $\alpha'$.
- The automaton $M_{el}$ for $el$ accepts a pair of words $(\alpha, \alpha')$ whenever each of them is accepted by $M_D$ and the length of $\alpha$ is equal to the length of $\alpha'$.
- The automaton $M_=$ for $=$ accepts a pair of words $(\alpha, \alpha)$ whenever $\alpha$ is accepted by $M_D$.

Restricting to the class of regular automatic trees allows for decidability results of model checking against logics that go beyond $\text{FO}$. 

7.3. MODEL CHECKING AGAINST CMSO OVER REGULAR AUTOMATIC TREES

7.3.3 Model checking against cMSO

We now describe the main result of this section, as stated by Theorem 13 where the model checking problem against cMSO is as follows.

Definition 39 Model checking against cMSO

**Input:** The canonical presentation \( \langle M_D, M_r, (M_i)_{1 \leq i \leq n}, (M_i^j)_{1 \leq i \leq p} \rangle \) of a regular automatic tree \( T \) and a closed cMSO-formula \( \varphi \) over the corresponding signature.

**Output:** Yes if \( T \models \varphi \), no otherwise.

Theorem 13 can be read as a variant of Theorem 11 where, on the one hand, the logic FO is extended, and, on the other hand, the class of automatic structures is restricted. It can also be read as a generalization of [Tho92, Th. 5.2].

The rest of this section is dedicated to the proof of Theorem 13. This proof goes over the proof made in [Tho92, Th. 5.2] to generalize the result to arbitrary regular automatic trees.

Before starting the proof, we may assume without loss of generality, that all the variables occurring in the formulas are second-order variables. This means to add an extra unary predicate \( \text{Sing}() \) which conveys that a set is a singleton, and to add inclusion formulas of the form \( X \subseteq Y \) so as to capture previous formulas of the form \( x \in X \). The reader may refer to [Tho92] for this routine transformation. The syntax then becomes as follows.

\[
\varphi ::= \text{Sing}(X) \mid X \subseteq Y \mid R_i(X_1 \ldots X_n) \mid \neg \varphi \mid (\varphi \land \varphi) \mid \exists X \varphi, \text{ where } X, Y, X_1, \ldots \in \mathcal{V}_2 \quad (7.1)
\]

The new syntax requires to adjust the semantics of the formulas, and in particular of those of the form \( R_i(X_1, \ldots, X_n) \), by imposing that each \( X_j \) is interpreted as a singleton, this is routine. The logic resulting from (7.1) is expressively equivalent to cMSO to the extent that a singleton is a chain. Therefore, in the following, we still use cMSO when using the syntax of (7.1).

A key idea to develop automata construction to model check against cMSO is that a set of addresses is a chain if, and only if, it is contained in the set of all prefixes of some infinite word. Given a chain \( C \subseteq \Sigma^* \), we let \( \text{Branches}(C) := \bigcap \{u \Sigma^* \mid u \in C\} \) be the set of infinite words whose set of prefixes contains \( C \). In particular, \( \text{Branches}(C) \) is a singleton if, and only if, \( C \) is infinite.

For \( \beta \in \text{Branches}(C) \), we write \( \text{mbranch}(\beta, C) \) for the infinite word over \( \Sigma \times \{0, 1\} \) whose first component is \( \beta \) and whose second component is marked by 1 if the current prefix of \( \beta \) belongs to \( C \), and by 0 otherwise. Formally, \( \text{mbranch}(\beta, C) = m[0]m[1]m[2] \ldots \text{ with } m[i] = (\beta[i], b) \) where \( b = 1 \) if \( \beta[0]\beta[1] \ldots \beta[i] \in C \), and \( b = 0 \) otherwise.

The words \( \text{mbranch}(\beta, C) \) are used to encode the chain \( C \). We will overload the encoding identity function \( \text{enc} \) of regular automatic trees to denote the encoding of chains. We letting \( \text{enc}(C) := \{\text{mbranch}(\beta, C) \mid \beta \in \text{Branches}(C)\} \). Also, we extend the notation to \( \text{enc}(C_1, \ldots, C_m) \) that contains infinite words over alphabet \( \Sigma \times \{0, 1\} \) by letting \( \text{enc}(C_1, \ldots, C_m) := \text{enc}(C_1) \odot \ldots \odot \text{enc}(C_m) \) where \( \odot \) is the convolution extended to sets of infinite words in a natural manner. For \( m = 0 \), \( \text{enc}(\cdot) \) is the singleton containing the unique infinite word over the singleton alphabet \( (\Sigma \times \{0, 1\})^0 \).

We now provide an automata-theoretic approach for model checking against cMSO formulas. We first establish the existence of a Büchi automaton \( \mathcal{C}_m \) that verifies if an infinite word over alphabet \( (\Sigma \times \{0, 1\})^m \) denotes a \( m \)-tuple of chains, as stated by Lemma 4.

Lemma 4 One can effectively construct a Büchi automaton \( \mathcal{C}_m \) that recognizes the encoding of \( m \)-tuples of chains, namely the language \( \bigcup_{C_1, \ldots, C_m \in \text{Ch}(T)} \text{enc}(C_1, \ldots, C_m) \).
CHAPTER 7. PROPOSITIONAL EPISTEMIC PLANNING

The automaton $C_m$ of Lemma 1 runs $m$ copies of the domain automaton $M_D$. Each copy reads one of the $m$ infinite words over $E$ extracted from the infinite input word over $(E \times \{0, 1\})^m$. Automaton $C_m$ rejects if one of these copies rejects.

Let $T = \langle D, r, S_1, \ldots, S_n, R_1, \ldots, R_p \rangle$ be a regular automatic tree over the set of directions $E = \{1, \ldots, n\}$ with $T = \langle M_D, M_r, (M'_i)_{1 \leq i \leq n}, (M_i)_{1 \leq i \leq p} \rangle$ its canonical presentation, and let $\varphi$ be a cMSO-formula\(^2\) with free variables $X_1, \ldots, X_m$. We define the set

$$\text{enc}(\varphi^T) := \bigcup_{C_1, \ldots, C_m \in \text{Ch}(T)} \text{enc}(C_1, \ldots, C_m) \quad (7.2)$$

Proposition 12 Given $\varphi$ a cMSO-formula\(^3\) with free variables $X_1, \ldots, X_m$, one can effectively construct a Büchi automaton $B_{\varphi, T}$ that recognizes the set $\text{enc}(\varphi^T)$.

PROOF.
We conduct the proof by induction on $\varphi$.

- $\varphi = \text{Sing}(X)$: Automaton $B_{\text{Sing}}$ is obtained by intersecting automaton $C_1$ with an automaton that verifies that the second component of $\text{enc}(C)$ has a single occurrence of symbol 1.

- $\varphi = X \subseteq Y$: Automaton $B_{X \subseteq Y}$ is obtained by intersecting automaton $C_2$ with an automaton that verifies that each time symbol 1 occurs in $\text{enc}(C_1)$ so does it in $\text{enc}(C_2)$.

- $\varphi = R_i(X_1 \ldots X_{r_i})$: Automaton $B_{R_i(X_1 \ldots X_{r_i})}$ is based on $r_i$ copies of automaton $B_{\text{Sing}}$, each one running on a $(E \times \{0, 1\})$-component of the infinite input word over $(E \times \{0, 1\})^r$, and a variant of automaton $M_i$ for $R_i$. This variant has inputs over $(E \times \{0, 1\})^r$ instead of $E^r$ and simulates automaton $M_i$ but replaces component-wise each letter after the unique encountered symbol 1 by the blank symbol $\square$, so as to mimic the convolution.

- The case $\land$ is a mere intersection, while the case for $\neg$ requires a complementation (see for instance [Var07]) but then automaton $C_m$ is required again.

- $\exists X \varphi$: It is sufficient to project automaton $B_{\varphi}$. If $\varphi$ has free variables $X = X_1, \ldots, X_m$ this projection corresponds to the mapping $(\Sigma \times \{0, 1\})^m \rightarrow (\Sigma \times \{0, 1\})^{m-1}$. Observe that if $X$ was the only free variable of $\varphi$ we would project onto the unary alphabet.

This achieves the proof of Proposition 12. ■

We can now conclude the proof of Theorem 13. Observe that model checking against formula $\varphi$ over the regular automatic tree $T$ amounts to deciding whether the language of the Büchi automaton $B_{\varphi, T}$ of Proposition 12 is non-empty. Indeed, this language is not empty if, and only if, there is some assignment $\sigma$ of the second order-variables $X_1, \ldots, X_m$ such that $T, \sigma \models \varphi$. In particular, if $\varphi$ is closed ($m = 0$), by convention we have:

- If $T \not\models \varphi$, the union in Equation (7.2) is empty as it ranges over an empty set;
- If $T \models \varphi$, the union in Equation (7.2) is not empty as it is equal to $\text{enc}()$.

\(^2\)in the language defined by the grammar 7.1
\(^3\)with syntax of 7.1
Notice that Proposition 10 from [Bar07] regarding the decidability of the full MSO-theory (and not only cMSO) for automatic presentations based on a singleton alphabet is now a direct corollary of Theorem 13 since every set of words over a singleton alphabet is a chain.

From Theorem 13 on the decidability of cMSO over regular automatic trees, and because binary relations $S^*$, $\leq$, $el$, $=$ come for free with automata constructions (Lemma 3), we have the following.

**Corollary 2** Model checking against $\text{cMSO}[r, S_1, \ldots, S_n, S_1^*, R_1, \ldots, R_p, S_1^*, \leq, el, =]$ is decidable over a regular automatic trees.

Notice that if we restrict to trees with only relations $S_1 \ldots S_n$, model checking against the full logic MSO becomes decidable (Rabin’s Theorem [Rab69]). However, considering extra relations (e.g. “equal level”) makes the model checking against MSO undecidable over regular automatic trees, as we already saw in Theorem 12 of Section 7.2, which is not the case for cMSO by Corollary 2.

Also, since every path quantifier in a path-MSO-formula can be translated in cMSO, and since considering extra arbitrary relations in trees, such as epistemic relations, does not harm this translation, we obtain the following result, which to our knowledge has not been considered in the literature.

**Corollary 3** Given a regular automatic tree $T = \langle D, r, S_1, \ldots, S_n, R_1, \ldots, R_p, S_1^* \rangle$ and a close path-MSO-formula $\varphi$ over the signature of $T$, it can be decided if $T \models \varphi$.

We now turn to logical formalisms that combine knowledge and time in the spirit of [?].

### 7.4 Logics of knowledge and time over regular automatic trees

We now exploit the peculiarities of regular automatic trees to consider extensions of several classic formalisms and study their expressivity. We first recall our criterion for expressivity.

**Definition 40** A logic $L$ is embedded into a logic $L'$, whenever there is an effective translation that maps every $L$-formula onto an equivalent $L'$-formula, namely for every regular automatic tree $T$, we have: $T \models \varphi$ if, and only if, $T \models \varphi'$.

Notice that when $L$ is embedded into $L'$, the decidability of the model checking against $L'$ entails the decidability of the model checking against $L$.

In tree structures, *time* is captured by the generalized successor binary relation $S := \bigcup_{i=1}^n S_i$, as in computation trees for temporal logics such as CTL [CE81], CTL* [HT87], etc. Depending on their arities, the other relations $R_1, \ldots, R_p$ have different roles. Unary relations label nodes with atomic propositions that range over some fixed set $AP = \{q, p, \ldots\}$. Binary relations, written $K_1 \ldots K_m$ as the epistemic modalities in multi-agent epistemic logic, will play the role of *knowledge* modalities as in classic epistemic logic. On this basis, we shortly write $\text{cMSO}[r, S_1, \ldots, S_n, (p)_{p \in AP}, K_1 \ldots K_m]$.

The ability to quantify over chains allows us to capture properties along branches of the trees that are naturally stated in linear-time mu-calculus. Recall that MSO along linear orders, hence branches, is expressively equivalent to Büchi automata that capture all $\omega$-regular properties, as shown by [Tho97], and so does the linear-time mu-calculus [Dam92]. We therefore introduce the logic $\text{BL}_{lin}^{\mu}K$ that is based on the linear-time mu-calculus [HKPS86, Var88], equipped with
knowledge modalities but also with second order quantifications over branches of the tree, just as CTL* extends LTL to the branching-time semantics. The logic $BL_{\mu}^K$ is called the branching epistemic linear-time mu-calculus; in the spirit of CTL*, it relies on two kinds of formulas: state formulas ($\Phi$) and path formulas ($\varphi$).

**Definition 41** The syntax of $BL_{\mu}^K$ is as follows.

- **State formulas:** $\Phi ::= p \mid K_i \Phi \mid \neg \Phi \mid (\Phi \land \Phi) \mid E_\varphi$ where $i \in \{1, \ldots, m\}$.
- **Path formulas:** $\varphi ::= Z \mid \Phi \mid \neg \varphi \mid (\varphi \land \varphi) \mid X_\mu Z. \varphi[Z]$ where $\varphi$ is closed in $E_\varphi$, $Z \in V$ and $Z$ is under the scope of an even number of negations in $\varphi[Z]$.

Formula $K_i \Phi$ is read as ‘Agent $i$ knows $\Phi$. Formula $E_\varphi$ is read as ‘there is a path starting from the current state that satisfies $\varphi$. Formula $X_\mu Z. \varphi[Z]$ is the linear mu-calculus fix-point construction. Formula $A_\varphi$ is an abbreviation of $\neg E \neg \varphi$ and means ‘$\varphi$ holds in all paths starting from the current state’. Formulas of $BL_{\mu}^K$ are interpreted in a tree $T = (D, r, S_1, \ldots, S_n, K_1 \ldots K_m, (p)_{p \in AP})$; state formulas are interpreted on nodes, while path formulas are interpreted on branches.

- **State formulas:**
  
  $T, d \models p$ if and only if $d \in p$;
  
  $T, d \models K_i \Phi$ if and only if for all $d' \in D$ such that $(d, d') \in K_i$ we have $T, d' \models \Phi$;
  
  $T, d \models \neg \Phi$ if and only if $T, d \not\models \Phi$;
  
  $T, d \models (\Phi \land \Phi)$ if and only if $T, d \models \Phi$ and $T, d \models \Psi$;
  
  $T, d \models E_\varphi$ if and only if there exists a maximal chain $C$ with least element $d$ (that is, a branch/path starting from $d$) such that $T, C \models \varphi$;

- **Path formulas:** we add a valuation $\sigma : V \rightarrow 2^N$ for the free second-order variables in the formulas, and write $\sigma^+ i$ for the valuation $\sigma^+ i(Z) = \{n \mid n + i \in \sigma(Z)\}$.

  $T, \pi, \sigma \models Z$ if and only if $0 \in \sigma(Z)$;
  
  $T, \pi, \sigma \models \Phi$ if and only if $T, \pi(0) \models \Phi$;
  
  $T, \pi, \sigma \models (\varphi \land \psi)$ if and only if $T, \pi, \sigma \models \varphi$ and $T, \pi, \sigma \models \psi$;
  
  $T, \pi, \sigma \models \neg \varphi$ if and only if $T, \pi, \sigma \not\models \varphi$;
  
  $T, \pi, \sigma \models X_\mu \varphi[Z]$ if and only if $T, \pi(1)\pi(2) \ldots \sigma^+ 1 \models \varphi$;
  
  $T, \pi, \sigma \models \mu Z. \varphi[Z]$ if and only if there is the least fix-point of $[\varphi[Z]]_\sigma^+$ defined by:

  $\varphi[Z]_\sigma^+ : 2^N \rightarrow 2^N$,

  $P \mapsto \{i \in N \mid \pi(i)\pi(i+1) \ldots (\sigma[Z \rightarrow P])^+ \models \varphi[Z]\}$.

A tree (resp. a forest) satisfies a state formula if it satisfies it from its root node (resp. from all its distinguished root nodes).

Notice that the least fix-point always exists. Indeed, the function $[\varphi[Z]]_\sigma^+$ is monotone (recall that we have required that every variable to occur under the scope of an even number of negations) and the Knaster-Tarski Theorem applies in the complete lattice $(2^N, \subseteq)$. Besides, we can alternatively define the least fix-point of $[\varphi[Z]]_\sigma^+$ as $\bigcap\{F \subseteq 2^N \mid [\varphi[Z]]_\sigma^+(F) \subseteq F\}$.

We here give examples of properties that can be expressed in $BL_{\mu}^K$.

**Example 39**

- $T, \pi \models \mu Z. p$ if, and only if, $T, \pi(0) \models p$.
- $T, \pi \models \mu Z. (XZ \lor p)$ if, and only if, there exists a node $\pi(i)$ along $\pi$ such that $T, \pi(i) \models p$. 


7.4. LOGICS OF KNOWLEDGE AND TIME OVER REGULAR AUTOMATIC TREES

- $\mathcal{T}, \pi \models \mu Z. (\psi \lor (\phi \land XZ))$ if, and only if, there exists a node $\pi(j)$ such that $\mathcal{T}, \pi(j) \models \psi$ and $\mathcal{T}, \pi(i) \models \phi$ for every $0 \leq i < j$.

By means of fix-points in $\text{BL}^\mu_{\text{K}}$, we capture the linear-time logic $\text{CTL}^* \text{K}$, and since we also have the existential path quantifier $E$, we can embed the full logic $\text{CTL}^*$ of $\text{HTSY}$ in $\text{BL}^\mu_{\text{K}}$. Now the epistemic modalities $K_i$ allow us to capture $\text{CTL}^* \text{K}$, the logic $\text{CTL}^*$ equipped with knowledge modalities. More precisely, we introduce the following macro for `$\phi$ until $\psi$': $\varphi U \psi$ is an abbreviation of formula $\mu Z.(\psi \lor (\phi \land XZ))$.

**Definition 42** $\text{CTL}^* \text{K}$ is the syntactic fragment of $\text{BL}^\mu_{\text{K}}$ defined by the following BNF:

- **State formulas:** $\Phi ::= \Phi \land \Phi \lor \neg \Phi \lor E \phi \lor K_i \Phi \lor p$ where $i \in \{1, \ldots, m\}$.
- **Path formulas:** $\varphi ::= \Phi \lor \neg \varphi \lor \varphi \land X \varphi \lor \varphi U \varphi$.

**Definition 43** $\text{CTLK}$ is the syntactic fragment of $\text{CTL}^* \text{K}$ defined by the following BNF:

- **State formulas:** $\Phi ::= \Phi \land \Phi \lor \neg \Phi \lor E \Phi \lor K_i \Phi \lor p$ where $i \in \{1, \ldots, m\}$.

The following result shows the expressive power of $\text{FO}[K_1 \ldots K_m, (p)_{p \in AP}, S, S^*, \leq, =]$.

**Proposition 13** $\text{CTLK}$ is embedded into $\text{FO}[K_1 \ldots K_m, (p)_{p \in AP}, S, S^*, \leq, =]$.

**Proof.**

The key idea is to use relation $S^*$ to consider finite paths and relation $\leq$ to make these paths as long as we want. We show by structural induction that for all $\text{CTLK}$ formula $\Phi$, we can build an $\text{FO}$-formula $f_\Phi(p)$ with one free first-order variable $x$, such that for every tree $(D, r, S_1, \ldots, S_0, R_1, \ldots, R_p)$ and node $d \in D$, the sub-tree $T|_d$ of $\mathcal{T}$ rooted in $d$ satisfies $\Phi$ if, and only if, $T_\nu[x \mapsto d] \models f_\Phi(\Phi)$. It is not hard to show that the formulas defined below meet this previous condition.

- $f_\Phi(p) := p(x)$; $f_\Phi(\neg \Phi) := \neg f_\Phi(\Phi)$; $f_\Phi(\Phi \land \Psi) := f_\Phi(\Phi) \land f_\Phi(\Psi)$;
- $f_\Phi(K_i \Phi) := \forall y K_i(x, y) \to f_\Psi(\Phi)$ where $y$ is a fresh variable;
- $f_\Phi(E \Phi) := \exists y S^*(x, y) \land f_\Psi(\Phi)$;
- $f_\Phi(E \Phi \Psi) = \exists y S^*(x, y) \land f_\Psi(\Psi) \land \forall z [(S^*(x, z) \land S^*(z, y) \land y \neq z) \to f_\Phi(\Psi)]$;
- The last case for $A(\Phi \Psi)$ is more involved: notice that if the formula $(\Phi \Psi)$ holds on every branch of a tree, there must exist a finite depth in the tree such that all the finite branches of the tree up to this depth already witness that $(\Phi \Psi)$. Indeed, if not, the sub-tree of all branches not satisfying $(\Phi \Psi)$ would be infinite, and by applying the König lemma to the finite-degree tree would yield a branch not satisfying $(\Phi \Psi)$, a contradiction. The reciprocal also holds. We therefore let $f_\Phi(A(\Phi \Psi)) := \exists y \forall t (p \leq t) \to \exists y [S^*(x, y) \land S^*(y, t) \land f_\Psi(\Psi) \land \forall z [(S^*(x, z) \land S^*(z, y) \land y \neq z) \to f_\Psi(\Phi)]$.

We end this section with the main Theorem [4] that states the decidability of model checking against $\text{BL}^\mu_{\text{K}}$ over regular automatic trees. First of all, it should be clear that the following holds.

**Theorem 14** $\text{BL}^\mu_{\text{K}}$ is embedded into $\text{cMSOK}$. 
PROOF.
The proof is conducted by induction over the $\text{BL}^{\mu}_{\text{lin}}$ formulas. The key idea is to memorize the current node in a first-order $x$ variable, possibly the current branch in a second-order variable $C$, and the variables $Z_1, \ldots$ occurring in the considered $\text{BL}^{\mu}_{\text{lin}}$ formula. This proof is rather long, and follows the argument to translate the propositional mu-calculus [Koz83] into $\text{MSO}$. We therefore only explain the case of a formula of the form $\mu Z. \varphi[Z]$ which translates as $\exists Z \, x \in Z \wedge Z \subseteq X \wedge (\forall z \, z \in Z \leftrightarrow \varphi'[z]) \wedge (\forall Y \, y \in Y \leftrightarrow \varphi'[y]) \rightarrow Z \subseteq Y$, where the formula $\varphi'[z]$ denotes the inductive translation of $\varphi$ (which depends on variable $z$) which expresses that the branch starting from $z$ satisfies $\varphi$. The second conjunct guarantees that $Z$ is the least fix-point.

\[ \blacksquare \]

**Corollary 4** Model checking against $\text{BL}^{\mu}_{\text{lin}}$ is decidable over automatic regular trees.

Figure 7.4 is a recap of the expressivity results we have obtained (arrows resulting from transitivity are omitted), where an arrow $L \rightarrow L'$ means that $L$ is embedded into $L'$.

7.5 Application to epistemic planning synthesis

As announced, we show that Theorem 13 together with Proposition 12 have an interesting impact in the domain of epistemic planning. The epistemic planning setting as introduced by [Bol17] relies on Dynamic epistemic logic, that we recall here. Next we explain how the original problem can be generalized to attain more expressive planning goals, such as statements (i)–(ii) of the introduction, while maintaining the decidability frontier for free. Our results generalize the ones obtained in [Man14, AMP14], but make great use of the already established property [Man14, Lemma 22, p. 109] that, under the assumption that preconditions and postconditions of events are propositional, the relational structure that contains all plan candidates is automatic, and actually it is a regular automatic tree (see Theorem 15).

7.5.1 DEL structures

In this subsection, following [Man14], we incorporate the initial epistemic model $\mathcal{M}$ and the infinitely many the products $\mathcal{M} \otimes \mathcal{E}^n := \mathcal{M} \otimes \mathcal{E} \otimes \cdots \otimes \mathcal{E}$ into a single structure, called a DEL structure, denoted by $\mathcal{ME}^*$. Worlds of $\mathcal{M} \otimes \mathcal{E}^n$, called histories, are naturally denoted by words of the form $w e_1 \ldots e_n$ where $w$ is a world of $\mathcal{M}$ and $e_1, \ldots, e_n$ are events of $\mathcal{E}$. E.g. the world $((w, e_1), e_2)$ is denoted $we_1e_2$. The pair $(\mathcal{M}, \mathcal{E})$ is called the DEL presentation of $\mathcal{ME}^*$. A DEL presentation $(\mathcal{M}, \mathcal{E})$ is propositional if $\mathcal{E}$ is propositional.

**Definition 44** [Man14, Def. 54, p. 105] The DEL structure denoted by $(\mathcal{M}, \mathcal{E})$ is the structure $\mathcal{ME}^* = (\mathcal{H}, (S_e)_{e \in \mathcal{E}}, (R_a)_{a \in \mathcal{AGT}}, (p)_{p \in \text{AP}})$, where $\mathcal{H}$ is the disjoint union of the sets of worlds of
The epistemic planning problem, as originally stated by Bol17, is defined as follows:

**Definition 45 Epistemic Planning Problem**

**Input:** A pointed epistemic model $M, w$, an event model $E$, an $EL$-formula $\psi$;

**Output:** Yes, if there is a sequence of events $e_1, \ldots, e_n$ in $E$ such that $\langle M \otimes E^n, w \rangle e_1 \ldots e_n \models \psi$.

We generalize this epistemic planning problem by considering a model checking problem against $BL_{\mu}\mu K$ over DEL structures.

**Definition 46 Generalized Epistemic Planning Problem**

**Input:** A pointed epistemic model $M, w$, an event model $E$, an $BL_{\mu}\mu K$-formula $\varphi$;

**Output:** Yes, if $\langle M \otimes E^*, w \rangle \models \varphi$.

---

[Sch18]: Available online at http://hintikkasworld.irisa.fr/
The problem of Definition 46 is indeed a generalization of epistemic planning problem of Definition 45 in the sense that the latter can be reduced to the former by model checking the formula \( \varphi := \text{EF} \psi \), where \( \psi \) is the planning goal.

The following example shows the relevance of generalized epistemic planning.

**Example 40** We give \( \text{BL}^{\text{lin}}_\mu K \)-formulas \( \varphi \) for the three statements (i)–(iii) of the introduction.

1. ‘invariantly, an intruder \( a \) does not know the location of the piece of jewelry more than 3 consecutive steps’ can be expressed as \( \text{EG}(\Theta \rightarrow (X \Theta \lor X^2 \Theta \lor X^3 \Theta)) \) where \( \Theta := \bigvee_{\ell \in \text{Loc}} K_a \text{pieceOfJewelleryIn}(\ell) \).

2. ‘all drones know that the region is safe every 20 steps’ can be expressed as \( \text{E}\nu Z . (\bigwedge_{a \in \text{AGT}} K_a \text{regionSafe} \land X^{20}Z) \).

3. ‘with the current plan, the drone \( a \) never knows the region is safe but every 10 steps, there is another plan to let the drone \( a \) eventually know the region is safe’ can be expressed as \( \text{EG}[\neg K_a \text{regionSafe} \land \nu Z . (\text{EF} K_a \text{regionSafe} \land X^{10}Z)] \).

The following result subsumes the decidability result for the epistemic planning problem for propositional DEL presentations ([YWL13],[Mau14]), and is a mere corollary of Theorems 15, 14 and 13.

**Theorem 16** The generalized epistemic planning problem is decidable for propositional DEL presentations.

In other terms, in the literature, decidability was established for reachability goals and Theorem 16 says that the problem remains decidable for goals that are arbitrary \( \text{BL}^{\text{lin}}_\mu K \)-formulas \( \varphi \). However, when considering planning, only formulas \( \varphi \) of the form \( \text{E} \varphi' \) are relevant. For such formulas, we can effectively build an automaton that recognizes exactly all plans achieving \( \varphi' \). This automaton arises from the automata constructions for \( \text{BL}^{\text{lin}}_\mu K \)-formulas, made possible by the automata constructions for cMSO-formulas, and the fact that every \( \text{BL}^{\text{lin}}_\mu K \)-formula can be effectively translated into a cMSO-formula. The algorithm to obtain this “plan automaton” is as follows.

1. Compute the cMSO-formula \( \chi \) equivalent to \( \varphi' \) (Th. 14). By the translation of \( \text{BL}^{\text{lin}}_\mu K \) into cMSO, formula \( \chi \) has a single free second-order variable \( X \), interpreted as a path, i.e. a plan;

2. Compute \( B_\chi \) (Proposition 12) which accepts all paths achieving goal \( \chi \), or equivalently \( \varphi' \).

Actually, automaton \( B_\chi \) reads infinite words over alphabet \( E \times \{0,1\} \), where the second component of the letters is always equal to 1, since the specified chain is require to be a path. Projecting a word accepted by \( B_\chi \) onto the first components of its letters provides a plans.

**7.6 Discussion**

We have adapted the seminal result of the decidability of the FO-theory of every automatic structure by augmenting the logic up to cMSO, a logic relying on chain-MSO of [HTS77, Tho87], but by restricting to the subclass of regular automatic trees. A nice application of this result is the decidability of the generalized epistemic planning problem for propositional DEL presentations.
Regarding the computational complexity of our algorithms, it should be observed that the automata construction to model check against cMSO (Proposition 12) is non elementary in the number of alternations between existential and universal quantifiers in the formula (each underlying negation yields an exponentiation blow-up for the complementation). Still, it would be relevant to investigate in practice, if the automata have particular shapes that do not reach this non-elementary worst-case upper-bound complexity.

Compared to the work of Maubert [Mau14] with CTL∗K, we offer the entire logic cMSO (or \(\text{BL}_{\text{lin}}^\mu\text{K}\)) that strictly subsumes CTL∗K, and yet allowing to solve the epistemic planning problems over the same class of planning domains (i.e. propositional DEL presentations). However, it should be noticed that [Mau14] also considers a different problem called the epistemic protocol synthesis problem, which differs from the generalized epistemic planning problem: in the epistemic protocol synthesis problem, one has to prune the tree structure so that the remaining satisfies a CTL∗K-goal. This subject is out of the scope of this paper, but suggests some comments.

The existence of a pruning, i.e. a sub-tree, that satisfies the protocol goal, requires the use of second-order quantifiers ranging over arbitrary subsets of nodes, that is the full logic MSO which cannot be model checked (Theorem 12). It is an open question whether there is a logic in between cMSO and full MSO to solve the epistemic protocol synthesis problem with \(\text{BL}_{\text{lin}}^\mu\text{K}\) specifications. The existence of a pruning of the tree that satisfies the protocol goal, requires the use of second-order quantifiers ranging over arbitrary subsets of nodes, that is the full logic MSO which cannot be model checked (Theorem 12). It is an open question whether or not there is room for a logic in between cMSO and full MSO to solve the epistemic protocol synthesis problem with \(\text{BL}_{\text{lin}}^\mu\text{K}\) specifications. Also, the synthesis technique deployed by [Mau14] actually applies to a family of tree structures that is larger than the one of regular automatic trees. At the moment, the technique does not adapt to logics which involve arbitrary fix-points. It is an open question whether or not the work of [Mau14] can be faithfully extended to deal the entire alternation-free fragment of \(\text{BL}_{\text{lin}}^\mu\text{K}\).
Part III

Applicability in AI
Chapter 8

Seeing and knowing

Figure 8.1: NASA’s Mars Exploration Rover.

In many practical settings requiring higher-order knowledge (video games, multi-UAV systems, multi-robot systems, robot interacting with humans, etc.), autonomous agents are located in a geometrical environment. For these applications, the approach advocated by Halpern and Vardi is to use model checking for reasoning about knowledge [HV91]. Thus, epistemic models are needed to give semantics to epistemic formulas. On the other hands, epistemic models are not directly available. Indeed, the information agents get from the environment are low level and comes from sensors and is about the world itself, for instance positions of agents.

In this chapter, we attempt to bridge the gap between sensor information and epistemic models. More precisely, we attempt to infer an epistemic model from geometrical information. Our proof-of-concept is simple: sensors of agent $a$ output the set of agents seen by $a$.

8.1 Inferring epistemic models

In this section, we consider a set $S$ of points in the geometrical environment. A possible world, called a $S$-world consists in positions of agents and a visibility function as given in the following definition. In other words, a possible world is a structured mathematical object that describes the position and the vision of all agents.

Definition 47 Let $S$ be a non-empty set. An $S$-world is a pair $(\text{pos}, \text{vis})$ where:

- $\text{pos} : \text{AGT} \to S$;
- $\text{vis} : \text{AGT} \to 2^S$ such that for all agents $a \in \text{AGT}$, $\text{pos}(a) \in \text{vis}(a)$.
In Definition 47, the function \( \text{pos} \) assigns a position in \( S \) to each agent in \( AGT \). The function \( \text{vis} \) maps each agent \( a \) to the set of points \( \text{vis}(a) \) seen by \( a \). We suppose that an agent sees itself. Now, we define the corresponding epistemic model of a given class \( C \) of \( S \)-worlds. Furthermore, we only consider structured atomic propositions of the form \( a \triangleright b \), where \( a, b \) are agents. The informal reading of \( a \triangleright b \) is ‘agent \( a \) sees agent \( b \).

**Definition 48** Given a class \( C \) of \( S \)-worlds, we define the epistemic model \( \mathcal{M}_C = (W, (R_a)_{a \in AGT}, V) \) where:

1. \( W = C \);
2. \( R_a \) over \( W \) is defined by:
   \[
   (\text{pos}, \text{vis}) R_a (\text{pos}', \text{vis}') \iff b \in \text{vis}(a), (\text{pos}(b) = \text{pos}'(b) \text{ and } \text{vis}(b) = \text{vis}'(b));
   \]
3. \( V(\langle \text{pos}, \text{vis} \rangle) = \{ a \triangleright b \mid \text{pos}(b) \in \text{vis}(a) \} \).

Item 2 of Definition 48 defines the epistemic relation \( R_a \) in an intuitive way: two \( S \)-worlds are indistinguishable for an agent \( a \) if agent \( a \) sees the same thing in both worlds. More precisely, for all agents \( b \) seen by \( a \), agent \( b \) have the same positions and the same vision in both \( S \)-worlds. Item 2 defines the epistemic relation \( R_a \) globally, meaning that there is common knowledge of the ability of agents to sense other agents and that all agents have the same ability. Item 3 says that proposition \( a \triangleright b \) holds in a given world iff agent \( b \) is seen by agent \( a \).

Let \( C \) be a class of \( S \)-worlds. We consider the following model checking, called the \( C \)-model checking problem:

- input: the description of a \( S \)-world \( w \), an epistemic formula \( \varphi \);
- output: yes if \( \mathcal{M}_C, w \models \varphi \); no otherwise.

Several classes \( C \) have been considered in the literature. The two next sections review them.

### 8.2 Agents than can move

Given an integer \( d \) and an angle \( \alpha \), Balbiani et al. consider the class \( C^d_\alpha \) of \( \mathbb{R}^d \)-worlds \( \langle \text{pos}, \text{vis} \rangle \) where \( \text{vis}(a) \) is a cone of angle \( \alpha \) centered in \( \text{pos}(a) \) (actually, in [BGS13], the angle \( \alpha \) is assumed to be equal to \( \pi \) so that agents see closed hyperplanes, but that assumption is not really important). Two indistinguishable \( C^2_\alpha \)-worlds for agent \( a \), with \( \alpha = \frac{\pi}{6} \), are given in Figure 8.2. For the one-dimensional case, we omit the parameter \( \alpha \) since angles are irrelevant. Figure 8.3 shows two indistinguishable \( C_1 \)-worlds for agent \( a \).

![Figure 8.2: Two indistinguishable \( C^2_\alpha \)-worlds for agent \( a \) with \( \alpha = \frac{\pi}{6} \).](image-url)
8.3. ROTATING CAMERAS

The \( C_d^2 \)-model checking is decidable, by reduction to the satisfiability of a first order formula over the theory of the real numbers, known to be decidable \([\text{I}]\). It is \( \text{PSPACE} \)-hard. The exact complexity of the model checking is still open, and is quite challenging. The main issue is the following: if \( d \geq 2 \), the model \( M_{C_d^2/\sim} \) defined as the quotient of \( M_{C_d^2} \) and the equivalence relation \( \sim \), defined by \( w \sim u \) if the same atomic propositions of the form \( a \triangleright b \) hold in both \( w \) and \( u \) is not bisimilar to \( M_{C_d^2} \). Let us give an example (actually a variant of the example given in \([?\text{I}]\) and \([\text{I}]\)) that explains that issue.

**Example 41** Figure 8.4 actually two \( C_d^{\pi/6} \)-worlds \( w \) and \( w' \) that satisfy exactly the same atomic formulas of the form \( \cdot \triangleright \cdot \) (agents \( b,c,d,e \) see no other agents and \( a \) sees \( b,c \) and \( d \), but \( K_a((e \triangleright b \land e \triangleright d) \rightarrow e \triangleright c) \) knows in \( w \) and not in \( w' \). Indeed, for \( w \), as agent \( a \) sees that \( c \) is in the segment \( bd \), if \( b,d \) are in the cone of vision of \( e \) and then \( c \) is also, and therefore, \( K_a((e \triangleright b \land e \triangleright d) \rightarrow c \triangleright c) \) in \( w \). However in \( w' \), world \( u' \) depicted Figure 8.5 is possible for agent \( a \) and does not satisfy \( (e \triangleright b \land e \triangleright d) \rightarrow e \triangleright c) \). Therefore, \( K_a((e \triangleright b \land e \triangleright d) \rightarrow e \triangleright c) \) does not hold in world \( w' \). In other words, there are no strong evidence that there exists a finite model equivalent to \( M_{C_d^2/\sim} \) with respect to a finite set of agents, if \( d \geq 2 \). We do not know whether a finite axiomatization for the validities over \( M_{C_d^2/\sim} \) exist.

However, the one-dimensional case is easier. It is known that the \( C_1 \)-model checking is in \( \text{PSPACE} \)-complete. If \( d = 1 \), we can make use of a symbolic representation. More precisely, \( M_{C_1/\sim} \) is bisimilar to \( M_{C_1} \) \([\text{BGS13}]\). As model \( M_{C_1/\sim} \) can be represented by accessibility relations (see Chapter 3), \( C_1 \)-model checking is in \( \text{PSPACE} \) (and also \( \text{PSPACE} \)-hard).

### 8.3 Rotating cameras

Gasquet et al. \([\text{GGS15}]\) considered another setting where positions of agents are fixed and common knowledge among all the agents but not the directions they are looking at. In other
words, the setting consists of rotating cameras. Gasquet et al. only consider the two-dimensional case. Formally, it consists in fixing a given pos' : AGT → ℜ² and a given angle α, and considering the class C_{α,pos'}² of ℜ²-worlds ⟨pos, vis⟩ where vis(a) is a cone of angle α centered in pos(a) and pos' = pos. In that setting, agents have the same positions in all worlds, just the direction of views may be different. Figure 8.6 shows two indistinguishable worlds for agent a in that settings.

Interestingly, when the positions of agents is common knowledge, there is a finite representation and the C_{α,pos'}²-model checking is in Pspace-complete [GGS15]. It is essentially due to the fact a symbolic representation exists: models M_{C_{α,pos'}} and M_{C_{α,pos'}/\sim} are bisimilar, where \sim is the equivalence relation ‘same truth values for the atomic propositions of the form a ⊥ b.’

8.4 Geometry in the syntax: poor’s man logic

Herzig et al. [HLM15] have proposed a language where geometrical constraints are written in the language and is not grounded in the models – only the semantics of the knowledge operator is still grounded. Namely, in the framework, we can express observability construtions such as ‘an agent a sees that an agent b sees the truth value of p’ (written S_aS_bp). In [CHL +16], this logic is extended with public announcement operators. It is proven that the model checking is PSPACE-complete, the model being a valuation over observability constructions.
8.5 Perspectives

It is natural to extend epistemic logic on geometrical environments with actions. If the environment is discrete and synchronous, event models are perfectly suitable to capture actions, such as private announcement of $p$ by agent $a$ to all agents that see agent $a$.

Interestingly, a long avenue of research would be to design a framework where actions are continuous in time. A promising approach could be to mix event models with differential equations and to build hybrid models.
Chapter 9

Asynchronous systems

This chapter is adapted from [KMS17].

9.1 Introduction

Asynchrony plays a central role in distributed systems such as robotic rescue teams, smart cities, autonomous vehicles, etc. In such systems, there may be an unpredictable delay between sending and receiving messages, and there is not always access to a centralized clock. Recently, with the proliferation of multi-agent systems (MAS) where independent agents interact, communicate, and make decisions under imperfect information, modeling the evolution of knowledge as informative events occur has become increasingly important for both verification and design. For instance, it is often crucial to know whether an agent has received some information, so it would be highly desirable to be able to analyze messages such as “agent $a$ knows that agent $b$ received message $m$”, i.e., we want to model

\[\text{messages with epistemic content},\]

and because we are considering automated systems where agents do not lie, make logical mistakes, or have inaccurate factual information (for instance autonomous vehicles communicating about their position), we also make the classic assumption that

\[\text{messages are true when they are sent}.\]

Public announcement logic (PAL) [Pla07] is one of the first and most influential proposals for modelling the relationship between knowledge and announcements. In PAL, true announcements are made to a group of agents. This logic later led to the powerful and much studied dynamic epistemic logic (DEL) [Van07], which can describe more complex forms of communication, such as semi-private announcements, private announcements, and much more. However, both these logics assume synchronicity: In PAL messages are immediately received by all agents at the same time, as soon as they are sent, and in DEL agents may perceive events differently, but events immediately change the epistemic state of agents as soon as they occur. In asynchronous settings, however, messages are not delivered instantly, and agents may receive them at different points in time, making PAL intrinsically unfit for reasoning about such settings. This fact becomes even more evident when we consider that in PAL, every announcement immediately leads to common knowledge, while common knowledge is not achievable in asynchronous systems.
The only work we know of considering how DEL can capture asynchrony is [DLW11], but in this logic an agent can only consider possible “future” events if they do not change her epistemic state. This is related to the principle of inertia [vL10, BBP16], which states that in absence of any observation, one assumes that nothing has happened. This assumption is natural in contexts where agents believe that they can observe all events at the time of their occurrence. In asynchronous systems however, agents should know that even when they do not observe anything, or when they do not receive any messages, it is possible that messages are being sent and received by other agents. Therefore the inertia principle does not apply in our setting, and agents should be able to imagine possible pending messages.

Our aim is to propose a logic in the spirit of PAL for reasoning about epistemic messages in asynchronous systems, that are true at the time of announcement, and where agents can imagine messages that have been sent but not yet received.

Because this is an ambitious endeavor, we make a few assumptions to start as simply as possible:

**Broadcasts:** all messages are sent to every agent

**External source:** messages are emitted by an external, omniscient source

**FIFO:** messages are received in the order they are sent.

The first assumption comes from PAL, and is natural in the context of smart cities for instance, where autonomous vehicles broadcast their current position or direction. The second one is a choice made to simplify the syntax by not having to model the origin of announcements, as in PAL. Announcements from an external, omniscient source can in some cases be used to model messages broadcast by agents within the system, in particular, an omniscient outside agent broadcasting that agent $a$ knows $\varphi$ is in many situations equivalent to agent $a$ broadcasting $\varphi$ to the other agents within the system. This captures the fact that in order for an agent within the system to make a true announcement, she should know that the announcement is true before she broadcasts it. Thus upon receiving an announcement made by agent $a$, another agent learns both the announcement and the fact that $a$ knows it, modeled within the framework where announcements come from an external source by the announcement of $K_a \psi$ ($K_a$ being the classic knowledge operator of epistemic logics, see for instance [FMHV03a]). However, depending on assumptions about the agents’ epistemic and reasoning capacities, this way of modeling agents’ announcements may not be completely faithful to the real situation. We discuss this issue briefly in the future work section.

Concerning the last assumption, FIFO is a simple but classic scheme of communication in asynchronous systems (see for instance [YG82, BZ83, CS08]).

Figure 9.1 depicts the architecture of such a system with three autonomous agents receiving messages from a public channel and reading them when they are ready to process them. To represent the fact that agents read messages in the order they were sent, we provide each one with a private FIFO channel. Each copy receives the same messages from the public channel, in the order in which they are announced, but the moment at which these messages are read differs from one agent to another.

In PAL, messages are received at the same time they are sent, and thus the announcement operator combines both sending and receiving. In contrast, in our setting, messages are not received immediately and they may be received at different times by different agents. The syntax reflects this aspect by providing both a sending operator, which adds new messages to the public channel, and a receiving operator for each agent, which allows her to read the first message in her FIFO queue that she has not read yet. Thus, in our logic, we provide the following modal constructions:
9.1. INTRODUCTION

FIFO for agent a

FIFO for agent b

FIFO for agent c

Figure 9.1: Agent architecture

• \( \langle \psi \rangle_{\text{async}} \varphi \), which means “\( \psi \) is currently true, and after its announcement, \( \varphi \) holds”;

• \( \bigcirc_a \varphi \), which means “after agent \( a \) reads the next announcement, \( \varphi \) holds”;

• \( K_a \varphi \), which means “agent \( a \) knows that \( \varphi \) holds”.

Interestingly, the natural semantics for this logic presents a challenging problem of circular definition: In order to define the truth of epistemic formulas, we classically quantify over the set of all states that the agent considers possible, where states include the current content of the public channel and pointers to the last message read by each agent. But some states are not consistent and must not be considered: intuitively a state is consistent if the announcements it contains were true at the time they were made. Therefore, defining consistent states requires defining the truth of formulas, and vice versa. PAL presents a similar circularity, as the definition of the update of a model by an announcement and the definition of the truth values are mutually dependent, thus this phenomenon is not inherent to the asynchronous setting. However, only asynchrony makes it a problem. Indeed in PAL a simple definition by mutual induction is possible. In an asynchronous setting, however, agents do not know what or how many messages other agents have received; in particular, an agent may consider it possible that some formula has been announced that is bigger than all those that have actually been announced, which makes a mutual induction impossible for lack of a decreasing quantity. This circularity problem is inherent in the asynchronous setting, and is independent from the assumptions of broadcasts, external source and FIFO described above. It only depends on the assumptions that announcements can talk about knowledge (9.1), that they must be true (9.2), and that agents can imagine pending messages (9.3).

We partially solve the issue by defining three restricted cases in which we manage to avoid circularity. The first one requires the Kripke model representing the initial epistemic situation to be a finite tree; the second one only allows announcements from the existential fragment of our logic, and the third one makes the assumption that only a bounded number of announcements can be made during each time unit (a strong form of non-Zeno assumption), and that agents have access to a global clock. In the second case, the semantics is defined thanks to an application of the Knaster-Tarski fixed point theorem [Tar55].

We then discuss some properties of our logics, compare them to PAL, and establish some validities that hold whenever the semantics is well-defined; we also study the model checking problem for our logic and establish the following complexity results:

<table>
<thead>
<tr>
<th>Restrictions</th>
<th>Complexity of model checking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propositional announcements</td>
<td>PSPACE-complete</td>
</tr>
<tr>
<td>Finite tree initial models</td>
<td>in PSPACE</td>
</tr>
<tr>
<td>Announcements from the existential fragment</td>
<td>in EXPTIME, PSPACE-hard</td>
</tr>
</tbody>
</table>
Finally, we study the satisfiability problem in the case of propositional announcements, and we establish that it is \( \text{NP} \text{-complete} \).

The chapter is organized as follows. In Section 9.2 we present our logic, and discuss the circularity problem that arises from the definition of the semantics, and present an example to illustrate the logic. In Section 9.3 we exhibit cases where it can be solved. We then present some properties in Section 9.4 (a comparison with PAL and some validities), we study the model checking problem in Section 9.5 and the satisfiability problem in Section 9.6. Finally we discuss related work in Section 9.7 and future work in Section 9.8.

This chapter is a summary of [KMS15] and [KMS17].

9.2 Settings

In this section we present our framework for reasoning about asynchronous epistemic announcements in a public channel. As in Chapter 2, \( AP \) is a countable infinite set of atomic propositions, and \( AGT \) is a finite set of agents. For pedagogical reasons, we first introduce models, then the syntax and finally the semantics of our logic, even though by doing so we need to refer to the language before we formally define it.

9.2.1 Models

Agents start with an initial state of knowledge of the world, which is modeled by an initial pointed epistemic model, or Kripke model. Then true announcements are made by some external entity, and sent in the public channel. The whole sequence of announcements that have been made up to the present moment is modeled as a sequence of formulas from our logic, whose syntax we introduce later in Section 9.2.2. Agents read these messages independently, possibly at different times, but in FIFO order. To represent which messages each agent has already read, and thus which ones remain to be read, we simply map each agent to the number of announcements she has read. Such a mapping is called a cut.

Initial Kripke model

An initial model is given as a Kripke model \( M = (W, \{R_a\}_{a \in AGT}, \Pi) \), as defined in Definition 1. It represents the initial knowledge of agents before any announcements are made, and it corresponds to the notion of initial knowledge in [Ray13], p. 5. In practice, \((M, w)\) is directly provided by the modeller or inferred from what agents perceive [BGS13, GGS15].

Announcements

We consider that, in a given scenario, not every formula may be announced, but rather that there is a certain set of relevant announcements. Furthermore, we allow the number of times an announcement can be made to be bounded. To represent this, we define the notion of announcement protocols (\( L_{async} \) is the language defined in Section 9.2.2).

Definition 49 An announcement protocol is a multiset of formulas in \( L_{async} \), where the multiplicity of an element \( \psi \) is either an integer or \( \infty \).

Example 42 The reader may imagine a card game where it is only possible to announce ‘agent a has a heart card’ once and ‘agent a does not know whether agent b has a heart card or not’ twice. We let the proposition \( \Diamond_a \) mean “agent a has a heart card,” and define the announcement protocol to be \( \{\Diamond_a, \ K_a \Diamond_b \land K_a \neg \Diamond_b, \ K_a \Diamond_b \land K_a \neg \Diamond_b\} \).
9.2. SETTINGS

Given an announcement protocol \( \mathcal{A} \), we denote by \( \text{Seq}(\mathcal{A}) \) the set of finite sequences \( \sigma = [\varphi_1, \ldots, \varphi_k] \) such that the multiset \( \{[\varphi_1, \ldots, \varphi_k]\} \) is a submultiset of \( \mathcal{A} \). We define the size of a sequence \( \sigma \) as \( |\sigma| := \sum_{i=1}^k |\varphi_i| \). For \( \sigma, \sigma' \in \text{Seq}(\mathcal{A}) \), we write \( \sigma \leq \sigma' \) if \( \sigma \) is a prefix of \( \sigma' \). The sequence \( \sigma|_k \) is the prefix of \( \sigma \) of length \( k \). Given a formula \( \varphi \) and a sequence of formulas \( \sigma \), \( \varphi :: \sigma \) (resp. \( \sigma :: \varphi \)) is the sequence obtained by adding \( \varphi \) at the beginning (resp. at the end) of \( \sigma \).

### States

We now define the set of possible states of the models in which the formulas of our logic will be evaluated.

**Definition 50** Let \( \mathcal{M} \) be an initial model and \( \mathcal{A} \) an announcement protocol. We define the set of possible states \( \mathcal{S}_{\mathcal{M}, \mathcal{A}} \) as follows:

\[
\mathcal{S}_{\mathcal{M}, \mathcal{A}} = \{ (w, \sigma, c) \mid w \in W, \sigma \in \text{Seq}(\mathcal{A}) \text{ and } c : AGT \to \{0, \ldots, |\sigma|\} \}
\]

The first element of a state represents the world the system is in. The second element is the list of messages that have already been announced. The last element, \( c \), is called a cut, and for each \( a \in AGT \), \( c(a) \) is the number of announcements of \( \sigma \) that agent \( a \) has received so far. Given two cuts \( c \) and \( c' \), we write \( c < c' \) if for all \( a \), \( c(a) = c'(a) \) and there exists \( b \) such that \( c(b) < c'(b) \); in other words, \( c < c' \) if all agents have received at least as many messages in \( c' \) as in \( c \), and at least one agent received strictly more messages in \( c' \). Typical elements of \( \mathcal{S}_{\mathcal{M}, \mathcal{A}} \) are denoted \( S, S' \), etc.

**Example 43** Consider the state \( S = (w, [\varphi, \psi, \chi], c) \) where \( c(a) = 2 \) and \( c(b) = 1 \). \( S \) represents the situation where in initial world \( w \), the sequence \( [\varphi, \psi, \chi] \) of formulas has been announced, agent \( a \) has received \( \varphi \) and \( \psi \), and agent \( b \) has only received \( \varphi \). Only \( \chi \) remains in the queue of \( a \) and has not been read yet, and only \( \psi \) and \( \chi \) remain in the queue of \( b \). We represent \( S \) as follows:

\[
\begin{align*}
w & \quad a : \quad b : \\
& \quad \varphi \quad \psi \quad \chi
\end{align*}
\]

and we may also write \( S = (w, [\varphi, \psi, \chi], \begin{array}{c} a \\ b \end{array} \rightarrow \begin{array}{c} 2 \\ 1 \end{array} ) \).

**Example 44** Consider the state \( S = (w, \epsilon, 0) \), where \( \epsilon \) denotes the empty sequence of formulas and \( 0 \) is the function that assigns 0 to all agents. \( S \) represents an initial world \( w \) in which no announcement has been made (and therefore no announcement has been received either). It can be represented as follows:

\[
\begin{align*}
& \quad w \\
& \quad a : \quad b : \quad \text{no messages}
\end{align*}
\]

**Example 45** State \( S = (w, [\varphi, \chi], 0) \), which represents the situation where in initial world \( w \), \( \varphi \) and \( \chi \) have successively been announced, but neither agent \( a \) or agent \( b \) received any announcement yet. We depict it as follows:

\[
\begin{align*}
& \quad w \\
& \quad a : \quad b : \\
& \quad \varphi \quad \chi
\end{align*}
\]
Consistent states

Definition 50 allows for all combinations of worlds, sequences of announcements allowed by the announcement protocol, and cuts. This definition is an over-approximation of the set of states we want to consider: indeed, because announcements must be true, some of the states in $\mathcal{S}$ are inconsistent. For example, suppose that $w$ is a world in $\mathcal{M}$ where $p$ does not hold. Because only true announcements can be made, $p$ cannot be announced in world $w$, and thus the state $(w, [p], 0)$ is inconsistent.

Example 46 Let us consider the following initial model, where $w, u, v$ and $z$ are worlds, $a$ and $b$ are agents and $p$ is a proposition. The arrows represent the agents’ accessibility relations, before any announcements have been made. So at world $w$, agent $a$ considers $u$ and $v$ possible, and agent $b$ considers world $z$ possible.

Now assuming that the announcement protocol $A$ contains $p, \varphi$ and $\psi$, a partial depiction of the asynchronous model $\mathcal{M} \otimes A$ is below. We depict the states $w, u, v,$ and $z$ where no announcement has been made, as well as copies of $u$ where two different sequences of announcements have been made, and received in one state by agent $b$ and in a different state by agent $a$. Of course, the entire model $\mathcal{M} \otimes A$ is infinite so we do not depict all the states here.

State $u$ is not consistent because $p$ has been announced even though $p$ is not true in $u$. This notion of inconsistency is the source of the circularity problem, as we discuss in Section 9.2.4. For now, we define the relations that capture which states an agent considers possible before removal of inconsistent ones.

Pre-accessibility relation and asynchronous pre-model

We now define, for each agent, a pre-accessibility relation that does not yet take consistency into account, but is only based on the agents’ accessibility relations in the initial model, and the messages it has already read.

Definition 51 The pre-accessibility relation for agent $a$, written $R_a$, is defined as follows: given $S = (w, \sigma, c)$ and $S' = (w', \sigma', c')$, we have $S R_a S'$ if:

1. $w R_a w'$, and
2. $\sigma|_{e(a)} = \sigma'|_{e'(a)}$. 
9.2. SETTINGS

The first clause simply says that for \( S' \) to be considered possible by \( a \) when in \( S \), world \( w' \) must be considered possible by \( a \) from \( w \). The second clause says that agent \( a \) is aware of, and only aware of, messages that she has received: therefore she can only consider possible states where she has received exactly the same messages. Then, because the principle of inertia does not apply to the asynchronous setting, she can imagine any possible sequence of pending announcements, as long as it is compatible with the announcement protocol. Also, as she has no information about what messages the other agents have received, \( c'(b) \) can be anything if \( b \neq a \): agent \( a \) considers it possible that \( b \) received more, or fewer, messages than she actually has. Note that the second clause also implies \( c(a) = c'(a) \).

Given an initial model \( M \) and an announcement protocol \( A \), we define the asynchronous pre-model \( M \otimes A := (S_{M,A}, \{R_a\}_{a \in AGT}) \), where \( S_{M,A} \) is the set of possible states, and for \( a \in AGT, R_a \) is the pre-accessibility relation for agent \( a \).

9.2.2 Language

We now introduce the syntax of our logic, which we call Asynchronous Broadcast Logic, or \( L_{async} \) for short. Note that we do not use the term “public announcement” in the name of our logic as it has a strong synchronous connotation: public announcements are often thought of as becoming common knowledge the moment they are made.

Definition 52 (Syntax) The set of \( L_{async} \)-formulas is given by the following grammar:

\[
\varphi ::= p \mid (\varphi \land \varphi) \mid \neg \varphi \mid K_a \varphi \mid \langle \varphi \rangle_{async} \varphi \mid \Box_a \varphi,
\]

where \( p \) ranges over \( AP \) and \( a \) ranges over \( AGT \).

The intuitive meaning of the last three operators is the following: \( K_a \varphi \) means that agent \( a \) knows \( \varphi \), \( \langle \psi \rangle_{async} \varphi \) means that \( \psi \) is true and after \( \psi \) has been put on the public channel, \( \varphi \) holds, and \( \Box_a \varphi \) means that agent \( a \) has a pending message, and after she has received and read it, \( \varphi \) holds. We define the dual of the announcement operator: \( [\psi] \varphi := \neg \langle \psi \rangle_{async} \neg \varphi \), meaning that if \( \psi \) is true, then \( \varphi \) holds after its announcement. \( |\varphi| \) is the length of \( \varphi \), and we denote by \( \text{propositional formula} \) a formula that uses no modalities, i.e., contains no occurrences of \( K_a \), \( \langle \varphi \rangle_{async} \), or \( \Box_a \).

In (synchronous) public announcement logic (see Definition 9), the operator \( \langle \psi \rangle \) captures both the broadcast and the reception of an announcement \( \psi \), because in the synchronous setting, sending and reception occur simultaneously. In our asynchronous setting, not only can sending and reception occur at different times, but also different agents may receive the same message at different times. Therefore we capture the broadcast of a formula \( \psi \) with operator \( \langle \psi \rangle_{async} \), while agent \( a \)’s reception of a broadcasted formula is captured by the operator \( \Box_a \).

9.2.3 Truth conditions

For the rest of the section, we fix an initial model \( M \) and an announcement protocol \( A \). As discussed in Section 9.2.1, some possible states from Definition 50 are inconsistent, because they contain announcements that were not true at the time they were announced. Also, because agents should not consider inconsistent states possible, we described how defining consistency is necessary to define the semantics of the knowledge operator, which in turn is necessary to define the consistency of states that contain epistemic announcements, hence a circularity problem.

We describe in Figure 9.2 the definition of consistency (represented with symbol \( \checkmark \)) as well as truth conditions for our logic. This definition is circular, and therefore the semantics as presented here is not well-founded, although it conveys the intended meaning of our operators. In the next section we will describe restricted cases in which we can provide a semantics that is well-defined.
CHAPTER 9. ASYNCHRONOUS SYSTEMS

Truth conditions for consistency:

\[(w, \epsilon, 0) \models \checkmark\] (always)
\[(w, \sigma, c) \models \checkmark\] if there is \(c' < c\) s.t. \((w, \sigma, c') \models \checkmark\), or
\[
\sigma = \sigma' : \psi, (w, \sigma', c) \in S_{M.A},
\]
\[(w, \sigma', c) \models \checkmark\] and \((w, \sigma', c) \models \psi\)

Truth conditions for formulas:

\[(w, \sigma, c) \models p\] if \(p \in \Pi(w)\)
\[(w, \sigma, c) \models (\varphi_1 \land \varphi_2)\] if \((w, \sigma, c) \models \varphi_1\) and \((w, \sigma, c) \models \varphi_2\)
\[(w, \sigma, c) \models \neg \varphi\] if \((w, \sigma, c) \not\models \varphi\)
\[(w, \sigma, c) \models K_a \varphi\] if for all \(S'\) s.t. \((w, \sigma, c) R_a S'\) and \(S' \models \checkmark\), \(S' \models \varphi\)
\[(w, \sigma, c) \models \langle \psi \rangle_{async} \varphi\] if \(\sigma : \psi \in \text{Seq}(A)\), \((w, \sigma, c) \models \psi\) and \((w, \sigma : \psi, c) \models \varphi\)
\[(w, \sigma, c) \models \bigcirc_a \varphi\] if \(c(a) < |\sigma|\) and \((w, \sigma, c^{+a}) \models \varphi\)
\[
\text{where } c^{+a}(b) = \begin{cases} 
  c(b) & \text{if } b \neq a \\
  c(b) + 1 & \text{if } b = a 
\end{cases}
\]

Figure 9.2: Consistency and semantics

The intuitive meaning of \((w, \sigma, c) \models \checkmark\) is that the state \((w, \sigma, c)\) is consistent, that is, all announcements in \(\sigma\) were true when they were made. The first clause is obvious: the initial state where no announcement has been made is consistent. The second clause gives two possibilities for a state to be consistent. Either there was an earlier consistent state \((w, \sigma, c')\) in which some agents received some already announced formulas, increasing the cut from \(c'\) to \(c\), or a new, true announcement \(\psi\) has been made from an earlier consistent state, extending the history from \(\sigma'\) to \(\sigma':\psi\).

For the formulas, the first three clauses are straightforward. The fourth clause says that agent \(a\) knows \(\varphi\) if \(\varphi\) holds in all consistent states that she considers possible. The fifth clause says that \(\langle \psi \rangle_{async} \varphi\) holds in a state \(S\) if \(\psi\) can be announced (it is true in \(S\)), and \(\varphi\) holds in the state obtained by adding \(\psi\) to the public channel. The last clause says that \(\bigcirc_a \varphi\) holds if agent \(a\) has at least one unread announcement in the channel, and \(\varphi\) holds after she reads the first unread message.

9.2.4 Circularity

By observing the truth conditions for consistency and for formulas in Figure 9.2, one can see that defining whether a state is consistent requires one to define whether an announcement can be made, and this requires the semantics of our logic to be defined. But to define the semantics of the knowledge operators, we need to define which consistent states are considered possible by the agent, which requires us to define which states are consistent, hence the circularity.

Let us consider the following example, where \(AGT = \{a\}\). Let the initial model be \(M = (W, R_a, \mathcal{W})\) where \(W = \{w\}\), \(R_a = \{(w, w)\}\) and \(\mathcal{W}(w) = \emptyset\), and let the announcement protocol be \(A = \{[K_a p]\}\). According to Figure 9.2, we have: \((w, [K_a p], 0) \models \checkmark\) if \((w, \epsilon, 0) \models K_a p\). But, as \((w, \epsilon, 0) R_a (w, [K_a p], 0)\), the definition of the truth value of \((w, \epsilon, 0) \models K_a p\) depends on the truth value of \((w, [K_a p], 0) \models \checkmark\). To sum up, the definition of \((w, [K_a p], 0) \models \checkmark\) depends on itself.

The circularity problem depends on assumptions (1), (2), and (3) from the introduction:

- Announcements can be epistemic
9.2. SETTINGS

- Announcements are true
- Agents can imagine pending messages

If one of these assumptions is dropped, the circularity problem is easily solved: if announcements do not need to be true, then all states are consistent; if announcements are only propositional formulas, consistency of a state \((w, \sigma, c)\) can be trivially checked by evaluating all propositional formulas in \(\sigma\) in the world \(w\). The last point is only a little bit less obvious: if agents cannot imagine pending announcements, then the definition of the pre-accessibility relation \(R_a\) for agent \(a\) (see Definition 51) is that \((w, \sigma, c)R_a(w', \sigma', c')\) if \(wR_aw'\), \(c(a) = c'(a)\) and \(\sigma|_{c(a)} = \sigma'\): the only sequence of announcements that she considers possible is the one she has already received. In that case, the length of the sequence of announcements \(|\sigma|\) together with the size of the formula to evaluate can be used to define truth conditions for consistency and for formulas by induction.

Indeed, evaluating a formula \(K_\omega \phi\) in a state \((w, \sigma, c)\) only requires evaluating the consistency of states \((w', \sigma', c')\) such that \(|\sigma'| \leq |\sigma|\), which in turn only requires evaluating formulas \(\psi \in \sigma\) in states \((w', \sigma'', c')\) where \(\sigma''\) is a strict prefix of \(\sigma\).

We also note that it is possible to solve the circularity problem by only constraining the last assumption instead of completely dropping it. Indeed, under a bounded non-Zeno behaviour assumption (only a bounded finite number of discrete events occur in a finite time), and assuming a global clock that is common knowledge, the imagination of the agents is sufficiently constrained to solve the circularity problem rather easily (see [KMS17]).

In relation with the above discussion, we point out that the circularity problem does not depend on the following assumptions:

- Announcements are broadcast
- Announcements are made by an external source
- Announcements are received in FIFO order.

In Section 9.3 we will describe several restricted settings in which we manage to overcome this problem. But first we present a small example to better understand the intuitions behind our logic.

9.2.5 Example

We consider two agents \(AGT = \{B, C\}\), where \(B\) stands for Bonnie and \(C\) for Clyde. Bonnie and Clyde go to rob a bank, and Bonnie stays in the car while Clyde goes to the vault. At noon, Bonnie notices that Clyde left the paper with the secret code to open the vault in the car. She uses her smartphone to broadcast the code on their chat group. But Clyde has also realized that he forgot the paper, and before he receives Bonnie’s message he sends a message saying that he does not know the code.

In the following, let \(p\) represent the fact that the secret code is 0000, and \(q\) the fact that the vault is open. The situation at noon is represented by the following initial pointed Kripke model \((M, w)\):

\[
\begin{array}{cc}
\text{a} : p, q & \text{B} \\
\downarrow & \downarrow & \downarrow \\
\text{B, C} & \text{w} : p, \neg q & \text{C} \\
\downarrow & \downarrow & \downarrow \\
\text{B, C} & \text{v} : \neg p, \neg q & \text{B, C}
\end{array}
\]
In the initial world \( w \), Bonnie knows \( p \), i.e., she knows the code, but Clyde does not. On the other hand, Clyde knows that \( q \) is not true, i.e., he knows that the vault is closed, but Bonnie does not (Clyde could have memorized the code before leaving the car, and thus he might have opened the vault). In fact, we observe that initially Bonnie knows that “the vault is open if, and only if, Clyde knows the code” or, in epistemic logic, \( KB(q \leftrightarrow KCp) \).

The initial state at noon is \( wB \begin{array}{c} C \end{array} \delta \) . In our scenario, first \( p \) is announced by Bonnie, and then \( \neg KCp \) is announced by Clyde. The actual state becomes \( wB \begin{array}{c} C \end{array} \delta \) . Intuitively, since only true announcements are made, we see that \( \neg KCp \) can only be announced before Clyde receives the announcement of \( p \). We would like to verify whether, after Bonnie receives both announcements but Clyde receives neither (the signal inside the bank is weak), that is in state \( wB \begin{array}{c} C \end{array} \delta \) , Bonnie knows \( \neg q \), i.e., does she know that the vault is not open, and what does she know about Clyde’s knowledge. In fact, we can prove that the following holds:

\[
(w, \epsilon, 0) \models \langle p \rangle async (\neg KCp) async \bigcirc B \bigcirc B (KB \neg q \land \neg KB KCp \land \neg KB \neg KCp) \tag{9.4}
\]

The meaning is that, after both announcements have been made and received by Bonnie but not by Clyde,

- Bonnie knows that the vault is not open: intuitively, because Clyde told her he didn’t have the code, and thus could not have opened it (recall that \( q \) represents the situation at noon, i.e., before Bonnie announced \( p \)). In state \( wB \begin{array}{c} C \end{array} \delta \) , all consistent possible states for \( B \) are of the form \( (w, \sigma, c) \) for some \( \sigma \) and \( c \): they share the same world \( w \) in which \( q \) does not hold. Indeed, Bonnie initially considers world \( u \) possible, but states with world \( u \) and announcement \( \neg KCp \) are not consistent. Therefore, Bonnie knows \( \neg q \).

- Bonnie does not know whether Clyde knows the code (because she does not know whether Clyde received her message).

In state \( wB \begin{array}{c} C \end{array} \delta \) , Bonnie considers state \( wB \begin{array}{c} C \end{array} \delta \) as possible, and in this state Clyde knows \( p \). But Bonnie also considers possible state \( wB \begin{array}{c} C \end{array} \delta \) , in which Clyde considers state \( wB \begin{array}{c} C \end{array} \delta \) possible, and thus does not know \( p \).

We note that this example highlights the differences between asynchronous broadcast logic and (synchronous) public announcement logic. Since sending and receiving occur at the same time in PAL, we can informally translate the asynchronous broadcast formula \( \langle p \rangle async (\neg KCp) async \bigcirc B \bigcirc B (KB \neg q \land \neg KB KCp \land \neg KB \neg KCp) \) to the PAL formula \( \langle \neg KCp \rangle (KB \neg q \land \neg KB KCp \land \neg KB \neg KCp) \). Assuming the same initial Kripke model and state \( w \), we first notice that in PAL any formula of the form \( \langle p \rangle (\neg KCp) \varphi \) is false because after a proposition \( p \) is announced, \( KCp \) holds in any circumstances, so that \( \neg KCp \) cannot be announced. We can try to simulate the state where Bonnie has received both announcements but Clyde received neither by using private announcements, made to Bonnie but not to Clyde. Consider the trivial translation of our \( L async \) formula into a formula with private announcements:

\[
\langle p \rangle privateB (\neg KCp) privateB (KB \neg q \land \neg KB KCp \land \neg KB \neg KCp),
\]
where $⟨\varphi⟩_{private_B}$ means that $\varphi$ is sent to $B$ and not to $C$. In all versions of PAL with any variant of synchronous private or semi-private announcement (e.g. $\mathbb{GG97}$, $\mathbb{BMS98b}$, $\mathbb{BM04}$, $\mathbb{BDM08}$), this formula is still false in $(M,w)$: because Bonnie receives $¬K_Cp$ immediately when it is sent, Clyde cannot receive $p$ between the announcement of $¬K_Cp$ and its reception by Bonnie, so that Bonnie knows that Clyde does not know $p$. Thus, this example shows that there is no obvious translation from asynchronous broadcast logic to a variant of DEL, and that asynchronous broadcast logic is indeed quite different from DEL.

The proof of (9.4) can be found in $\mathbb{KMS17}$. Note that here we anticipate the fact that we are in one of the cases where we can solve the circularity problem: indeed, all announcements are in the existential fragment of our language (see Section 9.3.2).

### 9.3 Solving the circularity problem

In this section we show how we solve the circularity problem identified in the last section for several restricted cases.

#### 9.3.1 When the initial model is a finite tree

If we assume in the initial model $M = (W, \bigcup_{a\in AGT} R_a, w)$ the relation $\bigcup_{a\in AGT} R_a$ forms a finite tree over $W$, then the circularity problem can be avoided. In this case, we can define a well-founded order on tuples of the form $(w,σ,c,ϕ)$, where $ϕ$ is either a formula in $L_{async}$ or $✓$, the idea being that a tuple $(w,σ,c,ϕ)$ means $w,σ,c | = ϕ$.

**Definition 53** The order $≺$ is defined as follows:

1. $w$ is a descendent of $w'$ in $M$,
2. or $w = w'$ and $|σ| + |ϕ| < |σ'| + |ϕ'|$,
3. or $w = w'$, $|σ| + |ϕ| = |σ'| + |ϕ'|$ and $c < c'$,

where $|✓| = 1$.

It is clear that $≺$ is a well-founded order, and with this order Figure 9.2 forms a well-founded inductive definition of consistency and semantics of our language.

We detail the non-trivial cases. For the second clause of Figure 9.2 observe that by Point 3 of Definition 53 if $c' < c$ then $(w,σ,c,✓) ∼ (w,σ,c',ϕ)$, and for all $w$, $σ'$, $c$ and $ϕ$, by Point 2 of Definition 53 we have $(w,σ',c,ϕ) ∼ (w,σ',c,ϕ)$.

For the clause for $K_aϕ$ of Figure 9.2 by Point 1 of Definition 53 we have that for all $ϕ$, $σ$, $σ'$, if $w'$ is a child of $w$ then $(w',σ',ϕ) ∼ (w,σ,c,K_iϕ)$.

Finally, for the clause for $⟨ψ⟩_{async}ϕ$ of Figure 9.2 by Point 2 of Definition 53 we have that $(w,σ::ψ,c,ϕ) ∼ (w,σ,c,⟨ψ⟩_{async}ϕ)$ for all $w,σ,c,ϕ$ and $ψ$ (note that $|⟨ψ⟩_{async}ϕ| = 1 + |ψ| + |ϕ|$).

**Example 47** Suppose that we have only one agent $a$. Let us consider initial model $M$:

```
  u : ¬p  a : w : p  a : v : p
```

where $⟨ϕ⟩_{private_B}$ means that $ϕ$ is sent to $B$ and not to $C$. In all versions of PAL with any variant of synchronous private or semi-private announcement (e.g. $\mathbb{GG97}$, $\mathbb{BMS98b}$, $\mathbb{BM04}$, $\mathbb{BDM08}$), this formula is still false in $(M,w)$: because Bonnie receives $¬K_Cp$ immediately when it is sent, Clyde cannot receive $p$ between the announcement of $¬K_Cp$ and its reception by Bonnie, so that Bonnie knows that Clyde does not know $p$. Thus, this example shows that there is no obvious translation from asynchronous broadcast logic to a variant of DEL, and that asynchronous broadcast logic is indeed quite different from DEL.

The proof of (9.4) can be found in $\mathbb{KMS17}$. Note that here we anticipate the fact that we are in one of the cases where we can solve the circularity problem: indeed, all announcements are in the existential fragment of our language (see Section 9.3.2).
In this model, \( p \) holds in the actual world \( w \), but agent \( a \) does not know it. Assume that \( p \) can be announced at least once (\( p \in \mathcal{A} \)). We show that, as expected, after \( p \) is announced and agent \( a \) receives this announcement, agent \( a \) knows that \( p \) holds. Formally, we prove that, in \( \mathcal{M} \otimes \mathcal{A} \), we have \( (w, \epsilon, 0) \models (p)_{\text{async}} \circ \alpha K_a \varphi \). To do so we in fact show that \( (w, [p], a \mapsto 1) \models K_a p \), from which it follows that \( (w, [p], 0) \models \circ \alpha K_a p \), hence the desired result. By Definition 24, for pre-accessibility relations, every state \( S \) such that \( (w, [p], a \mapsto 1) R_a S \) is of the form \( S = (w', p; \sigma, a \mapsto 1) \), where \( w' \in \{u, v\} \) and \( \sigma \) is a sequence of announcements. We must show that every such state either is inconsistent or satisfies \( p \).

First, for \( w' = u \). According to the clause for \( p \) in Figure 9.3, we have that \( (u, \epsilon, 0) \not\models p \), and by the second clause in Figure 9.3 it follows that \( (u, [p], 0) \not\models \varphi \), from which it also follows also that \( (u, [p], a \mapsto 1) \not\models \varphi \) and \( (u, p; \sigma, a \mapsto 1) \not\models \varphi \), for any \( \sigma \).

Now, for \( w' = v \), by the first clause for \( p \) in Figure 9.3, it follows that for all states of the form \( S = (v, p; \sigma, a \mapsto 1) \), \( S \models p \), so that finally every state related to \( (w, [p], a \mapsto 1) \) is either inconsistent or verifies \( p \). Note that we could also prove that \( S \) is consistent.

In practice, this setting can be used as an approximation scheme: taking the tree unfolding of models and cutting them at level \( \ell \) amounts to assuming that agents cannot reason about deeper nesting of knowledge. This approach is similar to the well known idea of bounded rationality [Jon99], where it is assumed that due to computational limits, agents have only approximate, bounded information about other agents’ knowledge, which is represented by allowing only finite-length paths in the Kripke model. We point out, however, that this method of approximation is only appropriate in certain settings. One issue is that it does not allow the accurate representation of transitive accessibility relations, where the leaves of an initial model of any depth \( \ell \) may be reached just by evaluating a formula with one knowledge operator. This setting calls for more work to clarify what the finite tree restriction really captures.

### 9.3.2 Announcing existential formulas

Now, we again allow the initial model to be arbitrary. In particular, we may use one of the common models of knowledge, for example an initial model whose underlying frame is \( \text{KD45} \) (relations are serial, transitive and Euclidean) or \( \text{S5} \) (relations are equivalence relations); see [FMHV03a]. However, we restrict the announcement protocol to the existential fragment of our logic, generated by the following rule:

\[
\varphi ::= p \mid \neg p \mid (\varphi \land \varphi) \mid (\varphi \lor \varphi) \mid \bar{\circ} a \varphi \mid \circ a \varphi \mid \langle \varphi \rangle_{\text{async}} \varphi
\]

where \( p \) ranges over \( \mathcal{AP} \) and \( a \) ranges over \( \mathcal{AGT} \). Formulas of the existential fragment are called existential formulas. If an announcement protocol contains only existential formulas, we call it an existential announcement protocol. For instance, the announcement protocol in Example 12 is existential.

Here we tackle the circularity problem by defining consistency and truth conditions separately. We first define as a fixed point the semantics of existential announcements in \( \mathcal{A} \), together with consistency. In a second step we define the semantics of the full logic with existential announcements as described in Figure 9.2, using the fixed point to evaluate consistency.

We fix an initial model \( \mathcal{M} = (W, \{R_a\}_{a \in \mathcal{AGT}}, w) \) and an existential announcement protocol \( \mathcal{A} \). Let \( B \) be the set of all pairs \( (S, \varphi) \) such that \( S \) is a state of \( \mathcal{M} \otimes \mathcal{A} \) and \( \varphi \) is either a formula in \( \mathcal{A} \) or \( \varphi \), the symbol for consistency. Observe that \( (\mathcal{P}(B), \subseteq) \) forms a complete lattice. We now consider the function \( f : \mathcal{P}(B) \rightarrow \mathcal{P}(B) \) defined in Figure 9.3. Function \( f \) takes a set \( \Gamma \) of truth pairs (pairs \( (S, \varphi) \) such that \( S \models \varphi \)), and extends it with the new truth pairs that can be inferred from \( \Gamma \) by applying each of the rules in Figure 9.2 once. For instance, if \( (w, \sigma, c) \models \varphi \)
Remark 3

If announcements of the form $\Gamma$ and $(\Gamma$ similarly follows from one of the truth conditions.

$\triangledown w,\sigma,c,\psi$ captures the intuitions we have about asynchrony.

9.4. SEMANTIC PROPERTIES

105

In this section we establish some semantic properties of our logic. First we compare it with programming languages [Win93] in the same spirit as what we do here to define consistency.

Remark 4

The Knaster-Tarski theorem is often used to define the denotational semantics of decreasing function either, we would not be able to apply the Knaster-Tarski theorem. It would thus no longer hold that $\phi(\Gamma)$ is in $\mathcal{F}(\phi(\Gamma))$, which explains line 3 of Figure 9.3. Every other line of Figure 9.3 similarly follows from one of the truth conditions.

Now, as we restrict to existential formulas, it is easy to see that $f$ is monotone, that is, if $\Gamma_1 \subseteq \Gamma_2$ then $f(\Gamma_1) \subseteq f(\Gamma_2)$. By the Knaster-Tarski theorem [Tar55], $f$ has a least fixed point $\Gamma^* := \bigcup_{n \in \mathbb{N}} f^n(\emptyset)$.

We can now define the truth condition for consistency as: $S \models$ if $(S, \vee) \in \Gamma^*$, and use Figure 9.3 to define the semantics of the language with existential announcements.

Remark 3

If announcements of the form $K_a\psi$ were allowed, we would have to add

$$\{ (w, \sigma, c, K_a\psi) | \text{ for all } (w', \sigma', c') \text{ such that } (w, \sigma, c)R_a(w', \sigma', c'), (w', \sigma', c', \vee) \notin \Gamma \text{ or } (w', \sigma', c', \psi) \in \Gamma \}$$

to the definition of $f$ in Figure 9.3. But then, if $(w, \sigma, c)R_a(w', \sigma', c')$ we would have:

- $(w, \sigma, c, K_a\psi) \in f(\emptyset)$;
- $(w, \sigma, c, K_a\psi) \notin f(\{(w', \sigma', c', \vee), (w', \sigma', c', \neg p)\})$

It would thus no longer hold that $f(\Gamma_1) \subseteq f(\Gamma_2)$ whenever $\Gamma_1 \subseteq \Gamma_2$. As $f$ is clearly not a decreasing function either, we would not be able to apply the Knaster-Tarski theorem.

Remark 4

The Knaster-Tarski theorem is often used to define the denotational semantics of programming languages [Win93] in the same spirit as what we do here to define consistency.

9.4 Semantic properties

In this section we establish some semantic properties of our logic. First we compare it with PAL, explaining why $L_{async}$ is not a conservative extension of PAL when we have at least two agents. Then we establish some validities of $L_{async}$ that show how the correctly defined semantics captures the intuitions we have about asynchrony.
For the rest of the section, we assume that we have a class of initial models and a class of announcement protocols for which the circularity problem can be solved and the semantics defined as in Figure 9.2 (for example, arbitrary initial models and positive announcements), and we discuss some validities of our logic.

9.4.1 Difference from PAL

We discuss the difference between the semantics of our logic and those of public announcement logic (PAL). In PAL, every time an announcement is made, the Kripke model is updated by removing possible worlds where the announcement is not true. This amounts to using the new information to delete epistemic alternatives that are no longer considered possible: since announcements are true, a world where an announcement is not true is not a possible world.

In our case, epistemic alternatives cannot be deleted at the time of the announcement, since announcements are not received immediately by the agents, and in general agents can even have an unbounded number of pending announcements to read. Instead, this pruning is performed directly in the semantics of the knowledge operator, by eliminating all possible states that are not consistent: the pruning is not performed at the moment of the announcement, but is delayed until a knowledge operator is evaluated. Thus, the update operation in PAL and the consistency check in our logic play the same role. This is also reflected in the circularity problem, which stems from a mutual dependence between the definition of the semantics and, in the case of PAL, that of the update, and in the case of our logic, that of consistency.

We also note that if there are at least two agents, our logic is not a conservative extension of PAL. An intuitive way of seeing this is that in PAL, an announcement immediately becomes common knowledge, while in our setting asynchrony makes common knowledge unachievable. One may be tempted to define a translation \( tr \) from PAL to \( L_{async} \), where all cases of the inductive definition are trivial, except that of the announcement operator which is

\[
\bullet \ tr(\langle \psi \rangle \varphi) := \langle tr(\psi) \rangle_{async} \bigcirc_{a_1} \cdots \bigcirc_{a_n} tr(\varphi), \text{where } AGT = \{a_1, \ldots, a_n\}.
\]

In the single-agent case, the translation \( tr \) yields a conservative extension of PAL, but it is not the case when there are at least two agents. One may think that “after the synchronous public announcement of \( \psi \), \( \varphi \) holds” is the same thing as “after the asynchronous broadcast of \( \psi \) and its reception by all agents, \( \varphi \) holds”. But we show that this is not the case.

In PAL, if \( p \) is announced, then \( p \) immediately becomes common knowledge, which we recall, means that all agents know \( p \), they all know that they all know \( p \), they all know that they all know that they all know \( p \), and so on. On the other hand, in asynchronous systems common knowledge cannot be reached \[HM90a, MT88\], and our logic illustrates this phenomenon. Even finite approximations of common knowledge fail to hold in our logic. For instance, while \( [p]_{PAL} K_a K_b p \) is a validity of PAL, its translation \( [p]_{async} K_a K_b p \) is not valid.

Proposition 14 There exist \( M \), an announcement protocol \( A \) and a consistent state \( S \in M \otimes A \) such that \( M \otimes A, S \not\models [p]_{async} K_a K_b p \).

Proof.

The idea is the following: after announcing \( p \), and after all agents have received the message \( p \), a does not know whether agent \( b \) has received \( p \) or not. Therefore, a does not know that \( b \) knows \( p \). Let us consider the following initial model \( M \):

\[
\begin{align*}
\text{a, b} & \xrightarrow{w} p \\
\text{a, b} & \xrightarrow{u : \neg p} a, b
\end{align*}
\]
9.4. SEMANTIC PROPERTIES

The actual world is w. Since p holds in w, it can be announced. Let A = \{\{p\}\}. We prove that \(M \otimes A, (w, e, 0) \models \square p \bigcirc_b K_a K_b p\). To see this, observe that after p has been announced and received by agent a and agent b (i.e., after evaluation of the first three operators of the formula), we reach state \(S = (w, [p], \varphi \triangleleft b \models \frac{1}{0})\). But in \(M \otimes A\), we have (we only represent a part of \(M \otimes A\), which is infinite):

\[
\begin{array}{c|c|c|c|c|c}
\text{a} & \uparrow & p & b & \downarrow & w \\
\hline
\end{array}
\]

Indeed in state \(S = (w, [p], \varphi \triangleleft b \models \frac{1}{0})\) agent a considers it possible that agent b did not receive announcement p, and thus she considers state \(S' = (w, [p], \varphi \triangleleft b \models \frac{1}{0})\) possible. In \(S'\), because b received no announcement, and in the initial model we have \(wR_a[b]u\), agent b considers it possible that the actual world is u and nothing has been announced, i.e., she considers state \(S'' = (u, e, 0)\) possible. Because p does not hold in \(S''\), we have that \(S' \not\models K_a K_b p\), which concludes the proof.

9.4.2 Validities

We say that a formula \(\varphi\) is valid if for every initial model \(M\) and every announcement protocol \(A\) in the classes considered, and for every consistent state \(S \in M \otimes A\), we have \(M \otimes A, S \models \varphi\). We write \(\models \varphi\) to express that \(\varphi\) is valid. In the following proposition we establish some validities that provide insights into our framework and show how our definitions correctly capture some natural properties that intuitively should hold in the asynchronous framework we consider.

**Proposition 15** For every \(\varphi \in L_{async}\) and propositional formula \(\psi\), we have that:

1. \(\models \bigcirc_a \bigcirc_b \varphi \leftrightarrow \bigcirc_b \bigcirc_a \varphi\)
2. \(\models \bigcirc_a \top \rightarrow (\bigcirc_a \varphi \leftrightarrow \neg \bigcirc_a \neg \varphi)\)
3. \(\models \neg \bigcirc_a \top \rightarrow [\psi] \bigcirc_a K_a \psi\)
4. \(\models \neg \bigcirc_a \top \rightarrow [\psi] \bigcirc_a (\neg b \bigcirc_a \top \rightarrow K_b \psi)\)

**Proof.**

We prove the first validity and the other three are left to the reader.

Suppose that we have \(M \otimes A, (w, \sigma, c) \models \bigcirc_a \bigcirc_b \varphi\). By Figure 9.2, this means that \(c(1) < |\sigma|\) and \(M \otimes A, (w, \sigma, c^{+a}) \models \bigcirc_b \varphi\), and the latter implies that \(c^{+a}(b) < |\sigma|\) and \(M \otimes A, (w, \sigma, (c^{+a})^{+b}) \models \varphi\). Now, because \((c^{+a})^{+b} = (c^{+b})^{+a}\), we obtain that \(M \otimes A, (w, \sigma, c^{+b}) \models \bigcirc_a \varphi\), and therefore \(M \otimes A, (w, \sigma, c) \models \bigcirc_b \bigcirc_a \varphi\). The proof for the other direction is symmetric.

Let us comment on these validities. The first one says that it is possible to permute the order of agents that receive next announcements in their respective queues. The second one says that if an agent has an announcement to read, then reading it is a deterministic operation. The third one says that if an agent has no pending announcement and some propositional formula is announced, then after reading his next pending announcement, the agent will know that formula. Intuitively, this is because the truth value of a propositional formula does not change, and the agents know this. The last validity illustrates the fact that in our framework, the behaviour of the public channel is common knowledge. Indeed it says that if, in a situation where agent a has read all the announced messages, a propositional formula \(\psi\) is announced and agent a reads it,
then agent $a$ knows that if agent $b$ has read all the announced messages (and in particular the last one, which is $\psi$), then agent $b$ also knows $\psi$. In some sense, it means that initially agent $a$ knows that agent $b$ will receive the same messages as herself. In the last two validities we restrict to propositional formulas in order to avoid Moore’s paradox [Van07].

We also establish the following proposition, which says that if all the $O_a$ operators in a formula $\varphi$ are under the scope of a knowledge operator, then its truth value is left unchanged by the announcement of any formula $\psi$. Indeed, the knowledge operator considers all possibilities for the content of the agent’s channel, so that the possibility that $\psi$ is in the channel is considered, whether $\psi$ was actually announced or not.

In the following, in addition to the assumption that models and announcement protocols are restricted to classes for which the semantics is defined, we consider announcement protocols in which each announcement can be made infinitely many times. We call such protocols free protocols.

**Proposition 16** Let $\varphi$ be a formula in $L_{\text{async}}$, in which every $O_a$ is under the scope of some $K_b$, and let $A_\infty$ be a free protocol. For every initial model $M$ and consistent state $S = (w, \sigma, c) \in M \otimes A_\infty$, for every $\psi \in A_\infty$, we have $M \otimes A_\infty, S \models (\psi)_\text{async} \varphi \leftrightarrow \psi \land \varphi$.

This result follows immediately from the following lemma:

**Lemma 5** Let $\varphi$ be a formula in $L_{\text{async}}$, in which every $O_a$ is under the scope of some $K_b$, and let $A_\infty$ be a free protocol. For every initial model $M$ and for every consistent state $(w, \sigma, c) \in M \otimes A_\infty$, for every $\psi \in A_\infty$ such that $(w, \sigma; \psi, c) \models \varphi$, we have $M \otimes A_\infty, (w, \sigma, c) \models \varphi$.

**Proof.**

By induction on $\varphi$. The Boolean cases are trivial.

Case $\varphi = K_b \varphi'$: Since $(w, \sigma, c)$ is a state, $c(a) \leq |\sigma|$. It is then easy to check that

$$
\{S \mid (w, \sigma; \psi, c) R_b S\} = \{S \mid (w, \sigma, c) R_a S\},
$$

and the result follows.

Case $\varphi = (\psi')_{\text{async}} \varphi'$: If $\psi' \not\in A_\infty$, the formula $\varphi$ trivially does not hold in both states. Otherwise, because $\psi'$ has infinite multiplicity in $A_\infty$, $\sigma; \psi' \in \text{Seq}(A_\infty)$. We therefore have

$$(w, \sigma; \psi, c) \models (\psi')_{\text{async}} \varphi' \iff (w, \sigma; \psi, c) \models \psi' \text{ and } (w, \sigma; \psi', c) \models \varphi'.
$$

Assume that $(w, \sigma; \psi, c) \models (\psi')_{\text{async}} \varphi'$, we prove that $(w, \sigma, c) \models (\psi')_{\text{async}} \varphi'$. We have that $(w, \sigma; \psi', c) \models \psi'$ (hence $(w, \sigma; \psi', c) \models \varphi'$) and $(w, \sigma; \psi', c) \models \varphi'$. Because $\psi'$ is a subformula of $\varphi$, each $O_a$ in it is in the scope of some $K_b$; we can thus apply the induction hypothesis for $(w, \sigma; \psi, c) \models \psi'$, obtaining that $(w, \sigma, c) \models \psi'$. By induction hypothesis on $(w, \sigma; \psi', c) \models \varphi'$, we get first that $(w, \sigma; \psi', c) \models \varphi'$, then $(w, \sigma, c) \models \varphi'$ and finally $(w, \sigma; \psi', c) \models \varphi'$ (observe that $(w, \sigma; \psi', c) \models \varphi'$). We have proved that $(w, \sigma, c) \models (\psi')_{\text{async}} \varphi'$.

The other direction is treated the same way.

Finally, the case $\varphi = O_a \varphi'$ is not possible as $O_a$ is not under the scope of any $K_b$.

### 9.5 Model checking

Here we address the model checking problem when $A$ is a finite multiset, that is, when the support set of $A$ is finite and the multiplicity of each element is an integer. More precisely, we consider the following decision problem:

- input: an initial pointed model $(M, w)$, a finite multiset of formulas $A$ (where multiplicities are written in *unary*), a formula $\varphi_0$.
In practice, model checking is used to check a scenario described by $A$ and $\varphi_0$ from a given initial situation $(\mathcal{M}, w)$.

### 9.5.1 Propositional announcements

In this section, we suppose that formulas in $A$ are propositional. Note that in this case (which is a particular case of existential announcements) the circularity problem does not exist, as consistency of a state $(w, \sigma, c)$ can be trivially checked by verifying that all propositional formulas in $\sigma$ hold in world $w$ of the initial model, according to the classic semantics of propositional logic.

We consider the model checking problem for $L_{async}$ where inputs $(\mathcal{M}, w, A, \varphi_0)$ are such that $A$ only contains propositional formulas. We call this problem the model checking problem for propositional protocols.

**Theorem 17** The model checking problem for propositional protocols is in $Pspace$.

**Proof.**

Figure 9.4 presents an algorithm that takes a pointed model $(\mathcal{M}, w)$, a finite multiset $A$, a sequence $\sigma \in \text{Seq}(A)$, a cut $c$ on $\sigma$ and a formula $\varphi$ as an input. To check the consistency of a state $(w, \sigma, c)$, we call $\text{checkconsistency}(\mathcal{M}, A, w, \sigma, c)$ which verifies that every (propositional) formula $\psi$ occurring in $\sigma$ evaluates to true with the valuation $w(w)$.

It is easily proven by induction that, for all $\psi$, the following property $P(\varphi)$ holds:

\[
\mathcal{M}, A, (w, \sigma, c) \models \varphi \text{ iff } \text{mc}(\mathcal{M}, A, w, \sigma, c, \varphi) \text{ returns true.}
\]

This establishes the correctness of the algorithm. We now analyze its complexity.

First, observe that because $A$ is finite and each element has finite multiplicity, we have that $\text{Seq}(A)$ only contains sequences of length linear in $|A|$ (recall that multiplicities are written in unary). It is therefore easy to see that the consistency check ($\ast\checkmark$) is done in polynomial time in the size of the input and thus requires a polynomial amount of space. Now, the number of nested calls of $\text{mc}$ is bounded by the size of the formula to check, and each call requires a polynomial amount of memory for storing local variables, so that the algorithm runs in polynomial space. ■

**Theorem 18** The model-checking problem for propositional protocols is $Pspace$-hard.

**Proof.**

See [KMS17]. ■

### 9.5.2 Finite tree initial model

In this section, we restrict the set of inputs $\mathcal{M}, A, w, \varphi_0$ of the model checking problem to those where the initial pointed models $(\mathcal{M}, w)$ are finite trees rooted in $w$.

**Theorem 19** The model-checking problem when we restrict initial models to finite trees is in $Pspace$.

**Proof.**

We consider the algorithm of Figure 9.4 again but now the consistency checking ($\ast\checkmark$) consists of calling the following procedure:
function $mc(M, A, w, \sigma, c, \varphi)$
match $\varphi$ do
  case $p$ : return $p \in V(w)$;
  case $\check{\varphi}$ : return checkconsistency($M, A, w, \sigma, c$)
  case $\lnot \psi$ : return not $mc(M, A, w, \sigma, c, \psi)$;
  case $(\psi_1 \land \psi_2)$ : return $mc(M, A, w, \sigma, c, \psi_1)$ and $mc(M, A, w, \sigma, c, \psi_2)$;
  case $K^a \psi$ :
    for $(u, \sigma', c')$ such that $wR_u \sigma' \in \text{Seq}(A)$ and $c'$ is a cut on $\sigma'$ do
      if $\sigma'[1..c(a)] = \sigma[1..c'(a)]$ and $mc(M, A, u, \sigma', c', \check{\varphi})$ then
        return false
      endIf
    endFor
  endMatch
endFunction

Figure 9.4: Model checking algorithm

function checkconsistency($M, A, w, \sigma, c$)
if $c = 0$
  return true
else
  for $c' < c$ do
    if $mc(M, A, w, \sigma, c', \check{\varphi})$ then
      return true
    endIf
  endFor
return $mc(M, A, w, \sigma', c, \check{\varphi})$ and $mc(M, A, w, \sigma', c, \psi)$ where $\sigma = \sigma :: \psi$
endFunction

Soundness and completeness are proven by induction on inputs using the order $\prec$ defined in Section 9.3.1.

Concerning the complexity, the argument given in the proof of Theorem 17 no longer holds. In order to bound the number of nested calls of $mc$, we have to remark that from a call of $mc$ to a sub-call of $mc$:

1. either we change the current world $w$ in the initial model for a successor $u$ in the finite tree;
2. or the quantity $|\sigma| + |\varphi| + \sum_{a \in AGT} c(a)$ is strictly decreasing, where $|\varphi|$ is the length of $\varphi$ and if $\sigma = [\varphi_1, \ldots, \varphi_k]$ then $|\sigma| = \sum_{i=1}^k |\varphi_i|$.

Now, the number of times (1) occurs is bounded by the depth $\text{depth}(M, w)$ of the finite tree $M, w$. As each $\varphi$ is either a subformula of the input formula $\varphi_0$ or a subformula of a formula in $A$, $|\varphi| \leq |\varphi_0| + |A|$ where $|A| := \sum_{\psi \in A} |\psi|$, and where each single formula $\psi$ is counted as...
9.6. SATISFIABILITY FOR PROPOSITIONAL ANNOUNCEMENTS

many times as it occurs in the multiset \( A \). Furthermore, \(|\sigma| \leq |A|\) and \( c(a) \leq |A| \). Thus, the quantity \(|\sigma| + |\varphi| + \sum_{a \in AGT} c(a)\) is bounded by \((|AGT| + 2)|A| + |\varphi_0|\). Therefore, the number of nested calls to \( mc \) is bounded by \( \text{depth}(\mathcal{M}, w) \times ((|AGT| + 2)|A| + |\varphi_0|) \). So the algorithm requires a polynomial amount of memory in the size of the input (recall that the multiplicity of \( A \) is encoded in unary).

9.5.3 Existential announcements

In this subsection, we design an exponential-time algorithm for the model checking problem in the case of existential announcements.

Given an input \( \mathcal{M}, A, w, \varphi_0 \), the algorithm first computes the least fixed point \( \Gamma^* \) of the function \( f \) defined in Section 9.3.2. Because the number of possible sequences in \( \text{Seq}(A) \) is exponential in \(|A|\), the set \( B \) of pairs \((S, \varphi)\) where \( S \in \mathcal{M} \otimes A \) and \( \varphi \in A \cup \{\checkmark\} \) is of size exponential in the size of the input, and therefore computing the fixed point requires exponential time in the size of the input. This gives us the semantics of consistency for states of \( \mathcal{M} \otimes A \).

Then, to evaluate \( \varphi_0 \), we use the procedure \( mc \) of Figure 9.4 where line \((\checkmark\) ), which checks the consistency of a state \((w, \sigma, c)\), is replaced by checking whether \((w, \sigma, c, \checkmark) \in \Gamma^*\). The algorithm \( mc \) also requires exponential time. To sum up:

**Theorem 20** The model-checking problem for existential announcements is in Exptime.

9.6 Satisfiability for propositional announcements

In this section, we address the satisfiability problem when \( A \) is a finite multiset of propositional formulas, that is, when the support set of \( A \) is finite, the multiplicity of each element is an integer and formulas in \( A \) are propositional. More precisely, we say that a formula \( \varphi_0 \) is \( A \)-satisfiable if there exists an initial pointed model \((\mathcal{M}, w)\) such that \( \mathcal{M} \otimes A, (w, \epsilon, 0) \models \varphi_0 \). We consider the following decision problem:

- **input**: a finite multiset of propositional formulas \( A \) (where multiplicities are written in unary), a formula \( \varphi_0 \);
- **output**: yes if \( \varphi_0 \) is \( A \)-satisfiable, no otherwise.

In practice, a typical application of the satisfiability problem would be to check that a class of systems described by a formula \( \varphi \) satisfies a property \( \psi \). To do so, one checks whether \( \varphi \land \neg \psi \) is satisfiable. If it is not, then indeed all \( \varphi \)-systems satisfy \( \psi \). If it is satisfiable, then the algorithm we present here (like all tableau methods) produces a counter-example, i.e., a model \((\mathcal{M}, w)\) such that \( \mathcal{M} \otimes A, (w, \epsilon, 0) \models \varphi \land \neg \psi \), or in other words, a \( \varphi \)-system that does not satisfy \( \psi \).

9.6.1 Tableau method description

Our tableau method manipulates terms that we call tableau terms, which are of the following kind:

- \((w \sigma c \varphi)\): \( w \) is a world symbol that represents a world of the model \( \mathcal{M} \) being constructed, \( \sigma \) is a sequence of formulas in \( \text{Seq}(A) \), \( c \) is a cut for \( \sigma \) and \( \varphi \) is a sub-formula of \( \varphi_0 \) that should be true in \( \mathcal{M} \otimes A, (w, \sigma, c) \).
- \((wR_u u)\): \( w \) and \( u \) are two world symbols such that \( wR_u u \) in the model \( \mathcal{M} \) being constructed.
• ⊥: Denotes an inconsistency.

A tableau rule is represented by a numerator $N$ above a line and a finite list of denominators $D_1, \ldots, D_k$ below this line, separated by vertical bars, representing nondeterministic choice:

$$
\frac{N}{D_1 \mid \ldots \mid D_k}
$$

The numerator and the denominators are finite sets of tableau terms.

A tableau for input $(A, \varphi_0)$ is a finite tree with a set of tableau terms at each node, whose root is:

$$
\Gamma_0 = \{(w_0 \in 0 \varphi_0)\}.
$$

A rule with numerator $N$ is applicable to a node carrying a set $\Gamma$ if $\Gamma$ contains an instance of $N$ for which the rule has not yet been applied. If no rule is applicable, $\Gamma$ is said to be saturated.

We call a node $n$ an end node if the set of tableau terms $\Gamma$ it carries is saturated, or if $\bot \in \Gamma$. The tableau is extended the following way:

1. Choose a leaf node $n$ carrying $\Gamma$ where $n$ is not an end node, and choose a rule applicable to $n$.

2. For each denominator $D_i$ of the rule, create one successor node for $n$ carrying the union of $\Gamma$ with an appropriate instanciation of $D_i$.

A branch in a tableau is a path from the root to an end node. A branch is closed if its end node contains $\bot$, otherwise it is open. A tableau is closed if all its branches are closed, otherwise it is open.

A pair $(A, \varphi_0)$ is said to be consistent if no tableau for $(A, \varphi_0)$ is closed.

The tableau rules are described in Figure 9.5, in which we write $(\sigma, c) \sim_a (\sigma', c')$ for $\sigma|_{c(a)} = \sigma'|_{c'(a)}$.

Remark 5 Rule $\text{ch}$ for choosing valuations is necessary for checking consistency of states in rules $K_a \varphi$ and $\checkmark$. For this reason, rule $\text{ch}$ is always applied in priority before rules $K_a \varphi$ and $\checkmark$. In a node carrying $\Gamma$ and saturated for rule $\text{ch}$, if $w$ is a world symbol in $\Gamma$, we say that $\sigma$ is true in $w$ if the valuation $\nu$, defined by $\nu(p) = 1$ if $(w \in 0 p) \in \Gamma$ and $\nu(p) = 0$ if $(w \in 0 \neg p) \in \Gamma$, satisfies every formula in $\sigma$ (recall that in this section announcements are propositional).

### 9.6.2 Tableau method soundness and completeness

In this section we prove that the tableau method is sound and complete. Note that we will establish that every tableau is finite in the complexity analysis of the tableau method (see Theorem 21).

Proposition 17 If $(A, \varphi_0)$ is consistent, then $\varphi_0$ is $A$-satisfiable.

Proof.

Suppose that $(A, \varphi_0)$ is consistent, and consider a tableau $t$ for $(A, \varphi_0)$. By assumption, this tableau is open, which means that it has an open branch. Consider one such open branch, and let $\Gamma$ be the set of tableau terms carried by its end node. We define the model $M = (W, \{R_a\}_{a \in A\{T, w\}})$, where

- $W = \{w \mid (w \sigma c \varphi) \in \Gamma \text{ for some } \sigma, c \text{ and } \varphi\}$,
9.6. SATISFIABILITY FOR PROPOSITIONAL ANNOUNCEMENTS

\[
\frac{(w \sigma c \varphi)}{(w \in \emptyset p) \mid (w \in \emptyset \neg p)} \text{ ch} \quad \text{for all atomic propositions } p \text{ appearing in } \varphi_0 \text{ and } A
\]

\[
\frac{(w \sigma c (\varphi \land \psi))}{(w \sigma c \varphi) (w \sigma c \psi)} \land \quad \frac{(w \sigma c \neg(\varphi \land \psi))}{(w \sigma c \neg\varphi) \mid (w \sigma c \neg\psi)} \neg\land
\]

\[
(w \sigma c p) \leftarrow p \quad (w \sigma c \neg p) \leftarrow \neg p \quad (w \sigma c \neg \varphi) \neg
\]

where \( p \in AP \)

\[
\frac{(w \sigma c \bigcirc_a \varphi)}{(w \sigma c^{+a} \varphi) \bigcirc_a} \text{ if } c(a) < |\sigma| \quad \frac{(w \sigma c \bigcirc_a \varphi)}{\bot} \text{ if } c(a) = |\sigma|
\]

\[
\frac{(w \sigma c \neg \bigcirc_a \varphi)}{(w \sigma c^{+a} \neg \varphi) \neg \bigcirc_a} \text{ if } c(a) < |\sigma|
\]

\[
\frac{(w \sigma c (\psi)_{async} \varphi)}{(w \sigma c) (w \sigma::\psi c \varphi) (\psi)_{async} \text{ if } \sigma::\psi \in \text{Seq}(A)} \quad \frac{(w \sigma c (\psi)_{async} \varphi)}{\bot} (\psi)_{async} \text{ if } \sigma::\psi \notin \text{Seq}(A)
\]

\[
\frac{(w \sigma c \neg(\psi)_{async} \varphi)}{(w \sigma c \neg\psi) \mid (w \sigma c \psi) (w \sigma::\psi c \neg \varphi) \neg(\psi)_{async} \text{ if } \sigma::\psi \in \text{Seq}(A)}
\]

\[
\frac{(w \sigma c K_a \varphi)(wR_a u)}{(u \sigma' c' \varphi) K_a \varphi} \quad \text{for all } (\sigma', c') \sim_a (\sigma, c) \text{ and } \sigma' \text{ true in } u \text{ (see Remark 4)}
\]

\[
\frac{(w \sigma c \neg K_a \varphi)}{(u \sigma'_1 c'_1 \neg \varphi)(wR_a u) \mid \cdots \mid (u \sigma_n c_n \neg \varphi)(wR_a u) \neg K_a \varphi \quad \text{where } (\sigma'_i, c'_i) \sim_a (\sigma, c) \text{ and } u \text{ is fresh}
\]

\[
\frac{(w \sigma c \varphi)}{\bot \checkmark} \quad \text{if } \sigma \text{ is not true in } w \quad \frac{(w \in \emptyset p)(w \in \emptyset \neg p)}{\bot} \quad \text{for } p \in AP
\]

Figure 9.5: Tableau rules
\( R_a = \{(w, u) \mid (w R_a u) \in \Gamma\} \) and

for each \( w \in W, u(w) = \{p \mid (w \epsilon 0 p) \in \Gamma\}. \)

We prove that for all \((w \sigma c \varphi) \in \Gamma\), it holds that \( M \otimes A, (w, \sigma, c) \models \varphi. \) Because \((w_0 \epsilon 0 \varphi_0)\) is in \( \Gamma_0 \subseteq \Gamma\), it follows that \( \varphi_0 \) is \( A\)-satisfiable.

If \( \varphi = p \), by saturation of rule \( p \) we have \((w \epsilon 0 p) \in \Gamma\), thus \( p \in u(w) \) by construction of \( M \), and \( M \otimes A, (w, \sigma, c) \models p. \)

If \( \varphi = \neg p \), by saturation of rule \( \neg p \) we have \((w \epsilon 0 \neg p) \in \Gamma \). We cannot have \((w \epsilon 0 p) \in \Gamma\), otherwise the branch would be closed by saturation of rule \( \bot \). Therefore \( p \notin u(w) \), and \( M \otimes A, (w, \sigma, c) \models \neg p. \)

For boolean connectives, the result follows by saturation of the appropriate tableau rule, plus application of the induction hypothesis.

If \( \varphi = \bigcirc_u \psi' \), we have that \( c(a) < |\sigma| \), otherwise \( \Gamma \) would contain \( \bot \) by saturation of rule \( \bigcirc_u \) and the branch would be closed. Therefore, again by saturation of rule \( \bigcirc_u \), \( \Gamma \) contains \((w \sigma c^{++} \varphi')\). By induction hypothesis we get that \( M \otimes A, (w, \sigma, c^{++}) \models \varphi' \), and thus \( M \otimes A, (w, \sigma, c) \models \bigcirc_u \psi'. \)

If \( \varphi = \neg \bigcirc_u \psi' \) we apply similar reasoning, except for the case \( c(a) = |\sigma| \) in which \( \varphi \) trivially holds.

If \( \varphi = \langle \psi \rangle_{async} \psi' \), the result follows by saturation of rule \( \langle \psi \rangle_{async} \psi' \) that \( (w \sigma c \psi) \) and \( (w \sigma c \psi') \) are in \( \Gamma \), and we conclude by the induction hypothesis.

If \( \varphi = \neg \langle \psi \rangle_{async} \psi' \) is not in \( Seq(A) \), \( \varphi \) trivially holds. Otherwise, by saturation of rule \( \neg \langle \psi \rangle_{async} \psi' \) either \((w \sigma c \neg \psi) \) is in \( \Gamma \), or both \((w \sigma c \psi) \) and \((w \sigma c \neg \psi) \) are in \( \Gamma \).

In both cases, we conclude by induction hypothesis.

If \( \varphi = K_a \psi', \) let \((u, \sigma', c') \) be such that \((w, \sigma, c) R^a(u, \sigma', c') \) and \( M \otimes A, (u, \sigma', c') \models \varphi \), i.e. \( \sigma' \) is true in \( u \) (see Remark 5). We have that \( w R^a u \), so by construction of \( M \), \((w R^a u) \in \Gamma \). Also, since \((w, \sigma, c) R^a(u, \sigma', c') \) we have that \( (\sigma, c) \sim_a (\sigma', c') \). By saturation of rule \( K_a \psi' \) we thus have that \((u, \sigma', c') \in \Gamma \), and by induction hypothesis \( M \otimes A, (u, \sigma', c') \models \varphi' \), which concludes.

If \( \varphi = \neg K_a \psi', \) by saturation of rule \( \neg K_a \psi' \) there exist \((\sigma', c') \sim_a (\sigma, c) \) and a world symbol \( u \) such that \( \Gamma \) contains \((u, \sigma', c', \neg \psi) \) and \((w R^a u) \). It follows that \((w, \sigma, c) R^a(u, \sigma', c') \). We also have that \( M \otimes A, (u, \sigma', c') \models \bot \) (or in other words, \( \sigma' \) is true in \( u \)), otherwise the branch would be closed by rule \( \bot \). Finally, by induction hypothesis, \( M \otimes A, (u, \sigma', c') \models \neg \psi' \), and thus \( M \otimes A, (w, \sigma, c) \models \neg K_a \psi'. \)

Proposition 18 If \( \varphi_0 \) is \( A \)-satisfiable, then \((A, \varphi_0)\) is consistent.

Proof.

Suppose that there is a pointed model \((M_0, w_0)\) such that \( M_0 \otimes A, (w_0, \epsilon, 0) \models \varphi_0. \) We must prove that every tableau for \((A, \varphi_0)\) has an open branch.

We let \( W_T \) denote the set of world symbols appearing in a set of tableau terms \( \Gamma \). Such a set \( \Gamma \) is said to be interpretable if, first, it does not contain \( \bot \) and, second, there is an initial model \( M = (W, \{R^a\}_{a \in AGT}, w) \) and a mapping \( f : W_T \rightarrow W \) such that:

- for each \((w R^a u) \in \Gamma \), \( f(w) R_a f(u) \) and
- for each \((w \sigma c \varphi) \in \Gamma \), \( M \otimes A, (f(w), \sigma, c) \models \varphi \) and \( M \otimes A, (f(w), \sigma, c) \models \varphi. \)

We write \( M, f \models \Gamma \) if these two conditions are met.

Observe that \( \Gamma_0 = \{(w_0 \epsilon 0 \varphi_0)\} \) does not contain \( \bot \), and by assumption there is a pointed model \((M_0, w_0)\) such that \( M_0 \otimes A, (w_0, \epsilon, 0) \models \varphi_0. \) So \( M_0, [w_0 \mapsto w_0] \models \Gamma_0, \) and
\(\Gamma_0\) is interpretable. We now prove that when a tableau rule is applied in a node that carries an interpretable set of tableau terms and is not an end node, then one of its successors carries an interpretable set. This implies that every tableau for \((A, \varphi_0)\) has a branch whose end node carries an interpretable set; in particular, this set does not contain \(\bot\), so the branch is open, which concludes.

In the following, \(\Gamma\) is the interpretable set of tableau terms in which the rule is applied, and \(M = (W, \{R_a\}_{a \in AGT}, w)\) and \(f : W \Gamma \rightarrow W\) are such that \(M, f \models \Gamma\).

We do not treat the case of rules for propositional logic as it is straightforward.

Rule \(ch\) for atomic proposition \(p\), on numerator \(\{(w \ \sigma \ c \ \varphi)\}\): if \(p \in w(f(w))\), then \(M \otimes A, (f(w), c, 0) \models p\), and thus \(M, f \models \Gamma \cup \{(w \ c \ 0 \ p)\}\); otherwise \(M, f \models \Gamma \cup \{(w \ c \ 0 \ \neg p)\}\).

So one of the successors is interpretable.

Rule \(\tilde{O}_a \varphi\) on numerator \(\{(w \ \sigma \ c \ \tilde{O}_a \varphi)\}\): by assumption, \(M \otimes A, (f(w), \sigma, c) \models \tilde{O}_a \varphi\).
Thus, according to the semantics, we necessarily have that \(c(a) < |\sigma|\). So the only successor in the tableau carries the set \(\Gamma \cup \{(w \ \sigma \ c^{ta} \varphi)\}\). Since \(w \ \sigma \ c \ \tilde{O}_a \varphi \models \Gamma\) and \(M, f \models \Gamma\), \(M \otimes A, (f(w), \sigma, c) \models \tilde{O}_a \varphi\) holds implies \(M \otimes A, (f(w), \sigma, c^{ta}) \models \tilde{O}_a \varphi\). Besides, because \(M \otimes A, (f(w), \sigma, c) \models \tilde{O}_a \varphi\), we have that \(M \otimes A, (f(w), \sigma, c^{ta}) \models \varphi\). It follows that \(M, f \models \Gamma \cup \{(w \ \sigma \ c^{ta} \varphi)\}\), and the successor is interpretable.

Rule \(\neg \tilde{O}_a \varphi\) on numerator \(\{(w \ \sigma \ c \ \neg \tilde{O}_a \varphi)\}\): the application of this rule requires that \(c(a) < |\sigma|\) hold. So the fact that \(M \otimes A, (f(w), \sigma, c) \models \neg \tilde{O}_a \varphi\) holds implies \(M \otimes A, (f(w), \sigma, c^{ta}) \models \neg \tilde{O}_a \varphi\). The consistency aspect is treated like for rule \(\tilde{O}_a \varphi\), and we obtain that \(M, f \models \Gamma \cup \{(w \ \sigma \ c \ \neg \tilde{O}_a \varphi)\}\), hence the successor is interpretable.

Rule \(\langle \psi \rangle_{async}\varphi\) on numerator \(\{(w \ \sigma \ c \ \langle \psi \rangle_{async}\varphi)\}\): we have that \(M \otimes A, (f(w), \sigma, c) \models \langle \psi \rangle_{async}\varphi\), so \(\sigma :: \psi \in \text{Seq}(A)\), which implies that it is the first version of the rule that is applied. We also have that \(M \otimes A, (f(w), \sigma, c) \models \psi\) and \(M \otimes A, (f(w), \sigma :: \psi, c) \models \varphi\). From the former and the fact that \(M, f \models \Gamma \cup \{(w \ \sigma \ c \ \langle \psi \rangle_{async}\varphi)\}\), we obtain that \(M \otimes A, (f(w), \sigma :: \psi, c) \models \varphi\). It follows that \(M, f \models \Gamma \cup \{(w \ \sigma \ c \ \psi, (w \ \sigma :: \psi :: \varphi)\}\), and thus the only possible successor is interpretable.

Rule \(\neg \langle \psi \rangle_{async}\varphi\) on numerator \(\{(w \ \sigma \ c \ \neg \langle \psi \rangle_{async}\varphi)\}\): First, because \(\{(w \ \sigma \ c \ \neg \langle \psi \rangle_{async}\varphi)\}\) \(\in \Gamma\), we have \(M \otimes A, (f(w), \sigma, c) \models \varphi\). Also, the fact that this rule requires that \(\sigma :: \psi \in \text{Seq}(A)\) hold. So the fact that \(M \otimes A, (f(w), \sigma, c) \models \neg \langle \psi \rangle_{async}\varphi\) holds implies that either \(M \otimes A, (f(w), \sigma, c) \models \neg \psi\) or \(M \otimes A, (f(w), \sigma :: \psi, c) \models \neg \varphi\). If \(M \otimes A, (f(w), \sigma, c) \models \neg \psi\), we obtain that \(M, f \models \Gamma \cup \{(w \ \sigma \ c \ \neg \psi)\}\), and the first successor is interpretable. Otherwise we have both \(M \otimes A, (f(w), \sigma :: \psi, c) \models \neg \varphi\) and \(M \otimes A, (f(w), \sigma, c) \models \psi\). The latter implies that \(M \otimes A, (f(w), \sigma :: \psi, c) \models \varphi\); we obtain that \(M, f \models \Gamma \cup \{(w \ \sigma :: \psi :: \varphi)\}\), and the second successor is interpretable.

Rule \(K_a \varphi\) on numerator \(\{(w \ \sigma \ c \ K_a \varphi)\},\) for some \((\sigma', c') \sim_a (\sigma, c)\) and \(\sigma'\) true in \(u\): First, since rule \(ch\) has the priority over rule \(K_a \varphi\), we know that \(\Gamma\) is saturated for rule \(ch\). Also, since \((wR_a u) \in \Gamma\) and tableau terms of this form can only be introduced by rule \(\neg K_a \varphi\) together with a tableau term of the form \((u \ \sigma'' \ c'' \ \varphi')\), then there is one such tableau term in \(\Gamma\). By saturation of rule \(ch\), it follows that for each \(p\) appearing in \(\varphi_0\) and \(A\), either \((u \ c \ 0 \ p)\) or \((u \ c \ 0 \ \neg p)\) is in \(\Gamma\). This defines a valuation \(\nu\) for \(u\) that, by assumption, makes \(\sigma'\) true (see Remark 5). Because \(M, f \models \Gamma\), we have that \(w(f(u))\) agrees with \(\nu\) on all atomic propositions in \(A\). Since by assumption \(\nu\) satisfies all formulas in \(\sigma'\), so does \(w(f(u))\), and therefore \(M \otimes A, f(u), \sigma', c' \models \varphi\). Now, since \(M, f \models \Gamma\) and \((wR_a u) \in \Gamma\), we have that \(f(w)R_a f(u)\), and because \((w \ \sigma \ c \ K_a \varphi) \in \Gamma\), it holds that \(M \otimes A, (f(w), \sigma, c) \models K_a \varphi\). Since \(f(w)R_a f(u)\) and \((\sigma, c) \sim_a (\sigma', c')\), we have that \((f(w), \sigma, c)R_a (f(u), \sigma', c')\). As we have seen that \(M \otimes A, (f(u), \sigma', c') \models \varphi\), we finally have that \(M \otimes A, (f(u), \sigma', c') \models \varphi\), thus \(M, f \models \Gamma \cup \{(u \ \sigma' \ c' \ \varphi')\}\), and the successor is interpretable.

Rule \(\neg K_a \varphi\) on numerator \(\{(w \ \sigma \ c \ \neg K_a \varphi)\}\): since \(M \otimes A, (f(w), \sigma, c) \models \neg K_a \varphi\), there exist
CHAPTER 9. ASYNCHRONOUS SYSTEMS

u ∈ W, σ′ and c′ such that \( (f(w), σ, c)R_a(u, σ′, c′), M ⊗ A_1(u, σ′, c′) \models \varphi \) and \( M ⊗ A_1(u, σ′, c′) \models \neg \varphi \). Recall that \( (f(w), σ, c)R_a(u, σ′, c′) \) means that \( f(w)R_a u \) and \( (σ, c) \sim_a (σ′, c′) \). Clearly, \( M, f[u \mapsto u] \models \{(u \ σ′ \ c′ \ \neg \varphi)\}(wR_a u) \), and because \( u \) is fresh, \( f[u \mapsto u] \) coincides with \( f \) on all world symbols appearing in \( Γ \), so that \( M, f[u \mapsto u] \models Γ \). Finally, the denominator corresponding to \( σ′, c′ \) is interpretable (there are only finitely many possible \( σ′ \) and \( c′ \), see proof of Theorem 21).

Rule \( \checkmark \) on numerator \( \{(w \ σ c \ φ)\} \): because \( Γ \) is interpretable, this rule cannot be applied. Indeed, assume it is applied. Because rule \( ch \) is applied in priority, \( Γ \) is saturated for rule \( ch \). With reasoning similar to that followed for rule \( K_wφ \), we obtain that the valuation \( ν \) defined by \( Γ \) for \( w \) coincides with \( u(f(w)) \) on all atomic propositions appearing in \( φ_0 \) and \( A \), and thus they agree on all formulas in \( σ \). Yet on the one hand, since \( (w \ σ c \ φ) ∈ Γ \) and \( M, f \models Γ \), we have that \( M ⊗ A_1(f(w), σ, c) \models \varphi \) and thus \( M, f \models Γ \). On the other hand, because the rule \( \checkmark \) is applied, \( ν \) does not satisfy all formulas in \( σ \), and we have a contradiction.

Rule \( \bot \) on numerator \( \{(w \ σ p \ 0), (w \ σ 0 \ \neg p)\} \): because \( M, f \models Γ \) this cannot happen, as otherwise we would have both \( p ∈ u(f(w)) \) and \( p ∉ u(f(w)) \).

Theorem 21 The satisfiability problem for finite propositional protocols is in NExptime.

Proof.
Let \( A \) be a propositional and finite protocol and \( φ_0 \) be the formula to check. The algorithm to check whether \( φ_0 \) is \( A \)-satisfiable consists of non-deterministically applying tableau rules of Figure 9.5 from the initial tableau \( \{(w \ σ 0 \ φ)\} \).

Each world symbol \( w \) except \( w_0 \) is created by rule \( \neg K_a \) with a formula \( φ_w \), and the number of times this rule is applied to terms with \( w \) as world symbol is linear in \( φ_w \). These world symbols can be ordered in a tree structure (a world symbol created by applying rule \( \neg K_a \) in a tableau term with world symbol \( w \) is a child of \( w \)), and the modal depth of \( φ_w \) formulas is strictly decreasing in the tree. So the number of created world symbols \( w \) is exponential in the size of \( φ_0 \).

In addition, recall that the number of possible sequences of announcements \( σ \) is exponential in the size of \( A \), and the number of possible cuts \( c \) is \( |A|^{AGT} \). Therefore, the number of different tableau terms \( (w \ σ c \ ψ) \) is exponential in \( |φ_0| + |A| \).

At each step, the algorithm is executing a rule that adds at least one term. As the number of terms is exponential, the number of rule applications is exponential, and thus the running time of the (non-deterministic) algorithm is exponential. So the satisfiability problem when the protocol is finite and propositional is in NExptime.

We now establish the matching lower bound.

Theorem 22 The satisfiability problem for finite propositional protocols with at least two agents is NExptime-hard.

Proof.
See in [KMS17].

9.7 Related work

We review several research areas related to different aspects of the present work.

9.7.1 Existing logics for asynchrony

As far as we know, there has not been much work on the relationship between knowledge, announcements and asynchrony. In [DLW11], asynchrony in dynamic epistemic logic is studied,
with the notion of asynchrony being that an agent cannot tell whether an event has occurred if her epistemic state is unchanged. This notion of asynchrony is different from the one we consider in this work: indeed in [DLW11], different agents can have a different idea of how many events have occurred so far, because some events might be completely unnoticed by some agents. So in one setting asynchrony is due to events being completely unobserved, while in the other (the one considered in this work) it is due to a delay between the occurrence of an event (the announcement) and its observation (the reception).

A logic dealing with knowledge and asynchrony is also developed in [PT92], but in this setting, messages do not have logical content: for example, the logic does not allow for announcements about knowledge or about the effect of other announcements. [FHV92] is concerned with knowledge in multi-agent, dynamic systems which may be asynchronous, but does not explicitly model communication, and in particular the effects of asynchronous sending and receiving of true announcements, which is the focus of our work.

Recently, van Ditmarsch developed a logic of asynchronous announcements in [vD17]. The major difference between our framework and that one is our third basic principle, that agents are able to imagine all possible pending messages. In van Ditmarsch’s work, agents in fact do not consider any pending or future announcements possible; they only consider a message possible after they have received it. So in our work, an agent $a$ has three sources of uncertainty: first, uncertainty about the state arising from the underlying Kripke model; second “past uncertainty,” that is, uncertainty about which of the messages that $a$ has received have already been received by other agents; and third, “future uncertainty,” uncertainty about what messages are pending in the channel but unread by $a$, or which messages may be broadcast in the future. In van Ditmarsch’s work, agents only have the first two sources of uncertainty: uncertainty arising from the underlying Kripke model, and “past uncertainty.” This means that agents may not consider the current state possible, and may even have false knowledge. For example, if agents $a$ and $b$ initially do not know true proposition $p$, and then $p$ is broadcast, in van Ditmarsch’s framework, if $a$ has received broadcast $p$ and $b$ has not, $b$ considers it impossible that $a$ knows $p$, even though $a$ does indeed know $p$. Symbolically, $K_a p \land K_b \neg K_a p$. In our logic this is not the case: even when $b$ has not received the broadcast of $p$, $b$ considers it possible that $p$ has been broadcast and received by $a$, so the formula $K_a p \land K_b \neg K_a p$ can never hold in our models. In general, $K_a \varphi \rightarrow \varphi$ holds in our logic, while this is not the case in van Ditmarsch’s logic.

### 9.7.2 Semi-private announcements and dynamic epistemic logic

On first glance, asynchronous broadcast logic has some similarities with semi-private announcement logic, [GG97, BMS98b, BM04, BDM08]. Logics with semi-private announcements follow the same basic idea as public announcement logic, but rather than announcements being received by the entire group of agents, each message is announced to a subset of agents, while the rest of the agents know the message was announced to that group, but do not know what the content of the message was. In the general setting, group $A$ receives message $m$ and updates their knowledge accordingly, while the agents not in group $A$ know that $A$ received either $m$ or its negation, $\neg m$, and update their knowledge accordingly. The identity of the group receiving each message is common knowledge for everyone. On the surface, this logic has some similarities with asynchronous broadcast logic: at any time, a certain group of agents has received each message, while others have not. However, like other variants of public announcement logic, logics of semi-private announcements are synchronous: a message is sent and received simultaneously, and thus common knowledge is achieved immediately by the group of agents receiving the message. Furthermore, even the group of agents who do not receive the message have synchronous information, since they immediately know that the other agents have received some message.
Overall, in this setting, the agents have less uncertainty about one another’s knowledge than in the asynchronous setting. In fact, the issues of semi-private messages and asynchrony are orthogonal; one could imagine an asynchronous logic of semi-private announcements, where each member of group $A$ eventually receives announcement $m$, and the rest of the agents eventually receive the information that group $A$ has been asynchronously sent either $m$ or $\neg m$.

### 9.7.3 Arbitrary public announcement logic

Arbitrary public announcement logic (APAL) [BBvD07] has some similarities to our approach. In this logic, one can ask whether some formula holds after any possible announcement; this is not possible in our logic, but because agents can imagine pending messages, our knowledge operator considers any possible future sequence of announcements that follows the protocol, which is a related idea. Interestingly, the satisfiability problem for APAL is undecidable, but decidability can be achieved by considering a constraint similar to our restriction to existential announcements [FvD08, vDFH].

### 9.7.4 Distributed systems

The systems we consider are closely related to the notion of total order broadcast in distributed systems [Ray13, p. 154]:

1. if a message is received, then it means that it has been broadcast;
2. no message is received twice;
3. if an agent received $\varphi$ before $\varphi'$, they all receive $\varphi$ before $\varphi'$;
4. $\varphi$ causally precedes $\varphi'$ implies that no agent receives $\varphi'$ before $\varphi$;
5. if a message is broadcast, all agents will eventually receive it.

The first point holds in our system since a message (a formula) is only received if it is in the queue, which is the list of broadcast messages. The second point holds because a message is received when an agent’s cut is increased to include that message from the queue, which only occurs once for each message. The third point holds because we have FIFO channels, and thus agents all receive messages in the same order, the order in which they are announced. The fourth point follows from the fact that in our systems we only consider a state $(w, \sigma; \psi, c)$ consistent if $(w, \sigma; \psi, c) \models \psi$, and because messages are received in order. The fifth point is not directly modelled in our systems since we only consider finite histories, but it is a kind of liveness constraint that we will probably be led to consider when we extend the logic with temporal operators (see next section).

More recently, [GL13] studies the model checking of distributed systems with respect to epistemic specifications. Although this work is in a synchronous setting, it is quite close to our approach in spirit, and shows that epistemic issues in distributed systems have practical implications, and a logical approach to these concerns can be fruitful.

Finally, we note that our definition of asynchronous models $M \otimes A$, especially the notion of cuts, is in the spirit of [Lam78].

### 9.8 Future work

We review several research areas related to different aspects of the present work.
9.8. FUTURE WORK

9.8.1 Existing logics for asynchrony

As far as we know, there has not been much work on the relationship between knowledge, announcements and asynchrony. In [DLW11], asynchrony in dynamic epistemic logic is studied, with the notion of asynchrony being that an agent cannot tell whether an event has occurred if her epistemic state is unchanged. This notion of asynchrony is different from the one we consider in this work: indeed in [DLW11], different agents can have a different idea of how many events have occurred so far, because some events might be completely unnoticed by some agents. So in one setting asynchrony is due to events being completely unobserved, while in the other (the one considered in this work) it is due to a delay between the occurrence of an event (the announcement) and its observation (the reception).

A logic dealing with knowledge and asynchrony is also developed in [PT92], but in this setting, messages do not have logical content: for example, the logic does not allow for announcements about knowledge or about the effect of other announcements. [FHV92] is concerned with knowledge in multi-agent, dynamic systems which may be asynchronous, but does not explicitly model communication, and in particular the effects of asynchronous sending and receiving of true announcements, which is the focus of our work.

Recently, van Ditmarsch developed a logic of asynchronous announcements in [vD17]. The major difference between our framework and that one is our third basic principle, that agents are able to imagine all possible pending messages. In van Ditmarsch’s work, agents in fact do not consider any pending or future announcements possible; they only consider a message possible after they have received it. So in our work, an agent \(a\) has three sources of uncertainty: first, uncertainty about the state arising from the underlying Kripke model; second “past uncertainty,” that is, uncertainty about which of the messages that \(a\) has received have already been received by other agents; and third, “future uncertainty,” uncertainty about what messages are pending in the channel but unread by \(a\), or which messages may be broadcast in the future. In van Ditmarsch’s work, agents only have the first two sources of uncertainty: uncertainty arising from the underlying Kripke model, and “past uncertainty.” This means that agents may not consider the current state possible, and may even have false knowledge. For example, if agents \(a\) and \(b\) initially do not know true proposition \(p\), and then \(p\) is broadcast, in van Ditmarsch’s framework, if \(a\) has received broadcast \(p\) and \(b\) has not, \(b\) considers it impossible that \(a\) knows \(p\), even though \(a\) does indeed know \(p\). Symbolically, \(K_a p \land K_b \neg K_a p\). In our logic this is not the case: even when \(b\) has not received the broadcast of \(p\), \(b\) considers it possible that \(p\) has been broadcast and received by \(a\), so the formula \(K_a p \land K_b \neg K_a p\) can never hold in our models. In general, \(K_a \varphi \rightarrow \varphi\) in our logic, while this is not the case in van Ditmarsch’s logic.

9.8.2 Semi-private announcements and dynamic epistemic logic

On first glance, asynchronous broadcast logic has some similarities with semi-private announcement logic, [GG97, BMS98b, BM04, BDM08]. Logics with semi-private announcements follow the same basic idea as public announcement logic, but rather than announcements being received by the entire group of agents, each message is announced to a subset of agents, while the rest of the agents know the message was announced to that group, but do not know what the content of the message was. In the general setting, group \(A\) receives message \(m\) and updates their knowledge accordingly, while the agents not in group \(A\) know that \(A\) received either \(m\) or its negation, \(\neg m\), and update their knowledge accordingly. The identity of the group receiving each message is common knowledge for everyone. On the surface, this logic has some similarities with asynchronous broadcast logic: at any time, a certain group of agents has received each message, while others have not. However, like other variants of public announcement logic, logics of semi-private announcements are synchronous: a message is sent and received simultaneously,
and thus common knowledge is achieved immediately by the group of agents receiving the message. Furthermore, even the group of agents who do not receive the message have synchronous information, since they immediately know that the other agents have received some message. Overall, in this setting, the agents have less uncertainty about one another’s knowledge than in the asynchronous setting. In fact, the issues of semi-private messages and asynchrony are orthogonal; one could imagine an asynchronous logic of semi-private announcements, where each member of group $A$ eventually receives announcement $m$, and the rest of the agents eventually receive the information that group $A$ has been asynchronously sent either $m$ or $\neg m$.

9.8.3 Arbitrary public announcement logic

Arbitrary public announcement logic (APAL) \cite{BBvD07} has some similarities to our approach. In this logic, one can ask whether some formula holds after any possible announcement; this is not possible in our logic, but because agents can imagine pending messages, our knowledge operator considers any possible future sequence of announcements that follows the protocol, which is a related idea. Interestingly, the satisfiability problem for APAL is undecidable, but decidability can be achieved by considering a constraint similar to our restriction to existential announcements \cite{FvD08, vDFH}.

9.8.4 Distributed systems

The systems we consider are closely related to the notion of total order broadcast in distributed systems \cite[p. 154]{Ray13}:

1. if a message is received, then it means that it has been broadcast;
2. no message is received twice;
3. if an agent received $\varphi$ before $\varphi'$, they all receive $\varphi$ before $\varphi'$;
4. $\varphi$ causally precedes $\varphi'$ implies that no agent receives $\varphi'$ before $\varphi$;
5. if a message is broadcast, all agents will eventually receive it.

The first point holds in our system since a message (a formula) is only received if it is in the queue, which is the list of broadcast messages. The second point holds because a message is received when an agent’s cut is increased to include that message from the queue, which only occurs once for each message. The third point holds because we have FIFO channels, and thus agents all receive messages in the same order, the order in which they are announced. The fourth point follows from the fact that in our systems we only consider a state $(w, \sigma; \psi, c)$ consistent if $(w, \sigma, c) \models \psi$, and because messages are received in order. The fifth point is not directly modelled in our systems since we only consider finite histories, but it is a kind of liveness constraint that we will probably be led to consider when we extend the logic with temporal operators (see next section).

More recently, \cite{GL13} studies the model checking of distributed systems with respect to epistemic specifications. Although this work is in a synchronous setting, it is quite close to our approach in spirit, and shows that epistemic issues in distributed systems have practical implications, and a logical approach to these concerns can be fruitful.

Finally, we note that our definition of asynchronous models $\mathcal{M} \otimes \mathcal{A}$, especially the notion of cuts, is in the spirit of \cite{Lam78}.
Bibliography


BIBLIOGRAPHY


BIBLIOGRAPHY


[vDFH] Hans van Ditmarsch, Tim French, and James Hales. Positive announcements (under submission).


Index

accessibility program, 31
action emulation, 27
action language, 28
action token, 27
action type, 27
agent, 7
announcement protocol, 96
arbitrary public announcement logic, 27
arrow update, 29
artificial intelligence, 7, 10
asynchronous, 28
asynchronous broadcast logic, 99
atomic proposition, 15
automatic presentation, 70
belief revision, 28
Belote, 17
bisimulation, 26, 89
Bonnie and Clyde, 101
branching epistemic linear-time mu-calculus, 78
Büchi automaton, 75
canonical presentation, 73
card game, 10
cellular automaton, 62
chain, 72
chain monadic second-order logic, 72
Chess, 10
circularity, 100
Cluedo, 10
common knowledge, 20, 49, 88
concurrent game structure, 28
convolution, 70
D, 18
decentralized partially observable Markov decision process, 29
decoding function, 71
decomposition, 29
decPOMDP, 28
DEL presentation, 80
DEL structure, 25, 80
distributed system, 7, 9, 118
encoding alphabet, 71
encoding function, 71
epistemic, 7
epistemic logic, 19
epistemic model, 15
epistemic planning, 61
epistemic planning problem, 81
epistemic protocol synthesis problem, 83
epistemic temporal logic, 29
equivalence, 27
equivalence relation, 18
Euclideanity, 18
event model, 21
explainable agency, 8
explanation, 8
explicit belief, 28
first-order logic, 69, 70
game, 7
Game Description Language, 28
game theory, 20
generalized epistemic planning problem, 81
Go, 10
gossip, 9
group announcement logic, 27
Hanabi, 17
Hintikka’s world, 15
human-aware robot, 8
implicit belief, 28
initial model, 96
interpreted system, 28
introspection, 18
iterated deletion of strictly dominated strategies, 20
KD45, 18 104
Knaster-Tarski theorem, 105
knowledge base, 11
knowledge-based program, 9
knowledge-based programs, 10
learning, 29
linear mu-calculus, 78
mAL, 28
Mettel2, 59
model checking, 11 88 108
monadic second-order logic, 69
mu-calculus, 78
muddy children, 15 33
multi-agent system, 7
multi-robot system, 10
negative introspection, 18
no forgetting, 25
node, 50
PDDL, 28
perfect recall, 25
pointed epistemic model, 15
positive introspection, 18
principle of inertia, 94
private announcement, 22
proposition, 15
psychology, 10
public action, 22
public announcement, 22 106
purely epistemic, 22
quotient, 89
ramification problem, 28
reachability problem, 11
real world, 15
reflexivity, 18
regular automatic tree, 73
relational structure, 69
robot, 8 10
rule 110, 62
S5, 18 64
Sally and Anne, 10 23
satisfiability problem, 49 111
seeing, 87
semantics, 20
semi-private announcement, 24
seriality, 18
social intelligence, 8
state, 15
STRIPS, 28
synchronicity, 25
syntactic fragments, 29
syntax, 19
T, 18
tableau method, 49 111
theorem proving, 41
timely common knowledge, 21
total order broadcast, 118
transition system, 28
transitivity, 18
tree, 69
truth condition, 20
undistinguishability, 18
uniform strategy, 10
unraveling, 15
video game, 10