

Title Most Definitely Pending

Anders Eide

Sometime in the future

Contents

| | | |
|----------|--|-----------|
| 1 | Preface | 3 |
| 2 | Introduction | 4 |
| 2.1 | Motivation | 4 |
| 2.2 | Structure | 5 |
| 3 | Background | 6 |
| 3.1 | History | 6 |
| 3.2 | Logic and Kripke models | 6 |
| 3.3 | Model checking | 7 |
| 3.4 | Language and semantics | 7 |
| 3.5 | State of the art | 11 |
| 4 | Theoretical work | 12 |
| 4.1 | Introduction | 12 |
| 4.2 | Language and semantics | 12 |
| 4.3 | Bisimulation | 12 |
| 5 | Algorithms and pseudocode | 14 |
| 5.1 | Enumeration of announcements in single agent cases | 14 |
| 5.2 | Generalizing the single agent case | 16 |
| 5.3 | Proof of suitability | 17 |
| 5.4 | Algorithm for bisimilarity check | 18 |
| 5.5 | Smallest bisimilar structure | 20 |
| 5.6 | Enumerating the set of announceable extensions | 20 |
| 6 | Model checking | 23 |
| 6.1 | Model checking for Group Announcement Logic | 23 |
| 6.2 | Complexity of the model checking problem | 23 |
| 6.3 | Generating counter examples | 23 |
| 7 | Implementation | 24 |
| 7.1 | Choice of platform | 24 |
| 7.2 | Language and interpretation | 24 |
| 7.3 | Model checking | 24 |
| 7.4 | Tech choices | 25 |
| 7.5 | Implementation details | 28 |
| 7.6 | Future work | 31 |
| 8 | Conclusion | 33 |
| 9 | Appendix A. List of features | 34 |

1 Preface

Abstract:

In this paper we will present a graphical model checking tool for group announcement logic called GALMC, capable of visualizing the process of checking formulas in a step-by-step fashion. We will define how to enumerate the set of ways a given coalition can restrict a model as well as present pseudocode algorithms describing how we have translated our definitions in our model checker.

2 Introduction

Abstract

In this paper we will present a graphical model checking tool for group announcement logic called GALMC, capable of visualizing the process of checking formulas in a step-by-step fashion. We will define how to enumerate the set of ways a given coalition can restrict a model as well as present pseudocode algorithms describing how we have translated our definitions in our model checker.

2.1 Motivation

(ASK TRULS: Greit med førsteperson i motivasjon?)

(TODO: Skriv om hele introduksjonen av GAL)

(TODO: Hente ned bilder av JFLAP i aksjon, med illustrasjoner av hvordan verktøyet og stepperen i det fungerer)

(TODO: Write sub-section on inspiration for tool about JFLAP, educational benefits ect)

(ASK TRULS: Footnotes i en masteroppgave? Lenke til nettsiden for JFLAP)

In 2010, Ågotnes et al. submitted a paper on their extension of Public Announcement Logic called Group Announcement Logic [?]. Having previously used other visual tools such as JFLAP¹ to aid student learning while teaching courses and seeing how helpful it can be to visualize the way something works, I wanted to create something similar that could aid students in learning how group announcement logic works. Looking at other branches of logic such as Computational Tree Logic it is also clear that the field of model checking epistemic logics such as GAL lags far behind. While there does exist model checkers for similar kinds of logic such as DEMO² for Public Announcement Logic, in my opinion DEMO would not lend itself very well to teaching as it requires the user to structure their models as plain sets of numbers and letters through the command line rather than let them see and build their models in a more easily understood manner. As such we not only wanted to make a model checker that supports group announcement logic, but also make it useful in an educational context, by making able to present how the various operators in the language work in a more visual manner. There is also an interesting theoretical challenge involved in model checking GAL, as the semantics behind the logic's group announcement operator involve quantifying over an infinite set of formulas that a given coalition can

¹Available from: <http://www.jflap.org/>

²Haskell source files and user guides available from: https://homepages.cwi.nl/~jve/software/demo_s5/

announce. To this end, we will come up with an algorithm for enumerating this infinite set of formulas by exploring the properties of minimal bisimilar structures and grouping these formulas by which states in our structures they are satisfied in.

(TODO: Nevne modellsjekker og læringsfordeler ved visualisering)

(TODO: Nevne APAL vs GAL, ulike måter å løse lignende 'problem', APAL tar ikke hensyn til agentenes kunnskap)

(TODO: Nevne interessante egenskaper ved GAL, de re/de dicto)

2.2 Structure

This paper is divided into the following sections:

A background section containing background information regarding the field of dynamic epistemic logic and Group Announcement Logic as well as a lot of the various definitions that will be used in the following sections.

A section containing the theoretical work presented in this paper, where we discuss the semantics of group announcement logic and will explore their definitions in order to find definitions that are more easily translatable into algorithms we can use in our model checker.

A section where we translate these definitions into algorithms presented through pseudocode and explain and discuss any differences from the logical definitions.

And finally a section where we present and discuss our implementation of these algorithms and the working software they are implemented in.

(TODO:

Discuss different approaches towards coalitional ability in dynamic epistemic logic, mention coalitional logics like ATL?

Discuss educational benefits from usage of model checker, visualization of semantics behind operators

Discuss scope of implementation, not suitable for research work, but potentially useful in educational setting)

3 Background

In this chapter we will give the reader some insight into the background of these systems of logic while determining the state of the art, before introducing various concepts and terms that will be used later on in this thesis.

(TODO: Reword in order to fit model checker discussion)

3.1 History

The field of epistemic logic is by no means a recent one, with most of the foundations upon which our modern systems and dialects are built having been published around the 1950s.[?]

”Information is communicated, so knowledge and belief are by no means static. Not surprisingly, many logicians have taken this into account. In the context of epistemic logic, there are many different approaches. Dynamic epistemic logic is an umbrella term for a number of extensions of epistemic logic with dynamic operators that enable us to formalize reasoning about information change. It came forth from developments in formal linguistics, computer science, and philosophical logic.”[?]

Hintikka broadly considered to be the father of modern epistemic logic, while he himself thinks von Wright should hold the honor. Von Wright was

3.2 Logic and Kripke models

(TODO: Fix intro) The logic this thesis will be working with, group announcement logic, is also one of these extensions of epistemic logic, but in addition to reasoning around information change also allows us to reason around what coalitions of agents are able to achieve through making public announcements in unison based on how they can change the information available to other agents in the system. Group announcement logic, like many other forms of epistemic logic revolve around the notion of so-called ‘possible worlds’ and agents which may or may not be able to distinguish between them. When working with these possible worlds, we usually refer to them as states in some system we are trying to simulate. We describe which agents are able to distinguish between these states based on an accessibility relation for each agent, consisting of pairs of states they are unable to differentiate. Since we are solely working with epistemic models in this thesis, also known as S5 models, these accessibility relations will also be equivalence relations (meaning they are reflexive, symmetric and transitive), and we will from here on also refer to them as such.

These simulations are then grouped into models consisting of a set of possible worlds or states, a set of equivalence relations for each agent we wish to model, as well as a set of boolean propositions which may or may not hold in a given state.

Throughout the rest of this thesis, we will refer to the previous by the following definition:

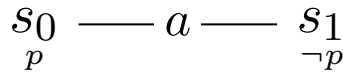
Definition 3.1 (Models) *Given a group of agents A , and a set of propositions P , a model M is a structure $M = (S, \sim, V)$, where*

- S is a set of states
- \sim is a function from every agent $a \in A$ to a 's equivalence relation $\sim_a \subseteq S \times S$.
- $V(p)$ is a valuation function that for every proposition $p \in P$ returns the set of states where p is true

We will also frequently use \sim as $s \sim_a t$, where $a \in A$ to signal that agent a is unable to distinguish between states s and t . When we wish to highlight specific states in a model we will denote this by writing (M, s) to specify that we are referring to state s in the model M , commonly known as a pointed model. This is the form that we will use when we are discussing the properties of a state s in the context of some model M .

A simple practical example of an epistemic model could be us imagining someone that doesn't know whether or not it is raining outside. If we focus solely on whether or not it is in fact raining outside, we might denote this proposition as p , where $p = \text{"It is raining outside"}$. Since this agent, a does not know whether it is raining, this means that in their mind there must be at least two possible worlds, or states; one where p is true, and one where p is false and that a is unable to tell these two states apart. If we label these states as s_0 and s_1 , we end up with the following model shown in Figure 3.2, where we use $\neg p$ to signify that p is not true in (M, s_1) (TODO: Fix this reference so it points to the correct figure)

Figure 3.1: A basic model with two states



Note that since we are working with S5 models, all nodes (states) also have reflexive edges to themselves, even if they are not explicitly drawn in these figures

3.3 Model checking

3.4 Language and semantics

Continuing with the model shown in Figure 3.2, we might want to express certain properties or verify that p is indeed true in (M, s_0) , for this we would

write $(M, s_0) \models p$, or that s_0 in the context of M *satisfies* p . More formally, $(M, s_0) \models p$ is true *iff* $s_0 \in V(p)$ where if we go back to Definition 3.1, we can see that V is a valuation function for propositions, meaning that it returns the set of states in M , where p is true.

In general however, we might want to build more complex formulas to check against our models than simple propositions, for this we need connectives; and logics that define their semantics.

Definition 3.2 (Group Announcement Logic)

$$\varphi ::= p \mid \neg\varphi \mid (\varphi \wedge \psi) \mid (\varphi \vee \psi) \mid \varphi \rightarrow \psi \mid K_a\varphi \mid [\varphi]\psi \mid [G]\varphi$$

Where p is a proposition such that $p \in P$, a is an agent i.e $a \in A$ and G is a set of agents i.e $G \subseteq A$

Definition 3.2 defines the language of \mathcal{L}_{GAL} or more specifically, the set of legal formulas that can be built in accordance to GAL. It inductively specifies in BNF-notation how each operator in the language can be used to create new formulas. This notation however merely specifies the *syntax* of the language, which ways we are allowed to arrange the symbols. In order to specify what each operator does, we also need semantics, which we will add through the satisfaction relation \models .

Definition 3.3 (GAL Semantics)

$$\mathcal{M}, s \models p \text{ iff } s \in V(p)$$

$$\mathcal{M}, s \models \neg\varphi \text{ iff } \mathcal{M}, s \not\models \varphi$$

$$\mathcal{M}, s \models \varphi \wedge \psi \text{ iff } \mathcal{M}, s \models \varphi \text{ and } \mathcal{M}, s \models \psi$$

$$\mathcal{M}, s \models \varphi \vee \psi \text{ iff } \mathcal{M}, s \models \varphi \text{ or } \mathcal{M}, s \models \psi$$

$$\mathcal{M}, s \models \varphi \rightarrow \psi \text{ iff } \mathcal{M}, s \not\models \varphi \text{ or } \mathcal{M}, s \models \psi$$

$$\mathcal{M}, s \models K_i\varphi \text{ iff for every } t \text{ such that } s \sim_i t, \mathcal{M}, t \models \varphi$$

$$\mathcal{M}, s \models [\varphi]\psi \text{ iff } \mathcal{M}, s \models \varphi \text{ implies that } \mathcal{M}|\varphi, s \models \psi$$

$$\mathcal{M}, s \models [G]\varphi \text{ iff for every set } \{\psi_i : i \in G\} \subseteq \mathcal{L}_{el}, \mathcal{M}, s \models [\bigwedge_{i \in G} K_i\psi_i]\varphi$$

(TODO: Mention tautologies and falsehoods, plus valid and satisfiable formulas ect)

Starting with the most basic component of our formulas we have propositions, commonly referred to as atoms or atomic formulas as propositions themselves are also formulas. If we want to check if some pointed model $\mathcal{M}, s \models p$ or satisfies some property p , then as we can see in Definition 3.3

we do this by seeing if the state s is an element in the set of states where p is true, more formally if $s \in V(p)$.

For the explanation of our operators we will be using φ and ψ to represent arbitrary formulas. Negation, \neg is relatively trivial, with $\neg\varphi$ simply meaning the negation of φ and that $\mathcal{M}, s \models \neg\varphi$ if, and only if $\mathcal{M}, s \not\models \varphi$. Conjunction and disjunction, \wedge and \vee are also pretty simple, translating to ‘and’ and ‘inclusive or’, as can be seen from their definitions in Definition 3.3. Implication, \rightarrow can be somewhat loosely translated to ‘if a , then b ’, except if a doesn’t hold, then the implication automatically holds regardless of b . More specifically, the only time an implication is false is when a is true and b is false. We will also use $\varphi \leftrightarrow \psi$, to denote biimplications, meaning $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$ throughout this thesis.

The previous operators are all relatively basic and only express properties regarding the structures they are checked against, the remaining operators in our language are more interesting, as they also express properties regarding the knowledge of the agents in our systems shifting us towards epistemic logic. The K_i operator is the first of these, with $\mathcal{M}, s \models K_a p$ expressing that in our pointed model agent a knows that the proposition p is true. Verifying that this is the case however is where things get interesting, as the previous operators only express properties regarding single states, their scope is also limited to that single state, whereas the K_i operator also requires us to check all the states that this agent is incapable of distinguishing from the current state. In order to check if $\mathcal{M}, s \models K_a \varphi$, we need to ascertain that all states a is unable to distinguish from s also satisfy φ . More specifically, that for all states $t \sim_a s$, that $\mathcal{M}, t \models \varphi$. This is because if there exists any such state that does not satisfy φ , then agent a considers it possible that φ is not satisfied since they cannot tell if t or s is the actual state they are in.

While the K_i operator lets us reason around the knowledge of our agents, the public announcement operator $[\varphi]\psi$ lets us update it, or at least add to it by informing the agents through a truthful announcement that some formula is true in the ‘current’ state as defined by the pointed model we are checking the announcement in. In Definition 3.3 we use the notation $\mathcal{M}|\varphi, s$ to denote \mathcal{M} ‘updated’ by φ , meaning \mathcal{M} minus all states which do not satisfy φ .

Definition 3.4 (Model Updates) \mathcal{M} updated by φ is defined as the following: $\mathcal{M}|\varphi = \langle S', \sim', V' \rangle$ where

$$\begin{aligned} S' &= \{s | s \in S \text{ and } \mathcal{M}, s \models \varphi\} \\ \sim'_a &= \sim_a \cap (S' \times S') \quad \forall a \in A \\ V'(p) &= V(p) \cap S' \quad \forall p \in P \end{aligned}$$

Informally, the definition above in Definition 3.4 can be read as filtering out all states in \mathcal{M} which do not satisfy φ and then constraining the equivalence relations for each agent and the valuation function to that filtered set of states.

The final and most interesting operator in \mathcal{L}_{GAL} is $[G]\varphi$, or the group announcement operator, where G is some coalition of agents such that $G \subseteq A$. $\mathcal{M}, s \models [G]\varphi$ expresses that there is no way for the group G to announce anything that can make φ false in \mathcal{M}, s . Note however that the formulas the agents in $[G]$ can announce are constrained to basic epistemic formulas, or to \mathcal{L}_{el} as defined in Definition 3.5 in order to avoid making our definition of group announcements circular. (TODO: Reword sentence) The syntax of $\{\psi_i : i \in G\}[\bigwedge_{i \in G} K_i \psi_i]\varphi$ intuitively means ‘the conjunction of all formulas $K_i \psi_i$ such that each agent i knows their formula ψ_i and that after this conjunction is announced, φ is true’. As the definition in Definition 3.3 specifies that this has to hold for *every* set of $\{\psi_i : i \in G\}$ however, it might be easier to think of it as there not existing a set such that $\mathcal{M}, s \not\models [\bigwedge_{i \in G} K_i \psi_i]\varphi$ or that G does *not* have the ability to prevent φ from coming true.

Definition 3.5 (Language of epistemic logic \mathcal{L}_{el})

$$\begin{aligned} \mathcal{M}, s &\models p \text{ iff } s \in V(p) \\ \mathcal{M}, s &\models \neg\varphi \text{ iff } \mathcal{M}, s \not\models \varphi \\ \mathcal{M}, s &\models \varphi \wedge \psi \text{ iff } \mathcal{M}, s \models \varphi \text{ and } \mathcal{M}, s \models \psi \\ \mathcal{M}, s &\models \varphi \vee \psi \text{ iff } \mathcal{M}, s \models \varphi \text{ or } \mathcal{M}, s \models \psi \\ \mathcal{M}, s &\models \varphi \rightarrow \psi \text{ iff } \mathcal{M}, s \not\models \varphi \text{ or } \mathcal{M}, s \models \psi \\ \mathcal{M}, s &\models K_i \varphi \text{ iff for every } t \text{ such that } s \sim_i t, \mathcal{M}, t \models \varphi \end{aligned}$$

Where all operators have their semantics defined as in Definition 3.3

We will also be using the duality of the two announcement operators, $\langle \varphi \rangle \psi$ and $\langle G \rangle \varphi$ which are defined as follows in Definition 3.6.

Definition 3.6 (Dual announcement operators)

$$\begin{aligned} \mathcal{M}, s &\models \langle \varphi \rangle \psi \text{ iff } \mathcal{M}, s \models \varphi \text{ and } \mathcal{M}|_{\varphi}, s \models \psi \\ \mathcal{M}, s &\models \langle G \rangle \varphi \text{ iff there exists a set } \{\psi_i : i \in G\} \subseteq \mathcal{L}_{el} \text{ such that:} \\ &\mathcal{M}, s \models \langle \bigwedge_{i \in G} K_i \psi_i \rangle \varphi \end{aligned}$$

The difference between $[\varphi]\psi$ and $\langle \varphi \rangle \psi$ is that the box notation ‘implies’ that ψ is true in the updated model, (TODO: reword sentence) while the diamond notation requires both that $\mathcal{M}, s \models \varphi$ and $\mathcal{M}|_{\varphi} \models \psi$. For group announcements, the box notation expresses that something has to hold after any possible set of announcements the coalition can make, while the dual $\langle G \rangle$ expresses that there exists at least one set of announcements for the

agents in G such that after their announcements φ is true. An interesting observation to make is that like in modal logics we have the same relation between $[\psi]\varphi$ and $\langle\psi\rangle\varphi$ as $\Box\varphi$ and $\Diamond\varphi$, namely that $[\psi]\varphi \leftrightarrow \neg\langle\psi\rangle\neg\varphi$

When we are discussing announcement operators we are usually also interested in the knowledge of the agents in our system, as such it is useful to be able to refer to the set of states an agent considers indistinguishable from the given state. For this we will be using the notion of equivalence classes, defined as the following:

Definition 3.7 (Equivalence classes) *Given a state s and some agent a , a 's equivalence class for s is denoted by $\llbracket s \rrbracket_a$ where*

$$\llbracket s \rrbracket_a = \{t \mid s \sim_a t\}$$

Somewhat related to equivalence classes, we will also be using the concept of formula extensions, referring to the set of states a formula is satisfied in, denoted by $\|\varphi\|$, but also to refer to a set of formulas with the same extension, i.e are satisfied in the same states.

Definition 3.8 (Formula extensions) *For some formula φ and some model \mathcal{M} , the extension of φ in \mathcal{M} is denoted as $\|\varphi\|_{\mathcal{M}}$ where*

$$\|\varphi\|_{\mathcal{M}} = \{s \in S \mid \mathcal{M}, s \models \varphi\}$$

3.5 State of the art

(TODO: Find out where to stuff prior art and model checker discussion)

Discuss activity in CTL, more active than epistemic logic
Mention Tarski's World as example of educational software
Mention DEMO and SMCDEL as examples of model checkers in epistemic logic.
Highlight DEMO's usability problem, shitty UI
Explain how GALMC will attempt to improve this

We will introduce a model checking tool (TODO: Mention Fitch, DEMO, SMCDEL++ and compare in terms of usability and goal)

4 Theoretical work

In this section we will present our theoretical work on exploring the group announcement operator in GAL. In doing this, we will be building on the definitions that were established and introduced in the previous section.

4.1 Introduction

4.2 Language and semantics

4.3 Bisimulation

(ASK TRULS: Hvordan best skille mellom bisimilære tilstander og modeller)

Sometimes we may want to express that two models are ‘the same’, i.e. they satisfy exactly the same set of formulas, despite possibly being structurally different. For this, we have the notion of bisimilarity, denoted by $M \Leftrightarrow M'$. As the concept of bisimilarity is quite central to our exploration of the semantics of the group announcement operator, we introduce the definition of bisimilarity as follows in Definition 4.1

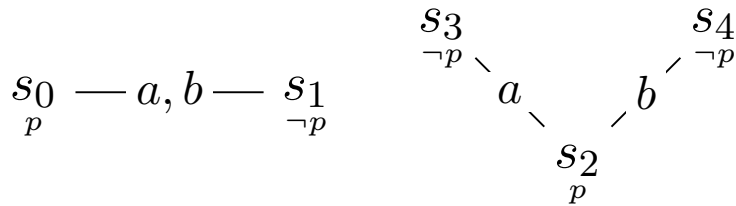
Definition 4.1 (Bisimulation) *Given two models $M = (S, \sim, V)$ and $M' = (S', \sim', V')$, a non-empty relation $\mathfrak{R} \subseteq S \times S'$ is a bisimulation between M and M' iff for all $s \in S$ with $(s, s') \in \mathfrak{R}$:*

atoms *for all $p \in P$: $s \in V(p)$ iff $s' \in V'(p)$;*

forth *for all $a \in A$ and all $t \in S$: if $s \sim_a t$, then there exists a $t' \in S'$ such that $s' \sim'_a t'$ and $(t, t') \in \mathfrak{R}$;*

back *for all $a \in A$ and all $t' \in S'$: if $s' \sim'_a t'$, then there exists a $t \in S$ such that $s \sim_a t$ and $(t', t) \in \mathfrak{R}$;*

Figure 4.1: Two bisimilar, but structurally different models



Building on the concept of bisimilar states, the bisimulation contraction of a model \mathcal{M} is the smallest bisimilar structure to \mathcal{M} , obtained by merging each set of bisimilar states in \mathcal{M} into a single state.

(TODO: Update description of algorithms relating to bisimulation contracting after finishing this clusterfuck)

Definition 4.2 (Bisimulation contracted models) *Given a model \mathcal{M} , one of its smallest bisimilar structures \mathcal{M}' is*

The reason why this concept is interesting is that since these bisimulation contracted models do not contain any bisimilar states, this means that per the definition of bisimilarity, there has to exist some set of formulas that uniquely identify each state in our model by being satisfied only in that specific state of our model. We will refer to these as labeling formulas.

Definition 4.3 (Labeling formulas) *Given a bisimulation contracted model \mathcal{M} , there exists at least one formula φ_s for every $s \in S$ such that $\mathcal{M}, t \models \varphi_s$ iff $s = t$. More precisely in terms of formula extensions:*

$$\forall s \in S, \exists \varphi_s \text{ such that } \|\varphi_s\| = \{s\}.$$

Additionally, we will also be referring to the set of labeling formulas for a given bisimulation contracted model \mathcal{M} as $F_{\mathcal{M}}$

Definition 4.4 (Set of labeling formulas) *Given a bisimulation contracted model \mathcal{M} , the set of formulas uniquely identifying each state in the model, $F_{\mathcal{M}}$ is defined as $F_{\mathcal{M}} = \{\varphi_s | s \in S\}$*

5 Algorithms and pseudocode

In this section we will describe the process of translating the definitions from the previous chapter into algorithms described through algorithms that will be used in our model checker.

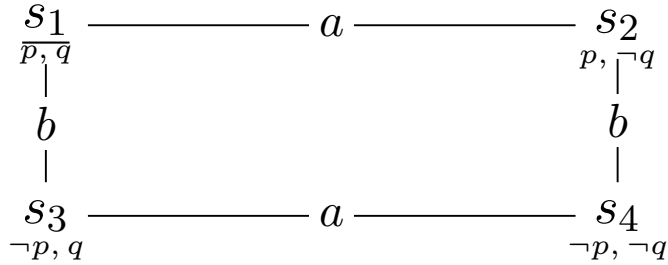
Going back to our revised semantics behind the group announcement operators in Definition 5.6 we can see that once we can determine how to enumerate the set of announceable extensions \mathcal{A}_G , implementing the semantics behind the group announcement operator is fairly straightforward. However, as our definition of \mathcal{A}_G uses the concept of bisimulation contracted models, we will first need to cover how we can check whether states are bisimilar and then apply that check to models as a whole in order to reduce them to their smallest bisimilar structures.

5.1 Enumeration of announcements in single agent cases

Going back to the definition of the semantics behind $\mathcal{M}, s \models \langle G \rangle \varphi$ in Definition 3.6, an informal way of explaining it would be that there exists at least one set of formulas the coalition can announce such that φ is true after their announcements.

Using our definitions of labeling formulas and formula extensions in Definition 3.8 and 4.3 to look at what kinds of formulas any given agent can announce, we note that the goal is to convey information to the other agents in the system. Therefore we do not need to look at the formulas themselves, but only at what consequence announcing them would have and whether or not the agent is able to announce them. For this reason we will be using the concept of formula extensions from Definition 3.8 instead of concrete formulas as announcing any given formula will eliminate all states not in that formula's extension from the updated model as defined by the semantics of model updates.

Figure 5.1: A basic model with no internally bisimilar states



If we attempt to determine which sets of formulas some agent i can announce in the model in Figure 5.1 we can see that the set of announceable formula extensions will always be a subset of the power set of states in the

model. Or more precisely, the set of announceable formula extensions for some agent i in a given pointed model \mathcal{M}, s is a subset of the power set of states in \mathcal{M} , where each set is announceable by i if and only if that set follows the following rules in Definition 5.1.

Definition 5.1 (Rules for eliminating formulas by their extension)

For any formula φ and bisimulation contracted pointed model \mathcal{M}, s , the formula's extension in \mathcal{M} , $\|\varphi\|_{\mathcal{M}}$ must satisfy the following rules in order for the formula to be announceable by some agent i in coalition G :

- $\|\varphi\|_{\mathcal{M}}$ must contain the actual state in our pointed model
- $\forall s \in \|\varphi\|_{\mathcal{M}}, \forall t \sim_i s \Rightarrow t \in \|\varphi\|_{\mathcal{M}}$

The reasoning behind these two rules is based on the semantics of the group announcement operators in Definition 3.3, we can see that we are essentially searching for a combination of formulas which when announced, make φ false. Because of this, having an agent announce that they knows something which is false, or something they do not actually know, will simply make the public announcement trivially true. This means there is no point in checking any announcement containing such a formula, therefore the formula:

- (1) has to be satisfied in the ‘actual’ state of our pointed model
- (2) has to be satisfied in every state the agent is incapable of distinguishing from that ‘actual’ state

Proposition 5.2 *For every extension $\|\varphi\|_{\mathcal{M}}$ that satisfies the rules in Definition 5.1 for some agent, any formula with the same extension can be announced by that agent*

From our definition of formula extensions in Definition 3.8, the extension of a formula is simply the set of states in which this formula is satisfied. Therefore if φ and ψ share the same extension in some model \mathcal{M} , then $\mathcal{M} \models \varphi \leftrightarrow \psi$. From this we can further infer that $\mathcal{M} \models K_a \varphi \leftrightarrow K_a \psi$ for every ψ with the same extension as φ

Definition 5.3 (The set of announceable extensions)

The set of announceable formula extensions \mathcal{A} for some agent i , given a pointed model \mathcal{M}, s is defined as the following:

$\mathcal{A}_{i,(\mathcal{M},s)} \subseteq \wp(\{\|\varphi\|_{\mathcal{M}} \mid \varphi \in F_{\mathcal{M}}\})$ where $\|\varphi\|_{\mathcal{M}} \in \mathcal{A}_{i,(\mathcal{M},s)}$ iff it follows the rules in Definition 5.1. Note that since every formula in $F_{\mathcal{M}}$ is only satisfied in a single state in S , $\wp(\{\|\varphi\|_{\mathcal{M}} \mid \varphi \in F_{\mathcal{M}}\})$ can be simplified to $\wp(S)$.

For a more practical explanation we will apply these rules to the model in Figure 5.1 for agent a . Using s_1 as the actual state of our pointed model, we start by generating the power set of states in our model and get the following:

$$\wp(S) = \{\emptyset, \{1\}\{2\}, \{3\}, \{4\}, \{1, 2\}, \dots, \{1, 2, 3\}, \dots \{1, 2, 3, 4\}\}$$

After applying rule (1) from Definition 5.1 to filter out all formula extensions not containing the actual state of our pointed model we get:

$$\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{1, 2, 3, 4\}\}$$

Applying rule (2) to remove all extensions relating to formulas that a does not know leaves us with:

$$\{\{1, 2\}, \{1, 2, 3, 4\}\}$$

In other words, given the model in Figure 5.1 agent a is able to announce any given formula φ iff $\|\varphi\|_{\mathcal{M},1} \in \{\{1, 2\}, \{1, 2, 3, 4\}\}$. Therefore, $\mathcal{A}_{a,(\mathcal{M},1)} = \{\{1, 2\}, \{1, 2, 3, 4\}\}$.

An interesting thing to note here is that we can combine our labeling formulas with disjunctions to create a formula which is satisfied in any subset of the original set of states we want. So for example, in order to create a formula with the extension of $\{s_1, s_2\}$ all we have to do is put disjunctions between the labeling formulas for s_1 and s_2 such that $\varphi_{\{s_1, s_2\}} = \varphi_{s_1} \vee \varphi_{s_2}$.

If we then want to apply this to checking whether $\mathcal{M}, s_1 \models \langle a \rangle K_b p$ where \mathcal{M} is still the model in Figure 5.1 then we can see that since $\{s_1, s_2\} \in \mathcal{A}_{a,(\mathcal{M},s_1)}$ there exists a formula extension that a can announce which would eliminate s_3 from the model. This would cause $K_b p$ to be satisfied in the updated model and therefore satisfy $\langle a \rangle K_b p$.

5.2 Generalizing the single agent case

Expanding what we have presented so far to encompass coalitions comprised of multiple agents is actually very easy. When we are assessing the ability of an agent to announce something which may change the valuation of a formula, we are simply checking whether or not that agent is capable of eliminating certain states in the updated model. In other words, if we wish to assess the ability of a whole coalition, all we need to do is look at which sets of states each agent in the coalition is able to eliminate in unison.

An interesting observation to make is that an agent i is always capable of eliminating any state they can distinguish from the actual state of some pointed model. This means that in order to find out which states a coalition can eliminate, we can simply take the power set of states and limit it to the combinations of states which fit the rules of Definition 5.1, where we slightly tweak rule 2 to the following:

Definition 5.4 (The set of extensions announceable by coalitions)

The set of announceable extensions $\mathcal{A}_{G,(\mathcal{M},s)}$ for some coalition G , given a bisimulation contracted pointed model \mathcal{M}, s is defined as the following:

$$\mathcal{A}_{G,(\mathcal{M},s)} = \{S' \subseteq S \mid \forall s' \in S', \neg \exists t \forall i \in G \ t \sim_i s', t \notin S' \text{ and } s \in S'\}$$

(TODO: Explain more clearly)

5.3 Proof of suitability

(TODO: reword intro)

In this section we will compare our definitions and work so far with the definitions presented by Ågotnes et al. in their paper on GAL. In their paper they describe how to check formulas of the kind $\langle G \rangle \varphi$ in the following manner:

Definition 5.5 (Definition of $\langle G \rangle \varphi$ by Ågotnes et al.) $\mathcal{M}, s \models \langle G \rangle \varphi$ iff there is a definable restriction $\mathcal{M}'' = (S'', \sim'', V')$ of \mathcal{M} such that $S'' = \bigcap_{i \in G} C_i$ where C_i are unions of classes of equivalence for \sim_i and $s \in S''$ and $\mathcal{M}', s \models \varphi$

Decomposing their definition we end up with S'' being the intersection of the unions of some subset of each agent's equivalence relation. More specifically, for each agent i , we choose which equivalence classes should be part of that agent's union of equivalence classes C_i and then check if there exists some combination of values for each C_i such that restricting the set of states to the intersection of these C_i s gives us a model which both contains the original state s and satisfies φ .

Comparing this definition to our definition of the announceable set of extensions for a coalition, we argue that our definition of $\mathcal{A}_{G,(\mathcal{M},s)}$ defines exactly these intersections of possible combinations of C_i s from the definition of Ågotnes et al. If we further decompose their definition, we end up with the two following restrictions:

$$S'' = \bigcap_{i \in G} C_i \text{ where } C_i \subseteq S, \forall s \in C_i, \llbracket s \rrbracket_i \subseteq C_i \quad (1)$$

$$s \in S'' \quad (2)$$

From this, we argue that our definition of $\mathcal{A}_{G,(\mathcal{M},s)}$ incorporates the same two restrictions, in turn quantifying the set of all possible restricted sets S'' . Decomposing our definition the same way we did Definition 5.5, we end up with $\mathcal{A}_{G,(\mathcal{M},s)}$ defined as the set of all subsets of S , S' which satisfy the following two restrictions:

$$\forall s' \in S' \neg \exists t \forall i \in G, t \sim_i s', t \notin S' \quad (3)$$

$$s \in S' \quad (4)$$

Expanding on our restriction in (3), we could write it out as ‘if there exists a state t indistinguishable by all agents from s , then either $t \in S'$ or $s \notin S'$ ’. A simpler way of phrasing this would be to say that for every state in S' , the intersection of its equivalence classes for all agents in the coalition has to be a subset of S' . Changing (3) to fit this simpler phrasing gives us

$$\forall s' \in S' \cap_{i \in G} \llbracket s' \rrbracket_i \subseteq S' \quad (5)$$

which should further clarify that combining restriction (4) and (5) provides the same set of possible values as (1) and (2). Based on this, we revise the semantics for the group announcement operators into the following:

Definition 5.6 (Group announcement operators, revised)

$$\begin{aligned} \mathcal{M}, s \models [G]\varphi & \text{ iff } \forall Ext \in \mathcal{A}_{G,(\mathcal{M},s)} \text{ then } \mathcal{M}, s \models [\varphi_{Ext}]\varphi \\ \mathcal{M}, s \models \langle G \rangle \varphi & \text{ iff } \exists Ext \in \mathcal{A}_{G,(\mathcal{M},s)} \text{ such that } \mathcal{M}, s \models \langle \varphi_{Ext} \rangle \varphi \end{aligned}$$

Where φ_{Ext} is a formula of the form $\bigvee_{s \in Ext} \varphi_s$

Our reason for revising these definitions is that the original definitions in 3.3 define satisfaction of $[G]\varphi$ by using a quantifier over an infinite set of formulas making it unfit for our goals of implementing a model checking tool. We will therefore be implementing the revised definition in 5.6 instead as the set of announceable extensions is far easier to enumerate than the set of announceable formulas. This is still equivalent to the original definition as we are simply grouping the infinite set of announceable formulas into a finite set of announceable extensions.

(TODO: Walk through example of using updated definition to generate set of announceable extensions for coalition based on previous example and model)

5.4 Algorithm for bisimilarity check

Using the definition of bisimilarity in Definition 4.1 we present our recursive function for checking bisimilarity between states. Given a set of states $States$, a set of agents $Agents$ and two states s and s' such that $s, s' \in States$, the function $rbc(s, s', States, Agents)$ determining whether s and s' are bisimilar is defined as Algorithm 1. (TODO: reword)

The resulting algorithm is fairly similar to the logical definition, with the *props* check being equivalent to the *atoms* clause and the *knowledgeCheck* function replacing the *forth* and *back* clauses. Note that our valuation function is flipped, going from a state to a set of propositions, rather than a proposition to a set of states. The pseudocode for the *knowledgeCheck* function used to translate *forth* and *back* is shown in Algorithm 2

Comparing our algorithm to the original definition of bisimilarity the main point of interest is how it is finite, since for each recursive call to $rbc()$

Algorithm 1 Recursive Bisimulation Check

```
function rbc(s, s', States, Agents)
  if s = s' then
    return true
  else if props(s) ≠ props(s') then
    return false
  else if States = ∅ then
    return true
  else
    States' ← States \ {s, s'}
    forth ← knowledgeCheck(s, s', States', Agents)
    back ← knowledgeCheck(s', s, States', Agents)
    return (forth and back)
  end if
end function
```

Algorithm 2 Knowledge Check

```
function knowledgeCheck(s, s', States, Agents)
  for all (t, Ags) in Neighbours(s, Agents, States') do
    for all a in Ags do
      hasMatching ← false
      for all (t', Ags') in neighbours(s', Agents, States') do
        if a ∈ Ags' and rbc(t, t', States', Agents) then
          hasMatching ← true
          break
        end if
      end for
      if !hasMatching then
        return false
      end if
    end for
  end for
  return true
end function
```

we prevent the two current states from being checked again, meaning at some point the algorithm is guaranteed to halt. The function *neighbours()* used in the *knowledgeCheck()* function simply returns a set of tuples for each state visible from *s* and the set of agents it is visible to, limited to states in *States*.

5.5 Smallest bisimilar structure

Building on the previous algorithm, the next step is using it to create an algorithm for constraining a model to one of its smallest bisimilar structures, by filtering out all bisimilar states. While we normally would not need to worry about which states are filtered, as we are generating a checking log to visualize the checking process for our users, we wanted to avoid having the ‘actual’ state of our pointed model filtered out. As such, we simply make sure that the actual state lies first in our set of states when calling *bisimContract* in our application.

Algorithm 3 Bisimulation contraction

```

function bisimContract(States, Agents, Edges)
  bisimMap  $\leftarrow$  Map < State, State >
  for all (state) in States do
    for all (otherState) in States \ (state  $\cup$  keys in bisimMap) do
      if rbc(state, otherState, States, Agents) then
        bisimMap.put(otherState, state)
      end if
    end for
  end for
  CS  $\leftarrow$  States \ (keys in bisimMap)
  CE  $\leftarrow$  {e  $\in$  Edges | startState(e)  $\notin$  CS and endState(e)  $\notin$  CS}
  contractedModel  $\leftarrow$  (CS, Agents, CE)
  return contractedModel
end function

```

5.6 Enumerating the set of announceable extensions

As we have now laid the groundwork of formulating (TODO: reword) how we can compute bisimulation contractions of models, we can move on to presenting how we can generate the set of announceable extensions. For this we will be using the definition of announceable extensions presented in Definition 5.4. While Ågotnes et al.’s definition in 5.5 is cleaner and more compact, our definition more closely resembles its pseudocode translation.

As can be seen, the algorithm for generating the set of announceable extensions is pretty much just generating the power set of states in the

Algorithm 4 Generating a coalition's set of announceable extensions

```
function genAnnExts(contractedModel, actState, coalition)
  states  $\leftarrow$  contractedModel.states
  extensions  $\leftarrow$   $\wp$ (states)
  for all extension in extensions do
    if actState  $\notin$  extension then
      remove extension from extensions
    else
      for all state in extension do
        eqClass  $\leftarrow$  genEqClass(state, states, coalition)
        for all eqstate in eqClass do
          if eqstate  $\notin$  extension then
            remove extension from extensions
            break
          end if
        end for
      end for
    end if
  end for
  return extensions
end function
```

model, i.e. the set of all possible extensions, and then filtering it according to the rules in Definition 5.1. The *genEqClass*(*state*, *agents*) function used is mostly identical to the *neighbours*() function used previously, except it returns the list of states that the coalition as a whole considers indistinguishable from the input state.

Now that we have not only our bisimulation contracted model, but also a way to generate all of the announceable formula extensions for any coalition, describing the algorithm for checking whether a group announcement formula is satisfied or not becomes entirely trivial. As these extensions are really just stand-ins for some announcement made by the agents as per the original definition in Definition 3.3, we can also regard them as constraints on our model. Going by our revised definition of the semantics behind the group announcement operator from definition 5.6, all our algorithm needs to do is to check whether all of the constrained models we get from applying these constraints to our bisimulation contracted model satisfy the inner formula (ASK TRULS: Hva kaller man den 'bakre' formelen i et announcement?) of the group announcement. As such, we translated the semantics of the group announcement operator into the following checking function, shown in Algorithm 5.

(TODO: Remove filterMapping and all discussion of it)

Like we previously mentioned we here make sure the set of states passed

Algorithm 5 Check function for group announcement operator

```
function check(state, innerForm, model, coalition)  
  contractedModel  $\leftarrow$  bisimContract(model)  
  extensions  $\leftarrow$  genAnnExts(contractedModel, state, coalition)  
  for all extension in extensions do  
    constMdl  $\leftarrow$  constrainMdlBy(contractedModel, extension)  
    extSatisfiesForm  $\leftarrow$  check(state, innerForm, constMdl, coalition)  
    if !extSatisfiesForm then  
      return false  
    end if  
  end for  
  return true  
end function
```

to *bisimContract* starts with the actual state we're checking our formula in, in order to simplify the visualization of our checking process. It should also be mentioned that the *check* function that gets called is implemented as an abstract function overridden by each operator in our system and that Algorithm 5 only shows the implementation for the group announcement operator. The *constrainMdlBy* function used here is merely a special case of updating a model through announcing the set of states directly instead of announcing a formula and constraining our model to the set of states that satisfy the given formula.

6 Model checking

6.1 Model checking for Group Announcement Logic

6.2 Complexity of the model checking problem

6.3 Generating counter examples

7 Implementation

In this chapter we will present our own implementation of a model checker for Group Announcement Logic and describe its inner workings.

7.1 Choice of platform

7.2 Language and interpretation

7.3 Model checking

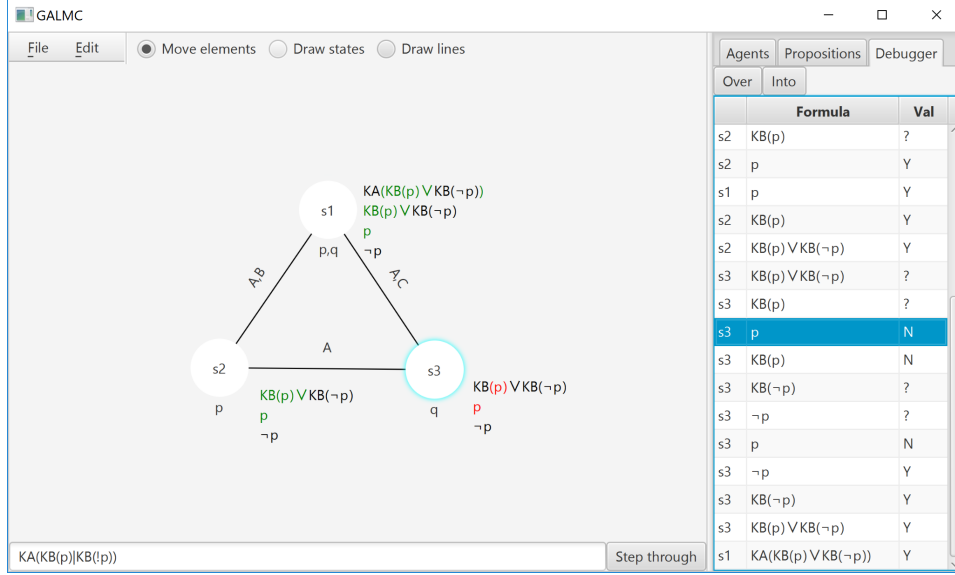
(TODO: Mention inspiration from JFLAP and experience with using it as educational tool)

In this chapter we will present our own implementation of a model checker for Group Announcement Logic called GALMC and describe its inner workings. Our initial goal with GALMC was to create an educational tool that could aid students with learning epistemic logic in a more visual manner by letting the user draw models almost as they would on paper or blackboard. The reasoning behind this was that by allowing the user to manipulate the model through a simple click-and-drag interface and seeing how it can affect the valuation of various formulas they might gain a deeper understanding of the semantics involved.

They would additionally be able to type in a formula and then have the states in their model light up, highlighting which states satisfy the given formula. Another key feature of the application is that in addition to simply checking which states in the user's model, they can also look more closely at why a formula is or is not satisfied in a given state. In order to help the user with this, the application visualizes the checking process step-by-step, one operator and state at a time, with progress being displayed by updating the color of each operator in the formula according to their current valuation.

Figure 7.3 shows a screenshot of GALMC in action, where the user is stepping through the process of checking a specific formula against a state in their model and seeing why their formula is or is not satisfied. It also shows how the application breaks down epistemic formulas into sub-formulas and display them next to each state they have to be checked in. Additionally, the application also visualizes the current valuation of each operator and proposition in the formula as you step through the checking process, as can be seen from the red and green parts of the formulas being checked, as well as the Val column in the debugger tab. Note that the user can also step forwards or backwards through this process at any time by either clicking the step they want to skip to, or browsing with the arrow keys.

Figure 7.1: Example of using GALMC’s step-by-step formula checking



7.4 Tech choices

Our model checker was implemented in Kotlin as it is a new and exiting language while also being based on the JVM, providing access to the vast libraries and tools written for Java, including JavaFX and a Java hook for ANTLR which will be discussed in more detail later in this section. Kotlin additionally has a smooth and concise syntax as well as lending itself very well towards writing functional code despite being object oriented through shorthands for lambda expressions, support for proper function types and distinctions between mutable and immutable structures and variables. Among the other benefits of the language is that Kotlin being a relatively fresh and recent language, is that it has been able to draw plenty of inspiration from other meaning it also has lots of lovely ‘modern’ language features such as type inference, string interpolation and default values for making function arguments optional, meaning you no longer have to write three different constructors as one would in good old Java. While the language is still relatively young, being first unveiled in 2011[?], it is being backed by JetBrains, who are well known for their suite of plugins and IDEs such as IntelliJ and PyCharm, meaning the language has excellent tooling support despite its age.

As for the choice of graphics library to build the application’s user interface in, the choice fell on a Kotlin wrapper for the de facto standard Java GUI library of JavaFX, called TornadoFX³. While JavaFX is a widely used and mature library with powerful features, we also feels it tends to be

³Library homepage at: <https://tornadofx.io>

somewhat clunky and verbose unless one dumps the layout and positioning of components into specialized XML-files. While this helps clean up classes representing UI-components, we also find it makes dynamic component generation somewhat clumsier. Our reasons for wanting to use TornadoFX over plain JavaFX is that TornadoFX, being a Kotlin library is able to have a much cleaner and prettier API by utilizing Kotlin features such as lambda expressions attached to receivers to create composable builder functions which generate your JavaFX component hierarchy in an imperative fashion. Another excellent feature of TornadoFX is its concise shorthands for creating dynamic bindings between UI components and observable sets of data. An example of this would be me using the standard `bindChildren()` function to dynamically create and destroy UI components representing states in the user's epistemic model based on changes to that internal list of objects which represent states in a single line of code, by simply feeding the `bindChildren()` function a reference to the observable list of states and a transformation function that converts the data structure representing a state, to the corresponding UI component, in my case simply the constructor of this component. If anything, I would say that TornadoFX's greatest feature is how its composable builder functions allows you to circumvent the normally inverse order of declaration and creation of UI components compared to their order in the component hierarchy, which can be seen in Figure 7.4. (TODO: Find out why Latex is fucking up this reference)

Figure 7.2: Code handling how the UI components representing states are built. Note the conciseness due to implicit contexts.

```

16 class StateFragment(val item: State) : Fragment() {
17     private val controller: StateController by inject()
18     private val canvasController: CanvasController by inject()
19     private val formulaController: FormulaFieldController by inject()
20
21     override val root: BorderPane =
22         borderpane { this: BorderPane
23             toggleClass(ModelStyles.hidden, item.hiddenProperty)
24             translateXProperty().bind(item.xProperty)
25             translateYProperty().bind(item.yProperty)
26
27             center = stackpane { this: StackPane
28                 circle { this: Circle
29                     toggleClass(ModelStyles.selected, item.selectedProperty)
30                     bindClass(item.validationStyleProp)
31
32                     radius = STATE_CIRCLE_RADIUS
33                     fill = Color.WHITE
34
35                     addMouseListeners()
36                 }
37                 label { this: Label
38                     textProperty().bind(item.nameProperty)
39                     isMouseTransparent = true
40                 }
41             }
42
43             bottom = label { this: Label
44                 textProperty().bind(stringBinding(item.propsProperty) { this: SimpleListProperty<PropositionItem>
45                     item.propsProperty.value.joinToString(separator = ",") { it.propString }
46                 })

```

As for parsing the formulas, I went with ANTLR⁴ for generating the

⁴<http://www.antlr.org/>

parsers I needed. ANTLR is a pretty powerful tool for generating parsers and lexers based on easily definable grammatical rules like the ones in Figure 7.4

Figure 7.3: Grammatical rules for parsing formulas in GALMC with ANTLR.

```

1  grammar GAL;
2
3  // Parser rules
4  formula : form EOF;
5  form : prop=PROP                                     #atomicForm
6        | op=NEG inner=form                             #negForm
7        | left=form op=CONJ right=form                  #conjForm
8        | left=form op=DISJ right=form                  #disjForm
9        | left=form op=IMPL right=form                  #implForm
10       | 'K' agent=AGENT '(' inner=form ')'            #knowsForm
11       | '(' inner=form ')'                            #parensForm
12       | '[' announced=form ']' inner=form             #announceForm
13       | '[' agents=']' inner=form                    #groupannForm
14       ;
15
16 agents : AGENT(COMMA AGENT)*;
17
18 // Lexer rules
19 WHITESPACE : ' ' -> skip;
20
21 AGENT      : [A-ZÆØÅ][a-zæøå]*([0-9])*;
22 PROP      : [a-zæøå]+([0-9])*; //Note: PROP is also used for agents
23 COMMA     : ',';
24 NEG       : '!';
25 CONJ      : '&';
26 DISJ      : '|';
27 IMPL      : '->';
28

```

These grammatical rules are used by ANTLR to generate parser and lexer classes which implement these rules in a manner that allow me to easily translate from raw text and lexical tokens into data structures of my own design which represent the various operators and encapsulate their semantics. One thing to note in Figure 7.4 are the signs used to represent negation, conjunction and disjunction. As the commonly used symbols for these operators do not exist on normal keyboards, the UI would either need extra buttons to facilitate inserting these symbols or use more easily inputable surrogate symbols. I chose the latter, going for the boolean equivalents of using exclamation marks for negations, not, ampersand for conjunctions, and, as well as the vertical bar, or ‘pipe’ character commonly representing the or operator. Note that GALMC automatically converts these characters to their ‘correct’ symbols when displaying the input formula however, as can be seen in figure 7.3. Another small concession I had to make in order to differentiate between agents and propositions was to force agent names to be capitalized as I would otherwise have to resort to using different symbols to differentiate between regular public announcements and group announce-

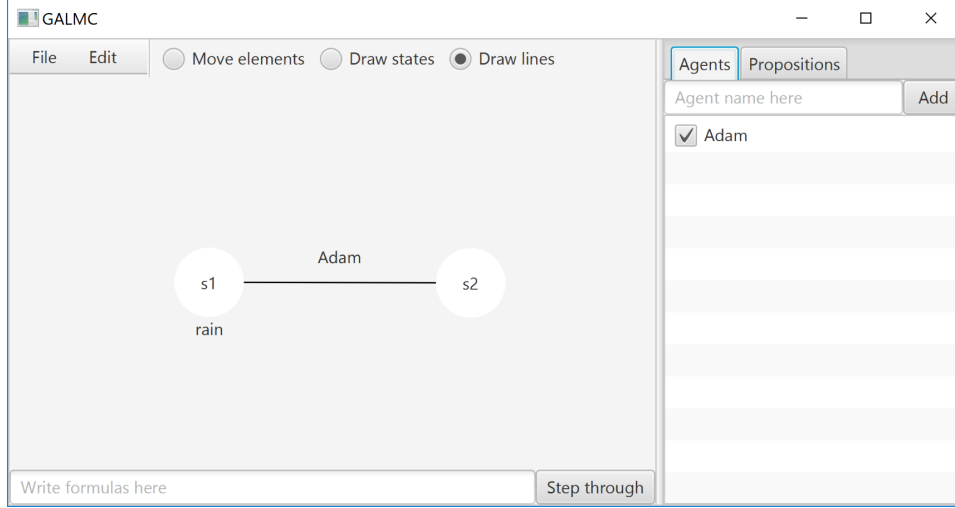
ments. Due to time constraints, the dual diamond announcement operators were not implemented, but both the grammar as well as the formula structures should be easily extendable in order to implement them as future work.

7.5 Implementation details

As the focus when making the application was mainly on making the it as easy to use as possible while presenting information in a visual manner that is easy to grasp, we ended up making several deviations from the logical definitions of the various structures that have been discussed throughout the thesis. Here we will discuss some of them as well as why these deviations were useful to us. A key difference here is how we chose to represent the components of our epistemic models themselves. In Definition 3.1 we present \sim as a function from each agent to their respective equivalence relation for every state in the model, whereas in GALMCwe instead chose to represent these equivalence relations as a set of edges represented as objects consisting of pairs of states and sets of agents. The reasons for this ties back into how we wanted to present an interactive view of the models in our application as it felt cleaner represent each edge between states as a concrete objects which we could then bind a UI-component to, than hold onto sets of sets of states for each agent. Since each edge also has a reference to the set of agents it is valid for, it becomes trivial to visualize this information as well.

We also chose to flip the valuation function by letting states hold a reference to the set of propositions they satisfy rather than each proposition being linked to the set of states they are satisfied in. Our reasoning here is much the same as we highlight which propositions are true in which states through bindings to each state's set of propositions, which is far simpler than having to go through the entire set of propositions each time the user updates which propositions a given state satisfies. An example of how this looks can be seen in Figure 7.5, with both states and the edge between them being just bindings to simple data structures and updating whenever their underlying data does.

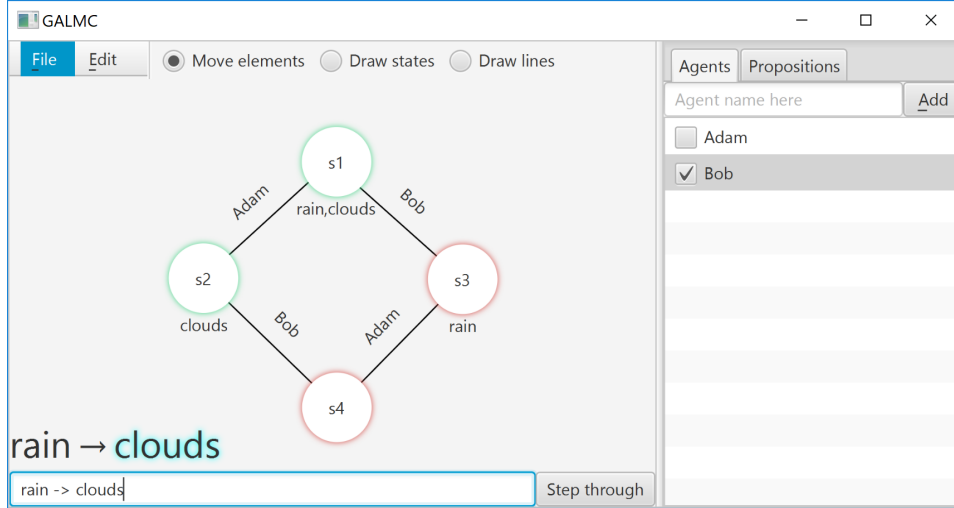
Figure 7.4: A basic model, visualized in GALMC



Additionally, we also made each state aware of which edges it is connected to, trivializing the logic behind finding ‘neighboring’ states for a given agent as we simply filter the set of edges our state is connected to based on each edge being valid for said agent and return a list of states these edges lead to.

Continuing our discussion of how we implemented our formula structures in GALMC, we use a text parser generated from a small ANTLR grammar file in order to parse formulas entered by the user into a tree-like structure representing their formula. When checking this formula the user then has a choice of whether they simply want to see which states in the model satisfy their formula, or whether they want a more detailed visualization of why their formula is or is not satisfied in a specific state. If the user then opts for the first option and check their formula against the whole model, then the tool will highlight the states as either green or red, depending on whether that state satisfies the input formula. The tool also generates an interactive visual representation of the formula where the user can mouse over each operator to check the sub-formula that operator represents against the model as seen in Figure 7.5. The idea behind this being that the user might be interested in quickly seeing which states in their model satisfy the various sub-formulas to help better understand how the original operator works. The way this was implemented was to basically create UI components for each operator in the formula and the sub-formula they represent and then check each sub-formula against the model as the user mouses over them, highlighting which part of the formula they represent.

Figure 7.5: Illustration of interactive formula display



How step-by-step visualization works is somewhat more involved. A high-level description of how it is implemented is that the ‘debugger’ hooks into the *check* function of the formula, and logs each step of the checking process. Each log then carries information about what the valuations of each operator was at that point in the process, so that this checking process can be played back and visualized in the form of showing the various operators change color as their valuations become known. One pretty cool feature of this step-by-step visualization is that it allows the user to see which states get filtered out by model updates and even see the checking process play out in each formula extension a given coalition can announce in the case of checking group announcement formulas. There were also plans for separately visualizing the set of announcements a coalition can make as well as showing what the updated models would look like, but unfortunately this had to be scrapped due to time constraints.

Figure 7.6: Snippet showing how various operators are implemented

```

67 class Negation(val inner: Formula, depth: Int): Formula(depth) {
68     override val needsParentheses = false
69
70     override fun check(state: State, model: Model, debugger: Debugger?): Boolean {
71         createDebugEntry(state, FormulaValue.UNKNOWN, debugger)
72         val result: Boolean = inner.check(state, model, debugger).not()
73         createDebugEntry(state, toFormulaValue(result), debugger)
74         return result
75     }
76
77     override fun toLabelItems(needsParens: Boolean): MutableList<FormulaLabelItem> {...}
78 }
79
80 class Disjunction(left: Formula, right: Formula, depth: Int): BinaryOperator(left, right, depth) {
81     override val opSymbol = "V"
82
83     override fun check(state: State, model: Model, debugger: Debugger?): Boolean {
84         createDebugEntry(state, FormulaValue.UNKNOWN, debugger)
85         val result: Boolean = left.check(state, model, debugger) || right.check(state, model, debugger)
86         createDebugEntry(state, toFormulaValue(result), debugger)
87         return result
88     }
89 }
90
91 class Conjunction(left: Formula, right: Formula, depth: Int): BinaryOperator(left, right, depth) {
92     override val opSymbol = "A"
93
94     override fun check(state: State, model: Model, debugger: Debugger?): Boolean {
95         createDebugEntry(state, FormulaValue.UNKNOWN, debugger)
96         val result: Boolean = left.check(state, model, debugger) && right.check(state, model, debugger)
97         createDebugEntry(state, toFormulaValue(result), debugger)
98         return result
99     }
100 }
101
102

```

(TODO: Create UML diagram of data structures and how they are connected)

7.6 Future work

(TODO: Skrive om å måle pedagogisk verdi, muligens peke ut som fremtidig masteroppgave)

Having developed what we consider to be a potentially highly useful education tool, the big elephant in the room when discussing future work is actually measuring its educational benefit. As both user testing and educational impact studies go beyond the scope of this thesis, we certainly hope that someone might be willing to take up the torch and prove the value of GALMC in such settings. While GALMC is fully functional and usable as an educational aid in its current state, there are also a fair few features that we simply did not have time to implement, a few of which we will discuss.

One of the simpler additions to the tool is implementing the dual, also known as ‘diamond’ version of the announcement operators. As these operators do not add any additional expressiveness or capabilities to the model checker they were never prioritized as they can always be expressed through the negation of the box operators. It would still be nice to have support for these operators directly however, to cut down on formula length and complexity when visualizing larger formulas. As both the ANTLR grammar and related formula components are easily extendable, implementing these operators would be fairly trivial as their underlying semantics are basically already implemented.

There are also a fair few additions to the UI we would have liked to im-

plement, such as separately displaying the set of formula extensions a coalition can announce or provide the user with more informative error messages when attempting to parse syntactically incorrect formulas. Visualizing these formula extensions should also not prove all too challenging as the extensions are already generated when checking formulas. Similarly, the ANTLR parsers provide most of the context necessary to present inform the user of which part of their string caused an error, although more complex reasoning around how to parse ambiguous structures in regards to how to handle missing parentheses and the like might be more challenging.

(TODO: Fix apostrophe positioning somehow)

There were also plans for generalizing GALMC's model serializer in order for to be able to export the models as formats beyond its current basic binary format such as GEXF⁵ in order to be able to view these models in other tools such as Gephi⁶. As the intended users of the tool are mainly students attempting to gain a better understanding of the semantics of the operators and structures in group announcement logic however, the feature was eventually scrapped as the models created would likely not be all that interesting to visualize in external tools anyway and the work involved would be fairly substantial for a feature that would probably go unused by most users. Continuing on model serialization, we would also have liked to be able to store additional information or metadata about each model, such as being able to write notes about interesting properties a model might have or formulas that highlight said properties when checked against these models.

⁵<https://gephi.org/gexf/format/>

⁶<https://gephi.org/>

8 Conclusion

Conclusion pending

9 Appendix A. List of features

Conclusion pending