Slide 1

COMP3152/9152
Lecture 2
Model Checking and Axiomatization
Ron van der Meyden

Reading, FHMV Ch 3

Slide 2

Axioms for Reasoning about Knowledge

Write $\mathcal{L}_{\{X\}}$ for the language based on a set of operators X.

E.g . $\mathcal{L}_{\{K_1,\ldots,K_n\}}$

$\mathcal{L}_{\{K_1,\ldots,K_n,C_G\}}$

$\mathcal{L}_{\{K_1,\ldots,K_n,C_G,D_G\}}$

Slide 3

Model Checking

Problem: Given a structure M, a world w of M and a formula ϕ, decide if $M, w \models \phi$.

Theorem: For finite M, and $\phi \in \mathcal{L}_{\{K_1,\ldots,K_n,C_G\}}$ there exists an algorithm that solves the problem in time linear in $|M| \cdot |\phi|$, where $|M|$ and $|\phi|$ are the amount of space needed to write down M and ϕ, respectively.

Slide 4

Subformulas

The set of subformulas $\texttt{subformulas}(\phi)$ of a formula are defined as follows:

$\texttt{subformulas}(p) = \{p\}$

$\texttt{subformulas}(\neg\phi) = \{\neg\phi\} \cup \texttt{subformulas}(\phi)$

$\texttt{subformulas}(\phi_1 \wedge \phi_2) =$
$\{\phi_1 \wedge \phi_2\} \cup \texttt{subformulas}(\phi_1) \cup \texttt{subformulas}(\phi_2)$

$\texttt{subformulas}(K_i\phi) = \{K_i\phi\} \cup \texttt{subformulas}(\phi)$

$\texttt{subformulas}(C_G\phi) = \{C_G\phi\} \cup \texttt{subformulas}(\phi)$

$\texttt{subformulas}(D_G\phi) = \{D_G\phi\} \cup \texttt{subformulas}(\phi)$

Slide 5

Examples:

The subformulas of $K_j(K_i p) \wedge C_G q$ are:

$K_j(K_i p) \wedge C_G q$

$K_j(K_i p)$, $C_G q$

$K_i p$, p, q

Slide 6

Algorithm

Input: A finite structure $M = \langle W, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n \rangle$ and a formula $\phi \in \mathcal{L}_{\{K_1,\ldots,K_n,C_G\}}$.

Order `subformulas`(ϕ) as $\phi_1, \phi_2, \ldots, \phi_k$ where $\phi_k = \phi$ and `subformulas`$(\phi_j) \subseteq \{\phi_1, \ldots, \phi_j\}$ for $0 < j$.

For $j = 1 \ldots k$,

For all worlds $w \in W$, label w by either ϕ_j or $\neg\phi_j$, as follows:

if $\phi_j = p$ then label w by p iff $\pi(w)(p) =$ `true`

if $\phi_j = \alpha \wedge \beta$ then label w by ϕ_j iff w is labelled by both α and β

if $\phi_j = K_i\alpha$ then

1. label w by $\neg\phi_j$ if w is labelled by $\neg\alpha$
2. if $w'\mathcal{K}_i w$ and w has been labelled by $\neg\phi_j$ then label w' by $\neg\phi_j$
3. label all other worlds by ϕ_j

Slide 7

If $\phi_j = C_G\alpha$,

1. Label all worlds w that are labelled by $\neg\alpha$ by $\neg C_G\alpha$
2. Do a depth first search from these worlds, label all worlds reached by $\neg C_G\alpha$
3. Label all worlds not labelled in the depth first search by $C_G\alpha$.

Slide 8

This algorithm can be implemented to run in time linear in $|M| \cdot |\phi|$.

Exercise: Extend this to an algorithm for $\mathcal{L}_{\{K_1,\ldots,K_n,C_G,D_G\}}$. What is the complexity of the extension?

Slide 9

Validity

A formula ϕ is *valid* if for all Kripke structures M and all states w of M, we have $M, w \models \phi$.

Write $\models \phi$ if ϕ is valid.

Question: how can we prove that/decide if a given formula ϕ is valid?

Slide 10

Axioms for Knowledge

K0. all substitution instances of valid formulas of propositional logic

K1. $K_i\varphi \wedge K_i(\varphi \Rightarrow \psi) \Rightarrow K_i\psi$

K2. $K_i\varphi \Rightarrow \varphi$

K3. $K_i\varphi \Rightarrow K_iK_i\varphi$

K4. $\neg K_i\varphi \Rightarrow K_i\neg K_i\varphi$

Slide 11

Rules of inference

Nec. (Necessitation) If φ then $K_i\varphi$

MP. (Modus Ponens) If φ and $\varphi \Rightarrow \psi$ then ψ.

Slide 12

Proofs

A *proof* of a formula ϕ is a sequence of formulas $\phi_1, \phi_2, \ldots, \phi_k$ such that $\phi_k = \phi$ and for all $j = 1 \ldots k$, either

1. ϕ_j is an axiom, or
2. ϕ_j follows from $\phi_1, \ldots, \phi_{j-1}$ using a rule of inference.

Write $\vdash \phi$ if there exists a proof of ϕ.

lide 13

Example

A proof of $p \Rightarrow K_i \neg K_i \neg p$:

1. $K_i \neg p \Rightarrow \neg p$ (K2)
2. $(K_i \neg p \Rightarrow \neg p) \Rightarrow (p \Rightarrow \neg K_i \neg p)$
   (K0, instance of $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$
3. $p \Rightarrow \neg K_i \neg p$ (1,2, MP)
4. $\neg K_i \neg p \Rightarrow K_i \neg K_i \neg p$ (K4)
5. $(p \Rightarrow \neg K_i \neg p) \Rightarrow ((\neg K_i \neg p \Rightarrow K_i \neg K_i \neg p) \Rightarrow (p \Rightarrow K_i \neg K_i \neg p))$
   (K0, instance of $(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C)$
6. $(\neg K_i \neg p \Rightarrow K_i \neg K_i \neg p) \Rightarrow (p \Rightarrow K_i \neg K_i \neg p)$ (4,5, MP)
7. $p \Rightarrow K_i \neg K_i \neg p$ (3,6, MP)

lide 14

Warning re the Deduction Theorem

For propositional logic, the following pattern of reasoning is sound:

If, assuming ϕ, ψ can be proved, then $\phi \Rightarrow \psi$ can be proved.

I.e., $\phi \vdash \psi$ implies $\vdash \phi \Rightarrow \psi$

This does not hold for the logic of knowledge!

Slide 15

Example (incorrect deduction):

1. p (assumption)
2. $K_i p$ (from 1 using Nec.)
3. $p \Rightarrow K_i p$ (using Deduction Theorem)

But $p \Rightarrow K_i p$ is NOT valid.

(Exercise - construct a structure in which it fails.)

Slide 16

For formulas $\phi \in \mathcal{L}_{\{K_1,\ldots,K_n,C_G\}}$.

Theorem: (Soundness) If $\vdash \phi$ then $\models \phi$.

Theorem: (Completeness) If $\models \phi$ then $\vdash \phi$.

where $\vdash$ is defined using the axioms and rules above.

lide 17

Proving Soundness

Suppose that $\phi_1, \phi_2, \ldots, \phi_k$ is a proof of ϕ.

Show that $\models \phi$ by induction on k, using

1. If ψ is an axiom then $\models \psi$
2. If the inputs to a rule of inference are valid then so is the output.

lide 18

Proving Completeness

Define ϕ to be consistent if not $\vdash \neg\phi$.

Define ϕ to be satisfiable if there exists a structure M and world w such that $M, w \models \phi$.

To prove: $\models \phi$ then $\vdash \phi$.

We prove: if ϕ is consistent then ϕ is satisfiable. (*)

This suffices: if not $\vdash \phi$
then not $\vdash \neg\neg\phi$
so $\neg\phi$ is satisfiable (by (*))
so not $\models \phi$.

Slide 19

Define $\texttt{subformulas}^+(\phi)$ to be
$\texttt{subformulas}(\phi) \cup \{\neg\psi \mid \psi \in \texttt{subformulas}(\phi)\}$.

Given a set $X \subseteq \texttt{subformulas}^+(\phi)$, define

$$\phi_X = \bigwedge_{\psi \in X} \psi$$

Define $X \subseteq \texttt{subformulas}^+(\phi)$ to be an *atom* if

1. ϕ_X is consistent
2. for all larger sets $Y \subseteq \texttt{subformulas}^+(\phi)$ such that $X \subset Y$, ϕ_Y is not consistent.

Slide 20

Now construct the structure $M = \langle W, \pi, \mathcal{K}_1, \ldots, \mathcal{K}_n \rangle$ where

1. W is the set of atoms of ϕ
2. $\pi(w)(p) = \texttt{true}$ iff $p \in w$
3. $w\mathcal{K}_i w'$ iff $w/K_i = w'/K_i$

where $w/K_i = \{\psi \mid K_i\psi \in w\}$

lide 21

Lemma 1: Let $X_1 \ldots, X_k$ be the set of all atoms of ϕ. Then $\vdash \phi_{X_1} \vee \ldots \vee \phi_{X_k}$.

Proof idea: if X is an inconsistent subset of $\texttt{subformulas}^{+}(\phi)$, then $\vdash \neg\phi_X$.

Lemma 2: For all $\psi \in \texttt{subformulas}^{+}(\phi)$ and worlds w of M, we have $M, w \models \psi$ iff $\psi \in W$.

Proof idea: induction on the complexity of ψ

So: if ϕ is consistent, then there exists an atom w containing ϕ, so there $M, w \models \phi$.

lide 22

Deciding Validity

Note that the proof actually shows that if ϕ is satisfiable iff there exists a model for ϕ with $2^{|\phi|}$ worlds.

This implies that there is an algorithm that decides if ϕ is satisfiable:

Construct all structures of size $2^{|\phi|}$.

Test if any of these satisfies ϕ, if so, return "yes", else return "no".

Slide 23

Axioms for Common Knowledge

Adding the following axioms and rule of inference gives a sound and complete axiomatization for $\mathcal{L}_{\{\mathcal{K}_1,\ldots,\mathcal{K}_n,C_G\}}$.

C1. $M \models E_G\varphi \iff \bigwedge_{i=1}^{m} K_i\varphi$

C2. $M \models C_G\varphi \Rightarrow E_G(\varphi \wedge C_G\varphi)$

Rules of Inference

RC. If $\vdash \varphi \Rightarrow E_G(\psi \wedge \varphi)$ then $\vdash \varphi \Rightarrow C_G\psi$

Slide 24

In the completeness proof, the same construction of M works when we add common knowledge.

For the proof of Lemma 2, we use

Lemma: Let R be the set of atoms w' such that $w \sim_G w'$ in M. Then $\vdash \phi_w \Rightarrow C_G(\bigvee_{w' \in R}(\phi_{w'}))$.

lide 25

Axioms for Distributed Knowledge

Adding the folowing axioms gives a sound and complete axiomatization when we add D_G to the language:

$\models D_{\{i\}}\phi \iff K_i\phi$

$\models D_G\phi \Rightarrow D_{G'}\phi$ if $G \subseteq G'$