advanced logic

2018 02 28

lecture 8

overview

- proof systems
- temporal logic using temporal frames

overview

- proof systems
- temporal logic using temporal frames

proof system for basic modal logic

extension:

$\vdash \phi$ if ϕ is a tautology from prop1

modal distribution (!):

$\vdash \Box(\phi \to \psi) \to \Box\phi \to \Box\psi$

modus ponens:

if $\vdash \phi \to \psi$ and $\vdash \phi$ then $\vdash \psi$

necessitation:

if $\vdash \phi$ then $\vdash \Box\phi$

substitution:

if $\vdash \phi$ then $\vdash \phi^\sigma$ for every substitution σ

recall: admissible rule definition

if provability of all of $\phi_1, \ldots, \phi_n$ implies provability of ψ,

then we have an admissible rule :

$$\frac{\phi_1 \ldots \phi_n}{\psi}$$

admissible rule DISTR

we have shown the following rule (scheme) DISTR to be admissible:

$$\frac{\phi \to \psi}{\Box\phi \to \Box\psi}$$

we can use DISTR in derivations

admissible rule PROP

PROP is a useful admissible proof rule (scheme):

if $(\phi_1 \wedge \ldots \wedge \phi_n) \rightarrow \psi$ is a tautology of prop1

then for every substitution σ the following is an admissible proof rule:

$$\frac{\phi_1^\sigma \ldots \phi_n^\sigma}{\psi^\sigma}$$

example derivation

if $\vdash \Box(\phi \wedge \psi)$ then $\vdash \Box\phi \wedge \Box\psi$

1.	$\Box(\phi \wedge \psi)$	assumption
2.	$a \wedge b \rightarrow a$	tautology from prop1
3.	$\phi \wedge \psi \rightarrow \phi$	subst, 2
4.	$\Box(\phi \wedge \psi) \rightarrow \Box\phi$	DISTR, 3
5.	$a \wedge b \rightarrow b$	tautology from prop1
6.	$\phi \wedge \psi \rightarrow \psi$	subst, 3
7.	$\Box(\phi \wedge \psi) \rightarrow \Box\psi$	DISTR, 6
8.	$\Box(\phi \wedge \psi) \rightarrow \Box\phi \wedge \Box\psi$	PROP, 4, 7

In the PROP-step we use the tautology
$(a \rightarrow b) \wedge (a \rightarrow c) \rightarrow (a \rightarrow b \wedge c)$

soundness and completeness

the proof system K is sound and complete with respect to all frames

$$\vdash_K \phi \quad \Leftrightarrow \quad \models \phi$$

consider the following axioms

distribution

DB: $\Box(p \to q) \to (\Box p \to \Box q)$

truth axiom or veridicality

A1: $\Box p \to p$

positive introspection

A2: $\Box p \to \Box\Box p$

negative introspection

A3: $\neg\Box p \to \Box\neg\Box p$

frame correspondences

for all frames $\mathcal{F} = (W, R)$ we have:

$\mathcal{F} \models$ A1 iff R is reflexive

$\mathcal{F} \models$ A2 iff R is transitive

$\mathcal{F} \models$ A3 iff R is euclidean

R is euclidean if: $\forall xyz\,(Rxy \wedge Rxz \to Ryz)$

reflexive frames are characterized by A1

reflexive-transitive frames are characterized by A1 and A2

frames with equivalence relations are characterized by A1 and A2 and A3

remark

Assume that a binary relation R is reflexive and euclidean.

Suppose that Rxy.

Because R is reflexive, we have Rxx.

Because R is euclidean, because of Rxy and Rxx we have Ryx.

So R is symmetric.

we extend system K step by step

system T: truth axiom added

A1: $\Box p \rightarrow p$

system $S4$: positive introspection added

A2: $\Box p \rightarrow \Box\Box p$

system $S5$: negative introspection added

A3: $\neg\Box p \rightarrow \Box\neg\Box p$

proof system: remark

we use Hilbert systems K, T, $S4$, $S5$

we can easily imagine other similar Hilbert proof systems

there are usually various options in the design of a proof system

for prop1:

natural deduction corresponds to lambda,

and Hilbert proofs correspond to Combinatory Logic

four times soundness and completeness

K is sound and complete for all frames

T is sound and complete for all reflexive frames

$S4$ is sound and complete for all reflexive-transitive frames

$S5$ is sound and complete for all frames with R an equivalence relation

we can use this to show a formula is not derivable in a proof system

example

show that $A3 = \neg\Box p \to \Box\neg\Box p$ is not derivable in $S4$

we give a reflexive-transitive frame in which $A3$ is not true

then we use soundness and completeness: if not true then not derivable

the frame we use: $(\{w, v\}, \{(w, w), (w, v), (v, v)\})$

with the valuation $V(p) = \{v\}$ we have $A3$ not true in w

$w \models \neg\Box p$ because $(w, w) \in R$ and $w \not\models p$

$v \models \Box p$ hence $v \not\models \neg\Box p$ and because also $(w, v) \in R$ we have $w \not\models \Box p$

derivation in proof system T: example

1. $\Box r \rightarrow r$
2. $\Box(p \rightarrow q) \rightarrow (p \rightarrow q)$
3. $(a \rightarrow (b \rightarrow c)) \rightarrow ((a \wedge b) \rightarrow c)$
4. $(\Box(p \rightarrow q) \rightarrow (p \rightarrow q)) \rightarrow ((\Box(p \rightarrow q) \wedge p) \rightarrow q)$
5. $(\Box(p \rightarrow q) \wedge p) \rightarrow q$

how should we annotate the steps?

derivation in S5: example

we prove $\vdash_{S5} \neg\Box\neg\Box p \to p$

1. $\neg\Box p \to \Box\neg\Box p$ (A3)

2. $\neg\Box\neg\Box p \to \Box p$ (PROP, 1)

3. $\Box p \to p$ (A1)

4. $\neg\Box\neg\Box p \to p$ (PROP, 2, 3)

Which tautologies from prop1 do we use?

$(\neg a \to b) \to (\neg b \to a)$, and

$((a \to b) \wedge (b \to c)) \to (a \to c)$

learning goals proof systems

make (very) elementary derivations

detect a mistake in a derivation

know and be able to use the soundness and completeness results

not necessary to know the axioms and the names of the proof systems

know the correspondence of a given axiom with a frame property

overview

- proof systems
- temporal logic using temporal frames

different approaches to temporal logic

linear time logic
Pnueli

branching time logic
Ben-Ari, Manna, Pnueli, Clarke and Emerson

more temporal logic
Kupferman, Venema

temporal logic: linear time and branching time

Moshe Vardi
paper

Rob van Glabbeek
paper

temporal model: definition

first approach to temporal logic: a special case of basic modal logic

definition: a frame $\mathcal{F} = (T, <)$ is a temporal frame if

$<$ is irreflexive: not $t < t$ for all t, and

$<$ is transitive: if $t < u$ and $u < v$ then $t < v$

example: $(\mathbb{N}, <)$ is a temporal frame

definition: a temporal model is

a temporal frame $(T, <)$ with a valuation $V : \mathsf{Var} \to \mathcal{P}(T)$

remark irreflexivity

recall: irreflexivity is not modally definable

temporal model: example

$\mathcal{M} = (\mathbb{N}, <, V)$ with $V(q) = \{n \mid n \geq 1000\}$ and $V(r) = \{2n \mid n \in \mathbb{N}\}$

then we have:

$0 \models \Diamond\Box q$

$n \not\models \Diamond\Box r$ for an arbitrary $n \in \mathbb{N}$

$\mathcal{M} \models \Box\Diamond r$

$\mathcal{M} \models \Box\Diamond\neg r$

properties of temporal frames

we consider some properties of temporal frames

with the intuition of ‘time’ in mind

some are definable in basic modal logic and some are not

right-linearity

intuition: all future points are related

definition: $(x < y) \wedge (x < z) \rightarrow (y < z) \vee (y = z) \vee (z < y)$

right-linearity is modally definable (see exercise class 4)

by $(\Diamond p \wedge \Diamond q) \rightarrow \Diamond(p \wedge \Diamond q) \vee \Diamond(p \wedge q) \vee \Diamond(\Diamond p \wedge q)$

and also by $\Box((p \wedge \Box p) \rightarrow q) \vee \Box((q \wedge \Box q) \rightarrow p)$

right-branching

intuition: right-branching is not-right-linear

so some point has two unrelated points in the future

definition: there exist x, y, z such that $x < y$ and $x < z$ but

$\neg(y < z) \wedge y \neq z \wedge \neg(z < y)$

right-branching is not modally definable

why?

discrete

intuition: every point with a successor has an immediate successor

definition: $(x < y) \rightarrow \exists z : x < z \wedge \neg \exists u : (x < u) \wedge (u < z)$

discreteness is modally definable in basic temporal logic (later)

dense

intuition: between any two points is a third one

definition: $x < z \to \exists y \, (x < y \wedge y < z)$

density is modally definable: by $\Diamond p \to \Diamond\Diamond p$

example

temporal frame: $(\{0,1\} \cup [2,3], <)$ with $<$ as usual

not dense: there is no x such that $0 < x < 1$

not discrete: 2 has no immediate successor

temporal frame $(\{0\} \cup \{2^{-n} \mid n \in \mathsf{nat}\}, <)$ with $<$ as usual

not dense: there is no x such that $2^{-1} < x < 1$

not discrete: 0 has a successor (for example 1) but no immediate successor

temporal frame $(\{0\}, \emptyset)$ is both dense and discrete