modally definable frame properties

property $P$ is modally definable if there exists a formula $\phi$ such that:

$\mathcal{F}$ has property $P$ iff $\mathcal{F} \models \phi$ (for every frame $\mathcal{F}$)

how do we prove this for given $P$ and $\phi$ usually?

assume a frame $\mathcal{F}$ with property $P$, prove that $\mathcal{F} \models \phi$

assume a frame $\mathcal{F}$ without property $P$, prove that $\mathcal{F} \not\models \phi$

that is, find a valuation $V$ and a world $w$ in $\mathcal{F}$ such that $\mathcal{F}, V, w \not\models \phi$

not modally definable frame properties

how do we prove that property $P$ is not modally definable?

suppose (towards a contradiction) that $P$ is modally definable by $\phi$

find ‘bisimilar’ frames $\mathcal{F}_1$ and $\mathcal{F}_2$ such that $\mathcal{F}_1$ has property $P$ but $\mathcal{F}_2$ does not have property $P$, then

$\mathcal{F}_1 \models \phi$, but there is a valuation $V_2$ and a world $w_2$ such that $\mathcal{F}_2, V_2, w_2 \not\models \phi$

use $V_2$ and $w_2$ to find $V_1$ and $w_1$ such that $\mathcal{F}_1, V_1, w_1$ and $\mathcal{F}_2, V_2, w_2$ are bisimilar

by assumption on $\phi$ we have $\mathcal{F}_1, V_1, w_1 \models \phi$

by ‘bisimilar equivalent to modal equivalence’ we have $\mathcal{F}_2, V_2, w_2 \models \phi$

contradiction with $\mathcal{F}_2, V_2, w_2 \not\models \phi$
operator definable

\[ \Delta \text{ a modal operator (modality) with } n \text{ arguments} \]

\[ \Delta \text{ is definable if there is a formula } \zeta(\rho_1, \ldots, \rho_n) \text{ such that} \]

\[ \Delta(\phi_1, \ldots, \phi_n) \text{ modally equivalent to } \zeta(\phi_1, \ldots, \phi_n) \]

(for all formulas \( \phi_1, \ldots, \phi_n \))

how to show that an operator is not modally definable?

suppose it is definable by some formula

find two bisimilar worlds such that

in one the formula should hold and in the other it shouldn’t hold

temporal logic: linear time and branching time

Moshe Vardi

paper

Rob van Glabbeek

paper

overview

• multi-modal logic

• towards propositional dynamic logic

overview

• multi-modal logic

• towards propositional dynamic logic
multi-modal logic

we assume a set of labels $I$
we consider for every label $i$ a relation $R_i$
we consider for every label $i$ a box-formula $\langle i \rangle \phi$
we already know various instances of multi-modal logic:
$I = \emptyset$ gives propositional logic
$I = \{0\}$ gives basic modal logic
$I = \{F, P\}$ gives temporal logic
and we will see $I = \text{Prog}(A)$ gives propositional dynamic logic

multi-modal logic: frames and models

let $I$ be a set of indices or labels
an $I$-frame is a pair $(W, \{R_i | i \in I\})$ with
$W \neq \emptyset$ a set of worlds or states
$R_i \subseteq W \times W$ for every $i \in I$
an $I$-model is a triple $(W, \{R_i | i \in I\}, V)$ with
$(W, \{R_i | i \in I\})$ an $I$-frame and $V : \text{Var} \to \mathcal{P}(W)$ a valuation

multi-modal logic: book

MLOM chapter 10.1

especially interesting if there is some connection between the $R_i$
such as past is the inverse of future

multi-modal logic: truth and validity

let $M = (W, \{R_i | i \in I\}, V)$ be an $I$-model
$M, w \models \phi$ is defined by induction on the definition of formulas
important clauses:
$M, w \models \langle \alpha \rangle \phi$ iff $M, v \models \phi$ for some $v$ with $R_\alpha Wv$
$M, w \models [\alpha] \phi$ iff $M, v \models \phi$ for all $v$ with $R_\alpha Wv$

truth in a model, valid in a frame, universal validity are defined as before
example

use index set \{a, b, c\}

give a model with a world where the formula

\((a)((b)[a]p \land [c]¬(a)p)\) is true

multi-modal logic: bisimulation

we use one index set \(I\)

let \(\mathcal{M} = (W, \{R_i \mid i \in I\}, V)\) and \(\mathcal{M}' = (W', \{R'_i \mid i \in I\}, V')\) be \(I\)-models

\(\emptyset \neq Z \subseteq W \times W'\) is a bisimulation if for every \((w, w')\in Z\)

\(w \in V(p)\) if and only if \(w' \in V'(p)\)

if \(R_i w v\) then there is \(v'\) with \(R'_i w' v'\) and \((v, v') \in Z\)

if \(R'_i w' v'\) then there is \(v\) with \(R_i w v\) and \((v, v') \in Z\)

bisimulation and modal equivalence

if two worlds are bimisimilar, then they are modally equivalent

we work with multi-modal formulas and \(I\)-models

modal equivalence and bisimulation

under the restriction that every \(R_i\) is finitely branching

(which does not imply that the model is finitely branching)

two worlds are bisimilar if and only if they are modally equivalent

theorem by Hennessy and Milner (1985)
until and next

until not definable in basic modal logic in temporal frames
until not definable in temporal modal logic in temporal frames
next not definable in basic modal logic in temporal frames

overview

multi-modal logic

towards propositional dynamic logic

for program verification

prove that a program meets its specification

while programs: example gcd

```plaintext
while y ≠ 0 do
  begin
    z := x mod y;
    x := y;
    y := z;
  end
```

x, y, z are program variables running over integers

a state assigns values to program variables

a trace is a sequence of states, example:

(15, 27, 0), (15, 27, 15), (27, 27, 15), (27, 15, 15), (27, 15, 12), (15, 15, 12),
(15, 12, 12), (15, 12, 3), (12, 12, 3), (12, 3, 3), (3, 3, 0), (3, 0, 0)
while programs: definition

basic program: assignment
\[ x := t \]

test
a formula

sequential composition
\[ \alpha; \beta \]

conditional or guarded choice
if \( \phi \) then \( \alpha \) else \( \beta \)

while or iteration
while \( \phi \) do \( \alpha \)

program correctness: first ideas

correctness specification:
formal description of how the program is supposed to behave

for our gcd program:
if the input values of \( x \) and \( y \) are positive integers \( c \) and \( d \),
then the output value of \( x \) is the gcd of \( c \) and \( d \), and
the program terminates

program correctness: more

we restrict attention to input-output behaviour

specification consists of
input condition \( \phi \) and output condition \( \psi \)

partial correctness:
if the program starts satisfying \( \phi \),
and if it halts,
then when it halts \( \psi \) is satisfied

total correctness:
it is partially correct,
and it terminates whenever started satisfying \( \phi \)

Hoare Logic

introduced by Tony Hoare (1934) in 1969
following work by Floyd from 1967
there is already work by Turing

Turing Award 1980
quicksort, Hoare Logic, Communicating Sequential Processes (CSP)
Hoare Logic towards dynamic logic

we use the programs as indices in multi-modal logic
the possible worlds are viewed as states

\((\alpha)\phi\)
we can execute \(\alpha\) and halt in state satisfying \(\phi\)

\([\alpha]\phi\)
if \(\alpha\) halts then in a state satisfying \(\phi\)

\(\{\phi\}\alpha\{\psi\}\) is encoded as \(\phi \rightarrow [\alpha]\psi\)

regular programs

atomic
\(a\) from a set of atomic programs

test
\(\phi?\) with \(\phi\) a test

sequential composition
\(\alpha;\beta\)

non-deterministic choice
\(\alpha \cup \beta\)

iteration
\(\alpha^*\)

while programs and regular programs

while programs can be encoded as regular programs:

if \(\phi\) then \(\alpha\) else \(\beta\) = \(\phi?; \alpha \cup \neg\phi?; \beta\)

while \(\phi\) do \(\alpha\) = \((\phi?; \alpha)^*; \neg\phi?\)
two approaches: exogenous logic and endogenous logic

exogenous: programs are explicit in the language

dynamic logic and Hoare Logic are exogenous

temporal logic and method by Floyd are endogenous

MLOM chapter 14.2