model checking using dynamic logic: KeY

specification in Java modeling language
is transformed into formula in dynamic logic
and compared with semantics in dynamic logic

more generally: dynamic logic is useful for sequential programming

see wiki for KeY
see home page of KeY

a conference: advances in modal logic

overview

- more propositional dynamic logic
- towards proof systems for modal logic
overview

more propositional dynamic logic

towards proof systems for modal logic

semantics of PDL

we have programs built from atomic programs,
and possibly dependent on propositions

we have formulas built from atomic formulas,
and possibly dependent on programs

truth of $\phi$ depends on
truth of strictly smaller formulas and relation of strictly smaller programs

consider for example $\phi = (a)p$

relation of $\alpha$ depends on
relation of strictly smaller programs and truth of strictly smaller formulas

consider for example $\alpha = p?; a$

alternative semantics

$\mathcal{M}, w \models (\alpha)\phi$ if and only if
there exists $w'$ such that $\mathcal{M}, w, w' \models \alpha$ and $\mathcal{M}, w' \models \phi$

$\mathcal{M}, w, w' \models a$ if $(w, w') \in R_a$ with $a$ an atomic program
extend this to sequential composition, choice, iteration, and test
$\mathcal{M}, w, w' \models ?\phi$ if $w = w'$ and $\mathcal{M}, w \models \phi$

obvious question

we start with $W$, for every atomic program $a$ a relation $R_a$, and $V$
we get both a semantics according to the PDL-model,
and one following the book

are the two semantics equivalent?
if $p$ then $a$ else $b$ encoded as $(p; a) \cup (\neg p; b)$

some formulas that are valid in all PDL-frames

$$
(\alpha; \beta)p \leftrightarrow (\alpha)(\beta)p \\
(\alpha \cup \beta)p \leftrightarrow (\alpha)p \lor (\beta)p \\
(\alpha^*)p \leftrightarrow p \lor (\alpha)(\alpha^*)p \\
(p?q) \leftrightarrow p \land q \\
[\alpha^*]p \leftrightarrow p \land [\alpha^*](p \rightarrow [\alpha]p) \text{ (induction principle)}
$$

example

while $p$ do $a$ encoded as $(p?; a)^*; \neg p$

formula $(while \ p \ do \ a)q$ is valid in model $\mathcal{M}$ in state $x$ iff there exist $n \geq 0$ and there exist $x_1, \ldots, x_n$ such that

$\mathcal{M}, x_1 \models p \land R_{a(x_0x_1)}$ \\
$\mathcal{M}, x_1 \models p \land R_{a(x_1x_2)}$ \\
$\vdots$ \\
$\mathcal{M}, x_{n-1} \models p \land R_{a(x_{n-1}x_n)}$ \\
$\mathcal{M}, x_n \not\models p \land \mathcal{M}, x_n \models q$

example

bisimulation for PDL-models

do we need to consider all infinitely many relations?

no, it is sufficient to consider all $R_a$ with $a$ atomic

because PDL-constructors are safe for bisimulation

intersection is not safe for bisimulation

inverse is not safe for bisimulation
\[ W = \{ u, v, w \} \]
\[ R_a = \{ (u, v), (u, w), (v, w), (w, v) \} \]
\[ V(p) = \{ u, v \} \]

we have \( u \models (a)\neg p \land (a)p \)

we have \( v \models [a]\neg p \)

we have \( w \models [a]p \)

in every world (state) we have \( (a^*)(aa)^*p \land (a^*)[(aa)^*] \neg p \)

\[ W = \{ s, t, u, v \} \]
\[ R_a = \{ (t, u), (v, t), (s, u), (u, s) \} \]
\[ R_b = \{ (u, v), (v, u), (s, t), t, s \} \]
\[ V(p) = \{ u, v \} \]
\[ V(q) = \{ t, v \} \]

we have \( p \leftrightarrow [(ab^*a^*)^*p \]

we have \( q \leftrightarrow [(ba^*b^*)^*q \]

\( p \) is alternatively true and false along all execution paths of \( a \) starting in current state with \( p \) true

\[ p \land [a^*]((p \rightarrow [a]\neg p) \land (\neg p \rightarrow [a]p)) \]

and equivalently

\[ [(aa)^*p \land [a(aa)^*] \neg p \]

which of the two directions is valid in PDL?

\[ [(a \cup b)^*p \leftrightarrow [a^*]p \land [b^*]p \]
example

which property is expressed?

\[(\text{while } p \text{ do } \alpha) \top \leftrightarrow (\alpha^*) \neg p\]

overview

- more propositional dynamic logic
- towards proof systems for modal logic

provability and derivability

soundness and completeness for pred1:
\[\vdash \phi \text{ if and only if } \models \phi\]

now for modal logic(s) ?

proof system for minimal modal logic

extension:
\[\vdash \phi \text{ if } \phi \text{ is a tautology from prop1}\]

modal distribution:
\[\vdash \Box(p \rightarrow q) \rightarrow \Box p \rightarrow \Box q\]

modus ponens:
if \[\vdash \phi \rightarrow \psi \text{ and } \vdash \phi\] then \[\vdash \psi\]

necessitation:
if \[\vdash \phi\] then \[\vdash \Box \phi\]

definition of ♦:
\[\Box \phi is \neg \Box \neg \phi\]
Plato (400 BC):

true opinion is in general insufficient for knowledge

see Stanford Encyclopedia of Philosophy