Formal Specification and Verification

Propositional Dynamic Logic 1

15.07.2014

Viorica Sofronie-Stokkermans

Matthias Horbach

e-mail: {sofronie,horbach}@uni-koblenz.de

Overview

- **Model checking:**

  Finite transition systems / CTL properties

  States are "entities" (no precise description, except for labelling functions)

  No precise description of actions (only $\rightarrow$ important)

Overview

- **Model checking:**

  Finite transition systems / CTL properties

  States are "entities" (no precise description, except for labelling functions)

  No precise description of actions (only $\rightarrow$ important)

Extensions in two possible directions:

- More precise description of the actions/events
  - Propositional Dynamic Logic
  - Hoare logic
- More precise description of states (and possibly also of actions)
  - succinct representation: formulae represent a set of states
  - deductive verification

Motivation

Example Program: Square

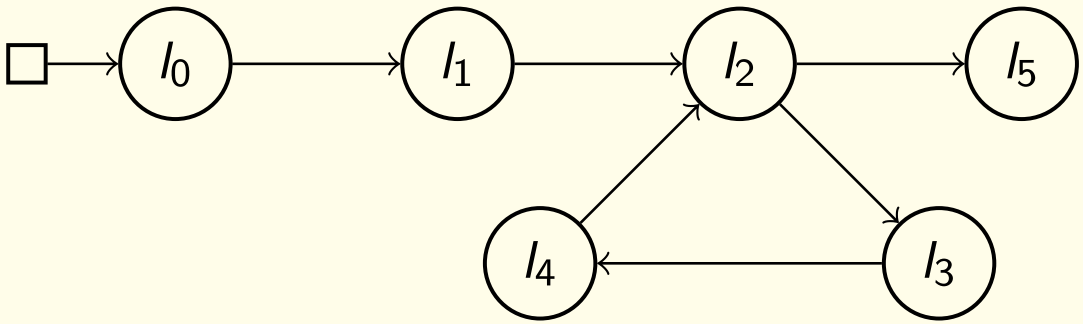
```
I := 0;
Y := 0;
while I < X do
  Y := Y+2*I+1;
  I := I+1
od
```

We would like to prove something like "$A\Diamond$(terminated $\wedge$ Y=X*X)".

Motivation

Example Program: Square

```
I := 0;
Y := 0;
while I < X do
  Y := Y+2*I+1;
  I := I+1
od
```

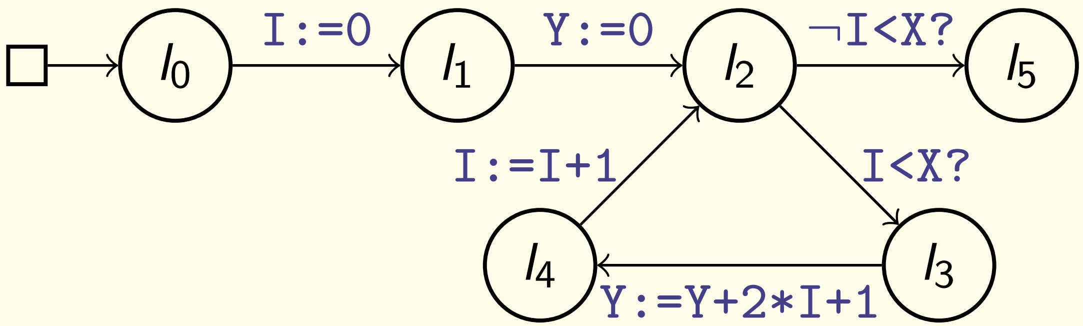


We would like to prove something like "$A\Diamond$(terminated $\wedge$ `Y=X*X`)".

Motivation

Example Program: Square

```
I := 0;
Y := 0;
while I < X do
  Y := Y+2*I+1;
  I := I+1
od
```



We would like to prove something like "$A\Diamond$(terminated $\wedge$ Y=X*X)".

CTL* too weak: Transitions carry meaning.

Dynamic Logic: [prog]Y=X*X

Motivation

A Simple Programming Language

Logical basis

Typed first-order predicate logic
(Types, variables, terms, formulas, . . .)

Assumption for examples

The signature contains a type Nat and appropriate symbols:

- function symbols $0, s, +, *$
  (terms s(0), s(s(0)), . . . written as 1,2, . . .)
- predicate symbols $\doteq, \leq, <, \geq, >$

NOTE: This is a “convenient assumption” not a definition

Motivation

Programs

- Assignments: $X := t$ X: variable, t:term
- Test: if B then a else b fi
  B: quant.-free formula, a, b: programs
- Loop: while B do a od
  B: quantifier-free formula, a: program
- Composition: a; b a, b programs

WHILE is computationally complete

Motivation

WHILE: Examples

Compute the square of X and store it in Y

$$Y := X * X$$

If X is positive then add one else subtract one

$$\text{if } X > 0 \text{ then } X := X + 1 \text{ else } X := X - 1 \text{ fi}$$

Motivation

WHILE: Example - Square of a Number

Compute the square of X (the complicated way)

Making use of: $n^2 = 1 + 3 + 5 + \cdots + (2 * n - 1)$

```
I := 0;
Y := 0;
while I < X do
  Y := Y+2*I+1;
  I := I+1
od
```

Motivation

WHILE: Operational Semantics

Given

A (fixed) first-order structure $\mathcal{A}$ interpreting the function and predicate symbols in the signature

State

$s = (\mathcal{A}, \beta)$ where β is a variable assignment (i.e. function interpreting the variables)

Motivation

State update

$s[e/X] = (\mathcal{A}, \beta[X \mapsto e])$

with $\beta[X \mapsto e](Y) = \begin{cases} e & \text{if } Y = X \\ \beta(Y) & \text{otherwise} \end{cases}$

Motivation

Define the relation $R(\alpha)$ as follows (we write $s[\alpha]s'$ instead of $sR(\alpha)s'$):

- $s[X := t]s'$ iff $s' = s[s(t)/X]$
- $s[\text{if } B \text{ then } \alpha \text{ else } \beta \text{ fi}]s'$ iff $s \models B$ and $s[\alpha]s'$ or $s \models \neg B$ and $s[\beta]s'$.
- $s[\text{while } B \text{ do } \alpha \text{ od}]s'$ iff there are states $s = s_0, \ldots, s_t = s'$ s.t.
  $s_i \models B$ for $0 \leq i \leq t-1$ and $s_t \models \neg B$ and $s_0[\alpha]s_1, s_1[\alpha]s_2, \ldots, s_{t-1}[\alpha]s_t$
- $s[\alpha; \beta]s'$ iff there is a state s'' such that $s[\alpha]s''$ and $s''[\beta]s'$

If α is a deterministic program, $[\alpha]$ is a partial function.

Motivation

A Different Approach to WHILE

Programs

- $X := t$ (atomic program)
- $\alpha ; \beta$ (sequential composition)
- $\alpha \cup \beta$ (non-deterministic choice)
- α^* (non-deterministic iteration, n times for some $n \geq 0$)
- $F?$ (test)
  remains in initial state if F is true,
  does not terminate if F is false

Motivation

Restriction to deterministic programs

Non-deterministic program constructors may only be used in

if B then α else β fi $\equiv (B?;\alpha) \cup ((\neg B)?;\beta)$

while B do α od $\equiv (B?;\alpha)^*;(\neg B)?$

Motivation

Expressing Program Properties

Logic for expressing properties

Full first-order logic (usually with arithmetic)

Partial correctness assertion (Hoare formula)

$$\{P\}\alpha\{Q\}$$

Meaning:
If α is started in a state satisfying P and terminates, then its final state satisfies Q.

Formally:
$\{P\}\alpha\{Q\}$ is valid iff for all states s, s', if $s \models P$ and $s[\alpha]s'$, then $s' \models Q$.

Examples

$\{X > 0\}X := X + 1\{X > 1\}$

$\{\text{even}(X)\}X := X + 2\{\text{even}(X)\}$
where $\text{even}(X) \equiv \exists Z(X = 2 * Z)$

$\{\mathit{true}\}\alpha_{\text{square}}\{Y = X * X\}$

Examples

$\{X > 0\} X := X + 1 \{X > 1\}$

$\{\text{even}(X)\} X := X + 2 \{\text{even}(X)\}$
where $\text{even}(X) \equiv \exists Z (X = 2 * Z)$

$\{\mathit{true}\} \alpha_{\text{square}} \{Y = X * X\}$

Verification: Use annotation of programs with "invariants"

Dynamic Logic

The idea of dynamic logic

- Annotated programs use formulas within programs
- Dynamic Logic uses programs within formulas
- Instead of "assert F" after program segment α, write: $[\alpha]F$

$\mapsto$ multi-modal logic

Dynamic Logic

Dynamic logic is a language for specifying programming languages.

The original work on dynamic logic is by Vaughan Pratt (1976) and by David Harel (1979).

Propositional Dynamic Logic

Propositional dynamic logic (PDL) is a multi-modal logic with structured modalities.

For each program α, there is:

– a box-modality $[\alpha]$ and

– a diamond modality $\langle\alpha\rangle$.

PDL was developed from first-order dynamic logic by Fischer-Ladner (1979) and has become popular recently.

Here we consider regular PDL.

Propositional Dynamic Logic

Syntax

Prog set of programs

$\text{Prog}_0 \subseteq \text{Prog}$: set of atomic programs

Π: set of propositional variables

The set of formulae $\textbf{Fma}^{PDL}_{\textbf{Prog},\Pi}$ of (regular) propositional dynamic logic and the set of programs P_0 are defined by simultaneous induction as follows:

PDL: Syntax

Formulae:

$$
\begin{array}{llll}
F, G, H & ::= & \bot & \text{(falsum)} \\
& \mid & \top & \text{(verum)} \\
& \mid & p & p \in \Pi_0 \text{ (atomic formula)} \\
& \mid & \neg F & \text{(negation)} \\
& \mid & (F \wedge G) & \text{(conjunction)} \\
& \mid & (F \vee G) & \text{(disjunction)} \\
& \mid & (F \rightarrow G) & \text{(implication)} \\
& \mid & (F \leftrightarrow G) & \text{(equivalence)} \\
& \mid & [\alpha]F & \text{if } \alpha \in \text{Prog} \\
& \mid & \langle\alpha\rangle F & \text{if } \alpha \in \text{Prog}
\end{array}
$$

Programs:

$$
\begin{array}{llll}
\alpha, \beta, \gamma & ::= & \alpha_0 & \alpha_0 \in \text{Prog}_0 \text{ (atomic program)} \\
& \mid & F? & F \text{ formula (test)} \\
& \mid & \alpha; \beta & \text{(sequential composition)} \\
& \mid & \alpha \cup \beta & \text{(non-deterministic choice)} \\
& \mid & \alpha^* & \text{(non-deterministic repetition)}
\end{array}
$$

Semantics

A PDL structure $\mathcal{K} = (S, R(), I)$ is a multimodal Kripke structure with an accessibility relation for each atomic program. That is it consists of:

- a non-empty set S of states
- an interpretation $R() : \mathsf{Prog}_0 \to S \times S$ of atomic programs that assigns a transition relation $R(\alpha)$ to each atomic program α
- an interpretation $I : \Pi \times S \to \{0, 1\}$

PDL: Semantics

The interpretation of PDL relative to a PDL structure $\mathcal{K} = (S, R(), I)$ is defined by extending $R()$ to Prog and extending I to $\mathrm{Fma}^{PDL}_{\mathrm{Prop}_0}$ by the following simultaneously inductive definition:

Interpretation of formulae/programs

$$
\begin{aligned}
val_{\mathcal{K}}(p, s) &= I(p, s) \qquad \text{if } p \in \Pi \\
val_{\mathcal{K}}(\neg F, s) &= \neg_{\text{Bool}} val_{\mathcal{K}}(F, s) \\
val_{\mathcal{K}}(F \wedge G, s) &= val_{\mathcal{K}}(F, s) \wedge_{\text{Bool}} val_{\mathcal{K}}(G, s) \\
val_{\mathcal{K}}(F \vee G, s) &= val_{\mathcal{K}}(F, s) \vee_{\text{Bool}} val_{\mathcal{K}}(G, s) \\
val_{\mathcal{K}}(F \rightarrow G, s) &= val_{\mathcal{K}}(F, s) \rightarrow_{\text{Bool}} val_{\mathcal{K}}(G, s) \\
val_{\mathcal{K}}(F \leftrightarrow G, s) &= val_{\mathcal{K}}(F, s) \leftrightarrow_{\text{Bool}} val_{\mathcal{K}}(G, s) \\
val_{\mathcal{K}}([\alpha]F, s) = 1 \textit{ iff } & \text{ for all } t \in S \text{ with } (s, t) \in R(\alpha), val_{\mathcal{K}}(F, t) = 1 \\
val_{\mathcal{K}}(\langle\alpha\rangle F, s) = 1 \textit{ iff } & \text{ for some } t \in S \text{ with } (s, t) \in R(\alpha), val_{\mathcal{K}}(F, t) = 1 \\
R([F?]) &= \{(s, s) \mid val_{\mathcal{K}}(F, s) = 1\} \\
& \quad (F? \text{ means: if } F \text{ then skip else do not terminate}) \\
R(\alpha \cup \beta) &= R(\alpha) \cup R(\beta) \\
R(\alpha; \beta) &= \{(s, t) \mid \text{ there exists } u \in S \ s.t.(s, u) \in R(\alpha) \text{ and } (u, t) \in R(\beta)\} \\
R(\alpha^*) &= R(\alpha)^* \\
&= \{(s, t) \mid \text{ there exist } n \geq 0 \text{ and } u_0, \dots, u_n \in S \text{ with} \\
& \qquad s = u_0, t = u_n, (u_0, u_1), \dots, (u_{n-1}, u_n) \in R(\alpha)\}
\end{aligned}
$$

Interpretation of formulae/programs

- $(\mathcal{K}, s)$ satisfies F (notation $(\mathcal{K}, s) \models F$) iff $val_{\mathcal{K}}(F, s) = 1$.
- F is valid in $\mathcal{K}$ (notation $\mathcal{K} \models F$) iff $(\mathcal{K}, s) \models F$ for all $s \in S$.
- F is valid (notation $\models F$) iff $\mathcal{K} \models F$ for all PDL-structures $\mathcal{K}$.

Hilbert-style axiom system for PDL

Axioms

$(D1)$	All propositional logic tautologies
$(D2)$	$[\alpha](A \rightarrow B) \rightarrow ([\alpha]A \rightarrow [\alpha]B)$
$(D3)$	$[\alpha](A \wedge B) \leftrightarrow [\alpha]A \wedge [\alpha]B$
$(D4)$	$[\alpha;\beta]A \leftrightarrow [\alpha][\beta]A$
$(D5)$	$[\alpha \cup \beta]A \leftrightarrow [\alpha]A \wedge [\beta]A$
$(D6)$	$[A?]B \leftrightarrow (A \rightarrow B)$
$(D7)$	$[\alpha^*]A \leftrightarrow A \wedge [\alpha][\alpha^*]A,$
$(D8)$	$[\alpha^*](A \rightarrow [\alpha]A) \rightarrow (A \rightarrow [\alpha^*]A)$

Inference rules

$$MP \qquad \frac{F \qquad F \rightarrow G}{G}$$

$$Gen \qquad \frac{F}{[\alpha]F}$$

We will show that PDL is determined by PDL structures, and has the finite model property.

Soundness and Completeness of PDL

Theorem. If the formula F is provable in the inference system for PDL then F is valid in all PDL structures.

Proof: Induction of the length of the proof, using the following facts:
1. The axioms are valid in every PDL structure. Easy computation.

2. If the premises of an inference rule are valid in a structure $\mathcal{K}$, the conclusion is also valid in $\mathcal{K}$.

(MP) If $\mathcal{K} \models F, \mathcal{K} \models F \rightarrow G$ then $\mathcal{K} \models G$ (follows from the fact that for every state s of $\mathcal{K}$ if $(\mathcal{K}, s) \models F, (\mathcal{K}, s) \models F \rightarrow G$ then $(\mathcal{K}, s) \models G$)

(Gen) Assume that $\mathcal{K} \models F$. Then $(\mathcal{K}, s) \models F$ for every state s of $\mathcal{K}$.
Let t be a state of $\mathcal{K}$. $(\mathcal{K}, t) \models [\alpha]F$ if for all t' with $(t, t') \in R(\alpha)$ we have $(\mathcal{K}, t') \models F$. But under the assumption that $\mathcal{K} \models F$ the latter is always the case. This shows that $(\mathcal{K}, t) \models [\alpha]F$ for all t.

Summary

Today:

- Motivation: WHILE programs and Hoare triples
- Syntax and semantics of PDL
- Soundness of the axiom system

Next time:

- Completeness and decidability
- A sequent calculus for PDL