Scaling Dynamic Logic for Intermediate states

Boriss Shelajev
joint work with Keiko Nakata and Tarmo Uustalu

Institute of Cybernetics at TUT

April 11, 2013

Introduction

Standard sequential program logics are insufficient for reasoning about nonterminating program runs

We extend a dynamic logic with new modalities to talk about resumptions, a pair of intermediate state and residual program

Expressions in DL

The logic consists of expressions of a two sorts

1. programs $(\alpha, \beta, \gamma, \dots)$
2. formulas $(\varphi, \psi, \dots)$

Syntax of programs

We work with non-deterministic and parallel While language and extend it with a special $cont_i$ statement

$$
\begin{aligned}
\mathit{Program}\ p := \quad & \\
& x := a \\
& \textbf{skip} \\
& p; p' \\
& p \mid\mid p' \\
& \textbf{if}\ b\ \textbf{then}\ p_t\ \textbf{else}\ p_f \\
& \textbf{while}\ b\ \textbf{do}\ p \\
& \textbf{cont}_i
\end{aligned}
$$

Syntax of formulas

We introduce two new modalities for reasoning about resumptions

$$\varphi := $$

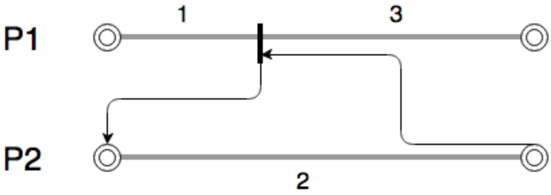
$$x = a$$

$$\varphi \vee \psi \mid \varphi \wedge \psi \mid \varphi \to \psi \mid 0 \mid 1$$

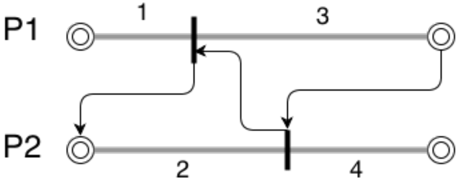
$$\langle p \rangle \varphi \mid [p]\varphi \mid \langle\!\langle p \rangle\!\rangle \varphi \mid [\![p]\!]\varphi$$

Example

$$\langle\langle p1 \rangle\rangle \langle p2 \rangle \langle \mathbf{cont}_0 \rangle \varphi$$



$$[\![p1]\!]\langle\!\langle p2\rangle\!\rangle\langle\mathbf{cont}_1\rangle[\mathbf{cont}_0]\varphi$$



Semantics

$\langle S, \sigma \rangle \rightarrow_{cs} \langle \sigma' \rangle$: states that running S under continuation stack cs from initial state σ terminate in the final state σ'

$\langle S, \sigma \rangle \Rightarrow_{cs} \langle S', \sigma' \rangle$: states that running S under continuation stack cs from initial state σ reaches an intermediate state σ with residual program S'

Natural semantics for While + **cont**

$$\frac{}{\langle x := a, \sigma\rangle \to_{cs} \langle \sigma[x \to [\![a]\!]\sigma]\rangle}\ ass \qquad \frac{}{\langle \mathbf{skip}, \sigma\rangle \to_{cs} \langle \sigma\rangle}\ skip$$

$$\frac{\langle S_1, \sigma\rangle \to_{cs} \langle \sigma'\rangle \quad \langle S_2', \sigma'\rangle \to_{cs} \langle S_2', \sigma''\rangle}{\langle S_1; S_2, \sigma\rangle \to_{cs} \langle \sigma''\rangle}\ comp2$$

$$\frac{[\![b]\!]\sigma = \mathbf{true} \quad \langle S_1, \sigma\rangle \to_{cs} \langle \sigma'\rangle}{\langle \mathbf{if}\ b\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2, \sigma\rangle \to_{cs} \langle \sigma'\rangle}\ ift \qquad \frac{[\![b]\!]\sigma = \mathbf{false} \quad \langle S_2, \sigma\rangle \to_{cs} \langle \sigma'\rangle}{\langle \mathbf{if}\ b\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2, \sigma\rangle \to_{cs} \langle \sigma'\rangle}\ iff$$

$$\frac{[\![b]\!]\sigma = \mathbf{true} \quad \langle S, \sigma\rangle \to_{cs} \langle \sigma'\rangle \quad \langle \mathbf{while}\ b\ \mathbf{do}\ S, \sigma'\rangle \to_{cs} \langle \sigma''\rangle}{\langle \mathbf{while}\ b\ \mathbf{do}\ S, \sigma\rangle \to_{cs} \langle \sigma''\rangle}\ whilet$$

$$\frac{[\![b]\!]\sigma = \mathbf{false}}{\langle \mathbf{while}\ b\ \mathbf{do}\ S, \sigma\rangle \to_{cs} \langle \sigma\rangle}\ whilef$$

$$\frac{\langle cs[i], \sigma\rangle \to_{cs} \langle \sigma'\rangle}{\langle \mathbf{cont}_i, \sigma\rangle \to_{cs} \langle \sigma'\rangle}\ cont$$

Natural semantics for intermediate states excl. final state

$$\frac{}{\langle S,\sigma\rangle \Rightarrow_{cs} \langle S,\sigma\rangle}\ \mathit{init} \quad \text{for ass, if, while}$$

$$\frac{\langle S_1,\sigma\rangle \Rightarrow_{cs} \langle S_1',\sigma'\rangle}{\langle S_1;S_2,\sigma\rangle \Rightarrow_{cs} \langle S_1';S_2,\sigma'\rangle}\ \mathit{comp1}$$

$$\frac{\langle S_1,\sigma\rangle \rightarrow_{cs} \langle \sigma'\rangle \quad \langle S_2,\sigma'\rangle \Rightarrow_{cs} \langle S',\sigma''\rangle}{\langle S_1;S_2,\sigma\rangle \Rightarrow_{cs} \langle S',\sigma''\rangle}\ \mathit{comp2}$$

$$\frac{[\![b]\!]\sigma = \mathbf{true} \quad \langle S_1,\sigma\rangle \Rightarrow_{cs} \langle S_1',\sigma'\rangle}{\langle \mathbf{if}\ b\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2,\sigma\rangle \Rightarrow_{cs} \langle S_1',\sigma'\rangle}\ \mathit{ift} \qquad \frac{[\![b]\!]\sigma = \mathbf{false} \quad \langle S_2,\sigma\rangle \Rightarrow_{cs} \langle S_2',\sigma'\rangle}{\langle \mathbf{if}\ b\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2,\sigma\rangle \Rightarrow_{cs} \langle S_2',\sigma'\rangle}\ \mathit{iff}$$

$$\frac{[\![b]\!]\sigma = \mathbf{true} \quad \langle S,\sigma\rangle \Rightarrow_{cs} \langle S',\sigma'\rangle}{\langle \mathbf{while}\ b\ \mathbf{do}\ S,\sigma\rangle \Rightarrow_{cs} \langle S';\mathbf{while}\ b\ \mathbf{do}\ S,\sigma'\rangle}\ \mathit{while1}$$

$$\frac{[\![b]\!]\sigma = \mathbf{true} \quad \langle S,\sigma\rangle \rightarrow_{cs} \langle \sigma'\rangle \quad \langle \mathbf{while}\ b\ \mathbf{do}\ S,\sigma'\rangle \Rightarrow_{cs} \langle S',\sigma'\rangle}{\langle \mathbf{while}\ b\ \mathbf{do}\ S,\sigma\rangle \Rightarrow_{cs} \langle S',\sigma'\rangle}\ \mathit{while2}$$

$$\frac{\langle cs[i],\sigma\rangle \Rightarrow_{cs} \langle S',\sigma'\rangle}{\langle \mathbf{cont}_i,\sigma\rangle \Rightarrow_{cs} \langle S',\sigma'\rangle}\ \mathit{cont}$$

Final state natural semantics for parallelism

$$\frac{\langle S_1, \sigma\rangle \Rightarrow_{cs} \langle S_1', \sigma'\rangle \quad \langle S_1' || S_2, \sigma'\rangle \rightarrow_{cs} \langle \sigma''\rangle}{\langle S_1 || S_2, \sigma\rangle \rightarrow_{cs} \langle \sigma''\rangle}\ \mathit{fpara}1$$

$$\frac{\langle S_2, \sigma\rangle \Rightarrow_{cs} \langle S_2', \sigma'\rangle \quad \langle S_1 || S_2', \sigma'\rangle \rightarrow_{cs} \langle \sigma''\rangle}{\langle S_1 || S_2, \sigma\rangle \rightarrow_{cs} \langle \sigma''\rangle}\ \mathit{fpara}2$$

$$\frac{\langle S_1, \sigma\rangle \rightarrow_{cs} \langle \sigma'\rangle \quad \langle S_2, \sigma'\rangle \rightarrow_{cs} \langle \sigma''\rangle}{\langle S_1 || S_2, \sigma\rangle \rightarrow_{cs} \langle \sigma''\rangle}\ \mathit{fpara}3$$

$$\frac{\langle S_2, \sigma\rangle \rightarrow_{cs} \langle \sigma'\rangle \quad \langle S_1, \sigma'\rangle \rightarrow_{cs} \langle \sigma''\rangle}{\langle S_1 || S_2, \sigma\rangle \rightarrow_{cs} \langle \sigma''\rangle}\ \mathit{fpara}4$$

Intermediate state natural semantics for parallelism

$$\frac{\langle S_1, \sigma\rangle \Rightarrow_{cs} \langle S_1', \sigma'\rangle \quad \langle S_1' || S_2, \sigma'\rangle \Rightarrow_{cs} \langle S, \sigma''\rangle}{\langle S_1 || S_2, \sigma\rangle \Rightarrow_{cs} \langle S, \sigma''\rangle}\ \mathit{ipara}1$$

$$\frac{\langle S_2, \sigma\rangle \Rightarrow_{cs} \langle S_2', \sigma'\rangle \quad \langle S_1 || S_2', \sigma'\rangle \Rightarrow_{cs} \langle S, \sigma''\rangle}{\langle S_1 || S_2, \sigma\rangle \Rightarrow_{cs} \langle S, \sigma''\rangle}\ \mathit{ipara}2$$

$$\frac{\langle S_1, \sigma\rangle \rightarrow_{cs} \langle \sigma'\rangle \quad \langle S_2, \sigma'\rangle \Rightarrow_{cs} \langle S, \sigma''\rangle}{\langle S_1 || S_2, \sigma\rangle \Rightarrow_{cs} \langle S, \sigma''\rangle}\ \mathit{ipara}3$$

$$\frac{\langle S_2, \sigma\rangle \rightarrow_{cs} \langle \sigma'\rangle \quad \langle S_1, \sigma'\rangle \Rightarrow_{cs} \langle S, \sigma''\rangle}{\langle S_1 || S_2, \sigma\rangle \Rightarrow_{cs} \langle S, \sigma''\rangle}\ \mathit{ipara}4$$

Semantics for modalities

- $\sigma \models_{cs} \langle S \rangle \varphi \iff$

  for some σ' s.t. $S, \sigma \rightarrow_{cs} \sigma'$ we have $\sigma' \models_{cs} \varphi$
- $\sigma \models_{cs} \langle\!\langle S \rangle\!\rangle \varphi \iff$

  for some S', σ' s.t. $S, \sigma \Rightarrow_{cs} S', \sigma'$ we have $\sigma' \models_{S':cs} \varphi$
- $\sigma \models_{cs} [S] \varphi \iff$

  for all σ' s.t. $S, \sigma \rightarrow_{cs} \sigma'$ we have $\sigma' \models_{cs} \varphi$
- $\sigma \models_{cs} [\![S]\!] \varphi \iff$

  for all S', σ' s.t. $S, \sigma \Rightarrow_{cs} S', \sigma'$ we have $\sigma' \models_{S':cs} \varphi$

Substitutions

$$
\begin{aligned}
\mathbf{cont}_i[S/\mathbf{cont}_i] &= S \\
\mathbf{cont}_j[S/\mathbf{cont}_i] &= \mathbf{cont}_j,\ i \neq j \\
x := a[S/\mathbf{cont}_i] &= x := a \\
\mathbf{skip}[S/\mathbf{cont}_i] &= \mathbf{skip} \\
(S'; S'')[S/\mathbf{cont}_i] &= S'[S/\mathbf{cont}_i]; S''[S/cont_i] \\
\mathbf{if}\ b\ \mathbf{then}\ S'\ \mathbf{else}\ S''[S/\mathbf{cont}_i] &= \mathbf{if}\ b\ \mathbf{then}\ S'[S/\mathbf{cont}_i]\ \mathbf{else}\ S''[S/\mathbf{cont}_i] \\
\mathbf{while}\ b\ \mathbf{do}\ S'[S/\mathbf{cont}_i] &= \mathbf{while}\ b\ \mathbf{do}\ S'[S/\mathbf{cont}_i] \\
(\varphi \wedge \psi)[S/\mathbf{cont}_i] &= \varphi[S/\mathbf{cont}_i] \wedge \psi[S/\mathbf{cont}_i] \\
(\varphi \vee \psi)[S/\mathbf{cont}_i] &= \varphi[S/\mathbf{cont}_i] \vee \psi[S/\mathbf{cont}_i] \\
\langle S' \rangle \varphi[S/\mathbf{cont}_i] &= \langle S'[S/\mathbf{cont}_i] \rangle \varphi[S/\mathbf{cont}_i] \\
[S']\varphi[S/\mathbf{cont}_i] &= [S'[S/\mathbf{cont}_i]]\varphi[S/\mathbf{cont}_i] \\
\langle\!\langle S' \rangle\!\rangle \varphi[S/\mathbf{cont}_i] &= \langle\!\langle S'[S/\mathbf{cont}_i] \rangle\!\rangle \varphi[S^{up}/\mathbf{cont}_{i+1}] \\
[\![S']\!] \varphi[S/\mathbf{cont}_i] &= [\![S'[S/\mathbf{cont}_i]]\!] \varphi[S^{up}/\mathbf{cont}_{i+1}]
\end{aligned}
$$

where S^{up} replaces every occurence of $\mathbf{cont}_i$ with $\mathbf{cont}_{i+1}$.

Substitution

Substitution property

$$\sigma \models_{cs} \varphi[S/cont_i] \iff \sigma \models_{cs[i \mapsto S]} \varphi$$

where the notation $cs[i \mapsto S]$ replaces the i-th element in cs by S

Expressivity

$$[\![S]\!]\langle \mathbf{cont}_0 \rangle \varphi - \textit{ should converge}$$

Property: $[\![S]\!]\langle \mathbf{cont}_0 \rangle \varphi \Rightarrow \langle S \rangle \varphi$

$$\langle\!\langle S \rangle\!\rangle [\mathbf{cont}_0] \varphi - \textit{"lucky" intermediate state}$$

Property: $[\![S]\!]\varphi \Rightarrow \langle\!\langle S \rangle\!\rangle [\mathbf{cont}_0] \varphi$

Axioms

$$
\begin{array}{rcl|rcl}
\langle x := a\rangle\varphi & \iff & \varphi[a/x] & \langle\!\langle x := a\rangle\!\rangle\varphi & \iff & \varphi \\
[x := a]\varphi & \iff & \varphi[a/x] & [\![x := a]\!]\varphi & \iff & \varphi \\
\langle\mathbf{skip}\rangle\varphi & \iff & \varphi & \langle\!\langle\mathbf{skip}\rangle\!\rangle\varphi & \iff & \mathit{false} \\
[\mathbf{skip}]\varphi & \iff & \varphi & [\![\mathbf{skip}]\!]\varphi & \iff & \mathit{true} \\
\langle S; S'\rangle\varphi & \iff & \langle S\rangle\langle S'\rangle\varphi & \langle\!\langle S; S'\rangle\!\rangle\varphi & \iff & \langle\!\langle S\rangle\!\rangle(\varphi[\mathbf{cont}_0; S'/\mathbf{cont}_0]) \\
 & & & & & \vee \langle S\rangle\langle\!\langle S'\rangle\!\rangle\varphi \\
[S; S']\varphi & \iff & [S][S']\varphi & [\![S; S']\!]\varphi & \iff & [\![S]\!](\varphi[\mathbf{cont}_0; S'/\mathbf{cont}_0]) \\
 & & & & & \wedge [S][\![S']\!]\varphi
\end{array}
$$

Axioms ctd

$$\langle\!\langle \textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2 \rangle\!\rangle \varphi \iff b \to \langle\!\langle S_1 \rangle\!\rangle \varphi \wedge \neg b \to \langle\!\langle S_2 \rangle\!\rangle \varphi$$
$$\langle \textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2 \varphi \rangle \iff b \to \langle S_1 \rangle \varphi \wedge \neg b \to \langle S_2 \rangle \varphi$$

$$[\![\textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2]\!] \varphi \iff b \to [\![S_1]\!] \varphi \wedge \neg b \to [\![S_2]\!] \varphi$$
$$[\textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2] \varphi \iff b \to [S_1] \varphi \wedge \neg b \to [S_2] \varphi$$

$$\langle\!\langle \textbf{while } b \textbf{ do } S \rangle\!\rangle \varphi \Rightarrow b \to \langle\!\langle S; \textbf{while } b \textbf{ do } S \rangle\!\rangle \varphi \wedge \neg b \to \varphi$$
$$\langle \textbf{while } b \textbf{ do } S \rangle \varphi \Rightarrow b \to \langle S; \textbf{while } b \textbf{ do } S \rangle \varphi \wedge \neg b \to \varphi$$

$$[\![\textbf{while } b \textbf{ do } S]\!] \varphi \Rightarrow b \to [\![S; \textbf{while } b \textbf{ do } S]\!] \varphi \wedge \neg b \to \varphi$$
$$[\textbf{while } b \textbf{ do } S] \varphi \Rightarrow b \to [S; \textbf{while } b \textbf{ do } S] \varphi \wedge \neg b \to \varphi$$

Axioms for parallelism

$$\langle S_1 || S_2 \rangle \varphi \iff \langle S_1 \rangle \langle S_2 \rangle \varphi \vee \langle\!\langle S_1 \rangle\!\rangle \langle \mathbf{cont}_0 || S_2^{up} \rangle \varphi^{up} \vee$$
$$\langle S_2 \rangle \langle S_1 \rangle \varphi \vee \langle\!\langle S_2 \rangle\!\rangle \langle \mathbf{cont}_0 || S_1^{up} \rangle \varphi^{up}$$

$$[S_1 || S_2] \varphi \iff [S_1][S_2] \varphi \wedge [\![S_1]\!] [\mathbf{cont}_0 || S_2^{up}] \varphi^{up} \wedge$$
$$[S_2][S_1] \varphi \wedge [\![S_2]\!] [\mathbf{cont}_0 || S_1^{up}] \varphi^{up}$$

$$\langle\!\langle S_1 || S_2 \rangle\!\rangle \varphi \iff \langle S_1 \rangle \langle\!\langle S_2 \rangle\!\rangle \varphi \vee \langle\!\langle S_1 \rangle\!\rangle \langle\!\langle \mathbf{cont}_0 || S_2^{up} \rangle\!\rangle \varphi^{up} \vee$$
$$\langle S_2 \rangle \langle\!\langle S_1 \rangle\!\rangle \varphi \vee \langle\!\langle S_2 \rangle\!\rangle \langle\!\langle \mathbf{cont}_0 || S_1^{up} \rangle\!\rangle \varphi^{up}$$

$$[\![S_1 || S_2]\!] \varphi \iff [S_1][\![S_2]\!] \varphi \wedge [\![S_1]\!] [\![\mathbf{cont}_0 || S_2^{up}]\!] \varphi^{up} \wedge$$
$$[S_2][\![S_1]\!] \varphi \wedge [\![S_2]\!] [\![\mathbf{cont}_0 || S_1^{up}]\!] \varphi^{up}$$

Related work

- A Sequent Calculus for First-Order Dynamic Logic with Trace Modalities, Bernhard Beckert, Steffen Schlager, Automated Reasoning, 2001
- Dynamic Logic with Trace Semantics, Bernhard Beckert, Daniel Bruns, Automated Deduction - CADE-24, 2013