Semantics for (Hybrid) Programming

Renato Neves

Universidade do Minho

HASLab
HIGH-ASSURANCE SOFTWARE LABORATORY

Table of Contents

Last Lectures

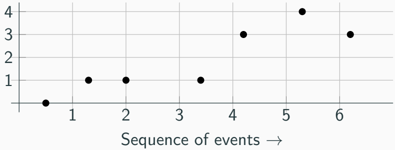
Explored a simple language (CCS) and its semantics

Used it to model and analyse communicating systems

Expanded our study to the timed setting, via UPPAAL

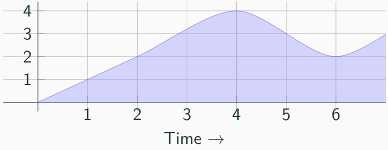
Used it to save us from zombies!

Going Beyond the Timed Setting



Described via classical methods of computation

+



Described via differential equations

Computational devices now interact with arbitrary physical processes (and not just time)

Which Language?

This time we explore a simple imperative language

No concurrency, no communication, and no higher-order func.

(languages with such features are still underdeveloped)

Perhaps some of you would like to improve them :-)

The Hybrid While-Language

Fix a stock of variables $X = \{\mathtt{x}_1, \ldots, \mathtt{x}_\mathtt{n}\}$. Then we have,

Linear Terms

$$\mathtt{LTerm}(X) \ni \mathtt{r} \mid \mathtt{r} \cdot \mathtt{t} \mid \mathtt{x} \mid \mathtt{t} + \mathtt{s}$$

real number

Atomic Programs

$$\mathtt{At}(X) \ni \mathtt{x} := \mathtt{t} \mid \mathtt{x}_1' = \mathtt{t}_1, \ldots, \mathtt{x}_\mathtt{n}' = \mathtt{t}_\mathtt{n} \ \mathtt{for} \ \mathtt{t}$$

"run" the system of differential equations for t seconds

Hybrid Programs

$$\mathtt{Prog}(X) \ni \mathtt{a} \mid \mathtt{p} \, ; \mathtt{q} \mid \mathtt{if}\ \mathtt{b}\ \mathtt{then}\ \mathtt{p}\ \mathtt{else}\ \mathtt{q} \mid \mathtt{while}\ \mathtt{b}\ \mathtt{do}\ \{\ \mathtt{p}\ \}$$

Overview

First we tackle a while-language, without differential equations, and its semantics

Then we move to the hybrid case and see how the corresponding semantics helps the engineer analyse hybrid programs

Throughout this journey, we will:

- write implementations in HASKELL
- do analysis in LINCE

Table of Contents

A Language of Linear Terms and its Semantics

Linear Terms

$\mathtt{LTerm}(X) \ni \mathtt{r} \mid \mathtt{r} \cdot \mathtt{t} \mid \mathtt{x} \mid \mathtt{t} + \mathtt{s}$

Let $\sigma : X \to \mathbb{R}$ be an environment, i.e. a memory on which the program performs computations

The expression $\langle \mathtt{t}, \sigma \rangle \Downarrow \mathtt{r}$ says that the linear expression $\mathtt{t}$ outputs $\mathtt{r}$ if the current memory is σ

$$\frac{}{\langle \mathtt{x}, \sigma \rangle \Downarrow \sigma(\mathtt{x})} \text{ (var)} \qquad \frac{}{\langle \mathtt{r}, \sigma \rangle \Downarrow \mathtt{r}} \text{ (con)}$$

$$\frac{\langle \mathtt{t}, \sigma \rangle \Downarrow \mathtt{r}}{\langle \mathtt{s} \cdot \mathtt{t}, \sigma \rangle \Downarrow \mathtt{s} \cdot \mathtt{r}} \text{ (scl)} \qquad \frac{\langle \mathtt{t}_1, \sigma \rangle \Downarrow \mathtt{r}_1 \qquad \langle \mathtt{t}_2, \sigma \rangle \Downarrow \mathtt{r}_2}{\langle \mathtt{t}_1 + \mathtt{t}_2, \sigma \rangle \Downarrow \mathtt{r}_1 + \mathtt{r}_2} \text{ (add)}$$

The Semantics at Work

The linear term $\mathtt{x} + 2 \cdot \mathtt{y}$ corresponds to the tree

$$\begin{tikzcd}[column sep=small]
 & (+) \arrow[dl] \arrow[dr] & \\
\mathtt{x} & & (2\ \cdot) \arrow[d] \\
 & & \mathtt{y}
\end{tikzcd}$$

Consider an environment σ such that $\sigma(\mathtt{x}) = 3$ and $\sigma(\mathtt{y}) = 4$. We can then build the following derivation tree:

$$\frac{\langle \mathtt{x}, \sigma \rangle \Downarrow 3 \qquad\qquad \dfrac{\langle \mathtt{y}, \sigma \rangle \Downarrow 4}{\langle 2 \cdot \mathtt{y}, \sigma \rangle \Downarrow 8}}{\langle \mathtt{x} + 2 \cdot \mathtt{y}, \sigma \rangle \Downarrow 11}$$

Exercises

- $\langle 2 \cdot \mathtt{x} + 2 \cdot \mathtt{y}, \sigma \rangle \Downarrow ?$
- $\langle 3 \cdot (2 \cdot \mathtt{x}) + 2 \cdot (\mathtt{y} + \mathtt{z}), \sigma \rangle \Downarrow ?$

Exercises

- $\langle 2 \cdot \mathrm{x} + 2 \cdot \mathrm{y}, \sigma \rangle \Downarrow$?
- $\langle 3 \cdot (2 \cdot \mathrm{x}) + 2 \cdot (\mathrm{y} + \mathrm{z}), \sigma \rangle \Downarrow$?

Boring computations? If so why not implement the semantics in HASKELL?

Equivalence of Linear Terms

The previous semantics yields the following notion of equivalence:
$\mathtt{t} \sim \mathtt{s}$ if for all environments σ

$$\langle \mathtt{t}, \sigma \rangle \Downarrow \mathtt{r} \text{ iff } \langle \mathtt{s}, \sigma \rangle \Downarrow \mathtt{r}$$

Examples of equivalent terms:

- $\mathtt{r} \cdot (\mathtt{x} + \mathtt{y}) \sim \mathtt{r} \cdot \mathtt{x} + \mathtt{r} \cdot \mathtt{y}$
- $0 \cdot \mathtt{x} \sim 0$
- $(\mathtt{r} \cdot \mathtt{s}) \cdot \mathtt{x} \sim \mathtt{r} \cdot (\mathtt{s} \cdot \mathtt{x})$?