Abstract interpretation with numeric intervals

Second assignment of the Software Verification course, A.Y. 2022/2023

Christian Micheletti

October 13, 2023

UNIVERSITÀ DEGLI STUDI DI PADOVA

Outline

1. The Language
   - Arithmetic Expressions
2. Introduction
3. First section

The Language

The language is a variation of the While language seen in class. It differs on:

- it admits some syntactic sugar (it's not minimal);
- its semantic functions are modified to allow divergence and state changes in both arithmetic and boolean expressions.

Arithmetic Expressions (1)

$$\begin{aligned} AExp ::= & n \mid x \mid -e \mid (e) \\ & \mid e_1 + e_2 \mid e_1 - e_2 \mid e_1 * e_2 \mid e_1 / e_2 \\ & \mid x\texttt{++} \mid \texttt{++}x \mid x\texttt{--} \mid \texttt{--}x \end{aligned}$$

$\mathcal{A} : AExp \to State \hookrightarrow \mathbb{Z} \times State$

$$\begin{aligned} \mathcal{A}[\![n]\!]\varphi = & (n_{\mathbb{Z}}, \varphi) \\ \mathcal{A}[\![x]\!]\varphi = & (\varphi(x), \varphi) \\ \mathcal{A}[\![(e)]\!]\varphi = & \mathcal{A}[\![e]\!]\varphi \\ \mathcal{A}[\![-e]\!]\varphi = & \begin{cases} (-a, \varphi') & \mathcal{A}[\![e]\!]\varphi = (a, \varphi') \\ \uparrow & (\mathcal{A}[\![e]\!]\varphi) \uparrow \end{cases} \end{aligned}$$

Arithmetic Expressions (2)

$\mathcal{A} : \mathit{AExp} \to \mathit{State} \hookrightarrow \mathbb{Z} \times \mathit{State}$

$$\mathcal{A}[\![e_1 / e_2]\!]\varphi = \begin{cases} (a_1 \div a_2, \varphi'') & \mathcal{A}[\![e_1]\!]\varphi = (a_1, \varphi') \\ & \wedge\ \mathcal{A}[\![e_2]\!]\varphi' = (a_2, \varphi'') \\ & \wedge\ a_2 \neq 0 \\ \uparrow & \text{otherwise} \end{cases}$$

$$\mathcal{A}[\![e_1 \ \mathbf{op}\ e_2]\!]\varphi = \begin{cases} (a_1 \ \mathit{op}\ a_2, \varphi'') & \mathcal{A}[\![e_1]\!]\varphi = (a_1, \varphi') \\ & \wedge\ \mathcal{A}[\![e_2]\!]\varphi' = (a_2, \varphi'') \\ \uparrow & \text{otherwise} \end{cases}$$

Arithmetic Expressions (3)

$\mathcal{A} : \mathit{AExp} \to \mathit{State} \hookrightarrow \mathbb{Z} \times \mathit{State}$

$$
\begin{aligned}
\mathcal{A}[\![x\texttt{++}]\!]\varphi =&(\varphi(x), \varphi[x \mapsto x+1]) \\
\mathcal{A}[\![\texttt{++}x]\!]\varphi =&\mathit{let}\ \varphi' = \varphi[x \mapsto x+1] \\
&\mathit{in}\ (\varphi'(x), \varphi') \\
\mathcal{A}[\![x\texttt{--}]\!]\varphi =&(\varphi(x), \varphi[x \mapsto x-1]) \\
\mathcal{A}[\![\texttt{--}x]\!]\varphi =&\mathit{let}\ \varphi' = \varphi[x \mapsto x-1] \\
&\mathit{in}\ (\varphi'(x), \varphi')
\end{aligned}
$$

Introduction

Etiam eu interdum ligula
Nunc mi eros, vulputate in ornare a, viverra eget quam

- Morbi **vitae lacus** porta neque tincidunt sodales
- Proin tincidunt, **neque** at tincidunt mollis
- Ut lacinia sem a nibh consequat porttitor

First section

Normal block

Fusce luctus venenatis felis quis semper

Alert block

$$E = (x_1 \vee \neg x_2 \vee \neg x_3) \wedge (x_1 \vee x_2 \vee x_4)$$

Example block

Proin tincidunt, neque at tincidunt mollis