Exercices
MPRI 2-6

Antoine Miné

September 19, 2017

Problem 1

We consider the simple programming language from course 04, slides 16–25, with integer semantics ($\mathbb{I} \overset{\text{def}}{=} \mathbb{Z}$). We enrich the language of expressions with a new operator: $\mathbf{wrap}[\ell,h]$. The operator is parameterized by two integer constants $\ell, h \in \mathbb{Z}$. The concrete semantics is extended as follows:

$$\begin{array}{lcl} \mathrm{E}[\![\, \mathbf{wrap}[\ell,h](e) \,]\!]\,\rho & \overset{\text{def}}{=} & \{\, \mathit{wrap}[\ell,h](v) \mid v \in \mathrm{E}[\![\, e \,]\!] \,\} \\ \text{where } \mathit{wrap}[\ell,h](v) & \overset{\text{def}}{=} & \min \{\, v' \mid v' \geq \ell \wedge \exists k \in \mathbb{Z} : v = v' + k(h-\ell+1) \,\} \end{array}$$

i.e., to evaluate an expression $\mathbf{wrap}[\ell,h](e)$, we first evaluate e by induction, and then put its result into the interval $[\ell,h]$ by modulo.

This operator is particularly useful to model the "wrap-around" effect of machine integer arithmetic. For instance $\mathbf{wrap}[0,255](x+y)$ corresponds to adding two unsigned bytes. In the following, we consider the expression e:

$$e : \mathbf{wrap}[-128,127](\mathbf{wrap}[0,255](x) + \mathbf{wrap}[0,255](y))$$

which takes two signed variables x and y, converts them to unsigned bytes, performs an addition, then converts back the result into a signed byte.

1. Assuming that $x \in [-1,1]$ and $y \in [-1,1]$ before e, give the concrete evaluation of the expression $\mathrm{E}[\![\, e \,]\!]$.

2. Give the best abstraction $\mathit{wrap}[\ell,h]^\sharp_i$ of the $\mathit{wrap}[\ell,h]$ operator in the interval abstract domain.

   Prove that it is indeed a best abstraction, but that it is not always exact.

   Give a necessary and sufficient condition on its argument for this abstract operator to be exact.

3. The assignment e is evaluated in the interval abstract domain as follows:

   $$v^\sharp_i \overset{\text{def}}{=} \mathit{wrap}[-128,127]^\sharp_i(\mathit{wrap}[0,255]^\sharp_i(x^\sharp) +^\sharp_i \mathit{wrap}[0,255]^\sharp_i(y^\sharp))$$

   where $+^\sharp_i$ is the standard interval addition, and $x^\sharp = y^\sharp = [-1,1]$.

   Give the value of $v^\sharp_i$. Is the result exact? Optimal? Why?

We now propose a *modular* interval domain $\mathcal{D}_m$ which can represent intervals up to a modular component $[a,b]+k\mathbb{Z}$:

$$\mathcal{D}_m \stackrel{\text{def}}{=} \{\, [a,b]+k\mathbb{Z} \mid a,b,\in \mathbb{Z}\cup\{\pm\infty\}, k\in\mathbb{N}\,\}$$

with concretization:

$$\gamma_m([a,b]+k\mathbb{Z}) \stackrel{\text{def}}{=} \{\, x+ky \mid a\leq x\leq b \wedge y\in\mathbb{Z}\,\}$$

Note that $\mathcal{D}_m$ contains regular intervals (when setting the modular component k to 0).

4. Show that there is no best abstraction function α in $\mathcal{D}_m$.

5. Propose abstractions $+^\sharp_m$ and $\mathit{wrap}[\ell,h]^\sharp_m$ of $+$ and $\mathit{wrap}[\ell,h]$ in $\mathcal{D}_m$ that ensure that the expression e is precisely analyzed.

   Prove the soundess of the abstract operators you proposed.

Problem 2

Consider the following family of programs (parameterized by α and β):

$$\texttt{X} := 0;\quad \texttt{while} \bullet\ 1=1\ \texttt{do}\quad \texttt{X} := \alpha\times\texttt{X}+[0,\beta]\quad \texttt{done}$$

where X is a variable with value in $\mathbb{R}$, and α and β are positive constants in $\mathbb{R}$. We wish to find a precise invariant for X at $\bullet$ using the interval domain.

1. Show that, in the concrete semantics, the set of possible values for X at $\bullet$ has the form $\texttt{X}\in[0,m[$ for some value m. Express m as a function of α and β.

   In the following, we will only consider the case where m is finite ($m<+\infty$).

2. Show that an interval of the form $[0,m']$ is an inductive invariant for X at $\bullet$ if and only if $m'\geq m$.

3. Consider the analysis of the program in the interval domain using a widening with thresholds, with threshold set T.

   Under which condition on T will the analysis find a bounded invariant (i.e., an invariant $[x,y]$ where $x\neq-\infty$ and $y\neq+\infty$)?

   Express the result of the analysis as a function of T, α and β.

   At which condition on T does the analysis find the exact concrete interval?

4. Show that, when the analysis finds a bounded but not optimal invariant, decreasing iterations can help.

5. Show that the value of α and β can be recovered by looking at some increasing iterations in the interval domain.

   Use this remark to construct a new interval widening that is able to find the exact concrete result in very few iterations, without the need of decreasing iterations. The definition of the widening shall not depend on α nor β, and you shall prove the soundness and the termination of your widening.