Lesson 4 – Exercises

Static Program Analysis and Constraint Solving
Master's Degree in Formal Methods in Computer Science
Year 2019/20

1. Assume the following collection functions $f_+, f_-, f_* : \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{Z}) \to \mathcal{P}(\mathbb{Z})$ for addition, substraction and product, respectively:

$$\begin{array}{rcl} f_+(X,Y) & = & \{x+y \mid x \in X, y \in Y\} \\ f_-(X,Y) & = & \{x-y \mid x \in X, y \in Y\} \\ f_*(X,Y) & = & \{x*y \mid x \in X, y \in Y\} \end{array}$$

Given their abstract counterparts: $\oplus, \ominus, \otimes$, and the corresponding Galois connection between $\mathcal{P}(\mathbb{Z})$ and $\mathcal{P}(\mathbf{Sign})$, prove the following facts:

$$\begin{array}{rll} \alpha(f_+(\gamma(\{-,+\}),\gamma(\{0\}))) \subseteq \{-,+\} & \text{that is,} & \{-,+\} \oplus \{0\} = \{-,+\} \\ \alpha(f_-(\gamma(\{0\}),\gamma(\{+\}))) \subseteq \{-\} & \text{that is,} & \{0\} \ominus \{+\} = \{-\} \\ \alpha(f_*(\gamma(\{0,-\}),\gamma(\{-\}))) \subseteq \{0,+\} & \text{that is,} & \{0,-\} \otimes \{-\} = \{0,+\} \end{array}$$

Answer

We get:

$$\gamma(\{-,+\}) = \{x \in \mathbb{Z} \mid x \neq 0\}$$
$$\gamma(\{0\}) = \{0\}$$

Therefore:

$$f_+(\{x \in \mathbb{Z} \mid x \neq 0\}, \{0\}) = \{x+0 \mid x \neq 0\} = \{x \in \mathbb{Z} \mid x \neq 0\}$$

Finally, we apply the abstraction function to the latter set:

$$\alpha(\{x \in \mathbb{Z} \mid x \neq 0\}) = \{-,+\}$$

Therefore, $\alpha(f_+(\gamma(\{-,+\}),\gamma(\{0\}))) = \{-,+\}$.

We follow a similar reasoning for the remaining cases:

$$\begin{array}{rl} & \alpha(f_-(\gamma(\{0\}),\gamma(\{+\}))) \\ = & \alpha(f_-(\{0\},\{x \in \mathbb{Z} \mid x > 0\})) \\ = & \alpha(\{0-x \mid x > 0\}) \\ = & \alpha(\{y \mid y < 0\}) \\ = & \{-\} \end{array}$$

$$\begin{array}{rl} & \alpha(f_*(\gamma(\{0,-\}),\gamma(\{-\}))) \\ = & \alpha(f_*(\{x \in \mathbb{Z} \mid x \leq 0\}),\{x \in \mathbb{Z} \mid x < 0\})) \\ = & \alpha(\{x * y \mid x \leq 0, y < 0\}) \\ = & \alpha(\{z \mid z \geq 0\}) \\ = & \{0,+\} \end{array}$$

2. The sign analysis explained in this lesson relies on the correspondence between the concrete domain $\mathbf{Var} \to \mathcal{P}(\mathbb{Z})$ and the abstract domain $\mathbf{Var} \to \mathcal{P}(\mathbf{Sign})$, where $\mathbf{Sign} = \{+,0,-\}$. In this exercise we are going to develop a sign analysis that relies on two different lattices:

   - Concrete domain: $\mathcal{P}(\mathbf{State})$, where $\mathbf{State} = \mathbf{Var} \to \mathbb{Z}$.
   - Abstract domain: $\mathcal{P}(\mathbf{State}^\sharp)$, where $\mathbf{State}^\sharp = \mathbf{Var} \to \mathbf{Sign}$.

   (a) Given the language of arithmetic expressions, define a collecting semantics:

   $$[\![e]\!]^* : \mathcal{P}(\mathbf{State}) \to \mathcal{P}(\mathbb{Z})$$

   The definition does not have to be compositional and can rely on standard denotational semantics $[\![e]\!]$.

   Answer

   Assuming that we are given a set Σ of states, we just have to evaluate $[\![e]\!]$ for each one of them and build a set with all the results, thus obtaining a set of numbers. Therefore:

   $$[\![e]\!]^* \; \Sigma = \left\{[\![e]\!] \; \sigma \mid \sigma \in \Sigma\right\}$$

   (b) Define the following abstraction and concretization functions:

   $$\begin{array}{rl} \alpha : & \mathcal{P}(\mathbb{Z}) \to \mathcal{P}(\mathbf{Sign}) \\ \gamma : & \mathcal{P}(\mathbf{State}^\sharp) \to \mathcal{P}(\mathbf{State}) \end{array}$$

   Answer

   Let us define an auxiliary function $Sgn : \mathbb{Z} \to \mathbf{Sign}$ that returns the sign of a given integer. That is,

   $$\forall x \in \mathbb{Z} : Sgn(x) = \begin{cases} 0 & \text{if } x = 0 \\ + & \text{if } x > 0 \\ - & \text{if } x < 0 \end{cases}$$

   The abstraction function α is defined as in the sign analysis explained in the slides of the lesson:

   $$\forall X \in \mathcal{P}(\mathbb{Z}) : \alpha(X) = \{Sgn(x) \mid x \in X\}$$

In order to define the concretization function we need an auxiliary function γ', which returns the concrete counterparts of a single abstract state. That is, $\gamma' : \textbf{State}^\sharp \to \mathcal{P}(\textbf{State})$. For example, given a state $\sigma^\sharp$ such that $\sigma^\sharp(x) = +$ for every x, γ will map this state to the set of states that map all their variables to positive numbers. In general, for any $\sigma^\sharp \in \textbf{State}^\sharp$:

$$\gamma'(\sigma^\sharp) = \left\{\sigma \in \textbf{State} \mid \forall x \in \textbf{Var} : \mathit{Sgn}(\sigma(x)) = \sigma^\sharp(x)\right\}$$

Lastly, given a set $\Sigma^\sharp$ of abstract states, we define γ in this set by joining the results of γ' when applied to every abstract state in $\Sigma^\sharp$:

$$\gamma(\Sigma^\sharp) = \bigcup_{\sigma^\sharp \in \Sigma^\sharp} \gamma'(\sigma^\sharp)$$

(c) Define a sign analysis with an abstract interpreter:

$$[\![e]\!]^\sharp : \mathcal{P}(\textbf{State}^\sharp) \to \mathcal{P}(\textbf{Sign})$$

In this case, the definition has to be compositional. You can assume the existence of operators $\oplus, \ominus, \otimes : \mathcal{P}(\textbf{Sign}) \times \mathcal{P}(\textbf{Sign}) \to \mathcal{P}(\textbf{Sign})$.

Answer

$$\begin{array}{rcl}
[\![n]\!]^\sharp\,\Sigma^\sharp & = & \{\mathit{Sgn}(n)\} \\
[\![x]\!]^\sharp\,\Sigma^\sharp & = & \{\sigma^\sharp(x) \mid \sigma^\sharp \in \Sigma^\sharp\} \\
[\![e_1 + e_2]\!]^\sharp\,\Sigma^\sharp & = & [\![e_1]\!]^\sharp\,\Sigma^\sharp \oplus [\![e_2]\!]^\sharp\,\Sigma^\sharp \\
[\![e_1 - e_2]\!]^\sharp\,\Sigma^\sharp & = & [\![e_1]\!]^\sharp\,\Sigma^\sharp \ominus [\![e_2]\!]^\sharp\,\Sigma^\sharp \\
[\![e_1 * e_2]\!]^\sharp\,\Sigma^\sharp & = & [\![e_1]\!]^\sharp\,\Sigma^\sharp \otimes [\![e_2]\!]^\sharp\,\Sigma^\sharp
\end{array}$$

(d) Prove that, for every $\Sigma^\sharp \in \mathcal{P}(\textbf{State}^\sharp)$ it holds that:

$$(\alpha \circ [\![e]\!]^* \circ \gamma)\,\Sigma^\sharp \sqsubseteq [\![e]\!]^\sharp\,\Sigma^\sharp$$

You can assume that $\oplus, \ominus, \otimes$ are correct approximations of the $+, -, *$ operators on sets of integers. In particular:

$$\begin{array}{rcll}
\alpha(f_+(\gamma_S(s_1), \gamma_S(s_2))) & \subseteq & s_1 \oplus s_2 & \text{for every } s_1, s_2 \in \mathcal{P}(\textbf{Sign}) \\
\alpha(f_-(\gamma_S(s_1), \gamma_S(s_2))) & \subseteq & s_1 \ominus s_2 & \text{for every } s_1, s_2 \in \mathcal{P}(\textbf{Sign}) \\
\alpha(f_*(\gamma_S(s_1), \gamma_S(s_2))) & \subseteq & s_1 \otimes s_2 & \text{for every } s_1, s_2 \in \mathcal{P}(\textbf{Sign})
\end{array}$$

where γ_S is the usual concretization function on sets of signs (do not confuse with the γ stated above).

Answer

Let us prove it by induction on the structure of e.

- **Case** $e \equiv n$. We get:

$$
\begin{array}{lll}
 & (\alpha \circ [\![n]\!]^* \circ \gamma)\ \Sigma^\sharp & \\
= & \alpha([\![n]\!]^*\ \gamma(\Sigma^\sharp)) & \\
= & \alpha(\{[\![n]\!]\ \sigma \mid \sigma \in \gamma(\Sigma^\sharp)\}) & \text{by definition of } [\![n]\!]^* \\
= & \alpha(\{n\}) & \text{by definition of } [\![n]\!] \\
= & \{Sgn(n)\} & \text{by definition of } \alpha \\
= & [\![n]\!]^\sharp\ \Sigma^\sharp & \text{by definition of } [\![n]\!]^\sharp
\end{array}
$$

- **Case** $e \equiv x$. We get:

$$
\begin{array}{lll}
 & (\alpha \circ [\![x]\!]^* \circ \gamma)\ \Sigma^\sharp & \\
 & \alpha([\![x]\!]^*\ \gamma(\Sigma^\sharp)) & \\
= & \alpha(\{[\![x]\!]\ \sigma \mid \sigma \in \gamma(\Sigma^\sharp)\}) & \text{by definition of } [\![x]\!]^* \\
= & \alpha(\{\sigma(x) \mid \sigma \in \gamma(\Sigma^\sharp)\}) & \text{by definition of } [\![x]\!] \\
= & \alpha(\{\sigma(x) \mid \sigma \in \bigcup_{\sigma^\sharp \in \Sigma^\sharp} \gamma'(\sigma^\sharp)\}) & \text{by definition of } \gamma' \\
= & \{Sgn(\sigma(x)) \mid \sigma \in \bigcup_{\sigma^\sharp \in \Sigma^\sharp} \gamma'(\sigma^\sharp)\} & \text{by definition of } \alpha \\
= & \bigcup_{\sigma^\sharp \in \Sigma^\sharp} \{Sgn(\sigma(x)) \mid \sigma \in \gamma'(\sigma^\sharp)\} & \\
= & \bigcup_{\sigma^\sharp \in \Sigma^\sharp} \{Sgn(\sigma(x)) \mid \forall z \in \mathbf{Var} : Sgn(\sigma(z)) = \sigma^\sharp(z)\} & \text{by definition of } \gamma' \\
= & \bigcup_{\sigma^\sharp \in \Sigma^\sharp} \{\sigma^\sharp(x) \mid \forall z \in \mathbf{Var} : Sgn(\sigma(z)) = \sigma^\sharp(z)\} & \\
\subseteq & \bigcup_{\sigma^\sharp \in \Sigma^\sharp} \{\sigma^\sharp(x)\} & \\
= & \{\sigma^\sharp(x) \mid \sigma^\sharp \in \Sigma^\sharp\} & \\
= & [\![x]\!]^\sharp\ \Sigma^\sharp & \text{by definition of } [\![x]\!]^\sharp
\end{array}
$$

- **Case** $e \equiv e_1 + e_2$. We get:

$$
\begin{array}{lll}
 & (\alpha \circ [\![e_1 + e_2]\!]^* \circ \gamma)(\Sigma^\sharp) & \\
= & \alpha([\![e_1 + e_2]\!]^*\ \gamma(\Sigma^\sharp)) & \\
= & \alpha\left(\{[\![e_1 + e_2]\!]\ \sigma \mid \sigma \in \gamma(\Sigma^\sharp)\}\right) & \text{by definition of } [\![e_1 + e_2]\!]^* \\
= & \alpha(\{[\![e_1]\!]\ \sigma + [\![e_2]\!]\ \sigma \mid \sigma \in \gamma(\Sigma^\sharp)\}) & \text{by definition of } [\![e_1 + e_2]\!]
\end{array}
$$

It is easy to show that:

$$
\left\{[\![e_1]\!]\ \sigma + [\![e_2]\!]\ \sigma \mid \sigma \in \gamma(\Sigma^\sharp)\right\} \subseteq f_+\left(\left\{[\![e_1]\!]\ \sigma \mid \sigma \in \gamma(\Sigma^\sharp)\right\}, \left\{[\![e_2]\!]\ \sigma \mid \sigma \in \gamma(\Sigma^\sharp)\right\}\right)
$$

In fact, given a number z in the left hand side, it holds that $z = x + y$ where $x = [\![e_1]\!]\ \sigma$, $y = [\![e_2]\!]\ \sigma$ for some $\sigma \in \gamma(\Sigma^\sharp)$. This implies that x belongs to the set $\{[\![e_1]\!]\ \sigma \mid \sigma \in \gamma(\Sigma^\sharp)\}$ and y belongs to the set $\{[\![e_2]\!]\ \sigma \mid \sigma \in \gamma(\Sigma^\sharp)\}$. Let us denote these two sets by Z_1 and Z_2 respectively. Therefore, we get that $z = x + y$ for some $x \in Z_1$ and some $y \in Z_2$, hence $z \in f_+(Z_1, Z_2)$. As a result, we get that $\{[\![e_1]\!]\ \sigma + [\![e_2]\!]\ \sigma \mid \sigma \in \gamma(\Sigma^\sharp)\} \subseteq f_+(Z_1, Z_2)$. Since α is monotonically increasing, we get:

$$
\alpha\left(\left\{[\![e_1]\!]\ \sigma + [\![e_2]\!]\ \sigma \mid \sigma \in \gamma(\Sigma^\sharp)\right\}\right) \subseteq \alpha(f_+(Z_1, Z_2))
$$

Now we know that α and γ_S make up a Galois connection. This means that $\gamma_S \circ \alpha \sqsupseteq id$. In particular, $Z_1 \subseteq \gamma_S(\alpha(Z_1))$ and $Z_2 \subseteq \gamma_S(\alpha(Z_2))$. Since α and f_+ are monotonically increasing, we get:

$$\alpha(f_+(Z_1, Z_2)) \subseteq \alpha(f_+(\gamma_S(\alpha(Z_1)), \gamma_S(\alpha(Z_2))))$$

We also know that $\oplus$ is a correct approximation to f_+, hence:

$$\alpha(f_+(\gamma_S(\alpha(Z_1)), \gamma_S(\alpha(Z_2)))) \subseteq \alpha(Z_1) \oplus \alpha(Z_2)$$

Now let us examine $\alpha(Z_1)$. By expanding its definition we get:

$$\begin{array}{lll} & \alpha(Z_1) & \\ = & \alpha(\{[\![e_1]\!]\ \sigma \mid \sigma \in \gamma(\Sigma^\sharp)\}) & \text{by definition of } Z_1 \\ = & \alpha([\![e_1]\!]^*\ \gamma(\Sigma^\sharp)) & \text{by definition of } [\![e_1]\!]^* \\ = & (\alpha \circ [\![e_1]\!]^* \circ \gamma)(\Sigma^\sharp) & \\ \subseteq & [\![e_1]\!]^\sharp\ \Sigma^\sharp & \text{by induction hypothesis} \end{array}$$

and similarly with $\alpha(Z_2)$. Therefore:

$$\alpha(Z_1) \oplus \alpha(Z_2) \subseteq [\![e_1]\!]^\sharp\ \Sigma^\sharp \oplus [\![e_2]\!]^\sharp\ \Sigma^\sharp = [\![e_1 + e_2]\!]^\sharp\ \Sigma^\sharp$$

which proves the result.

- **Cases** $e \equiv e_1 - e_2$ **and** $e \equiv e_1 * e_2$. They are similar to the case of addition, but now we use the approximation properties of $\ominus$ and $\otimes$, respectively.

3. We can define the sign analysis described in the lesson (in which the abstract domain was $\mathbf{Var} \to \mathcal{P}(\mathbf{Sign})$) as an abstraction of the analysis given in Exercise 2.

   (a) Define a Galois connection between $\mathcal{P}(\mathbf{State}^\sharp)$ (being $\mathbf{State}^\sharp$ defined as in Exercise 2) and $\mathbf{Var} \to \mathcal{P}(\mathbf{Sign})$.

Answer

We use $\sigma^\sharp$ and $\rho^\sharp$ to denote elements from $\mathbf{State}^\sharp$, $\Sigma^\sharp$ to denote elements from $\mathcal{P}(\mathbf{State}^\sharp)$, and $\sigma^{\sharp\sharp}$ to denote elements from $\mathbf{Var} \to \mathcal{P}(\mathbf{Sign})$.

For every set $\Sigma^\sharp$ of elements in $\mathbf{State}^\sharp$, its abstraction is given by:

$$\alpha(\Sigma^\sharp) = \lambda x. \left\{\sigma^\sharp(x) \mid \sigma^\sharp \in \Sigma^\sharp\right\}$$

Given a state $\sigma^{\sharp\sharp}$, its concretization is given by:

$$\gamma(\sigma^{\sharp\sharp}) = \{\sigma^\sharp \mid \forall x \in \mathbf{Var} : \sigma^\sharp(x) \in \sigma^{\sharp\sharp}(x)\}$$

Now let us prove that α and γ actually make up a Galois connection. It is easy to show that α and γ are monotonically increasing. Let us prove that $\gamma \circ \alpha \supseteq id$ or, equivalently, that $\gamma(\alpha(\Sigma^\sharp)) \supseteq \Sigma^\sharp$ for every $\Sigma^\sharp$.

Assume some $\Sigma^\sharp$. For every state $\rho^\sharp \in \Sigma^\sharp$ and any variable $x \in \mathbf{Var}$ it trivally holds that $\rho^\sharp(x) \in \{\sigma^\sharp(x) \mid \sigma^\sharp \in \Sigma^\sharp\}$, since $\rho^\sharp$ is contained within $\Sigma^\sharp$. Therefore we know that:

$$\Sigma^\sharp \subseteq \{\rho^\sharp \mid \forall x \in \mathbf{Var} : \rho^\sharp(x) \in \{\sigma^\sharp(x) \mid \sigma^\sharp \in \Sigma^\sharp\}\} \tag{1}$$

Now let us prove that $\gamma(\alpha(\Sigma^\sharp)) \supseteq \Sigma^\sharp$:

$$\begin{array}{lll} & \gamma(\alpha(\Sigma^\sharp)) & \\ = & \gamma\left(\lambda x. \left\{\sigma^\sharp(x) \mid \sigma^\sharp \in \Sigma^\sharp\right\}\right) & \text{by definition of } \alpha \\ = & \{\rho^\sharp \mid \forall z \in \mathbf{Var} : \rho^\sharp(z) \in \left(\lambda x. \left\{\sigma^\sharp(x) \mid \sigma^\sharp \in \Sigma^\sharp\right\}\right)(z)\} & \text{by definition of } \gamma \\ = & \{\rho^\sharp \mid \forall z \in \mathbf{Var} : \rho^\sharp(z) \in \left\{\sigma^\sharp(z) \mid \sigma^\sharp \in \Sigma^\sharp\right\}\} & \text{by applying the } \lambda\text{-abstraction} \\ \supseteq & \Sigma^\sharp & \text{by property (1) shown above} \end{array}$$

Now we prove that $(\alpha \circ \gamma) \sqsubseteq id$ or, equivalently, that $\alpha(\gamma(\sigma^{\sharp\sharp}))$ for any $\sigma^{\sharp\sharp}$.

$$\begin{array}{lll} & \alpha(\gamma(\sigma^{\sharp\sharp})) & \\ = & \alpha(\{\sigma^\sharp \mid \forall x \in \mathbf{Var} : \sigma^\sharp(x) \in \sigma^{\sharp\sharp}(x)\}) & \text{by definition of } \gamma \\ = & \lambda z.\{\rho^\sharp(z) \mid \rho^\sharp \in \{\sigma^\sharp \mid \forall x \in \mathbf{Var} : \sigma^\sharp(x) \in \sigma^{\sharp\sharp}(x)\}\} & \text{by definition of } \alpha \\ = & \lambda z.\{\rho^\sharp(z) \mid \forall x \in \mathbf{Var} : \rho^\sharp(x) \in \sigma^{\sharp\sharp}(x)\} & \\ \subseteq & \lambda z.\sigma^{\sharp\sharp}(z) & \\ = & \sigma^{\sharp\sharp} & \end{array}$$

(b) If $[\![e]\!]^{\sharp\sharp}$ is the sign analysis described in the lesson, prove its correctness by showing that $[\![e]\!]^\sharp \circ \gamma \sqsubseteq [\![e]\!]^{\sharp\sharp}$, where $[\![e]\!]^\sharp$ is the analysis of Exercise 2. In this case we get that both $[\![e]\!]^\sharp$ and $[\![e]\!]^{\sharp\sharp}$ yield elements of $\mathcal{P}(\mathbf{Sign})$, so we do not have to apply the abstraction function to the set of signs returned by $[\![e]\!]^\sharp$.

Answer

Let us prove it by structural induction on e.

- **Case** $e \equiv n$. For any $\sigma^{\sharp\sharp}$, we get:

$$[\![n]\!]^\sharp\, \gamma(\sigma^{\sharp\sharp}) = \{Sgn(n)\} = [\![n]\!]^{\sharp\sharp}\, \sigma^{\sharp\sharp}$$

- **Case** $e \equiv x$. For any $\sigma^{\sharp\sharp}$, we get:

$$\begin{array}{ll} & [\![x]\!]^\sharp\, \gamma(\sigma^{\sharp\sharp}) \\ = & \{\sigma^\sharp(x) \mid \sigma^\sharp \in \gamma(\sigma^{\sharp\sharp})\} \\ = & \{\sigma^\sharp(x) \mid \forall z \in \mathbf{Var} : \sigma^\sharp(z) \in \sigma^{\sharp\sharp}(z)\} \\ \subseteq & \sigma^{\sharp\sharp}(x) \\ = & [\![x]\!]^{\sharp\sharp}\, \sigma^{\sharp\sharp} \end{array}$$

- **Case** $e \equiv e_1 + e_2$. For any $\sigma^{\sharp\sharp}$, we get:

$$\begin{array}{ll} & [\![e_1 + e_2]\!]^\sharp\, \gamma(\sigma^{\sharp\sharp}) \\ = & [\![e_1]\!]^\sharp\, \gamma(\sigma^{\sharp\sharp}) \oplus [\![e_2]\!]^\sharp\, \gamma(\sigma^{\sharp\sharp}) \\ = & ([\![e_1]\!]^\sharp \circ \gamma)(\sigma^{\sharp\sharp}) \oplus ([\![e_2]\!]^\sharp \circ \gamma)(\sigma^{\sharp\sharp}) \\ \subseteq & [\![e_1]\!]^{\sharp\sharp}\, \sigma^{\sharp\sharp} \oplus [\![e_2]\!]^{\sharp\sharp}\, \sigma^{\sharp\sharp} \\ = & [\![e_1 + e_2]\!]^{\sharp\sharp}\, \sigma^{\sharp\sharp} \end{array}$$