Exercises to the lecture
Semantics
Sheet 2

Prof. Dr. Roland Meyer
Jan Grünke Delivery until 30.04.2025 at 23:59

Exercise 2.1 (Abstract Interpretation)
Recall that a *Galois insertion* is a Galois connection where $\alpha \circ \gamma = id$ holds. Let $(\mathbb{P}(\mathbb{Z}^{\{x,y\}}), \subseteq)$ and $(\mathbb{P}(\{even, odd\}^{\{x,y\}}), \subseteq)$ be complete lattices.

a) Define a Galois insertion (α, γ) for the above lattices. Show that it is a Galois insertion.

b) Let the semantics $[\![b]\!]$ for boolean expressions b denote the set of states that satisfy b. Show that $[\![assume\ b]\!]^{\#}(s) := s \cap \alpha([\![b]\!])$ is a sound approximation for $[\![assume\ b]\!]$.

c) Give the best approximation $[\![x--]\!]^{\#}$ for $[\![x--]\!]$. Is the best approximation also an exact approximation?

Exercise 2.2 (Best and Exact Approximations)
Let (α, γ) be a Galois connection between $(C, \subseteq)$ and $(A, \sqsubseteq)$. Let $f : C \mapsto C$ be a function. Prove or disprove:

a) An exact approximation of f is also the best approximation of f.

b) If (α, γ) is a Galois insertion, then an exact approximation of f is also a best approximation of f.

c) There is an abstract domain $(A', \sqsubseteq')$ and a Galois insertion (α', γ') between $(C, \subseteq)$ and $(A', \sqsubseteq')$ so that f has a computable exact approximation.

d) Consider a sound approximation $f^{\#}$ for f. Then, $f^{\#}$ is an exact approximation if and only if $f^{\#} \circ \alpha \sqsubseteq \alpha \circ f$.

Exercise 2.3 (Well Quasi Orderings)
Prove or disprove that the following are well quasi orderings:

a) The lexicographical order $(\{0,1\}^*, \leq_{lex})$ over binary words:

$u \leq_{lex} v$ if and only if u is a prefix of v or the first symbol $u[\ell]$ that does not coincide with $v[\ell]$ satisfies $u[\ell] < v[\ell]$.

Note that $u[\ell]$ refers to the ℓ-th symbol of u.

b) The colexicographical order $(\{0,1\}^*, \leq_{colex})$ defined by:

$u \leq_{colex} v$ if and only if u is a postfix of v or the last symbol $u[\ell]$ that does not coincide with $v[\ell]$ satisfies $u[\ell] < v[\ell]$.

c) The radix order $(\{0,1\}^*, \leq_{radix})$ over binary words:

$$u \leq_{radix} v \text{ if and only if } |u| < |v| \text{ or } |u| = |v| \wedge u \leq_{lex} v$$

d) The quasi ordering $(\mathbb{N}, |)$, where $a \mid b$ means that a divides b.

e) The quasi ordering $(\mathbb{N} \times \mathbb{N}, \leq_2)$ with $(n, m) \leq_2 (n', m')$ if $n \leq n'$ and $m \leq m'$.

Exercise 2.4 (Termination for Well-structured Programs)
Let $(\Sigma, \mathit{COM}, [\![-]\!])$ be a well-structured domain with wpo $\leq \subseteq \Sigma \times \Sigma$ that is a simulation wrt. $[\![\mathit{com}]\!]$ for all $\mathit{com} \in \mathit{COM}$. Let p be a (well-structured) program. Recall that we lift the well-structured domain to configurations $\Gamma_p \subseteq W(\mathit{COM}) \times \Sigma$. Here, Γ_p denotes the restriction of configurations to the finitely many control states that occur in p.
Assume that

- $\sigma \leq \sigma'$ is decidable for each $\sigma, \sigma' \in \Sigma$,
- the set $\mathit{post}(\sigma, \mathit{com}) = \{\sigma' \mid (\sigma, \sigma') \in [\![\mathit{com}]\!]\}$ is finite for each $\sigma \in \Sigma$ and $\mathit{com} \in \mathit{COM}$, and post is a computable function.

Then, p is called *terminating for* $\sigma_0 \in \Sigma$ if every computation (transition sequence in small-step semantics) starting in $(p, \sigma_0) \in \Gamma$ is finite.

Show that the *termination problem* is decidable. That is, given a well-structured program p and inital state σ_0 like above, decide whether p is terminating for σ_0.