SS 2025 17.04.2025

Exercises to the lecture
Semantics
Sheet 1

Prof. Dr. Roland Meyer
Jan Grünke Delivery until 23.04.2025 at 23:59

Exercise 1.1 (Semantics of Arithmetic & Boolean Expressions)
Let arithmetic expressions $AExp$ and boolean expressions $BExp$ be given by the following grammar

$$a ::= x \mid n \mid a_1 + a_2 \mid a_1 * a_2$$
$$b ::= true \mid a_1 <= a_2 \mid !b \mid b_1 \mathbin{\&\&} b_2$$

with variables $x \in \mathit{Vars}$ and $n \in \mathbb{Z}$. Let states be a functions from variables to integers $\Sigma := \mathbb{Z}^{\mathit{Vars}}$ and configurations be $\Gamma := BExp \times \Sigma$.

(a) Define a small-step semantic $TS[\![-]\!]$ for arithmetic and boolean expressions.

(b) Define denotational semantics $PT[\![-]\!] : AExp \to \mathbb{Z}^{\Sigma}$ for arithmetic expressions and $PT[\![-]\!] : BExp \to \mathcal{P}(\Sigma)$ for boolean expressions.

(c) Evaluate $[0 * (x + 3) <= 4] \mathbin{\&\&} !(x <= 2)$ in both semantics for $\sigma := \{x \mapsto 1\} \in \Sigma$.

Exercise 1.2 (k-Induction)
In this exercise we consider k-inductive invariants that are a generalisation of inductive invariants. An invariant I is *k-inductive* if

1. $\forall 0 \leq i < k.\ Init{\to^i} \subseteq I$.
2. $(I{\to_I^{k-1}}){\to} \subseteq I$ with $\to_I := \to \cap (I \times I)$

holds. Note that standard inductive invariants are 1-inductive.
Consider the program p, given by

```
1: x := 1
   y := 2
   z := 3
2: while true do
3:     t := x
       x := y
       y := z
       z := t
4: end while
```

with configurations $\Gamma := \{1, \ldots, 4\} \times \Sigma$ and states $\Sigma := \mathbb{Z}^{\{x,y,z,t\}}$. For this exercise, we combine several commands into one, e.g. the first command is $[x := 1; y := 2; z := 3]$. This simplifies the transition relation of the small-step semantics which, for example, contains the following transition $(1, [0, 0, 0, 0]) \to (2, [1, 2, 3, 0])$.
The goal of this excercise is to prove safety for p wrt. $Bad := \{2\} \times \{\sigma \in \Sigma \mid [\![x = y]\!](\sigma)\}$.
A naive invariant for p that is safe wrt. Bad is $\overline{Bad}$.

(a) Show that $\overline{Bad}$ is not 1-inductive.

(b) Show that $\overline{Bad}$ is k-inductive for some $k > 1$.

(c) Give an 1-inductive invariant I_1 that is a strengthening of $\overline{Bad}$ ($I_1 \subseteq \overline{Bad}$).

(d) Show that k-induction is sound and complete for proving safety for all $k \in \mathbb{N}_{>0}$: $Reach(p) \cap Bad = \emptyset$ if and only if there is a k-inductive invariant for p that is safe wrt. Bad.

Exercise 1.3 (Galois Connections)
For each of the following pairs (α, γ), state whether it is a Galois connection. If this is not the case, give a counterargument or counterexample for each.

	L	M	α	γ
a)	$(\mathbb{Z}_{\pm\infty}, \leq)$	$(\mathbb{P}(\mathbb{Z}), \subseteq)$	$z \mapsto \{z\}, -\infty \mapsto \emptyset, \infty \mapsto \mathbb{Z}$	$m \mapsto \bigsqcup\{z \mid z \in m\}$
b)	$(\mathbb{P}(\mathbb{Z}), \subseteq)$	$(\mathbb{Z}_{\pm\infty}, \leq)$	$l \mapsto \bigsqcup\{z \mid z \in l\}$	$z \mapsto \{z\}, -\infty \mapsto \emptyset, \infty \mapsto \mathbb{Z}$
c)	$(\mathbb{Z} \cup \{\bot, \top\}, \sqsubseteq)$	$(\mathbb{P}(\mathbb{Z}), \subseteq)$	$z \mapsto \{z\}, \top \mapsto \mathbb{Z}, \bot \mapsto \emptyset$	$m \mapsto \bigsqcup\{a \mid a \in m\}$
d)	$(\mathbb{Z}_{\pm\infty}, \leq)$	$(\mathbb{Z}^2_{\pm\infty}, \leq^2)$	$l \mapsto (l, l)$	$(l_1, l_2) \mapsto l_1$
e)	$(\mathcal{P}(\mathbb{R}^2), \subseteq)$	$(\operatorname{conv} \mathbb{R}^2, \subseteq)$	$l \mapsto \operatorname{conv}(l)$	$m \mapsto m$

Here we use

- $z \in \mathbb{Z}, l \in L, m \in M$.
- $\mathbb{Z}_{\pm\infty} := \mathbb{Z} \cup \{-\infty, +\infty\}$ and for all $z \in \mathbb{Z}. -\infty \leq z \leq +\infty$ holds.
- $z_1 \sqsubseteq z_2$ iff $z_1 = \bot \vee z_2 = \top$.
- $(l_1, l_2) \leq^2 (l_3, l_4)$ if $l_1 \leq l_3$ and $l_2 \leq l_4$ for $l_1, l_2, l_3, l_4 \in \mathbb{Z}_{\pm\infty}$.
- $\operatorname{conv} \mathbb{R}^2$ the *convex sets* over $\mathbb{R}^2$ or $\operatorname{conv}(l)$ the *convex hull* of l. A subset $m \subseteq \mathbb{R}^2$ is called convex if every connecting line between two points in m itself lies completely in m. The convex hull $\operatorname{conv}(l)$ is the smallest convex set m that contains l.