General Remarks

- Please hand in your solutions in groups of 3. Either hand in your solutions at the beginning of the exercise class or put them into the box at the chair.
- If you have questions regarding the exercises and/or lecture, feel free to write us an email or visit us at our office.

Exercise 1 (Galois Insertions): (4 Points)

For most Galois connection we considered so far we observed the special case that $\alpha(\gamma(m)) = m$. These Galois connections are referred to as *Galois insertions*:

(α, γ) is a *Galois insertion* between the complete lattices L and M if and only if:

$$\alpha : L \to M \textit{ and } \gamma : M \to L \text{ are monotone functions}$$

that satisfy:

$$\begin{array}{rcll} \gamma(\alpha(l)) & \sqsupseteq & l & \forall\, l \in L \\ \alpha(\gamma(m)) & = & m & \forall\, m \in M \end{array}$$

Show that for a Galois connection (α, γ) between L and M the following claims are equivalent:

(i) (α, γ) is a Galois insertion

(ii) γ is injective

(iii) α is surjective

(iv) $\forall\, m_1, m_2 : \; m_1 \sqsubseteq m_2 \Leftrightarrow \gamma(m_1) \sqsubseteq \gamma(m_2)$

Exercise 2 (Modulo Abstraction): (4 Points)

For a single integer, modulo abstraction is defined by the mapping $\mathbb{Z} \to \{0, \ldots, n-1\} : z \mapsto (z \mod n)$ for some fixed $n \geq 1$.

a) Give the definition of the corresponding abstraction and concretization functions operating on sets of integers, and show that they form a Galois connection.

b) Extract the functions $+^\sharp_n$, $*^\sharp_n$, $(\mod m)^\sharp_n$ and relations $=^\sharp_n$, $>^\sharp_n$ as safe approximations of $+$, $*$, $\mod m$, $=$ and $>$.

c) Depict the reachable fragment of the abstract transition system for the following `WHILE`-program for the modulo abstraction with $n = 4$.

```
x := 3 * x;
while (¬(x mod 4 = 0))
  if (x mod 4 = 1)
    x := 3 * x;
  x := x + 1;
```

Exercise 3 (Granularity of Sign Abstraction): (2 Points)

Consider the following WHILE program:

```
while  x > y  do
    y := -x;
    x := x * y;
```

Let x and y be input variables. Determine the abstract states reachable from the initial state using the extraction function $\beta : \mathbb{Z} \to \{-, 0, +\}$, $\beta(z) := sgn(z)$ (lifted to the following abstract domains in a straightforward manner)

1. for the abstract domain $Var \to 2^{SGN}$
2. for the abstract domain $2^{Var \to SGN}$

where $SGN = \{-, 0, +\}$.