# Exercises 7

**Exercise 1** (Iterating sp and wp)**.** This question is inspired by relationships in a transition system. Let $S$ be a non-empty set of states and $r \subseteq S \times S$. As usual, define

- for every $P \subseteq S$, $sp(P, r) = \{x' \mid \exists x \in P.(x, x') \in r\}$
- for every $Q \subseteq S$, $wp(r, Q) = \{x \mid \forall x'.(x, x') \in r \rightarrow x' \in Q\}$

Let $C = 2^S = \{X \mid X \subseteq S\}$ be the set of all sets of states. Let also: $Init \subseteq S$ and $Good \subseteq S$. Define:

- $F : C \rightarrow C$ as $F(X) = Init \cup sp(X, r)$
- $B : C \rightarrow C$ as $B(Y) = Good \cap wp(r, Y)$
- $l = \bigcup_{i \geq 0} F^i(\emptyset)$
- $h = \bigcap_{i \geq 0} B^i(S)$

The ordering relation we consider is $\subseteq$ relation on $C$. For each of the following determine if the property holds or not. If it holds, prove it. If it doesn't, give a counterexample.

1. $F$ is monotonic
   **Solution:** *True. When $X$ becomes a superset, so does $sp(X, r)$ and thus $Init \cup sp(X, r)$.* $\Diamond$
2. $B$ is monotonic **Solution:** *True. When $Y$ becomes a superset, so does $wp(r, Y)$ as $Q$ appears on the right-hand side of $\rightarrow$ in the definition of wp. Also $\cap$ is monotonic, so the entire expression becomes a superset.* $\Diamond$
3. $l$ is the least fixed point of $F$. **Solution:** *True. $F$ is omega-continuous with respect to $\subseteq$ relation on $S$, with a proof a minor variation of "Union-Distributivity in case of Increasing Sequence" in Lecture 14.* $\Diamond$
4. $h$ is the greatest fixed point of $B$. **Solution:** *True. This can be shown directly using the $\supseteq$ instead of $\subseteq$ order, or as follows. From Lecture 13 we have that $wp(r, Q) = S \setminus sp(S \setminus Q, r^{-1})$ so*

$$B(Y) = Good \cap S \setminus sp(S \setminus Y, r^{-1})$$

*Define $B_1(Z) = S \setminus B(S \setminus Z)$ (thus $B(Y) = S \setminus B_1(S \setminus Y)$) and let $Bad = S \setminus Good$. Then*

$$B_1(Z) = Bad \cup sp(Z, r^{-1})$$

*which has the same form as for $F$ (but with $r^{-1}$ as relation and $Bad$ playing the role of $Init$). Consider the sequence*

$$\emptyset, B_1(\emptyset), \ldots, B_1^i(\emptyset), \ldots$$

*which represents states that can be reached going from error states backwards. The elements of that sequence are complements of the sequence*

$$S, B(S), \ldots, B^i(S), \ldots$$

*which follows by induction on $i$ and definition of $B_1$:*

$B_1^{i+1}(S) = B_1(B_1^i(\emptyset)) =$ *(I.H.)* $B_1(S \setminus B^i(S)) =$ *(definition of $B_1$)* $S \setminus B(B^i(S)) = S \setminus B^{i+1}(S)$

*The sequence of $B_1$ converges to least fixed point of $B_1$, so the sequence of $B$ converges to the greatest fixed point of $B$. The result to which it converges is given using $\bigcup$ when the sequence is increasing and using $\bigcap$ when it is decreasing. $\Diamond$*

5. $l \subseteq h$. **Solution:** *Not necessarily. In fact, this condition holds precisely when $Good$ is an invariant of a transition system with the initial set $Init$ and a transition relation $r$. $l$ represents reachable states starting from $Init$ and making steps using relation $r$. On the other hand, $h$ represents states that are guaranteed to stay inside the set $Good$. As a counterexample, let $S = \{0, 1\}$, $Init = Good = \{0\}$ and $r = \{(0, 1)\}$. Then $l = \{0, 1\}$. Computation shows that $h = \emptyset$ because $Good \cap wp(r, Good) = \{0\} \cap \{1\} = \emptyset$. $\Diamond$*

6. $l \subseteq Good$ implies $Init \subseteq h$ **Solution:** *True. Both conditions are stating that reachable states remain inside $Good$, that is, that there is no finite sequence $s_0, s_1, \ldots, s_n$ such that $n \geq 0$, $s_0 \in Init$, $s_n \in Bad$ and, for all $0 \leq i < n$, $(s_i, s_{i+1}) \in r$:*

$$\begin{array}{l} l \subseteq Good \\ \bigcup_{i \geq 0} F^i(\emptyset) \subseteq Good \\ \forall i \geq 0.\ F^i(\emptyset) \subseteq Good \\ \forall i \geq 0.\ F^i(\emptyset) \cap Bad = \emptyset \\ \forall i. \geq 0.\ r^i[Init] \cap Bad = \emptyset \end{array}$$

*whereas*

$$
\begin{array}{l}
Init \subseteq h \\
Init \subseteq \bigcap_{i \geq 0} B^i(S) \\
\forall i \geq 0.\ Init \subseteq B^i(S) \\
\forall i \geq 0.\ Init \subseteq (S \setminus B_1^i(\emptyset)) \\
\forall i \geq 0.\ Init \cap B_1^i(\emptyset) = \emptyset \\
\forall i \geq 0.\ Init \cap \left(r^{-1}\right)^i [Bad] = \emptyset
\end{array}
$$

$\Diamond$

7. $Init \subseteq h$ implies $l \subseteq Good$ **Solution:** *True. See the explanation for the previous case.* $\Diamond$

**Exercise 2** (Fix points in lattices)**.** Consider a complete lattice with the set of elements $L$ and the partial order $\sqsubseteq$. (Remember that in a complete lattice, every set $X \subseteq L$ has the least upper bound and the greatest lower bound.)

Let $G : L \to L$ be a monotonic function with respect to $\sqsubseteq$. Let

$$Fix = \{x \in L \mid G(x) = x\}$$

be the set of all fixed points. Let $x, y \in Fix$ be two fixed points. Prove or disprove:

1. $x \sqcup y \sqsubseteq G(x \sqcup y)$ **Solution:** *True. We have $x \sqsubseteq x \sqcup y$ (because $x \sqcup y$ is an upper bound on $\{x, y\}$). By monotonicity of $G$, then $G(x) \sqsubseteq G(x \sqcup y)$. Analogously we obtain $G(y) \sqsubseteq G(x \sqcup y)$. This means that $G(x \sqcup y)$ is one upper bound on the set $\{G(x), G(y)\}$. Thus, the least among the upper bounds is smaller than it:*

   $$G(x) \sqcup G(y) \quad \sqsubseteq \quad G(x \sqcup y)$$

   *We have $G(x) = x$ and $G(y) = y$ because $x, y \in Fix$, so the desired property holds.* $\Diamond$

2. $G(x \sqcup y) \sqsubseteq x \sqcup y$ **Solution:** *False. The property would hold if $G$ was distributing over $\sqcup$, so we need to find an example where this is not the case. There are many counterexamples, but let us take inspiration from the counter-example to union-distributivity of contexts $E$ in Lecture 14. Take $L$ to be the set of all relations on the set $S = \{1, 2, 3\}$ with $\sqcup$ be $\cup$ and and define $G(r) = \Delta_S \cup (r \circ r)$. Then any reflective and transitive relation is a fixed point of $G$, including*

   $$r_1 = \{(1, 1), (1, 2), (2, 2)\}$$

   $$r_2 = \{(2, 2), (2, 3), (3, 3)\}$$

*We gave $r_1 \cup r_2 = \{(1,1),(1,2),(2,2),(2,3),(3,3)\}$, which is not transitive. $G(r_1 \cup r_2)$ does contain $(1,3)$, so the inclusion does not hold.* $\Diamond$

3. $x \sqcup y \in Fix$ **Solution:** *False. By definition, $x \sqcup y \in Fix$ means $G(x \sqcup y) = x \sqcup y$ and this implies $G(x \sqcup y) \sqsubseteq x \sqcup y$, which we have just shown to be false.* $\Diamond$

4. Let $B = \{b \in Fix \mid x \sqsubseteq b \wedge y \sqsubseteq b\}$. Then $B$ has the least element, that is, an element $z \in B$ such that $\forall b \in B.\ z \sqsubseteq b$ (Possibly difficult.) **Solution:** *True. The statement says that there exists the least upper bound, with respect to our existing ordering, in the set of fixed points. Note that this will not generally be $x \sqcup y$ but, by definition we will have $x \sqcup y \sqsubseteq z$ as $z \in B$. Inspired by the proof that the least fixed point of $G$ is*

$$\sqcap\{u \in L \mid G(u) \sqsubseteq u\}$$

*let us consider a similar set restricted to elements above $x \sqcup y$ and define:*

$$M = \{u \in L \mid x \sqcup y \sqsubseteq u \ \wedge\ G(u) \sqsubseteq u\}$$

*We then repeat the proof for the version of Tarski's fixed point theorem that we stated at the beginning of Lecture 20, but using $M$ instead of $Post$ as the set. Let $z = \sqcap M$. Take any $u \in M$. Then $z \sqsubseteq u$ as $z$ is a lower bound. By monotonicity, $G(z) \sqsubseteq G(u) \sqsubseteq u$. Thus, $G(z)$ is a lower bound on $M$. Since $z$ is the greatest of the lower bounds on $M$, we get $G(z) \sqsubseteq z$. By definition of $M$, it is also the case that $x \sqcup y$ is a lower bound on $M$, so $x \sqcup y \sqsubseteq z$. Thus, $z \in M$. By monotonicity $G(G(z)) \sqsubseteq G(z)$ and $G(x \sqcup y) \sqsubseteq G(z)$. By previous part, $x \sqcup y \sqsubseteq G(x \sqcup y) \sqsubseteq G(z)$. We thus get that also $G(z) \in M$. Since $z$ is a lower bound on $M$, $z \sqsubseteq G(z)$. Thus, we have $G(z) = z$, so $z \in Fix$. So, everything worked similarly as in the original proof.*

*From $z \in M$ we have $x \sqsubseteq z$ and $y \sqsubseteq z$. We have also shown $z \in Fix$, so $z \in B$. We will show that $z \sqsubseteq b$ for all $b \in B$. Fix arbitrary $b \in B$. Then $x \sqcup y \sqsubseteq b$ and $G(b) = b$ so $G(b) \sqsubseteq b$. Thus also $b \in M$ (indeed, $B \subseteq M$). Since $z$ is a lower bound on $M$, we have $z \sqsubseteq b$. Thus, we have shown that $z$ is the least element of $B$.* $\Diamond$

**Exercise 3** (Abstract interpretation)**.** Consider a program on two integer variables, that is the set of states is $C = 2^{\mathbb{Z}\times\mathbb{Z}}$. We want to represent these states in an abstract domain such that this set of state is represented exactly for the first variable, and as intervals for the second variables.

1. Express the lattice $A$ corresonding to this domain. **Solution:** *Note $\mathcal{I}(\mathbb{Z})$ the set of intervals. $A$ can be represented as the set of functions $Z \to \mathcal{I}(\mathbb{Z})$. Note that this is not the same as $2^{\mathbb{Z}} \times \mathcal{I}(\mathbb{Z})$. To obtain the*

*intuition of why a set of function appears, consider that the concrete set $2^{\mathbb{Z}\times\mathbb{Z}}$ is isomorphic to*

$$(\mathbb{Z}\times\mathbb{Z})\to 2$$

*, where $2=\{0,1\}$. Then in turn, it is isomorphic to*

$$\mathbb{Z}\to(\mathbb{Z}\to 2)$$

*and finally to*

$$\mathbb{Z}\to 2^{\mathbb{Z}}$$

*So in fact the concrete state over $x$ and $y$ can be seen as the space of function that to any value $x$ maps the set of "possible" values of $y$. Now we restrict those sets of possible value to intervals, giving*

$$A=\mathbb{Z}\to\mathcal{I}(\mathbb{Z})$$

*We now need to prove this is a lattice. Note $\sqcup_{\mathcal{I}}(\mathbb{Z})$ and $\sqcap_{\mathcal{I}}(\mathbb{Z})$ the standard meet and join operations on intervals. We can define the intersection between $f$ and $g\in\mathbb{Z}\to\mathcal{I}(\mathbb{Z})$ as:*

$$(f\sqcup g)(a)=f(a)\sqcup_{\mathcal{I}}(\mathbb{Z})g(a)$$

*And similarly for $\sqcap$. From the fact that intervals form a lattice, it is immediate that those satisfy the properties of lattices. $\Diamond$*

2. Give expressions for $\alpha : C\to A$ and $\gamma : A\to C$ and show that this form a Galois Connection. **Solution:** *Define*

$$\alpha(s)(x)=\mathcal{I}(\{y|(x,y)\in s\})$$

*Where $\mathcal{I}(x)=[\min(x),\max(x)]$, and*

$$\gamma(f)=\{(x,y)\mid y\in f(x)\}.$$

*It is slightly tedious but not difficult to check that those two functions satisfy the conditions*

$$\alpha(s)\sqsubseteq f\iff s\subseteq\gamma(f)$$

*. $\Diamond$*

**Exercise 4** (Program analysis)**.** Consider the program that manipulates two integer variables $x$ and $y$. Consider any assignement of the form $x=e$, where $e$ is a linear combination of integer variables, for example

$$x=2*x-5*y$$

Consider an abstract analysis with independant intervals for both variables. Describe an algorithm that given the syntax tree of $e$, and intervals for $x$ (noted $[a_x, b_x]$) and $y$ (noted $[a_y, b_y]$) computes the new interval $[a, b]$ for $x$ after the assignement statement. **Solution:** *Consider the algorithm that takes as input $a_x, b_x, a_y, b_y, e_x, e_y, e_1$ where $e_x, e_y, e_1$ are the $x$ coefficient, $y$ coefficient and constant offset of $e$, respectively.*

```
1  def nextInterval(ax, bx, ay, by, ex, ey, e1): (Int, Int) = {
2          var nax = min(ex*ax, ex*bx)
3          var nbx = max(ex*ax, ex*bx)
4
5          var nay = min(ey*ay, ey*by)
6          var nby = max(ey*ay, ey*by)
7
8          (nax + nay + e1, nbx + nby + e1)
9  }
```

$\Diamond$