Exercises 6

Exercise 1 (Galois Connection)**.** Remember that a Galois connection is defined by two monotonic functions $\alpha : C \to A$ and $\gamma : A \to C$ between partial orders $\leq$ on C and $\sqsubseteq$ on A, such that

$$\forall a, c. \quad \alpha(c) \sqsubseteq a \iff c \leq \gamma(a) \tag{$*$}$$

a) Show that the condition $(*)$ is equivalent to the conjunction of these two conditions:

$$\forall c. \quad c \leq \gamma(\alpha(c)) \tag{1}$$
$$\forall a. \quad \alpha(\gamma(a)) \sqsubseteq a \tag{2}$$

Solution:

We first show that $(*) \implies (1)$ *and* $(*) \implies (2)$

$$\begin{aligned} & \alpha(c) \sqsubseteq \alpha(c) && \text{by reflexivity of } \sqsubseteq \\ \implies & c \leq \gamma(\alpha(c)) && \text{by } (*) \end{aligned}$$

$$\begin{aligned} & \gamma(a) \leq \gamma(a) && \text{by reflexivity of } \sqsubseteq \\ \implies & \alpha(\gamma(a)) \sqsubseteq a && \text{by } (*) \end{aligned}$$

For the converse we have:

$$\begin{aligned} & \alpha(c) \sqsubseteq a \\ \implies & \gamma(\alpha(c)) \leq \gamma(a) && \text{by monotony of } \gamma \\ \implies & c \leq \gamma(\alpha(c)) \leq \gamma(a) && \text{by } (1) \\ \implies & c \leq \gamma(a) && \text{by transitivity of } \leq \end{aligned}$$

and

$$\begin{aligned} & c \leq \gamma(a) \\ \implies & \alpha(c) \sqsubseteq \alpha(\gamma(a)) && \text{by monotonicity of } \alpha \\ \implies & \alpha(c) \sqsubseteq \alpha(\gamma(a)) \sqsubseteq a && \text{by } (2) \\ \implies & \alpha(c) \sqsubseteq a && \text{by transitivity of } \sqsubseteq \end{aligned}$$

$\Diamond$

b) Let α and γ satisfy the condition of a Galois connection. Show that the following three conditions are equivalent:

1. $\alpha(\gamma(a)) = a$ for all a
2. α is a surjective function
3. γ is an injective function

Solution:

One way to tackle this problem is to show $3 \iff 1$ *and* $1 \iff 2$.

3. $\implies$ **1.** :

Let $a \in A$*:*

$$\begin{aligned}
& \alpha(\gamma(a)) \sqsubseteq a && \text{by (2)} \\
\implies & \gamma(\alpha(\gamma(a))) \leq \gamma(a) && \text{by monotonicity of } \gamma \\
\implies & \gamma(a) \leq \gamma(\alpha(\gamma(a))) \leq \gamma(a) && \text{by (1)} \\
\implies & \gamma(\alpha(\gamma(a))) = \gamma(a) && \text{by antisymmetry of } \leq \\
\implies & \alpha(\gamma(a)) = a && \text{by injectivity of } \gamma
\end{aligned}$$

¬3. $\implies$ **¬1.** :

Suppose there are $a_1 \neq a_2$ *such that* $\gamma(a_1) = \gamma(a_2)$*. We then have* $\alpha(\gamma(a_1)) = \alpha(\gamma(a_2))$*. If* 1. *was true we would have* $a_1 = a_2$ *which is a contradiction.*

1 $\implies$ **2** :

If $\alpha(\gamma(a)) = a$ *for every* $a \in A$*, then for any* a *there exists a* $x \in C$ *such that* $\alpha(x) = a$ *(*x *being* $\gamma(a)$*).*

2 $\implies$ **1** :

Let $a \in A$*, since* α *is surjective, we have, in particular, that there is a* $x \in C$ *such that* $\alpha(x) = a$*.*

$$\begin{aligned}
& \alpha(x) = a && \\
\implies & \alpha(x) \sqsubseteq a && \text{by reflexivity of } \sqsubseteq \\
\implies & x \leq \gamma(a) && \text{by } (*) \\
\implies & \alpha(x) \sqsubseteq \alpha(\gamma(a)) && \text{by monotonicity of } \alpha \\
\implies & a \sqsubseteq \alpha(\gamma(a)) && \\
\implies & a \sqsubseteq \alpha(\gamma(a)) \sqsubseteq a && \text{by (2)} \\
\implies & \alpha(\gamma(a)) = a && \text{by antisymmetry of } \sqsubseteq
\end{aligned}$$

◊

c) State the condition for $c = \gamma(\alpha(c))$ to hold for all c. When C is the set of sets of concrete states and A is a domain of static analysis, is it more reasonable to expect that $c = \gamma(\alpha(c))$ or $\alpha(\gamma(a)) = a$ to be satisfied, and why?

Solution: *When switching to the domain of static analysis we lose information. Therefore, we would expect that $\alpha(\gamma(a)) = a$. However, having $\gamma(\alpha(c)) = c$ would not make sense as it means that the abstract domain holds more information than the set of concrete states. If we still want this condition to hold we would need for γ to be surjective or α to be injective. γ and α would be then the inverse of each other.* ◊

Exercise 2 (lub and glb)**.** Let $(A, \sqsubseteq)$ be a partial order such that every set $S \subseteq A$ has the greatest lower bound.
Prove that then every set $S \subseteq A$ has the least upper bound, or show a counterexample.
What about the lattice with three elements $\{0, 1_a, 1_b\}$ the relations $0 \leq 1_a$ and $0 \leq 1_b$?

Solution: *Suppose we have some arbitrary set $S \subseteq A$, then we know that $\sqcap S$ exists.*
Let U be the set of all its upper bounds, i.e. $U = \{x | \forall y \in S. y \sqsubseteq x\}$. Since every subset of A has a greatest lower bound, we know that $a = \sqcap U$ exists. Now we want to show that a is an upper bound on S and that it is the least one.

We want to show that $\forall y \in S. y \sqsubseteq a$.
Let L be the set of lower bounds on U, i.e. $L = \{z | \forall x \in U. z \sqsubseteq x\}$.
Clearly, $S \subseteq L$, since U are the upper bounds on S.
Then a is the greatest element in L, and thus $\forall y \in S. y \sqsubseteq a$ and so a is an upper bound on S.

Now take any upper bound $x \in U$. Since $a = \sqcap U$, we have $a \sqsubseteq x$ and so a is the least upper bound. ◊

Exercise 3 (Lattices)**.** Consider algebraic structures with signature $(\vee, \wedge)$, each of arity 2, and satisfying the following axioms:

$x \vee y = y \vee x$	($\vee$-Com)	$x \wedge y = y \wedge x$	($\wedge$-Com)
$(x \vee y) \vee z = x \vee (y \vee z)$	($\vee$-Assoc)	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$	($\wedge$-Assoc)
$x \vee x = x$	($\vee$-Idem)	$x \wedge x = x$	($\wedge$-Idem)
$x \vee (x \wedge y) = x$	($\vee$-Abs)	$x \wedge (x \vee y) = x$	($\wedge$-Abs)

a) Show that for any x and y, $x \wedge y = x$ if and only if $x \vee y = y$.

Solution: *Let x, y be two elements of the lattice.*

$(\Longrightarrow)$:

$$\begin{aligned} & x \wedge y = x \\ \Longrightarrow\ & (x \wedge y) \vee y = x \vee y \\ \Longrightarrow\ & y \vee (x \wedge y) = x \vee y && \text{by } (\vee\text{-Com}) \\ \Longrightarrow\ & y \vee (y \wedge x) = x \vee y && \text{by } (\wedge\text{-Com}) \\ \Longrightarrow\ & y = x \vee y && \text{by } (\vee\text{-Abs}) \end{aligned}$$

$(\Longleftarrow)$:

$$\begin{aligned} & x \vee y = y \\ \Longrightarrow\ & x \wedge (x \vee y) = x \wedge y \\ \Longrightarrow\ & x = x \wedge y && \text{by } (\wedge\text{-Abs}) \end{aligned}$$

$\Diamond$

b) Define $x \leq y$ by $x \wedge y = x$. Show that $\leq$ is a partial order relation.

Solution:

Reflexivity: *Immediate from* ($\wedge$-Idem)

Antisymmetry:

$$\begin{aligned} & x \leq y \leq x \\ \Longrightarrow\ & x \wedge y = x \text{ and } y \wedge x = y \\ \Longrightarrow\ & x \wedge y = x \text{ and } y \vee x = x && \text{by a)} \\ \Longrightarrow\ & (y \vee x) \wedge y = x \\ \Longrightarrow\ & y \wedge (y \vee x) = x && \text{by } (\wedge\text{-Com}) \\ \Longrightarrow\ & y = x && \text{by } (\wedge\text{-Abs}) \end{aligned}$$

Transitivity:

$$\begin{aligned} & x \leq y \leq z \\ \Longrightarrow\ & x \wedge y = x \text{ and } y \wedge z = y \\ \Longrightarrow\ & x \wedge y = x \text{ and } x \wedge (y \wedge z) = x \\ \Longrightarrow\ & x \wedge y = x \text{ and } (x \wedge y) \wedge z = x && \text{by } (\wedge\text{-Assoc}) \\ \Longrightarrow\ & x \wedge z = x \\ \Longrightarrow\ & x \leq z \end{aligned}$$

$\Diamond$

c) Show that $\wedge$ and $\vee$ are respectively the binary *greatest lower bound* and *least upper bound* for $\leq$.

Solution: *Let x, y be two elements of the lattice. We will first prove that $x \wedge y$ is a lower bound i.e. $x \wedge y \leq x$ and $x \wedge y \leq y$. We will then show that it is the smallest among them, that is if $z \leq x$ and $z \leq y$ then $z \leq x \wedge y$.*

$$\begin{aligned}
& x \vee (x \wedge y) = x && \text{by } (\vee\text{-Abs}) \\
\Longrightarrow\ & x \wedge (x \wedge y) = x \wedge y && \text{by } a) \\
\Longrightarrow\ & (x \wedge y) \wedge x = x \wedge y && \text{by } (\wedge\text{-Com}) \\
\Longrightarrow\ & x \wedge y \leq x
\end{aligned}$$

$$\begin{aligned}
& y \vee (y \wedge x) = y && \text{by } (\vee\text{-Abs}) \\
\Longrightarrow\ & y \vee (x \wedge y) = y && \text{by } (\wedge\text{-Com}) \\
\Longrightarrow\ & y \wedge (x \wedge y) = x \wedge y && \text{by } a) \\
\Longrightarrow\ & (x \wedge y) \wedge y = x \wedge y && \text{by } (\wedge\text{-Com}) \\
\Longrightarrow\ & x \wedge y \leq y
\end{aligned}$$

Let z an element of the lattice:

$$\begin{aligned}
& z \leq x \text{ and } z \leq y \\
\Longrightarrow\ & z \wedge x = z \text{ and } z \wedge y = z \\
\Longrightarrow\ & (z \wedge x) \wedge y = z \\
\Longrightarrow\ & z \wedge (x \wedge y) = z && \text{by } (\wedge\text{-Assoc}) \\
\Longrightarrow\ & z \leq x \wedge y
\end{aligned}$$

Therefore $\wedge$ is the binary greatest lower bound for $\leq$. The proof for $\vee$ is analogous. $\Diamond$

Exercise 4 (post)**.** let S be any set, $r \subseteq S \times S$ a binary relation and $I \subseteq S$. Define $post : 2^S \to 2^S$ by $post(X) = I \cup r[X]$. Prove that $post$ is monotonic. Does $post$ admit a least fixed point?

Solution: *We first show that post is monotonic.*

$$\begin{aligned}
& X \subseteq Y \\
\Longrightarrow\ & r[X] \subseteq r[Y] \\
\Longrightarrow\ & I \cup r[X] \subseteq I \cup r[Y] \\
\Longrightarrow\ & post(X) \subseteq post(Y)
\end{aligned}$$

Since $(2^S, \subseteq)$ is a complete lattice (see Exercise 5), Tarski's fixed point theorem ensures the existence of a fixpoint for G. $\Diamond$

Exercise 5. Partitioning

a) Show that for any set S, $(2^S, \subseteq)$ is a lattice.

Solution: *We can show that 2^S is a complete lattice by showing that $\subseteq$ is a partial order and that every subset of 2^S has a greatest lower bound and a least upper bound. Reflexivity, antisymmetry and transitivity of $\subseteq$ can easily be checked by unfolding the definitions.*

Given $P \subseteq 2^S$, we claim that $\bigcup_{s \in P} s$ is the least upper bound of P. Indeed we have $\forall s' \in P,\ s' \subseteq \bigcup_{s \in P} s$ and for any $b \in 2^S$,

$$(\forall s' \in P, s' \subseteq b) \leftrightarrow \bigcup_{s \in P} s \subseteq b$$

Analogously we can prove that $\bigcap_{s \in P} s$ is the greatest lower bound of P.

$\Diamond$

b) Consider a set $S = P \times V$. For each set $g \in 2^{P \times V}$, define $\bar{g} : P \to 2^V$ by $\bar{g}(p) = \{v \mid (p, v) \in g\}$. Show that the bar function $\bar{\cdot}$ defines a bijection between $2^{P \times V}$ and $P \to 2^V$.

Solution: *We show that the bar function is a bijection by defining another operator and proving that they are the inverse of each other:*

$$inv : \bar{g} \mapsto \{(p, v) \mid v \in \bar{g}(p)\}$$

$$\begin{aligned} inv(\bar{g}) &= \{(p, v) \mid v \in \bar{g}(p)\} \\ &= \{(p, v) \mid v \in \{v \mid (p, v) \in g\}\} \\ &= \{(p, v) \mid (p, v) \in g\} \\ &= g \end{aligned}$$

Let $f : P \to 2^V$:

$$\begin{aligned} \overline{inv(f)} &= p \mapsto \{v \mid (p, v) \in inv(f)\} \\ &= p \mapsto \{v \mid (p, v) \in \{(p, v) \mid v \in f(p)\}\} \\ &= p \mapsto \{v \mid v \in f(p)\} \\ &= p \mapsto f(p) \\ &= f \end{aligned}$$

$\Diamond$

c) Consider the set of all functions $P \to 2^V$. Define a lattice on this set that is isomorphic to $(2^{P \times V}, \subseteq)$.

Solution:

We define the following operators and relations on $P \to 2^V$ and prove that $\bar{\cdot}$ is a lattice isomorphism:

$$f_1 \cap f_2 = p \mapsto f_1(p) \cap f_2(p) \qquad f_1 \cup f_2 = p \mapsto f_1(p) \cup f_2(p)$$
$$f_1 \subseteq f_2 \iff \forall p \in P.\, f_1(p) \subseteq f_2(p)$$

In particular we have that $f_1 \subseteq f_2 \iff f_1 \cap f_2 = f_1$. We start by proving that it is a homomorphism:

$$\begin{aligned}
\overline{g_1 \cap g_2} &= p \mapsto \{v \mid (p, v) \in g_1 \cap g_2\} \\
&= p \mapsto \{v \mid (p, v) \in g_1 \wedge (p, v) \in g_2\} \\
&= p \mapsto \{v \mid (p, v) \in g_1\} \cap \{v \mid (p, v) \in g_2\} \\
&= p \mapsto \overline{g_1}(p) \cap \overline{g_2}(p) \\
&= \overline{g_1} \cap \overline{g_2}
\end{aligned}$$

$$\begin{aligned}
\overline{g_1 \cup g_2} &= p \mapsto \{v \mid (p, v) \in g_1 \cup g_2\} \\
&= p \mapsto \{v \mid (p, v) \in g_1 \vee (p, v) \in g_2\} \\
&= p \mapsto \{v \mid (p, v) \in g_1\} \cup \{v \mid (p, v) \in g_2\} \\
&= p \mapsto \overline{g_1}(p) \cup \overline{g_2}(p) \\
&= \overline{g_1} \cup \overline{g_2}
\end{aligned}$$

We then derive $\overline{g_1} \subseteq \overline{g_2} \iff g_1 \subseteq g_2$ from the above equalities.

$$\begin{aligned}
\overline{g_1} \subseteq \overline{g_2} &\iff \overline{g_1} \cap \overline{g_2} = \overline{g_1} \\
&\iff \overline{g_1 \cap g_2} = \overline{g_1} \\
&\iff g_1 \cap g_2 = g_1
\end{aligned}$$

$\Diamond$