Semantics of Programming Languages
Solutions to Assignment 11

Patrick Maier, Jan Schwinghammer
http://www.ps.uni-sb.de/courses/sem-ws01/

Exercise 11.1 Let $x \in D$ and $y \in D^\#$. We have to show that $\alpha(x) \sqsubseteq y \Leftrightarrow x \leq \gamma(y)$.

Assume $\alpha(x) \sqsubseteq y$, then by definition of $\sqsubseteq$, for all $l \in L$, $\alpha(x)(l) \leq y(l)$. So for all $l \in L$, $x \wedge \delta(l) = \alpha(x)(l) \leq y(l) \leq \bigvee_{l \in L} y(l) = \gamma(y)$, i. e., $\gamma(y)$ is an upper bound of $x \wedge \delta(l)$. Therefore, $\bigvee_{l \in L}(x \wedge \delta(l)) \leq \gamma(y)$. And finally by the cover property of δ and by distributivity of the join over meets in $\mathbf{D}$, $x = x \wedge \top = x \wedge \bigvee_{l \in L} \delta(l) = \bigvee_{l \in L}(x \wedge \delta(l)) \leq \gamma(y)$.

Now assume $x \leq \gamma(y)$ and fix $k \in L$. From $x \leq \gamma(y) = \bigvee_{l \in L} y(l)$ and distributivity follows $x \wedge \delta(k) \leq (\bigvee_{l \in L} y(l)) \wedge \delta(k) = \bigvee_{l \in L}(y(l) \wedge \delta(k))$. Note that by definition of $D^\#$, for all $l \in L$, $y(l) \in \{x' \wedge \delta(l) \mid x' \in D\}$, i. e., for all $l \in L$ exists $x' \in D$ such that $y(l) = x' \wedge \delta(l) \leq \delta(l)$. Therefore, $y(l) \wedge \delta(k) = y(k)$ if $l = k$. If $l \neq k$ then $y(l) \wedge \delta(k) = \bot$ because $y(l) \wedge \delta(k) \leq \delta(l) \wedge \delta(k) = \bot$ by the disjointness property of δ. Thus, $\bigvee_{l \in L}(y(l) \wedge \delta(k)) = y(k)$, so finally $\alpha(x)(k) = x \wedge \delta(k) \leq \bigvee_{l \in L}(y(l) \wedge \delta(k)) = y(k)$. As k was chosen arbitrary, we conclude $\alpha(x) \sqsubseteq y$ by definition of $\sqsubseteq$.

Exercise 11.2 For any set X, proving that $\langle 2^X, \subseteq, \bigcup, \bigcap \rangle$ is a complete lattice amounts to showing that

1. 2^X is non-empty,
2. $\langle 2^X, \subseteq \rangle$ is a poset, i. e., $\subseteq$ is a reflexive, transitive and antisymmetric binary relation on 2^X, and
3. for all $S \subseteq 2^X$, $\bigcup S$ is the least upper bound and $\bigcap S$ the greatest lower bound of S in $\langle 2^X, \subseteq \rangle$.

These are all elementary facts. Just to exemplify a proof of these facts, we show the first half of 3. Let $S \subseteq 2^X$. For all $A \in S$, $A \subseteq \bigcup S$, so $\bigcup S$ is an upper bound of S. Let $U \in 2^X$ be an upper bound of S, i. e., $A \subseteq U$ for all $A \in S$. Then $\bigcup S \subseteq U$ (since for every $x \in \bigcup S$ there is an $A \in S$ such that $x \in A \subseteq U$), so $\bigcup S$ is the least upper bound of S.

To show that the join completely distributes over meets, let $A \in 2^X$ and $S \subseteq 2^X$. Then $A \cap \bigcup S = \bigcup\{A \cap B \mid B \in S\}$ because for all $x \in X$,

$$\begin{aligned} x \in A \cap \bigcup S &\Leftrightarrow x \in A \text{ and } x \in \bigcup S \\ &\Leftrightarrow x \in A \text{ and } \exists B \in S : x \in B \\ &\Leftrightarrow \exists B \in S : x \in A \text{ and } x \in B \\ &\Leftrightarrow \exists B \in S : x \in A \cap B \\ &\Leftrightarrow x \in \bigcup\{A \cap B \mid B \in S\}. \end{aligned}$$

For the second part of the exercise, the natural partition of $\mathbf{D}$ indexed by the program points PP is the one which gathers stores with the same value of the program counter pc, i. e., $\delta(p) = \{s \in \mathit{Store} \mid s(pc) = p\}$. Obviously, $\bigcup_{p \in PP} \{s \in \mathit{Store} \mid s(pc) = p\} = \mathit{Store}$, so δ has the cover property. It also has the disjointness property, i. e., $\{s \in \mathit{Store} \mid s(pc) = p\} \cap \{s \in \mathit{Store} \mid s(pc) = q\} = \emptyset$ for $p, q \in PP$ with $p \neq q$, since stores are functions.

Exercise 11.3 Exercise 11.2 shows that we can apply exercise 11.1 to $\mathbf{D}$ and δ. We obtain the abstract domain $\mathbf{D}^\# = \langle D^\#, \sqsubseteq \rangle$ with $D^\# = \prod_{p \in PP} \{S \cap \delta(p) \mid S \in 2^{\mathit{Store}}\}$ and for all $d, d' \in D^\#$, $d \sqsubseteq d' \Leftrightarrow \forall p \in PP : d(p) \subseteq d'(p)$.

It is easy to see that $D^\# = \prod_{p \in PP} 2^{\delta(p)}$. What remains to prove is that the α and γ which we get from exercise 11.1 are really the required ones. Obviously, $\bigcup_{p \in PP} d(p) = \gamma(d)$ for all $d \in D^\#$. Furthermore, for all $S \in 2^{\mathit{Store}}$ and $p \in PP$, $\{s \in S \mid s(pc) = p\} = S \cap \{s \in \mathit{Store} \mid s(pc) = p\} = S \cap \delta(p) = \alpha(S)(p)$.

Exercise 11.4 The order on $(2^{\mathit{Store}'})^{PP}$ is pointwise inclusion, i. e., for all $e, e' \in (2^{\mathit{Store}'})^{PP}$, $e \sqsubseteq' e'$ iff $\forall p \in PP : e(p) \subseteq e'(p)$.

Define $\varphi : D^\# \to (2^{\mathit{Store}'})^{PP}$ such that for all $p \in PP$, $(\varphi(d))(p) = \{s' \in \mathit{Store}' \mid \exists s \in d(p)\ \forall x \in \mathit{Var}' : s'(x) = s(x)\}$. In words: $\varphi(d)$ eliminates the program counter pc from the stores in $d(p)$ by restricting them to variables in Var'.

We have to prove that φ is full monotone (i. e., $d \sqsubseteq d^* \Leftrightarrow \varphi(d) \sqsubseteq' \varphi(d^*)$ for all $d, d' \in D^\#$) and bijective.

- Let $d, d^* \in D^\#$ such that $d \sqsubseteq d^*$ and fix an arbitrary $p \in PP$. Then $d(p) \subseteq d^*(p)$, so $(\varphi(d))(p) = \{s' \in \mathit{Store}' \mid \exists s \in d(p)\ \forall x \in \mathit{Var}' : s'(x) = s(x)\} \subseteq \{s' \in \mathit{Store}' \mid \exists s \in d^*(p)\ \forall x \in \mathit{Var}' : s'(x) = s(x)\} = (\varphi(d^*))(p)$. As p was chosen arbitrary, $\varphi(d) \sqsubseteq' \varphi(d^*)$, hence φ is monotone.

- Let $d, d^* \in D^\#$ such that $\varphi(d) \sqsubseteq' \varphi(d^*)$ and fix an arbitrary $p \in PP$ and $s \in d(p)$. Then there is $s' \in (\varphi(d))(p)$ such that $s'(x) = s(x)$ for all $x \in \mathit{Var}'$, and since $(\varphi(d))(p) \subseteq (\varphi(d^*))(p)$, there exists $s^* \in d^*(p)$ such that $s^*(x) = s'(x) = s(x)$ for all $x \in \mathit{Var}'$. By exercise 11.3, we know that $d(p), d^*(p) \in 2^{\delta(p)}$, so $s, s^* \in \delta(p)$, which means $s(pc) = p = s^*(pc)$. Hence $s(x) = s^*(x)$ for all $x \in \mathit{Var}$ and therefore $s = s^* \in d^*(p)$. As s was chosen arbitrary, $d(p) \subseteq d^*(p)$, and p was chosen arbitrary, $d \sqsubseteq d^*$, hence φ is even full monotone.

- Full monotone functions are always injective: Let $d, d^* \in D^\#$ such that $\varphi(d) = \varphi(d^*)$. Then $\varphi(d) \sqsubseteq' \varphi(d^*) \wedge \varphi(d^*) \sqsubseteq' \varphi(d)$, so by full monotony $d \sqsubseteq d^* \wedge d^* \sqsubseteq d$, hence $d = d^*$.

- Finally, let $e \in (2^{\mathit{Store}'})^{PP}$. We define $d \in (2^{\mathit{Store}})^{PP}$ such that for all $p \in PP$, $d(p) = \{s \in \mathit{Store} \mid s(pc) = p, \exists s' \in e(p)\ \forall x \in \mathit{Var}' : s(x) = s'(x)\}$. Obviously, $d \in D^\# = \prod_{p \in PP} 2^{\delta(p)}$, see exercise 11.3. It is also obvious that for all $p \in PP$, $(\varphi(d))(p) = e(p)$, i. e., $\varphi(d) = e$, hence φ is surjective.

Exercise 11.5 We define $\alpha' = \varphi \circ \alpha$ and $\gamma' = \gamma \circ \varphi^{-1}$ where α and γ are the Galois connection from exercise 11.3 and φ is the isomorphism from exercise 11.4. To see that this really is a Galois connection, let $S \in 2^{Store}$ and $e \in (2^{Store'})^{PP}$. Then

$$\varphi(\alpha(S)) \sqsubseteq' e \Leftrightarrow \alpha(S) \sqsubseteq \varphi^{-1}(e) \Leftrightarrow S \subseteq \gamma(\varphi^{-1}(e))$$

where the last equivalence is due to $\langle 2^{Store}, \subseteq \rangle \underset{\alpha}{\overset{\gamma}{\rightleftharpoons}} \mathbf{D}^{\#}$ being a Galois connection.

To prove the rest, it suffices to show that α is an order isomorphism and $\gamma = \alpha^{-1}$. We prove this by showing that $\gamma \circ \alpha = id_D$, that $\alpha \circ \gamma = id_{D^{\#}}$ and that α is full monotone.

- Let $S \in 2^{Store}$. Then $\gamma(\alpha(S)) = \bigcup_{p \in PP} \{s \in S \mid s(pc) = p\} = S$. Hence $\gamma \circ \alpha = id_D$.
- Let $d \in D^{\#} = \prod_{p \in PP} 2^{\delta(p)}$ and fix an arbitrary $p \in PP$. Then $\alpha(\gamma(d))(p) = \{s \in \bigcup_{q \in PP} d(q) \mid s(pc) = p\}$. As $d(p) \subseteq \delta(p)$, $s(pc) = p$ for all $s \in d(p)$, so $d(p) \subseteq \alpha(\gamma(d))(p)$. And since α and γ form a Galois connection, $\alpha \circ \gamma$ is reductive, i. e., $\alpha(\gamma(d))(p) \subseteq d(p)$. As p was chosen arbitrary, $\alpha \circ \gamma = id_{D^{\#}}$.
- Let $S, S' \in 2^{Store}$ such that $\alpha(S) \sqsubseteq \alpha(S')$ and fix an arbitrary $s \in S$. Let $p = s(pc)$, then $s \in \alpha(S)(p) \subseteq \alpha(S')(p) \subseteq S'$. As s was chosen arbitrary, $S \subseteq S'$, hence α is full monotone. (Note that we already knew that α was monotone because α and γ form a Galois connection.)

Final remark: These exercises showed that it makes no difference whether control flow is treated implicitly (program counter is part of the store) or explicitly. Exercise: Define the *post* (or *next*) operator in both cases.