1 Denotational Semantics of while-do

Last time, guided by the intuition that the programs while b do c and if b then c ; while b do c else skip should be equivalent, we defined the denotation of the statement while b do c as the least solution to the equation

$$W \triangleq \lambda\sigma \in \Sigma.\begin{cases}(W)^*(\mathcal{C}[\![c]\!]\sigma), & \text{if } \mathcal{B}[\![b]\!]\sigma,\\ \sigma, & \text{otherwise}\end{cases}$$

in $\Sigma \to \Sigma_\perp$; that is, the least fixpoint of the operator

$$\mathcal{F} \triangleq \lambda w \in \Sigma \to \Sigma_\perp .\, \lambda\sigma \in \Sigma.\begin{cases}(w)^*(\mathcal{C}[\![c]\!]\sigma), & \text{if } \mathcal{B}[\![b]\!]\sigma,\\ \sigma, & \text{otherwise}\end{cases}$$

of type $(\Sigma \to \Sigma_\perp) \to (\Sigma \to \Sigma_\perp)$. More simply, we might write

$$\mathcal{F} \triangleq \lambda w \in \Sigma \to \Sigma_\perp .\, \lambda\sigma \in \Sigma.\, \textit{if } \mathcal{B}[\![b]\!]\sigma \textit{ then } (w)^*(\mathcal{C}[\![c]\!]\sigma) \textit{ else } \sigma$$

with the understanding that the if-then-else here is purely mathematical. Here if $w : \Sigma \to \Sigma_\perp$, then $(w)^* : \Sigma_\perp \to \Sigma_\perp$ is the *lift* of w, which sends $\perp$ to $\perp$ and x to $w(x)$ for $x \in \Sigma - \{\perp\}$.

In order to show that the least fixpoint of $\mathcal{F}$ exists, we will apply the Knaster–Tarski theorem. However, we only proved the Knaster–Tarski theorem for the partial order of subsets of some universal set ordered by set inclusion $\subseteq$. We need to extend it to the more general case of chain-complete partial orders (CPOs). To apply this theorem, we must know that the function space $\Sigma \to \Sigma_\perp$ is a CPO and that $\mathcal{F}$ is a continuous map on this space.

2 Chain-Complete Partial Orders and Continuous Functions

Recall that a binary relation $\sqsubseteq$ on a set X is a *partial order* if it is

- *reflexive*: $x \sqsubseteq x$ for all $x \in X$;
- *transitive*: for all $x, y, z \in X$, if $x \sqsubseteq y$ and $y \sqsubseteq z$, then $x \sqsubseteq z$;
- *antisymmetric*: for all $x, y \in X$, if $x \sqsubseteq y$ and $y \sqsubseteq x$, then $x = y$.

It is a *total order* if for all $x, y \in X$, either $x \sqsubseteq y$ or $y \sqsubseteq x$.

If $A \subseteq X$, we say that x is an *upper bound* for A if $y \sqsubseteq x$ for all $y \in A$. We say that x is a *least upper bound* or *supremum* of A if

- x is an upper bound for A, and
- for all other upper bounds y of A, $x \sqsubseteq y$.

Upper bounds and suprema need not exist. For example, the set of natural numbers $\mathbb{N}$ under its natural order $\leq$ has no supremum in $\mathbb{N}$. However, if the supremum of any set exists, it is unique. A partially ordered set is said to be *complete* if all subsets have suprema. The supremum of a set C, if it exists, is denoted $\bigsqcup C$.

Note that all elements of X are (vacuously) upper bounds of the empty set $\varnothing$, so if the supremum of $\varnothing$ exists, then it is necessarily the least element of the entire set. In this case we give it the name $\bot$.

A *chain* is a subset of X that is totally ordered by $\sqsubseteq$. For example, in the partial order of subsets of $\{0, 1, 2\}$ ordered by set inclusion, the set $\{\varnothing, \{2\}, \{1, 2\}, \{0, 1, 2\}\}$ is a chain. A partially ordered set is *chain-complete* if all nonempty chains have suprema. A chain-complete partially ordered set is called a CPO. The empty chain $\varnothing$ is not included in the definition of chain-complete, but if the empty chain also has a supremum, then it is necessarily the least element $\bot$ of the CPO. A CPO with a least element $\bot$ is called *pointed*.

Let X and Y be CPOs (we use $\sqsubseteq$ to denote the partial order in both X and Y). A function $f : X \to Y$ is *monotone* if f preserves order; that is, for all $x, y \in X$, if $x \sqsubseteq y$ then $f(x) \sqsubseteq f(y)$. For example, the exponential function $\lambda x.\, e^x : \mathbb{R} \to \mathbb{R}$ is monotone. A function $f : X \to Y$ is *continuous* if f preserves suprema of nonempty chains; that is, if $C \subseteq X$ is a nonempty chain in X, then $\bigsqcup_{x \in C} f(x)$ exists and equals $f(\bigsqcup C)$. Here $\bigsqcup_{x \in C} f(x)$ is alternate notation for $\bigsqcup \{f(x) \mid x \in C\}$.

Every continuous map is monotone: if $x \sqsubseteq y$, then $y = \bigsqcup\{x, y\}$, so by continuity $f(y) = f(\bigsqcup\{x, y\}) = \bigsqcup\{f(x), f(y)\}$, which implies that $f(x) \sqsubseteq f(y)$.

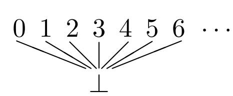
In the definition of continuity, we excluded the empty chain $\varnothing$. If it were included, then a continuous function would have to preserve $\bot$; that is, $f(\bot) = \bot$. A continuous function that satisfies this property is called *strict*. We do not include $\varnothing$ in the definition of continuous functions, because we wish to consider non-strict functions, such as the $\mathcal{F}$ of Section 1.

3 The Knaster–Tarski Theorem in CPOs

Let $F : D \to D$ be any continuous function on a pointed CPO D. Then F has a least fixpoint $\mathit{fix}\, F \stackrel{\triangle}{=} \bigsqcup_n F^n(\bot)$. The proof is a direct generalization of the proof for set operators given in an earlier lecture, where $\bot$ was $\varnothing$ and $\bigsqcup$ was $\bigcup$. In a nutshell: by monotonicity, the $F^n(\bot)$ form a chain; since D is a CPO, the supremum $\mathit{fix}\, F$ of this chain exists; and by continuity, $\mathit{fix}\, F$ is preserved by F.

4 Flat Domains

Let S be a set with the *discrete ordering*, which means that any two distinct elements of S are $\sqsubseteq$-incomparable. We can make S into a pointed CPO $S_\bot$ by adding a new bottom element $\bot$ and defining $\bot \sqsubseteq \bot \sqsubseteq x \sqsubseteq x$ for all $x \in S$, but nothing else. This is called a *flat domain*. For example, $\mathbb{N}_\bot$ looks like



Any flat domain is chain-complete, since every chain is finite, and every finite nonempty chain has a maximum element, which is its supremum.

5 Continuous Functions on CPOs Form a CPO

Now we claim that if C and D are CPOs, then the space of continuous functions $f : C \to D$ is a CPO under the pointwise ordering

$$f \sqsubseteq g \quad \stackrel{\triangle}{\Longleftrightarrow} \quad \forall x \in C\ f(x) \sqsubseteq g(x).$$

This space is denoted $[C \to D]$. It is easily verified that $\sqsubseteq$ is a partial order on $[C \to D]$. If D is pointed with bottom element $\bot$, then $[C \to D]$ is also pointed with bottom element $\bot \stackrel{\triangle}{=} \lambda x \in C.\, \bot$.

We need to show that $[C \to D]$ is chain-complete. Let $\mathcal{C}$ be a nonempty chain in $[C \to D]$. Define

$$G \;\triangleq\; \lambda x \in C.\, \bigsqcup_{g \in \mathcal{C}} g(x).$$

First, G is a well-defined function, since for any $x \in C$, $\{g(x) \mid g \in \mathcal{C}\}$ is a chain in D, therefore its supremum $\bigsqcup_{g \in \mathcal{C}} g(x)$ exists. Also, the function G is continuous, since for any nonempty chain E in C,

$$\begin{array}{rcll} G(\bigsqcup E) & = & \bigsqcup_{g \in \mathcal{C}} g(\bigsqcup E) & \text{by the definition of } G \\ & = & \bigsqcup_{g \in \mathcal{C}} \bigsqcup_{x \in E} g(x) & \text{since each } g \in \mathcal{C} \text{ is continuous} \\ & = & \bigsqcup_{x \in E} \bigsqcup_{g \in \mathcal{C}} g(x) & \text{by the lemma below} \\ & = & \bigsqcup_{x \in E} G(x) & \text{again by the definition of } G. \end{array}$$

The third step in the above argument uses the following lemma.

Lemma 1. *If a_{xy} is a doubly-indexed collection of members of a partially ordered set such that*

(i) *for all x, $\bigsqcup_y a_{xy}$ exists,*

(ii) *for all y, $\bigsqcup_x a_{xy}$ exists, and*

(iii) *$\bigsqcup_y \bigsqcup_x a_{xy}$ exists,*

then $\bigsqcup_x \bigsqcup_y a_{xy}$ exists and is equal to $\bigsqcup_y \bigsqcup_x a_{xy}$.

Proof. Clearly $\bigsqcup_y \bigsqcup_x a_{xy}$ is an upper bound for all a_{xy}, therefore it is an upper bound for all $\bigsqcup_y a_{xy}$; and if b is any other upper bound for all $\bigsqcup_y a_{xy}$, then $a_{xy} \sqsubseteq b$ for all x, y, therefore $\bigsqcup_y \bigsqcup_x a_{xy} \sqsubseteq b$, so $\bigsqcup_y \bigsqcup_x a_{xy}$ is the least upper bound for all $\bigsqcup_y a_{xy}$; that is, $\bigsqcup_x \bigsqcup_y a_{xy} = \bigsqcup_y \bigsqcup_x a_{xy}$. □

To apply this lemma, we need to know that

(i) for all $g \in \mathcal{C}$, $\bigsqcup_{x \in E} g(x)$ exists,

(ii) for all $x \in E$, $\bigsqcup_{g \in \mathcal{C}} g(x)$ exists, and

(iii) $\bigsqcup_{g \in \mathcal{C}} \bigsqcup_{x \in E} g(x)$ exists.

But (i) holds because all $g \in \mathcal{C}$ are continuous, therefore $\bigsqcup_{x \in E} g(x) = g(\bigsqcup E)$; (ii) holds because $\{g(x) \mid g \in \mathcal{C}\}$ is a chain in D, and D is chain-complete; and (iii) follows from (i) and (ii) by taking $x = \bigsqcup E$.

6 Fixpoints and the Semantics of while-do

Now let us return to the denotational semantics of the while loop. We previously defined the function

$$\begin{array}{rcl} \mathcal{F} & : & (\Sigma \to \Sigma_\perp) \;\to\; (\Sigma \to \Sigma_\perp) \\ \mathcal{F} & \triangleq & \lambda w \in \Sigma \to \Sigma_\perp .\, \lambda \sigma \in \Sigma.\, \textit{if } \mathcal{B}[\![b]\!]\sigma \textit{ then } (w)^*(\mathcal{C}[\![c]\!]\sigma) \textit{ else } \sigma. \end{array}$$

Any function $\Sigma \to \Sigma_\perp$ is continuous, since chains in the discrete space Σ contain at most one element, thus the space of functions $\Sigma \to \Sigma_\perp$ is the same as the space of continuous functions $[\Sigma \to \Sigma_\perp]$. Moreover, the lift $(w)^* : \Sigma_\perp \to \Sigma_\perp$ of any function $w : \Sigma \to \Sigma_\perp$ is continuous.

By previous arguments, the function space $[\Sigma \to \Sigma_\perp]$ is a pointed CPO, and $\mathcal{F}$ maps this space to itself. To obtain a least fixpoint by Knaster–Tarski, we need to know that $\mathcal{F}$ is continuous.

Let us first check that it is monotone. This will ensure that, when trying to check the definition of continuity, when C is a chain, $\{\mathcal{F}(d) \mid d \in C\}$ is also a chain, so that $\bigsqcup_{d \in C} \mathcal{F}(d)$ exists. Suppose $d \sqsubseteq d'$. We want to show that $F(d) \sqsubseteq F(d')$. But for all σ,

$$\begin{aligned} \mathcal{F}(d)(\sigma) &= \textit{if } \mathcal{B}[\![b]\!]\sigma \textit{ then } (d)^*(\mathcal{C}[\![c]\!]\sigma) \textit{ else } \sigma \\ &\sqsubseteq \textit{if } \mathcal{B}[\![b]\!]\sigma \textit{ then } (d')^*(\mathcal{C}[\![c]\!]\sigma) \textit{ else } \sigma \\ &= \mathcal{F}(d')(\sigma). \end{aligned}$$

Here we have used the fact that the operator $(\cdot)^*$ is monotone, which is easy to check.

Now let us check that $\mathcal{F}$ is continuous. Let C be an arbitrary chain. We want to show that $\bigsqcup_{d \in C} \mathcal{F}(d) = \mathcal{F}(\bigsqcup C)$. We have

$$\begin{aligned} \bigsqcup_{d \in C} \mathcal{F}(d) &= \bigsqcup_{d \in C} \lambda\sigma.\, \textit{if } \mathcal{B}[\![b]\!]\sigma \textit{ then } (d)^*(\mathcal{C}[\![c]\!]\sigma) \textit{ else } \sigma \\ &= \lambda\sigma.\, \bigsqcup_{d \in C} \textit{if } \mathcal{B}[\![b]\!]\sigma \textit{ then } (d)^*(\mathcal{C}[\![c]\!]\sigma) \textit{ else } \sigma \\ &= \lambda\sigma.\, \textit{if } \mathcal{B}[\![b]\!]\sigma \textit{ then } \bigsqcup_{d \in C} (d)^*(\mathcal{C}[\![c]\!]\sigma) \textit{ else } \sigma \\ &= \lambda\sigma.\, \textit{if } \mathcal{B}[\![b]\!]\sigma \textit{ then } (\bigsqcup C)^*(\mathcal{C}[\![c]\!]\sigma) \textit{ else } \sigma \quad = \quad \mathcal{F}(\bigsqcup C), \end{aligned}$$

since $\mathcal{B}[\![b]\!]\sigma$ does not depend on d and since the lift operator $(\cdot)^*$ is continuous.