Formal Methods in software development

a.a.2017/2018

Prof.Anna Labella

Exercises

We say that a chain, $x_0 \sqsubseteq x_1 \sqsubseteq x_2 \sqsubseteq \ldots$, is *eventually constant* if there exists a natural number k such that for all natural numbers $n \geq k$, we have $x_n = x_k$.

(a) Show that every eventually constant chain has a lub.

(b) Deduce that every finite poset is a cpo.

(c) Show that every monotone function preserves lubs of eventually constant chains.

(d) Deduce the following result: Let D, E be cpos such that all chains in D are eventually constant. All monotone functions $f : D \to E$ are continuous.

Programs as functions

In view of an interpretation of programs in terms of continuous partial functions ….

Why functions?

Because a command can be thought of as a function from states to states
In general a non-total one

Why continuous?

Because we have to preserve l.u.b., in particular fixed points

Programs as functions

We have to guarantee that some constructions give rise to cpo's and to continuous functions

Remember that continuous partial functions are in a cpo.

Binary product of cpo's and domains

The *product* of two cpo's $(D_1, \sqsubseteq_1)$ and $(D_2, \sqsubseteq_2)$ has underlying set

$$D_1 \times D_2 = \{(d_1, d_2) \mid d_1 \in D_1 \,\&\, d_2 \in D_2\}$$

and partial order $\sqsubseteq$ defined by

$$(d_1, d_2) \sqsubseteq (d_1', d_2') \overset{\text{def}}{\Leftrightarrow} d_1 \sqsubseteq_1 d_1' \,\&\, d_2 \sqsubseteq_2 d_2'$$

Lubs of chains are calculated componentwise:

$$\bigsqcup_{n \geq 0} (d_{1,n}, d_{2,n}) = (\bigsqcup_{i \geq 0} d_{1,i}, \bigsqcup_{j \geq 0} d_{2,j}).$$

If $(D_1, \sqsubseteq_1)$ and $(D_2, \sqsubseteq_2)$ are domains so is $(D_1 \times D_2, \sqsubseteq)$ and $\perp_{D_1 \times D_2} = (\perp_{D_1}, \perp_{D_2})$.

Proposition 3.1.1 (Projections and pairing). *Let D_1 and D_2 be cpo's. The* projections

$$\pi_1 : D_1 \times D_2 \to D_1 \qquad \pi_2 : D_1 \times D_2 \to D_2$$

$$\pi_1(d_1, d_2) \stackrel{\text{def}}{=} d_1 \qquad \pi_2(d_1, d_2) \stackrel{\text{def}}{=} d_2$$

are continuous functions. If $f_1 : D \to D_1$ and $f_2 : D \to D_2$ are continuous functions from a cpo D, then

$$\langle f_1, f_2 \rangle : D \to D_1 \times D_2$$

$$\langle f_1, f_2 \rangle(d) \stackrel{\text{def}}{=} (f_1(d), f_2(d))$$

is continuous.

Continuous functions of two arguments

Proposition. *Let D, E and F be cpo's. A function $f : D \times E \to F$ is monotone if and only if it is monotone in each argument separately:*

$$\forall d, d' \in D, e \in E.\, d \sqsubseteq d' \;\Rightarrow\; f(d,e) \sqsubseteq f(d',e)$$
$$\forall d \in D, e, e' \in E.\, e \sqsubseteq e' \;\Rightarrow\; f(d,e) \sqsubseteq f(d,e').$$

Moreover, it is continuous if and only if it preserves lubs of chains in each argument separately:

$$f(\bigsqcup_{m\geq 0} d_m\,,\, e) = \bigsqcup_{m \geq 0} f(d_m, e)$$
$$f(d\,,\, \bigsqcup_{n\geq 0} e_n) = \bigsqcup_{n \geq 0} f(d, e_n).$$

Diagonalising a double chain

Lemma. *Let D be a cpo. Suppose the doubly indexed family of elements $d_{m,n} \in D$ ($m, n \geq 0$) satisfies*

$$(\dagger) \qquad m \leq m' \ \&\ n \leq n' \ \Rightarrow\ d_{m,n} \sqsubseteq d_{m',n'}.$$

Then

$$\bigsqcup_{n\geq 0} d_{0,n} \sqsubseteq \bigsqcup_{n\geq 0} d_{1,n} \sqsubseteq \bigsqcup_{n\geq 0} d_{2,n} \sqsubseteq \ldots$$

and

$$\bigsqcup_{m\geq 0}\left(\bigsqcup_{n\geq 0} d_{m,n}\right) = \bigsqcup_{k\geq 0} d_{k,k} = \bigsqcup_{n\geq 0}\left(\bigsqcup_{m\geq 0} d_{m,n}\right).$$

What is a product?

Given A and B, two structures of the same kind we are looking for an object with two projections in A and B, preserving the structure and s.t.
given another object with two morphisms *f* and *g* in A and B, there is a unique λ making the following diagram commute:

$$
\begin{tikzcd}
 & A \times B \arrow[dl, "\pi_A"'] \arrow[dr, "\pi_B"] & & X \arrow[ll, dashed, "\exists!\lambda"'] \arrow[dl, bend right, "g"'] \arrow[dlll, bend left=40, "f"] \\
A & & B &
\end{tikzcd}
$$

Theorem

Product, if it does exist, is unique up to isomorphisms

examples

Examples

Cartesian product in Sets
Intersection in P(X)
Conjunction in a boolean algebra ………..

What is a sum?

Given A and B, two structures of the same kind we are looking for an object with two injections from A and B, preserving the structure and s.t.
given another object with two morphisms *h* and *k* from A and B, there is a unique μ making the following diagram commute:

$$\begin{tikzcd}
A + B \arrow[rr, dashed, "\exists!\mu"] & & X \\
A \arrow[u, "i_A"] \arrow[urr, bend right, "h"'] & B \arrow[ul, "i_B"'] \arrow[ur, "k"] &
\end{tikzcd}$$

Theorem

Sum, if it does exist, is unique up to isomorphisms

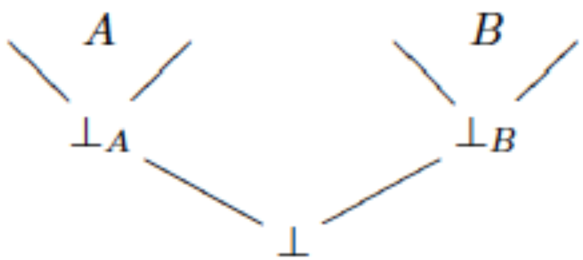
Duality

Examples

Disjoint union in Sets
Union in P(X)
Disjunction in a boolean algebra ………..

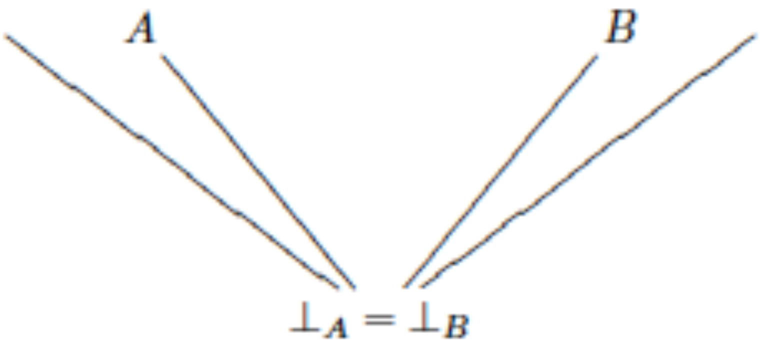
Example: in the universe of domains

Given two domains A and B, we could add a bottom element

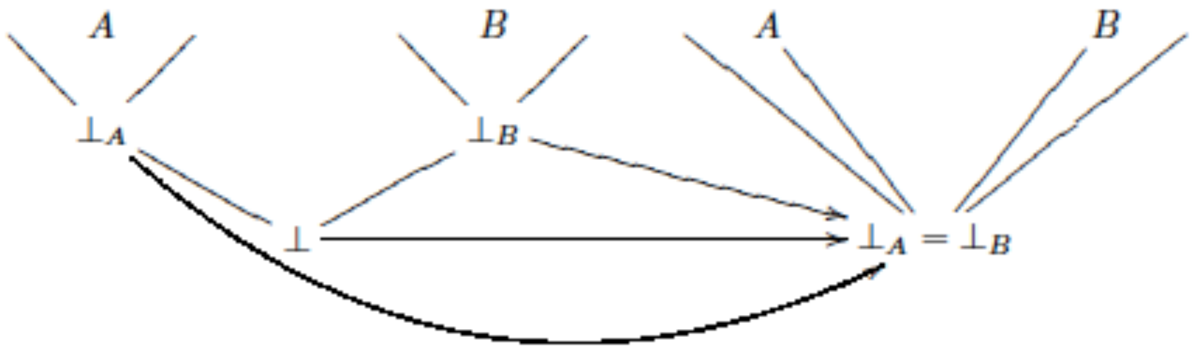


Examples

or make the two bottom elements coincide



Which is the sum?



e.g.