Roberto Bruni, Ugo Montanari

Models of Computation

– Monograph –

March 14, 2016

Springer

Mathematical reasoning may be regarded rather schematically as the exercise of a combination of two facilities, which we may call intuition and ingenuity.

Alan Turing[1]

[1] The purpose of ordinal logics (from Systems of Logic Based on Ordinals), Proceedings of the London Mathematical Society, series 2, vol. 45, 1939.

Contents

Acronyms

$\sim$	operational equivalence in IMP (see Definition 3.3)
$\equiv_{den}$	denotational equivalence in HOFL (see Definition 10.4)
$\equiv_{op}$	operational equivalence in HOFL (see Definition 10.3)
$\simeq$	CCS strong bisimilarity (see Definition 11.5)
$\approx$	CCS weak bisimilarity (see Definition 11.16)
$\cong$	CCS weak observational congruence (see Section 11.7.2)
$\approx_d$	CCS dynamic bisimilarity (see Definition 11.17)
$\overset{\circ}{\sim}_E$	π-calculus early bisimilarity (see Definition 13.3)
$\overset{\circ}{\sim}_L$	π-calculus late bisimilarity (see Definition 13.4)
$\sim_E$	π-calculus strong early full bisimilarity (see Section 13.5.3)
$\sim_L$	π-calculus strong late full bisimilarity (see Section 13.5.3)
$\overset{\bullet}{\approx}_E$	π-calculus weak early bisimilarity (see Section 13.5.4)
$\overset{\bullet}{\approx}_L$	π-calculus weak late bisimilarity (see Section 13.5.4)
$\mathscr{A}$	interpretation function for the denotational semantics of IMP arithmetic expressions (see Section 6.2.1)
ack	Ackermann function (see Example 4.18)
Aexp	set of IMP arithmetic expressions (see Chapter 3)
$\mathscr{B}$	interpretation function for the denotational semantics of IMP boolean expressions (see Section 6.2.2)
Bexp	set of IMP boolean expressions (see Chapter 3)
$\mathbb{B}$	set of booleans
$\mathscr{C}$	interpretation function for the denotational semantics of IMP commands (see Section 6.2.3)
CCS	Calculus of Communicating Systems (see Chapter 11)
Com	set of IMP commands (see Chapter 3)
CPO	Complete Partial Order (see Definition 5.11)
$\text{CPO}_\perp$	Complete Partial Order with bottom (see Definition 5.12)
CSP	Communicating Sequential Processes (see Section 16.2)
CTL	Computation Tree Logic (see Section 12.1.2)
CTMC	Continuous Time Markov Chain (see Definition 14.15)

DTMC	Discrete Time Markov Chain (see Definition 14.14)
Env	set of HOFL environments (see Chapter 9)
fix	(least) fixpoint (see Definition 5.2.2)
FIX	(greatest) fixpoint
gcd	greatest common divisor
HML	Hennessy-Milner modal Logic (see Section 11.5)
HM-Logic	Hennessy-Milner modal Logic (see Section 11.5)
HOFL	A Higher-Order Functional Language (see Chapter 7)
IMP	A simple IMPerative language (see Chapter 3)
int	integer type in HOFL (see Definition 7.2)
Loc	set of locations (see Chapter 3)
LTL	Linear Temporal Logic (see Section 12.1.1)
LTS	Labelled Transition System (see Definition 11.2)
lub	least upper bound (see Definition 5.7)
$\mathbb{N}$	set of natural numbers
$\mathscr{P}$	set of closed CCS processes (see Definition 11.1)
PEPA	Performance Evaluation Process Algebra (see Chapter 16)
Pf	set of partial functions on natural numbers (see Example 5.13)
PI	set of partial injective functions on natural numbers (see Problem 5.12)
PO	Partial Order (see Definition 5.1)
PTS	Probabilistic Transition System (see Section 14.3.2)
$\mathbb{R}$	set of real numbers
$\mathscr{T}$	set of HOFL types (see Definition 7.2)
Tf	set of total functions from $\mathbb{N}$ to $\mathbb{N}_\perp$ (see Example 5.14)
Var	set of HOFL variables (see Chapter 7)
$\mathbb{Z}$	set of integers

Part II
IMP: a simple imperative language

This part focuses on models for sequential computations that are associated to IMP, a simple imperative language. The syntax and natural semantics of IMP are studied in Chapter 3, while its denotational semantics is presented in Chapter 6, where it is also reconciled with the operational semantics. Chapter 4 explains several induction principles exploited to prove properties of programs and semantics. Chapter 5 fixes the mathematical basis of denotational semantics. The concepts in Chapters 4 and 5 are extensively used in Chapter 6 and in the rest of the monograph.

Chapter 5
Partial Orders and Fixpoints

Good old Watson! You are the one fixed point in a changing age.
(Sherlock Holmes)

Abstract This chapter is devoted to the introduction of the foundations of the denotational semantics of computer languages. The concepts of complete partial orders with bottom and of monotone and continuous functions are introduced and then the main fixpoint theorem is presented. The chapter is concluded by studying the immediate consequence operator that is used to relate logical systems and fixpoint theory.

5.1 Orders and Continuous Functions

As we have seen, the operational semantics gives us a very concrete semantics, since the inference rules describe step by step the bare essential operations on the state required to reach the final state of computation. Unlike the operational semantics, the denotational one provides a more abstract view. Indeed, the denotational semantics gives us directly the meaning of the constructs of the language as particular functions over domains. Domains are sets whose structure will ensure the correctness of the constructions of the semantics.

As we will see, one of the most attractive features of the denotational semantics is that it is compositional, namely, *the meaning of a composite program is given by combining the meanings of its constituents*. The compositional property of denotational semantics is obtained by defining the semantics by structural recursion. Obviously there are particular issues in defining the interpretation of the "while" construct of IMP, since the semantics of this construct, as we saw in the previous chapters, is inerently recursive. General recursion is forbidden in structural recursion, which allows only the use of sub-terms. The solution to this problem is given by solving equations of the type $x = f(x)$, namely by finding the fixpoint(s) of suitable functions f. On the one hand we would like to ensure that each recursive definition that we introduce has a fixpoint. Therefore we will restrict our study to a particular class of functions: continuous functions. On the other hand, the aim of the theory we will develop, called domain theory, will be to identify one solution when more than

one are available, and to provide an approximation method for computing it, which is given by the fixpoint theorem (Theorem 5.6).

5.1.1 Orders

We introduce the general theory of partial orders which will bring us to the concept of domain.

Definition 5.1 (Partial order). A *partial order* is a pair $(P, \sqsubseteq_P)$ where P is a set and $\sqsubseteq_P \subseteq P \times P$ is a binary relation (i.e., it is a set of pairs of elements of P) which is:

reflexive: $\forall p \in P.\ p \sqsubseteq_P p$
antisymmetric: $\forall p, q \in P.\ p \sqsubseteq_P q \wedge q \sqsubseteq_P p \Longrightarrow p = q$
transitive: $\forall p, q, r \in P.\ p \sqsubseteq_P q \wedge q \sqsubseteq_P r \Longrightarrow p \sqsubseteq_P r$

We call $(P, \sqsubseteq_P)$ a *poset* (for *partially ordered set*).

We will conveniently omit the subscript P from $\sqsubseteq_P$ when no confusion can arise. We write $p \sqsubset q$ when $p \sqsubseteq q$ and $p \neq q$.

Example 5.1 (Powerset). Let $(\wp(S), \subseteq)$ be the powerset of a set S together with the inclusion relation. It is easy to see that $(\wp(S), \subseteq)$ is a poset.

reflexive: $\forall s \subseteq S.\ s \subseteq s$
antisymmetric: $\forall s_1, s_2 \subseteq S.\ s_1 \subseteq s_2 \wedge s_2 \subseteq s_1 \Rightarrow s_1 = s_2$
transitive: $\forall s_1, s_2, s_3 \subseteq S.\ s_1 \subseteq s_2 \subseteq s_3 \Rightarrow s_1 \subseteq s_3$

Actually, partial orders are a generalization of the concept of powerset ordered by inclusion. Thus we should not be surprised by this result.

Remark 5.1 (Partial orders vs well-founded relations). Partial order relations should not be confused with the well-founded relations studied in the previous chapter. In fact:

- Any well-founded relation (on a non-empty set) is not reflexive (otherwise an infinite descending chain could be constructed by iterating over the same element).
- Any well-founded relation is antisymmetric (the premise $p \sqsubseteq q \wedge q \sqsubseteq p$ must be always false, otherwise an infinite descending chain could be constructed).
- A well-founded relation can be transitive, but it is not necessarily so (e.g., the immediate precedence relation over natural numbers is well-founded but not transitive, instead the 'less than' relation is well-founded and transitive).
- Any (non-empty) partial order has an infinite descending chain (take any element p and the chain $p \sqsupseteq p \sqsupseteq p \ldots$) and is thus non well-founded.
- If we take the relation $\sqsubset$ induced by a partial order $\sqsubseteq$, then it can be well-founded, but it is not necessarily so (e.g., the strict inclusion relation over $\wp(\mathbb{N})$ has an infinite descending chain whose ith element is the set $\{ n \mid n \in \mathbb{N} \wedge n \geq i \}$).

- If we take the reflexive and transitive closure $\prec^*$ of a well-founded relation $\prec$, then it is a partial order (reflexivity and transitivity are obvious, for the antisymmetric property, suppose that there are two elements $p \neq q$ such that $p \prec^* q \wedge q \prec^* p$ then there would be a cycle over p using $\prec$, contradicting the assumption that $\prec$ is well-founded).

Two elements $p, q \in P$ are called *comparable* if $p \sqsubseteq q$ or $q \sqsubseteq p$. When any two elements of a partial order are comparable, then it is called a *total* order.

Definition 5.2 (Total order). Let $(P, \sqsubseteq)$ be a partial order such that:

$$\forall p, q \in P.\ p \sqsubseteq q \ \vee\ q \sqsubseteq p$$

we call $(P, \sqsubseteq)$ a *total order*.

Example 5.2. Given a set S, its powerset $(\wp(S), \subseteq)$ ordered by inclusion is a total order if and only if $|S| \leq 1$. In fact, in one direction suppose that $(\wp(S), \subseteq)$ is a total order and take $p, q \in S$; clearly $\{p\} \subseteq \{q\} \vee \{q\} \subseteq \{p\}$ holds only when $p = q$, i.e., S must have at most one element. Vice versa, if $S = \varnothing$ then $\wp(S) = \{\varnothing\}$ and $\varnothing \subseteq \varnothing$; if $S = \{p\}$ for some p, then $\wp(S) = \{\varnothing, \{p\}\}$ and $\varnothing \subseteq \varnothing \subseteq \{p\} \subseteq \{p\}$.

Theorem 5.1 (Subsets of an order). *Let $(P, \sqsubseteq_P)$ be a partial order and let $Q \subseteq P$. Then $(Q, \sqsubseteq_Q)$ is a partial order, with $\sqsubseteq_Q \stackrel{\text{def}}{=} \sqsubseteq_P \cap (Q \times Q)$. Similarly, if $(P, \sqsubseteq_P)$ is a total order then $(Q, \sqsubseteq_Q)$ is a total order.*

The proof is left as an easy exercise to the reader (see Problem 5.1).

Let us see some examples that will be very useful to understand the concepts of partial and total orders.

Example 5.3 (Natural Numbers). Let $(\mathbb{N}, \leq)$ be the set of natural numbers with the usual order; $(\mathbb{N}, \leq)$ is a total order.

reflexive:	$\forall n \in \mathbb{N}.\ n \leq n$
antisymmetric:	$\forall n, m \in \mathbb{N}.\ n \leq m \wedge m \leq n \Longrightarrow m = n$
transitive:	$\forall n, m, z \in \mathbb{N}.\ n \leq m \wedge m \leq z \Longrightarrow n \leq z$
total:	$\forall n, m \in \mathbb{N}.\ n \leq m \vee m \leq n$

Example 5.4 (Discrete order). Let $(P, \sqsubseteq)$ be a partial order defined as follows:

$$\forall p \in P.\ p \sqsubseteq p$$

Obviously $(P, \sqsubseteq)$ is a partial order. We call $(P, \sqsubseteq)$ a *discrete order*.

Example 5.5 (Flat order). A *flat order* is a partial order $(P, \sqsubseteq)$ for which there exists an element $\bot \in P$ such that

$$\forall p, q \in P.\ p \sqsubseteq q \Leftrightarrow\ p = \bot \vee p = q$$

The element $\bot$ is called *bottom* and it is unique. In fact, suppose that two such elements $\bot_1, \bot_2$ exist. Then, we have $\bot_1 \sqsubseteq \bot_2$ and also $\bot_2 \sqsubseteq \bot_1$; thus by antisymmetry we have $\bot_1 = \bot_2$.

5.1.2 Hasse Diagrams

The aim of this section is to provide a tool that allows us to represent orders in a comfortable way.

First of all we could think to use graphs to represent an order. In this framework each element of the order is represented by a node of the graph and the order relation by the arrows (i.e., we would have an arrow from a to b if and only if $a \sqsubseteq b$).

This notation is not very manageable, indeed we repeat many times redundant information. For example in the usual natural numbers order we would have $n+1$ incoming arrows and infinite outgoing arrows, for a node labelled by n. We need a more compact notation, which leaves implicit some information that can be inferred by exploiting the property of partial orders. This notation is represented by the Hasse diagrams. The idea is to omit: 1) every reflexive arc (from a node to itself), because we know by reflexivity that such an arc is present for every node; and 2) every arc from a to c when there is a node b with an arc from a to b and one from b to c, because the presence of the arc from a to c can be inferred by transitivity.

Definition 5.3 (Hasse Diagram). Given a poset $(A, \sqsubseteq)$, let R be the binary relation defined by:

$$\frac{x \sqsubseteq y \quad y \sqsubseteq z \quad x \neq y \neq z}{xRz} \qquad \frac{\varnothing}{xRx}$$

We call *Hasse diagram* the relation H defined as:

$$H \stackrel{\text{def}}{=} \sqsubseteq \setminus R$$

Note that the first rule can be written more concisely as

$$\frac{x \sqsubset y \quad y \sqsubset z}{xRz}$$

The Hasse diagram omits the information deducible by transitivity and reflexivity. A simple example of Hasse diagram is in Figure 5.1.

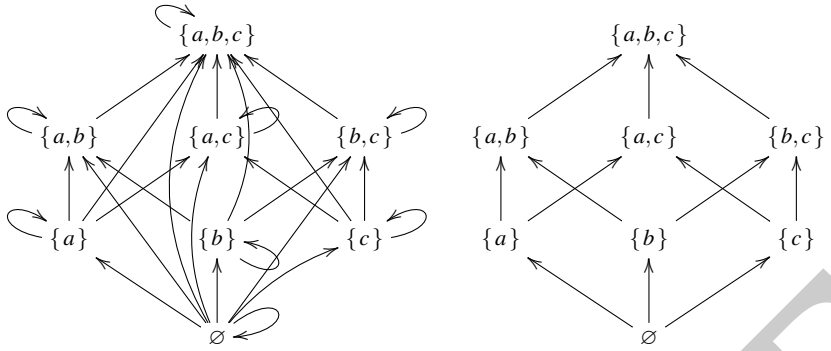
To ensure that all the needed information is contained in the Hasse diagram we rely on the following theorem.

Theorem 5.2 (Order relation, Hasse diagram Equivalence). *Let $(P, \sqsubseteq)$ a partial order with P a finite set, and let H be its Hasse diagram. Then, the transitive and reflexive closure H^* of H is equal to $\sqsubseteq$.*

Proof. Formally, we want to prove the two inclusions $H^* \subseteq \sqsubseteq$ and $\sqsubseteq \subseteq H^*$ separately, where the relation H^* is defined by the inference rules below:

$$\frac{}{xH^*x} \qquad \frac{xHy}{xH^*y} \qquad \frac{xH^*y \wedge yH^*z}{xH^*z}$$

$H^* \subseteq \sqsubseteq$: Suppose $x\,H^*\,y$. Then, there exists (see Problem 4.4) $k \in \mathbb{N}$ and $z_0, \ldots, z_k$ such that



(a) $\wp(\{a,b,c\})$ ordered by inclusion (b) Hasse diagram for $\wp(\{a,b,c\})$

Fig. 5.1: Hasse diagram for the powerset over $\{a,b,c\}$ ordered by inclusion

$$x = z_0 \ \wedge \ z_0 H z_1 \ \wedge \ \ldots \wedge \ z_{k-1} H z_k \ \wedge \ z_k = y$$

Since $H \subseteq \sqsubseteq$ by definition, we have

$$x = z_0 \ \wedge \ z_0 \sqsubseteq z_1 \ \wedge \ \ldots \wedge \ z_{k-1} \sqsubseteq z_k \ \wedge \ z_k = y$$

Hence, by transitivity of $\sqsubseteq$ it follows that $x \sqsubseteq y$.

$\sqsubseteq \subseteq H^*$: Given $x \sqsubseteq y$, let us denote by $]x,y[$ the set of elements strictly contained between x and y, i.e.,

$$]x,y[\stackrel{\text{def}}{=} \{z \mid x \sqsubset z \wedge z \sqsubset y\}.$$

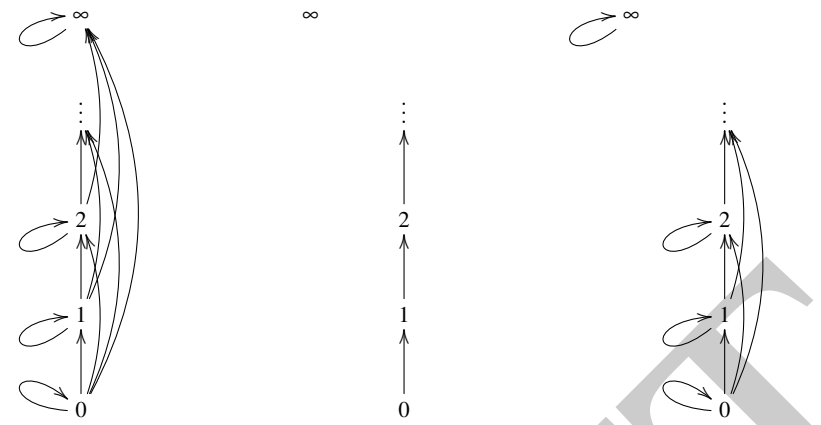
Clearly $]x,y[$ is finite because P is finite. We prove that xH^*y by mathematical induction on the number of elements in $]x,y[$.

Base case: When $]x,y[$ is empty, it means that $(x,y) \notin R$. Hence xHy and thus xH^*y.

Inductive case: Suppose $]x,y[$ has $n+1$ elements. Take $z \in]x,y[$. Clearly the sizes of $]x,z[$ and $]z,y[$ are strictly smaller than that of $]x,y[$, and since $x \sqsubset z$ and $z \sqsubset y$, by inductive hypothesis it follows that xH^*z and zH^*y. Hence xH^*y. □

The above theorem only allows to represent finite orders.

Example 5.6 (Infinite order). Let us see that the Hasse diagrams does not work well with infinite orders. Let $(\mathbb{N} \cup \{\infty\}, \leq)$ be the usual order on natural numbers extended with a top element ∞ such that $n \leq \infty$ and $\infty \leq \infty$. From Definition 5.3 it follows that for any $n \in \mathbb{N}$ we have $nR\infty$ (because $n < n+1 < \infty$) and that for any $n,k \in \mathbb{N}$ it holds $nRn+2+k$ (because $n < n+1 < n+2+k$). Moreover, for any $x \in \mathbb{N} \cup \{\infty\}$ we have xRx. In particular, the Hasse diagram eliminates all the arcs between each



(a) $(\mathbb{N}\cup\{\infty\},\leq)$ (b) H induced by $(\mathbb{N}\cup\{\infty\},\leq)$ (c) H^* induced by $(\mathbb{N}\cup\{\infty\},\leq)$

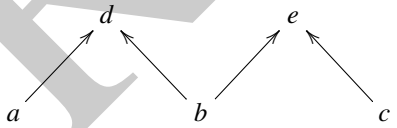
Fig. 5.2: Infinite orders and Hasse diagrams

natural number and ∞. Now using the transitive and reflexive closure we would like to get back the original order. Using the inference rules we obtain the usual order on natural numbers without any relation between ∞ and the natural numbers (recall that we only allow finite proofs). The situation is illustrated in Figure 5.2

Definition 5.4 (Least element). Let $(P,\sqsubseteq_P)$ be a partial order and take $Q \subseteq P$. An element $\ell \in Q$ is a *least* element of $(Q,\sqsubseteq_Q)$ if:

$$\forall q \in Q.\ \ell \sqsubseteq_Q q$$

Example 5.7 (No least element). Let us consider the order associated with the Hasse diagram:



The sets $\{a,b,d\}$ and $\{a,b,c,d,e\}$ have no least element. As we will see the elements a,b and c are minimal since they have no smaller elements in the order.

Theorem 5.3 (Uniqueness of the least element). *Let $(P,\sqsubseteq)$ be a partial order. P has at most one least element.*

Proof. Let $\ell_1,\ell_2 \in P$ be both least elements of P, then $\ell_1 \sqsubseteq \ell_2$ and $\ell_2 \sqsubseteq \ell_1$. Now by using the antisymmetric property we get $\ell_1 = \ell_2$. □

The counterpart of the least element is the concept of *greatest* element. We can define the greatest element as the least element of the reverse order $\sqsubseteq^{-1}$ (defined by letting $x \sqsubseteq^{-1} y \Leftrightarrow y \sqsubseteq x$).

Definition 5.5 (Minimal element). Let $(P, \sqsubseteq_P)$ be a partial order and take $Q \subseteq P$. An element $m \in Q$ is a *minimal element* of $(Q, \sqsubseteq_Q)$ if:

$$\forall q \in Q.\ q \sqsubseteq_Q m \Rightarrow q = m$$

As for the least element we have the dual of minimal elements, called *maximal elements*: They are the minimal elements of the reverse order $\sqsubseteq^{-1}$.

Remark 5.2 (Least vs minimal elements). Note that the definition of minimal and least element (maximal and greatest) are quite different.

- The least element ℓ is the (unique) smallest element of a set.
- A minimal element m is just such that no smaller element can be found in the set, i.e., $\forall q \in Q. q \not\sqsubset m$ (but there is no guarantee that all the elements $q \in Q$ are comparable with m).
- The least element of an order is obviously minimal, but a minimal element is not necessarily the least.

Definition 5.6 (Upper bound). Let $(P, \sqsubseteq)$ be a partial order and $Q \subseteq P$ be a subset of P, then $u \in P$ is an *upper bound* of Q if:

$$\forall q \in Q.\ q \sqsubseteq u$$

Note that unlike a maximal element and the greatest element an upper bound does not necessarily belong to the subset Q of elements we are considering.

Definition 5.7 (Least upper bound). Let $(P, \sqsubseteq)$ be a partial order and $Q \subseteq P$ be a subset of P. Then, $p \in P$ is the *least upper bound* of Q if and only if p is the least element of the upper bounds of P. Formally, we require that:

1. p is an upper bound of Q ($\forall q \in Q.\ q \sqsubseteq p$);
2. for any upper bound u of Q, then $p \sqsubseteq u$ ($\forall u \in P.\ (\forall q \in Q.\ q \sqsubseteq u) \Rightarrow p \sqsubseteq u$);

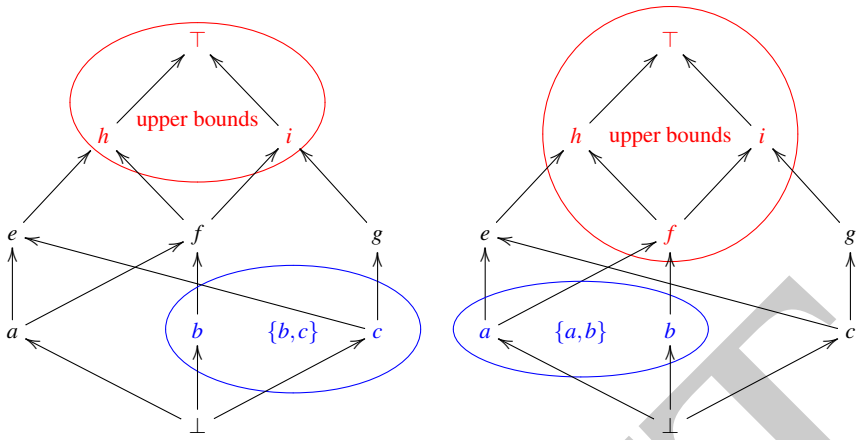
and we write $lub(Q) = p$.

It follows immediately from Theorem 5.3 that the least upper bound, when it exists, is unique.

Example 5.8 (lub). Now we will clarify the concept of *lub* with two examples. Let us consider the order represented by the Hasse diagram in Figure 5.3 (a). The set of upper bounds of the subset $\{b, c\}$ is the set $\{h, i, \top\}$. This set has no least element (i.e., h and i are not comparable) so the set $\{b, c\}$ has no lub. In Figure 5.3 (b) we see that the set of upper bounds of the set $\{a, b\}$ is the set $\{f, h, i, \top\}$. The least element of the latter set is f, which is thus the lub of $\{a, b\}$.

5.1.3 Chains

One of the main concept in the study of partial orders is that of a *chain*, which is formed by taking a subset of totally ordered elements.



(a) The subset $\{b,c\}$ has no lub

(b) The subset $\{a,b\}$ has lub f

Fig. 5.3: Two subsets of a poset, and their upper bounds

Definition 5.8 (Chain). Let $(P,\sqsubseteq)$ be a partial order, we call *chain* a function $C : \mathbb{N} \to P$ such that:

$$\forall n \in \mathbb{N}.\ C(n) \sqsubseteq C(n+1)$$

We will often write $C = \{d_i\}_{i\in\mathbb{N}}$, where $\forall i \in \mathbb{N}.\ d_i = C(i)$, i.e.,

$$d_0 \sqsubseteq d_1 \sqsubseteq d_2 \ldots$$

Definition 5.9 (Finite chain). Let $C : \mathbb{N} \to P$ be a chain such that the image of C is a finite set, then we say that C is a *finite chain*. Otherwise we say that C is infinite.

Note that a finite chain has still infinitely many elements $\{d_i\}_{i\in\mathbb{N}}$, but only finitely many different ones. In particular, it has one index k and one element d such that $\forall i \in \mathbb{N}.\ d_{k+i} = d$.

Example 5.9 (Finite and infinite chains). Take the partial order $(\mathbb{N},\leq)$. The chain of even numbers

$$0 \leq 2 \leq 4 \leq \cdots$$

is an infinite chain. Instead, the constant chain

$$1 \leq 1 \leq 1 \leq \cdots$$

is a finite chain.

Definition 5.10 (Limit of a chain). Let C be a chain. The lub of the image of C, if it exists, is called *the limit of* C. If d is the limit of the chain $C = \{d_i\}_{i\in\mathbb{N}}$, we write $d = \bigsqcup_{i\in\mathbb{N}} d_i$.

Remark 5.3. Each finite chain has a limit. Indeed each finite chain has a finite totally ordered image: obviously this set has a lub (the greatest element of the set).

Lemma 5.1 (Prefix independence of the limit). *Let $n \in \mathbb{N}$ and let C and C' be two chains such that $C = \{d_i\}_{i\in\mathbb{N}}$ and $C' = \{d_{n+i}\}_{i\in\mathbb{N}}$. Then C and C' have the same limit, if any.*

Proof. Let us prove a stronger property, namely that the chains C and C' have the same set of upper bounds.

Obviously if c is an upper bound of C, then c is an upper bound of C', since each element of C' is contained in C.

Vice versa if c is an upper bound of C', we need to show that $\forall j \in \mathbb{N}.\ j \leq n \Rightarrow d_j \sqsubseteq c$. Since $d_n \sqsubseteq c$ and $\forall j \in \mathbb{N}.\ j \leq n \Rightarrow d_j \sqsubseteq d_n$ by transitivity of $\sqsubseteq$ it follows that c is an upper bound of C.

Now since C and C' have the same set of upper bound elements, they have the same *lub*, if it exists at all. □

The main consequence of Lemma 5.1 is that we can always eliminate from or add a finite prefix to a chain preserving the limit.

A stronger result guarantees that any infinite subsequence of a chain C has the same set of upper bounds as C and thus the same limit, if any (see Problem 5.13).

5.1.4 Complete Partial Orders

The aim of partial orders and continuous functions is to provide a framework that allows the definition of the denotational semantics when recursive equations are needed. Complete partial orders extend the concept of partial orders to support the limit operation on chains, which is a generalization of the countable union operation on a powerset. Limits will have a key role in finding fixpoint solutions to recursive equations.

Definition 5.11 (Complete partial orders). Let $(P, \sqsubseteq)$ be a partial order. We say that $(P, \sqsubseteq)$ is *complete* (CPO) if each chain has a limit (i.e. each chain has a lub).

From Remark 5.3, it follows immediately that if a partial order has only finite chains then it is complete.

Definition 5.12 (CPO with bottom). Let $(D, \sqsubseteq)$ be a CPO, we say that $(D, \sqsubseteq)$ is a *CPO with bottom* ($CPO_\perp$) if it has a least element $\perp$ (called *bottom*).

Let us see some examples, that will clarify the concept of CPO. To avoid ambiguities, sometimes we will denote the bottom element of the CPO D by $\perp_D$.

Example 5.10 (Powerset completeness). Let us consider again the previous example of powerset (Example 5.1). We show that the partial order $(\wp(S), \subseteq)$ is complete. Take any chain $\{s_i\}_{i\in\mathbb{N}}$ of subsetes of S. Then:

$$lub(s_0 \subseteq s_1 \subseteq s_2 \ldots) = \{d \mid \exists k \in \mathbb{N}.\ d \in s_k\} = \bigcup_{i \in \mathbb{N}} s_i \in \wp(S)$$

Example 5.11 (Partial order without upper bounds). Now let us take the usual order on natural numbers $(\mathbb{N}, \leq)$. Obviously all its finite chains have a limit (i.e., the greatest element of the chain). Vice versa infinite chains have no limits (i.e., there is no natural number greater than infinitely many natural numbers). To make the order a CPO all we have to do is to add an element greater than all the natural numbers. So we add the element ∞ and extend the order relation by letting $x \leq \infty$ for all $x \in \mathbb{N} \cup \{\infty\}$. The new poset $(\mathbb{N} \cup \{\infty\}, \leq)$ is a CPO, because ∞ is the limit of any infinite chain.

Example 5.12 (Partial order without least upper bound). Let us define the partial order $(\mathbb{N} \cup \{\infty_1, \infty_2\}, \sqsubseteq)$ as follows:

$$(\sqsubseteq \restriction \mathbb{N}) = \leq, \quad \forall x \in \mathbb{N} \cup \{\infty_1\}.\ n \sqsubseteq \infty_1, \quad \forall x \in \mathbb{N} \cup \{\infty_2\}.\ x \sqsubseteq \infty_2$$

Where $\sqsubseteq \restriction \mathbb{N}$ is the restriction of $\sqsubseteq$ to natural numbers. This partial order is not complete, indeed each infinite chain has two upper bounds (i.e., ∞_1 and ∞_2) which are not comparable, hence there is no least upper bound.

The next example illustrates a fundamental CPO, that will be exploited in the next chapters: the set of partial functions on natural numbers:

Example 5.13 (Partial functions). Let $\mathbf{Pf} \stackrel{\text{def}}{=} (\mathbb{N} \rightharpoonup \mathbb{N})$ be the set of partial functions from natural numbers to natural numbers. Recall that a partial function is a relation $f \subseteq \mathbb{N} \times \mathbb{N}$ with the *functional* property:

$$\forall n, m, k \in \mathbb{N}.\ n\, f\, m \wedge n\, f\, k \ \Rightarrow\ m = k$$

So the set **Pf** can be viewed as:

$$\mathbf{Pf} \stackrel{\text{def}}{=} \{\ f \subseteq \mathbb{N} \times \mathbb{N} \mid \forall n, m, k \in \mathbb{N}.\ n\, f\, m \wedge n\, f\, k \Rightarrow m = k\ \}$$

Let us denote by $f(n)\downarrow$ the predicate $\exists m \in \mathbb{N}.\ (n, m) \in f$ (i.e., $f(n)\downarrow$ holds when the function f is defined on n). Now it is easy to define a partial order $\sqsubseteq$ on **Pf**. We let:

$$f \sqsubseteq g \ \Leftrightarrow\ (\forall n \in \mathbb{N}.\ f(n)\downarrow \Rightarrow\ (g(n)\downarrow \wedge f(n) = g(n)))$$

Thus f precedes g if whenever f is defined on n also g is defined on n and $f(n) = g(n)$. When $f(n)$ is not defined, then $g(n)$ can be defined and take any value. When both f and g are seen as (functional) relations, then the above definition boils down to check that f is included in g. Of course, the poset $(\wp(\mathbb{N} \times \mathbb{N}), \subseteq)$ has the empty relation as bottom element (i.e., the function undefined everywhere), and each infinite chain has as limit the countable union of the relations in the chain.

To show that **Pf** is complete, we need to show that the limits of chains whose elements are in **Pf** satisfy also the functional property, i.e., they are elements of **Pf**.

Theorem 5.4. *Let $f_0 \subseteq f_1 \subseteq f_2 \subseteq \ldots$ be a chain in* **Pf***, i.e., each relation f_i satisfies the functional property, i.e.,*

$$\forall i \in \mathbb{N}.\ \forall n,m,k \in \mathbb{N}.\ n\, f_i\, m \wedge n\, f_i\, k \Rightarrow m = k.$$

Then, the relation $f \stackrel{\text{def}}{=} \cup_{i\in\mathbb{N}} f_i$ satisfies the functional property, namely:

$$\forall n,m,k \in \mathbb{N}.\ n\, f\, m \wedge n\, f\, k \Rightarrow m = k.$$

Proof. Let us take generic $n,m,k \in \mathbb{N}$ such that the premise $n\, f\, m \wedge n\, f\, k$ of the implication holds. We need to prove the consequence $m = k$. By $n\, f\, m$, it exists $j \in \mathbb{N}$ with $n\, f_j\, m$ and, by $n\, f\, k$ it exists $h \in \mathbb{N}$ with $n\, f_h\, k$. We take $o = \max\{j,h\}$ then it holds $n\, f_o\, m \wedge n\, f_o\, k$. Since $f_o \in$ **Pf**, it satisfies the functional property and thus from $n\, f_o\, m \wedge n\, f_o\, k$ we can conclude that $m = k$. □

Example 5.14 (Partial functions as total functions). Let us show a second way to define a CPO on the partial functions on natural numbers. Let $\mathbb{N}_\perp \stackrel{\text{def}}{=} \mathbb{N} \cup \{\perp\}$ and $(\mathbb{N}_\perp, \sqsubseteq_{\mathbb{N}_\perp})$ be the flat order obtained by adding $\perp$ to the discrete order of the natural numbers. In other words we have $x \sqsubseteq_{\mathbb{N}_\perp} y$ iff $x = y$ or $x = \perp$. Then take the set of total functions $\mathbf{Tf} = (\mathbb{N} \to \mathbb{N}_\perp)$. Equivalently:

$$\mathbf{Tf} \stackrel{\text{def}}{=} \{\ f \subseteq \mathbb{N} \times \mathbb{N}_\perp \ \mid\ (\forall n,m,k \in \mathbb{N}.\ n\, f\, m \wedge n\, f\, k \Rightarrow m = k) \wedge (\forall n \in \mathbb{N}.\ \exists x \in \mathbb{N}_\perp.\ n\, f\, x)\ \}$$

We define the following order on **Tf**

$$f \sqsubseteq g \ \Leftrightarrow\ \forall n \in \mathbb{N}.\ f(n) \sqsubseteq_{\mathbb{N}_\perp} g(n).$$

That is, if $f(n) = \perp$ then $g(n)$ can assume any value, including $\perp$; otherwise it must be $g(n) = f(n)$. The bottom element of the order is the function that returns $\perp$ for every argument. Note that the above order is complete, In fact, the limit of a chain obviously exists as a relation, and it is easy to show, analogously to the partial function case, that it is in addition a total function. The proof is left as an exercise to the reader (see Problem 5.11).

Example 5.15 (Limit of a chain of partial functions). Let $\{f_i : \mathbb{N} \to \mathbb{N}_\perp\}_{i\in\mathbb{N}}$ be a chain in **Tf** such that for any $i \in \mathbb{N}$ we have:

$$f_i(n) \stackrel{\text{def}}{=} \begin{cases} 3 & \text{if } n \leq i \wedge 2 \mid n \\ \perp & \text{otherwise} \end{cases}$$

where the predicate $k \mid n$ is true when k divides n (i.e., $2 \mid n$ is true when n is even and false otherwise). Let us consider some evaluations of the functions f_i with $i \in [0,4]$:

$$\begin{array}{lllll} f_0(0)=3 & f_0(1)=\bot & f_0(2)=\bot & f_0(3)=\bot & f_0(4)=\bot\cdots \\ f_1(0)=3 & f_1(1)=\bot & f_1(2)=\bot & f_1(3)=\bot & f_1(4)=\bot\cdots \\ f_2(0)=3 & f_2(1)=\bot & f_2(2)=3 & f_2(3)=\bot & f_2(4)=\bot\cdots \\ f_3(0)=3 & f_3(1)=\bot & f_3(2)=3 & f_3(3)=\bot & f_3(4)=\bot\cdots \\ f_4(0)=3 & f_4(1)=\bot & f_4(2)=3 & f_4(3)=\bot & f_4(4)=3\ \cdots \end{array}$$

Thus the limit of the chain is the function f that returns 3 when applied to even numbers and $\bot$ otherwise:

$$f(n) \stackrel{\text{def}}{=} \begin{cases} 3 & \text{if } 2 \mid n \\ \bot & \text{otherwise} \end{cases}$$

In general, the limit $f \stackrel{\text{def}}{=} \bigsqcup_{i\in\mathbb{N}} f_i$ of a chain in **Tf** is a function $f : \mathbb{N} \to \mathbb{N}_\bot$ such that $f(n) = m$ for some $m \neq \bot$ if and only if there exists an index $k \in \mathbb{N}$ with $f_k(n) = m$. Note also that when $i \leq j$ and $f_i(n) \neq \bot$ it must be the case that $f_j(n) = f_i(n)$. On the contrary, when $i \leq j$ and $f_j(n) = \bot$ it means that $f_i(n) = \bot$.

5.2 Continuity and Fixpoints

5.2.1 Monotone and Continuous Functions

In order to define a class of functions over CPOs which ensures the existence of their fixpoints we introduce two general properties of functions: *monotonicity* and *continuity*.

Definition 5.13 (monotonicity). Let $f : D \to E$ be a function over two CPOs $(D, \sqsubseteq_D)$ and $(E, \sqsubseteq_E)$, we say that f is *monotone* if

$$\forall d, d' \in D.\ d \sqsubseteq_D d' \Rightarrow f(d) \sqsubseteq_E f(d')$$

We say that a monotone function *preserves the order*. So if $\{d_i\}_{i\in\mathbb{N}}$ is a chain on $(D, \sqsubseteq_D)$ and $f : D \to E$ is a monotone function, then $\{f(d_i)\}_{i\in\mathbb{N}}$ is a chain on $(E, \sqsubseteq_E)$. Often we will consider functions whose domain and codomain coincide (i.e., $E = D$), in which case we just say that f is a function on $(D, \sqsubseteq_D)$.

Example 5.16 (Non monotone function). Let us define a CPO $(\{\bot, 0, 1\}, \sqsubseteq)$ such that $\bot \sqsubseteq 0$, $\bot \sqsubseteq 1$ and $x \sqsubseteq x$ for any $x \in \{\bot, 0, 1\}$. Now define a function f over $(\{\bot, 0, 1\}, \sqsubseteq)$ as follows:

$$f(\bot) = 0 \quad f(0) = 0 \quad f(1) = 1$$

This function is not monotone, indeed $\bot \sqsubseteq 1$ but $f(\bot) = 0$ and $f(1) = 1$ are not comparable (see Figure 5.4, so the function f does not preserve the order.

Continuity guarantees that taking the image of the limit of a chain is the same as taking the limit of the images of the elements in the chain.

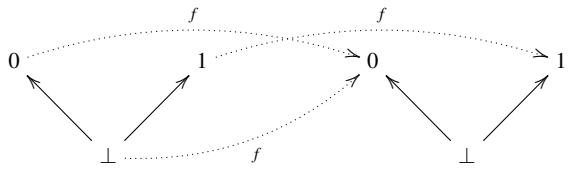


Fig. 5.4: A non monotone function

Definition 5.14 (Continuity). Let $f : D \to D$ be a monotone function on a CPO $(D, \sqsubseteq)$, we say that f is a continuous function if for each chain in $(D, \sqsubseteq)$ we have:

$$f(\bigsqcup_{i \in \mathbb{N}} d_i) = \bigsqcup_{i \in \mathbb{N}} f(d_i)$$

Note that, as it is the case for most definitions of continuity, the operations of applying function and taking the limit can be exchanged. For this reason, we say that a continuous function *preserves limits*.

Remark 5.4. Let $(D, \sqsubseteq)$ be a CPO that has only finite chains. Then any chain $\{d_i\}_{i \in \mathbb{N}}$ in D is such that there are $d \in D$ and $k \in \mathbb{N}$ such that $\forall i \in \mathbb{N}.\ d_{i+k} = d$ and it has a limit (d) that is also an element of the chain. Thus any monotone function $f : D \to D$ is continuous, because $\forall i \in \mathbb{N}.\ f(d_{i+k}) = f(d)$ (i.e., the chain $\{f(d_i)\}_{i \in \mathbb{N}}$ is finite and its limit is $f(d)$).

Interestingly, continuous functions are closed under composition.

Theorem 5.5 (Continuity of composition). *Let $(D, \sqsubseteq_D)$, $(E \sqsubseteq_E)$, and $(F \sqsubseteq_F)$ be three CPOs, and $f : D \to E$, $g : E \to F$ be two continuous functions. Their composition*

$$h \stackrel{\text{def}}{=} g \circ f : D \to F$$

defined by letting $h(d) = g(f(d))$ for all $d \in D$ is continuous.

Proof. Let $\{d_i\}_{i \in \mathbb{N}}$ be a chain in D. We want to prove that $h(\bigsqcup_{i \in \mathbb{N}} d_i) = \bigsqcup_{i \in \mathbb{N}} h(d_i)$. We have:

$$\begin{array}{lll} h(\bigsqcup_{i \in \mathbb{N}} d_i) = g(f(\bigsqcup_{i \in \mathbb{N}} d_i)) & & \text{by definition of } h = g \circ f \\ = g(\bigsqcup_{i \in \mathbb{N}} f(d_i)) & & \text{by continuity of } f \\ = \bigsqcup_{i \in \mathbb{N}} g(f(d_i)) & & \text{by continuity of } g \\ = \bigsqcup_{i \in \mathbb{N}} h(d_i) & & \text{by definition of } h = g \circ f \end{array}$$

□

Remark 5.5. The composition $g \circ f$ is sometimes denoted also by $f; g$.

Example 5.17 (A monotone function which is not continuous). Let $(\mathbb{N} \cup \{\infty\}, \leq)$ be the CPO from Example 5.11. Define a function $f : \mathbb{N} \cup \{\infty\} \to \mathbb{N} \cup \{\infty\}$ such that:

$$f(x) \stackrel{\text{def}}{=} \begin{cases} 0 & \text{if } x \in \mathbb{N} \\ 1 & \text{if } x = \infty \end{cases}$$

It is immediate to check that f is monotone:

- for $n, m \in \mathbb{N}$, if $n \leq m$ we have $f(n) = 0 \leq 0 = f(m)$;
- for $n \in \mathbb{N}$, we have $n \leq \infty$ and $f(n) = 0 \leq 1 = f(\infty)$;
- for $\infty \leq \infty$ we have of course $f(\infty) \leq f(\infty)$.

Let us consider the chain $\{d_i\}_{i \in \mathbb{N}}$ of even numbers:

$$0 \leq 2 \leq 4 \leq 6 \leq \ldots$$

whose limit is ∞. The chain $\{f(d_i)\}_{i \in \mathbb{N}}$ is instead the constant chain

$$0 \leq 0 \leq 0 \leq 0 \leq \ldots$$

whose limit is 0. So we have

$$f(\bigsqcup_{i \in \mathbb{N}} d_i) = f(\infty) = 1 \quad \neq \quad 0 = \bigsqcup_{i \in \mathbb{N}} f(d_i)$$

The monotone function f does not preserve the limits and thus it is not continuous.

5.2.2 Fixpoints

Now we are ready to study fixpoints of continuous functions.

Definition 5.15 (Pre-fixpoint and fixpoint). Let f be a continuous function over a $CPO_\perp$ $(D, \sqsubseteq)$. An element p is a *pre-fixpoint* if

$$f(p) \sqsubseteq p.$$

An element $d \in D$ is a *fixpoint* of f if

$$f(d) = d.$$

Of course any fixpoint of f is also a pre-fixpoint of f, i.e., the set of fixpoints of f is included in the set of its pre-fixpoints.

We will denote by $\text{gfp}(f)$ the greatest fixpoint of f and by $\text{lfp}(f)$ the least fixpoint of f, when they exist.

Let $f : D \to D$ and $d \in D$. We denote by $f^n(d)$ the repeated application of f to d for n times, i.e.,

$$f^0(d) \stackrel{\text{def}}{=} d$$
$$f^{n+1}(d) \stackrel{\text{def}}{=} f(f^n(d))$$

Lemma 5.2. *Let $(D, \sqsubseteq)$ be a partial order and $f : D \to D$ be a monotone function. The elements $\{f^n(\bot)\}_{n\in\mathbb{N}}$ form a chain in D.*

Proof. The property $\forall n \in \mathbb{N}.\ f^n(\bot) \sqsubseteq f^{n+1}(\bot)$ can be readily proved by mathematical induction on n.

Base case: For $n = 0$ we have $f^0(\bot) = \bot \sqsubseteq f^1(\bot) = f(\bot)$, as $\bot$ is the least element of D.

Inductive case: Let us assume that the property holds for n, i.e., that

$$f^n(\bot) \sqsubseteq f^{n+1}(\bot).$$

We want to prove that the property holds for $n+1$, i.e., that

$$f^{n+1}(\bot) \sqsubseteq f^{n+2}(\bot).$$

In fact by definition we have $f^{n+1}(\bot) = f(f^n(\bot))$ and $f^{n+2}(\bot) = f(f^{n+1}(\bot))$. Since f is monotone and by the inductive hypothesis we have:

$$f^{n+1}(\bot) = f(f^n(\bot)) \sqsubseteq f(f^{n+1}(\bot)) = f^{n+2}(\bot).$$

□

When $(D, \sqsubseteq)$ is complete then the chain $\{f^n(\bot)\}_{n\in\mathbb{N}}$ must have a limit $\bigsqcup_{n\in\mathbb{N}} f^n(\bot)$.

Next theorem ensures that the least fixpoint of a continuous function always exists and that it is computed by the above limit.

Theorem 5.6 (Kleene's Fixpoint theorem). *Let $f : D \to D$ be a continuous function on a CPO$_\bot$ D. Then, let*

$$\mathrm{fix}(f) = \bigsqcup_{n\in\mathbb{N}} f^n(\bot).$$

The element $\mathrm{fix}(f) \in D$ has the following properties:

1. *$\mathrm{fix}(f)$ is a fixpoint of f, namely*

$$f(\mathrm{fix}(f)) = \mathrm{fix}(f)$$

2. *$\mathrm{fix}(f)$ is the least pre-fixpoint of f, namely*

$$f(d) \sqsubseteq d \Rightarrow \mathrm{fix}(f) \sqsubseteq d$$

Since any fixpoint is a pre-fixpoint, $\mathrm{fix}(f)$ is also the least fixpoint of f.

Proof. We prove the two items separately.

1. By continuity we will show that $\mathrm{fix}(f)$ is a fixpoint of f:

$$\begin{aligned} f(\mathrm{fix}(f)) &= f(\bigsqcup_{n\in\mathbb{N}} f^n(\bot)) && \text{(by definition of fix)} \\ &= \bigsqcup_{n\in\mathbb{N}} f(f^n(\bot)) && \text{(by continuity of } f\text{)} \\ &= \bigsqcup_{n\in\mathbb{N}} f^{n+1}(\bot) && \text{(by definition of } f^{n+1}\text{)} \end{aligned}$$

So we need to compute the limit of the chain:

$$f(\bot) \sqsubseteq f^2(\bot) \sqsubseteq f^3(\bot) \sqsubseteq \ldots$$

Since the limit is independent from any finite prefix of the chain, it coincides with the limit of the chain

$$f^0(\bot) = \bot \sqsubseteq f(\bot) \sqsubseteq f^2(\bot) \sqsubseteq f^3(\bot) \sqsubseteq \ldots$$

$$\begin{aligned} \bigsqcup_{n\in\mathbb{N}} f^{n+1}(\bot) &= \bigsqcup_{n\in\mathbb{N}} f^n(\bot) && \text{(by Lemma 5.1)} \\ &= \mathrm{fix}(f) && \text{(by definition of fix)} \end{aligned}$$

2. We want to prove that $\mathrm{fix}(f)$ is the least pre-fixpoint. We prove that any pre-fixpoint of f is an upper bound of the chain $\{f^n(\bot)\}_{n\in\mathbb{N}}$. Let d be a pre-fixpoint of f, i.e.,

$$f(d) \sqsubseteq d \tag{5.1}$$

By mathematical induction we show that

$$\forall n \in \mathbb{N}. f^n(\bot) \sqsubseteq d$$

i.e., that d is an upper bound for the chain $\{f^n(\bot)\}_{n\in\mathbb{N}}$:

base case: obviously $f^0(\bot) = \bot \sqsubseteq d$
inductive case: let us assume $f^n(\bot) \sqsubseteq d$, we want to prove that $f^{n+1}(\bot) \sqsubseteq d$:

$$\begin{aligned} f^{n+1}(\bot) &= f(f^n(\bot)) && \text{(by definition of } f^{n+1}\text{)} \\ &\sqsubseteq f(d) && \text{(by monotonicity of } f \\ & && \text{and inductive hypothesis)} \\ &\sqsubseteq d && \text{(because } d \text{ is a pre-fixpoint)} \end{aligned}$$

Since d is an upper bound for $\{f^n(\bot)\}_{n\in\mathbb{N}}$ and $\mathrm{fix}(f)$ is the limit (i.e., the least upper bound) of the same chain, it must be $\mathrm{fix}(f) \sqsubseteq d$.

□

Now let us make two examples which show that bottom element and the continuity property are required to compute the least fixpoint.

Example 5.18 (Bottom is necessary). Let $(\{\mathbf{true}, \mathbf{false}\}, \sqsubseteq)$ be the discrete order of boolean values. Obviously it is complete (because only finite chains of the form

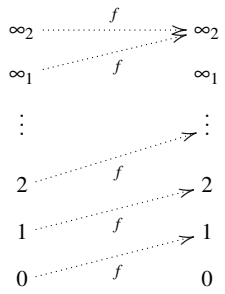


Fig. 5.5: Continuity is necessary

$x \sqsubseteq x \sqsubseteq x \sqsubseteq \ldots$ exist) and it has no bottom element, as **true** and **false** are not comparable. The identity function is monotone and has two fixpoints, but there is no least fixpoint. On the contrary, the negation function is also monotone but has no fixpoint.

Example 5.19 (Continuity is necessary). Let us consider the $\mathrm{CPO}_\bot$ $(\mathbb{N} \cup \{\infty_1, \infty_2\}, \sqsubseteq)$ where:

$$\sqsubseteq \restriction \mathbb{N} = \leq, \quad \forall d \in \mathbb{N} \cup \{\infty_1\}.\ d \sqsubseteq \infty_1, \quad \forall d \in \mathbb{N} \cup \{\infty_1, \infty_2\}.\ d \sqsubseteq \infty_2.$$

The bottom element is 0. We define a monotone function f as follows (see Figure 5.5):

$$f(n) \stackrel{\text{def}}{=} \begin{cases} n+1 & \text{if } n \in \mathbb{N} \\ \infty_2 & \text{otherwise} \end{cases}$$

Note that f is not continuous. Let us consider the chain of even numbers $\{d_i\}_{i \in \mathbb{N}}$. It follows that $\{f(d_i)\}_{i \in \mathbb{N}}$ is the chain of odd numbers. We have:

$$\bigsqcup_{i \in \mathbb{N}} d_i = \infty_1 \qquad \bigsqcup_{i \in \mathbb{N}} f(d_i) = \infty_1$$

Therefore:

$$f\left(\bigsqcup_{i \in \mathbb{N}} d_i\right) = f(\infty_1) = \infty_2 \neq \infty_1 = \bigsqcup_{i \in \mathbb{N}} f(d_i)$$

Note that f has only one fixpoint, indeed:

$$f(\infty_2) = \infty_2$$

But such fixpoint is not reachable by taking $\bigsqcup_{n \in \mathbb{N}} f^n(0) = \infty_1$.

5.3 Immediate Consequence Operator

In this section we reconcile two different approaches for defining semantics: inference rules, like those used for defining the operational semantics of IMP, and fixpoint theory, that will be applied to define the denotational semantics of IMP. We show that the set of theorems of a logical system R can be defined as the least fixpoint of a suitable operator, called *immediate consequence operator* and denoted $\widehat{R}$.

5.3.1 The Operator $\widehat{R}$

Let us consider a set F of well-formed formulas and a set R of inference rules over them. We define an operator $\widehat{R}$ over $(\wp(F), \subseteq)$, the $CPO_\perp$ of sets of well-formed formulas ordered by inclusion.

Definition 5.16 (Immediate consequence operator $\widehat{R}$). Let R be a logical system. We define a function $\widehat{R} : \wp(F) \to \wp(F)$ as follows (for any $S \subseteq F$):

$$\widehat{R}(S) \stackrel{\text{def}}{=} \{y \mid \exists (X/y) \in R.\, X \subseteq S\}$$

The function $\widehat{R}$ is called *immediate consequence operator*.

The operator $\widehat{R}$, when applied to a set of well-formed formulas S, calculates a new set of formulas by applying the inference rules of R to the facts in S in all possible ways, i.e., $\widehat{R}(S)$ is the set of conclusions we can derive in one step from the hypothesis in S using rules in R. We will show that the set of theorems of R is equal to the least fixpoint of the immediate consequence operator $\widehat{R}$.

To apply the fixpoint theorem, we need to prove that $\widehat{R}$ is monotone and continuous.

Theorem 5.7 (Monotonicity of $\widehat{R}$). *$\widehat{R}$ is a monotone function.*

Proof. Let $S_1 \subseteq S_2$. We want to show that $\widehat{R}(S_1) \subseteq \widehat{R}(S_2)$. Let us assume $y \in \widehat{R}(S_1)$, then there exists a rule $(X/y) \in R$ with $X \subseteq S_1$. So we have $X \subseteq S_2$ and $y \in \widehat{R}(S_2)$. □

Theorem 5.8 (Continuity of $\widehat{R}$). *Let R be a logical system such that for any $(X/y) \in R$ the set of premises X is finite. Then $\widehat{R}$ is continuous.*

Proof. Let $\{S_i\}_{i\in\mathbb{N}}$ be a chain in $\wp(F)$. We want to prove that

$$\bigcup_{i\in\mathbb{N}} \widehat{R}(S_i) = \widehat{R}(\bigcup_{i\in\mathbb{N}} S_i).$$

As usual we prove the two inclusions separately:

$\subseteq$) Let $y \in \bigcup_{i\in\mathbb{N}} \widehat{R}(S_i)$ so there exists a natural number k such that $y \in \widehat{R}(S_k)$. Since

$$S_k \subseteq \bigcup_{i\in\mathbb{N}} S_i$$

by monotonicity

$$\widehat{R}(S_k) \subseteq \widehat{R}\left(\bigcup_{i\in\mathbb{N}} S_i\right)$$

hence $y \in \widehat{R}(\bigcup_{i\in\mathbb{N}} S_i)$.

$\supseteq$) Let $y \in \widehat{R}(\bigcup_{i\in\mathbb{N}} S_i)$ so there exists a rule $X/y \in R$ with $X \subseteq \bigcup_{i\in\mathbb{N}} S_i$. Since X is finite, there exists a natural number k such that $X \subseteq S_k$. In fact, for every $x \in X$ there will be a natural number k_x with $x \in S_{k_x}$ and letting $k = \max\{k_x\}_{x\in X}$ we have $X \subseteq S_k$. Since $X \subseteq S_k$ we have $y \in \widehat{R}(S_k) \subseteq \bigcup_{i\in\mathbb{N}} \widehat{R}(S_i)$ as required. □

5.3.2 Fixpoint of $\widehat{R}$

Now we are ready to present the fixpoint of $\widehat{R}$. For this purpose let us define I_R as the set of theorems provable in R:

$$I_R \stackrel{\text{def}}{=} \bigcup_{i\in\mathbb{N}} I_R^i$$

where

$$I_R^0 \stackrel{\text{def}}{=} \varnothing$$
$$I_R^{n+1} \stackrel{\text{def}}{=} \widehat{R}(I_R^n) \cup I_R^n$$

Note that the generic I_R^n contains all theorems provable with derivations of depth[1] at most n, and I_R contains all theorems provable by using the rule system R.

Theorem 5.9. *Let R a rule system, it holds:*

$$\forall n \in \mathbb{N}.\ I_R^n = \widehat{R}^n(\varnothing)$$

Proof. By induction on n

base case: $I_R^0 = \widehat{R}^0(\varnothing) = \varnothing$.

inductive case: We assume $I_R^n = \widehat{R}^n(\varnothing)$ and want to prove $I_R^{n+1} = \widehat{R}^{n+1}(\varnothing)$. Then:

$$\begin{aligned}
I_R^{n+1} &= \widehat{R}(I_R^n) \cup I_R^n && \text{(by definition of } I_R^{n+1}\text{)}\\
&= \widehat{R}(\widehat{R}^n(\varnothing)) \cup \widehat{R}^n(\varnothing) && \text{(by inductive hypothesis)}\\
&= \widehat{R}^{n+1}(\varnothing) \cup \widehat{R}^n(\varnothing) && \text{(by definition of } \widehat{R}^{n+1}\text{)}\\
&= \widehat{R}^{n+1}(\varnothing) && \text{(because } \widehat{R}^{n+1}(\varnothing) \supseteq \widehat{R}^n(\varnothing)\text{)}
\end{aligned}$$

[1] See Problem 4.12.

In the last step of the proof we have exploited the property $\widehat{R}^{n+1}(\varnothing) \supseteq \widehat{R}^n(\varnothing)$, which is an instance of Lemma 5.2 (by taking $D = \wp(F)$, $\sqsubseteq = \subseteq$, $\bot = \varnothing$ and $f = \widehat{R}$). □

Theorem 5.10 (Fixpoint of $\widehat{R}$). *Let R a logical system, it holds:*

$$\mathrm{fix}(\widehat{R}) = I_R$$

Proof. By continuity of $\widehat{R}$ (Theorem 5.8) and the fixpoint theorem (Theorem 5.6), we know that the least fixpoint of $\widehat{R}$ exists and that

$$\mathrm{fix}(\widehat{R}) \stackrel{\text{def}}{=} \bigcup_{n\in\mathbb{N}} \widehat{R}^n(\varnothing)$$

Then, by Theorem 5.9:

$$I_R \stackrel{\text{def}}{=} \bigcup_{n\in\mathbb{N}} I_R^n = \bigcup_{n\in\mathbb{N}} \widehat{R}^n(\varnothing) \stackrel{\text{def}}{=} \mathrm{fix}(\widehat{R})$$

as required. □

Example 5.20 (Rule system with discontinuous $\widehat{R}$). Let us consider the logical system R below:

$$\frac{}{P(1)} \qquad \frac{P(x)}{P(x+1)} \qquad \frac{\forall n \in \mathbb{N}.\, P(1+2\times n)}{P(0)}$$

To ensure the continuity of $\widehat{R}$, Theorem 5.8 requires that the system has only rules with finitely many premises. The third rule of our system instead has infinitely many premises; it corresponds to

$$\frac{P(1) \quad P(3) \quad P(5) \quad \cdots}{P(0)}$$

The continuity of $\widehat{R}$, namely the fact that for all chains $\{S_i\}_{i\in\mathbb{N}}$ we have $\bigcup_{i\in\mathbb{N}} \widehat{R}(S_i) = \widehat{R}(\bigcup_{i\in\mathbb{N}} S_i)$, does not hold in this case. Indeed if we take the chain

$$\{P(1)\} \subseteq \{P(1),P(3)\} \subseteq \{P(1),P(3),P(5)\} \ldots$$

We have:

i	0		1		2
S_i	$\{P(1)\}$	$\subseteq$	$\{P(1),P(3)\}$	$\subseteq$	$\{P(1),P(3),P(5)\}$
$\widehat{R}(S_i)$	$\{P(1),P(2)\}$	$\subseteq$	$\{P(1),P(2),P(4)\}$	$\subseteq$	$\{P(1),P(2),P(4),P(6)\}$

Then we have:

$$\bigcup_{i\in\mathbb{N}} S_i = \{P(1),P(3),P(5),\ldots\}$$
$$\bigcup_{i\in\mathbb{N}} \widehat{R}(S_i) = \{P(1),P(2),P(4),P(6),\ldots\}$$
$$\widehat{R}(\bigcup_{i\in\mathbb{N}} S_i) = \{P(1),P(2),P(4),\ldots \underbrace{P(0)}_{\text{3rd rule}}\}$$

because the third rule applies only when the predicate P holds for all the odd numbers, as in $\bigcup_{i\in\mathbb{N}} S_i$. Let us now compute the limit of $\widehat{R}$

$$\text{fix}(\widehat{R}) = \bigcup_{n\in\mathbb{N}} \widehat{R}^n(\varnothing) = \{P(1),P(2),P(3),P(4),\ldots\}$$

In fact, we have:

$$\begin{aligned}
\widehat{R}^0(\varnothing) &= \varnothing \\
\widehat{R}^1(\varnothing) &= \{P(1)\} \\
\widehat{R}^2(\varnothing) &= \{P(1),P(2)\} \\
\widehat{R}^3(\varnothing) &= \{P(1),P(2),P(3)\} \\
&\ldots
\end{aligned}$$

But $\text{fix}(\widehat{R})$ is not a fixpoint of $\widehat{R}$, because $P(0) \notin \text{fix}(\widehat{R})$ but $P(0) \in \widehat{R}(\text{fix}(\widehat{R}))$!

$$\widehat{R}(\text{fix}(\widehat{R})) = \{P(0),P(1),P(2),P(3),P(4),\ldots\} \neq \text{fix}(\widehat{R})$$

Example 5.21 (Balanced parentheses). Let us consider the grammar for balanced parentheses, from Example 2.5

$$S \quad ::= \quad \varepsilon \quad | \quad (S) \quad | \quad SS$$

The corresponding logical system is:

$$\frac{\varnothing}{\varepsilon \in L_S} \qquad \frac{s \in L_S}{(s) \in L_S} \qquad \frac{s_1 \in L_S \quad s_2 \in L_S}{s_1 s_2 \in L_S}$$

So we can use the $\widehat{R}$ operator and the fixpoint theorem to find all the strings generated by the grammar:

$$\begin{aligned}
L_{S0} &= \widehat{R}^0(\varnothing) = \varnothing \\
L_{S1} &= \widehat{R}(S_0) = \{\varepsilon\} \\
L_{S2} &= \widehat{R}(S_1) = \{\varepsilon,\ (\,)\} \\
L_{S3} &= \widehat{R}(S_2) = \{\varepsilon,\ (\,),\ ((\,)),\ (\,)(\,)\} \\
&\ldots
\end{aligned}$$

So the language generated by the grammar is $L_S = \mathrm{fix}(\widehat{R})$.

Problems

5.1. Prove Theorem 5.1. *Hint:* The proof is easy, because the axioms of partial and total orders are all universally quantified.

5.2. Let $(\wp(\mathbb{N}), \subseteq)$ be the $\mathrm{CPO}_\perp$ of sets of natural numbers, ordered by inclusion. Assume a set $X \subseteq \mathbb{N}$ is fixed. Let $f, g : \wp(\mathbb{N}) \longrightarrow \wp(\mathbb{N})$ be the functions:

$$f(S) \stackrel{\text{def}}{=} S \cap X$$
$$g(S) \stackrel{\text{def}}{=} (\mathbb{N} \setminus S) \cap X$$

1. Are f and g monotone?
2. Are they continuous?
3. Do the answers to the above questions depend on the given set X?

5.3. Define three functions $f_i : D_i \to D_i$ over three suitable CPO D_i for $i \in [1,3]$ (not necessarily with bottom) such that

1. f_1 is continuous, has fixpoints but not a least fixpoint;
2. f_2 is continuous and it has no fixpoint;
3. f_3 is monotone but not continuous.

5.4. Define a partial order $\mathscr{D} = (D, \sqsubseteq)$ that is not complete.

1. Let $x \sqsubset' y$ if and only if $y \sqsubseteq x$ and $x \neq y$.
   Is the non reflexive reversed order $\mathscr{D}' = (D, \sqsubset')$ a well-founded relation?
2. In general, is it possible that $\mathscr{D}'$ is well-founded for some $\mathscr{D}$?

5.5. Let $V^* \cup V^\infty$ be the set of finite (V^*) and infinite (V^∞) strings over the alphabet $V = \{a, b, c\}$, and let $\alpha \sqsubseteq \alpha\beta$, where juxtaposition in $\alpha\beta$ denotes string concatenation and $\alpha\beta = \alpha$ if α is infinite.

1. Is the structure $(V^* \cup V^\infty, \sqsubseteq)$ a partial order?
2. If yes, is it a complete partial order?
3. Does there exist a bottom element?
4. Which are the maximal elements?

5.6. Let $(D_1, \sqsubseteq_1)$ and $(D_2, \sqsubseteq_2)$ be two CPOs such that $D_1, D_2 \subseteq D$. Consider the structures:

- $(D_1 \cup D_2\ ,\ \sqsubseteq)$, where $x \sqsubseteq y$ iff $x \sqsubseteq_1 y \vee x \sqsubseteq_2 y$
- $(D_1 \cap D_2\ ,\ \preceq)$, where $x \preceq y$ iff $x \sqsubseteq_1 y \wedge x \sqsubseteq_2 y$

1. Are they always partial orders?

2. If so, are they complete?

In case of negative answers, exhibit some counterexample.

5.7. Let X and Y be sets and $X_\perp$ and $Y_\perp$ be the corresponding flat domains. Show that a function $f : X_\perp \to Y_\perp$ is continuous if and only if one of the following conditions holds:

1. f is *strict*, i.e., $f(\perp) = \perp$.
2. f is constant.

5.8. Let $\{\top\}$ be a one-element set and $\{\top\}_\perp$ the corresponding flat domain. Let Ω be the domain of *vertical natural numbers*

$$0 \leq 1 \leq 2 \leq 3 \leq \ldots \leq \infty.$$

Show that the set of continuous functions from Ω to $\{\top\}_\perp$ is in bijection with Ω.
Hint: Define what the possible continuous functions from Ω to $\{\top\}_\perp$ are.

5.9. Let $D = \mathbb{N} \cup \{\infty_0, \infty_1\}$ and $\sqsubseteq$ be the relation over D such that:

- for any pair of natural numbers $n, m \in \mathbb{N}$, we let $n \sqsubseteq m$ iff $n \leq m$;
- for any natural number $n \in \mathbb{N}$, we let $n \sqsubseteq \infty_0$ iff n is even;
- for any natural number $n \in \mathbb{N}$, we let $n \sqsubseteq \infty_1$ iff n is odd;
- and we set $\infty_0 \sqsubseteq \infty_0 \sqsubseteq \infty_1 \sqsubseteq \infty_1$.

Is $(D, \sqsubseteq)$ a CPO? Explain.

5.10. Consider the set $\mathbb{N} \times \mathbb{N}$ of pairs of natural numbers with the lexicographic order relation $\sqsubseteq$ defined by letting:

$$(n, m) \sqsubseteq (n', m') \quad \text{if} \quad n < n' \vee (n = n' \wedge m < m')$$

1. Prove that $\sqsubseteq$ is a partial order with bottom.
2. Show that the chain $\{(0, k)\}_{k \in \mathbb{N}}$ has a lub.
3. Exhibit a chain without lub.
4. Consider the subset $[0, n] \times \mathbb{N}$, with the same order, and then show, also in this case, a chain without lub .
5. Finally, prove that $[0, n] \times (\mathbb{N} \cup \infty)$ with the same order (where $x \leq \infty$ for any $x \in \mathbb{N}$), is complete with bottom, and show a monotone, non continuous function on it.

5.11. Prove that the set **Tf** of total functions from $\mathbb{N}$ to $\mathbb{N}_\perp$ defined in Example 5.14 forms a complete partial order.

5.12. Consider the set **PI** of partial injective functions from $\mathbb{N}$ to $\mathbb{N}$. A partial injective function f can be seen as a relation $\{(x, y) \mid x, y \in \mathbb{N} \wedge y = f(x)\} \subseteq \mathbb{N} \times \mathbb{N}$ such that

- $(x, y), (x, y') \in f$ implies $y = y'$, (i.e., f is a partial function), and
- $(x, y), (x', y) \in f$ implies $x = x'$, (i.e., f is injective).

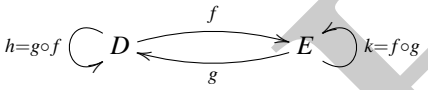
Accordingly, the elements of **PI** can be ordered by inclusion.

1. Prove that $(\mathbf{PI}, \subseteq)$ is a complete partial order.
2. Prove that the function $F : \mathbf{PI} \to \mathbf{PI}$ with $F(f) = \{(2 \times x, y) \mid (x, y) \in f\}$ is monotone and continuous.
   (Hint: Consider F as computed by the immediate consequences operator $\widehat{R}$, with R consisting only of the rule $(x, y)/(2 \times x, y)$.)

5.13. Let $(D, \sqsubseteq)$ be a CPO, $\{d_i\}_{i \in \mathbb{N}}$ a chain in D and $f : \mathbb{N} \to \mathbb{N}$ a function such that for all $i, j \in \mathbb{N}$ if $i < j$ then $f(i) < f(j)$. Prove that:

$$\bigsqcup_{i \in \mathbb{N}} d_{f(i)} = \bigsqcup_{i \in \mathbb{N}} d_i$$

5.14. Let D, E be two $\mathrm{CPO}_\perp$ and $f : D \to E$, $g : E \to D$ be two continuous functions between them. Their compositions $h = g \circ f : D \to D$ and $k = f \circ g : E \to E$ are known to be continuos and thus have least fixpoints.



Let $e_0 = \mathrm{fix}\, k \in E$. Prove that $g(e_0) = \mathrm{fix}\, h \in D$ by showing that:

1. $g(e_0)$ is a fixpoint for h, and
2. that $g(e_0)$ is the least pre-fixpoint for h.