Topics in Domain Theory and Point-free Topology *

Erik Palmgren
Department of Mathematics, Uppsala University

May 23, 2002

These notes for the course Domain Theory MN1 cover some topics not treated in the main textbook [MTD] such as interval arithmetic, digital topology, signed-digit expansions, abstract interpretation and Galois connections, combinatorics of partial orders, and gives a different treatment of formal spaces. They are intended to be used as supplementary reading. We refer in the following to

[MTD] Viggo Stoltenberg-Hansen, Ingrid Lindström and Edward R. Griffor. *Mathematical Theory of Domains.* Cambridge University Press 1994.

[NDT] Viggo Stoltenberg-Hansen, *Notes on Domain Theory,* Marktoberdorf 2001.

1 Interval numbers and canonical extensions

Interval computation has long history within numerical methods. More recently it has been used for demonstrating theorems about dynamical systems using a computer (Warwick Tucker, *The Lorenz attractor exists.* PhD thesis, Uppsala 1998). An early, still very readable book on interval analysis is

[IA] Ramon E. Moore. *Interval analysis.* Prentice-Hall 1966.

Newer references and developments can be found on URL:

`www.cs.utep.edu/interval-comp`

The connection between interval analysis and domain theory is made explicit in

*Supplementary course notes for Domain Theory MN1, spring 2002.

[EE] Martín Escardó and Abbas Edalat. Real PCF and integration. *Information and Computation* 160 (2000), 128-166.

We use the definitions of [IA]. An *interval number* is a closed bounded real interval

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$$

where $a \leq b$. Note that $[a, a]$ is the set $\{a\}$ consisting only of the real number a. When there is no danger of confusion we identify such degenerate intervals with real numbers, and thus write a for $[a, a]$. The set of interval numbers

$$\mathcal{I} = \{[a, b] : a \leq b\}$$

is ordered by reverse inclusion

$$[a, b] \sqsubseteq [c, d] \Longleftrightarrow_{\text{def}} [a, b] \supseteq [c, d].$$

Theorem 1.1 $(\mathcal{I}, \sqsubseteq)$ *is an ω-complete partial order.*

Proof. Clearly, since $\subseteq$ is a partial order, its reversal $\sqsubseteq$ is also a partial order. Consider an ω-chain

$$[a_1, b_1] \sqsubseteq [a_2, b_2] \sqsubseteq [a_3, b_3] \sqsubseteq \cdots$$

Hence (a_n) is a bounded increasing sequence of real numbers. This sequence thus has a least upper bound $a = \lim_n a_n$. Similarly, the decreasing sequence (b_n) has a greatest lower bound $b = \lim_n b_n$. From this it follows directly that $[a, b]$ is a least upper bound of the ω-chain. [X]

Theorem 1.2 $\mathcal{I}_{[c,d]} = \{[a, b] \in \mathcal{I} : [c, d] \sqsubseteq [a, b]\}$ *is an ω-cpo where the least element is $\perp = [c, d]$.* [X]

Remark Theorem 1 and 2 can easily be strengthened to show that $\mathcal{I}$ is a directed complete partial order, and that $\mathcal{I}_{[a,b]}$ is a cpo, by considering suprema and infima over arbitrary sets.

The usual order $<$ on real numbers extend to interval numbers as follows

$$[a, b] < [c, d] \Longleftrightarrow_{\text{def}} b < c.$$

$$[a, b] \leq [c, d] \Longleftrightarrow_{\text{def}} b \leq c.$$

Thus for instance $[1,2] < [3,4]$. Note however that this not at total order: $[0,2] \not< [1,3]$, $[1,3] \not< [0,2]$ and $[0,2] \neq [1,3]$. The relation respects the information order $\sqsubseteq$ in the following sense

$$I < J, I \sqsubseteq I', J \sqsubseteq J' \Longrightarrow I' < J'.$$

Operations on intervals. For any function $f : \mathbb{R}^n \to \mathbb{R}$ define for intervals $I_1, \ldots, I_n \in \mathcal{I}$ *the canonical extension*

$$If(I_1, \ldots, I_n) = \{f(x_1, \ldots, x_n) : x_1 \in I_1, \ldots x_n \in I_n\}. \tag{1}$$

Observe that if f has a discontinuity then $If(J)$ need not be an interval. For instance let $f(x) = 1$ for $x \geq 0$ and $f(x) = 0$ for $x < 0$. Then $f([-1,2]) = \{0,1\}$.

Theorem 1.3 *If $f : I_1 \times \cdots \times I_n \to \mathbb{R}$ is continuous, then $If(I_1, \ldots, I_n)$ is an interval.*

Proof. $K = I_1 \times \cdots \times I_n$ is closed and bounded. Since f is continuous it attains infimum and supremum on K, say at x and y respectively. Clearly, $f(K) \subseteq [f(x), f(y)]$. The inclusion $\supseteq$ follows from the intermediate value theorem using the continuous function

$$g(t) = f(x(1-t) + yt) \qquad (0 \leq t \leq 1). \quad [\mathtt{X}]$$

Using this theorem we see that the arithmetical operations extend to intervals. Thus for $I, J, K \in \mathcal{I}$, where $0 \notin K$,

$$I + J, \quad I \cdot J, \quad I - J, \quad I/K$$

will be intervals. Explicitly:

$$\begin{aligned}
[a,b] + [c,d] &= [a+c, b+d] \\
[a,b] - [c,d] &= [a-d, b-c] \\
[a,b] \cdot [c,d] &= [\min(ac, ad, bc, bd), \max(ac, ad, bc, bd)] \\
[a,b]/[c,d] &= [a,b] \cdot [1/d, 1/c]
\end{aligned}$$

Further operations are suggested by the information ordering $\sqsubseteq$

$$
\begin{aligned}
[a,b] \sqcap [c,d] &= [\min(a,c), \max(b,d)] \\
[a,b] \sqcup [c,d] &= [\max(a,c), \min(b,d)] \text{ if } \max(a,c) \le \min(b,d)
\end{aligned}
$$

The operation $I \sqcap J$ is always defined and is the infimum of I and J with respect to $\sqsubseteq$ (check this). Note that $[0,1] \sqcap [2,3] = [0,3]$, so it is not simply the union, but the smallest interval containing the union. We have

$$I \sqsubseteq J \Longleftrightarrow I \sqcap J = I.$$

The supremum $I \sqcup J$ is only defined if I and J intersect. For instance $[0,2] \sqcup [1,3] = [1,2]$.

2 Algebraic laws for interval numbers

Theorem 2.1 *The operations $+$ and $\cdot$ on $\mathcal{I}$ are associative and commutative. Moreover $0 = [0,0]$ and $1 = [1,1]$ are identities with respect to $+$ and $\cdot$.*

Proof. This follows straightforwardly from the definition (1). [X]

The distributivity law

$$I(J+K) = IJ + IK$$

fails however. Notice that

$$[-1,1]([0,1] + [-1,0]) = [-1,1] \cdot [-1,1] = [-1,1]$$

but

$$[-1,1] \cdot [0,1] + [-1,1] \cdot [-1,0] = [-1,1] + [-1,1] = [-2,2].$$

Proposition 2.2 *For $I, J, K \in \mathcal{I}$*

$$I(J+K) \subseteq IJ + IK \qquad \textit{(subadditivity)}$$

where equality holds whenever $JK > 0$ or I is a real number.

Proof. Exercise, see [IA]. (Hint for $JK > 0$: rewrite $ab + cd$ as $(at + c(1-t))(b+d)$ where $t = b/(b+d)$.) [X]

Exercise Which method of evaluating polynomials does subadditivity suggest, in order to get sharper approximation? (Answer: Horner's method. Observe $a_0 + a_1 I + a_2 I^2 + \cdots \supseteq a_0 + I(a_1 + I(a_2 + \cdots))$.

Proposition 2.3 *For $I, J > 0$*

$$(I+J)^n = \sum_{k=0}^{n} \binom{n}{k} I^k J^{n-k}.$$

Proof. From $I > 0$ and $J > 0$ follows by Proposition 2.2 that the left hand side is

$$\sum_{i_1=0}^{1} \sum_{i_2=0}^{1} \cdots \sum_{i_n=0}^{1} K_{i_1} K_{i_2} \cdots K_{i_n}$$

where $K_0 = I$ and $K_1 = J$. Counting terms equal to $I^k J^{n-k}$ now gives the right hand side as usual. [X]

The arithmetical operations commutes with the infimum operation as follows.

Theorem 2.4 *For intervals I, J, K we have*

$$\begin{aligned} (I \sqcap J) + K &= (I + K) \sqcap (J + K) \\ (I \sqcap J) \cdot K &= (I \cdot K) \sqcap (J \cdot K) \\ -(I \sqcap J) &= -I \sqcap -J \end{aligned}$$

and for $I \sqcap J$ not containing 0:

$$1/(I \sqcap J) = (1/I) \sqcap (1/J).$$

Proof. Left as an exercise. [X]

Since every interval I is of the form $a \sqcap b$, where a and b are real numbers, the properties given by Theorem 2.4 determine the definition of the arithmetical operations. For instance,

$$\begin{aligned} [a,b] \cdot [c,d] &= (a \sqcap b) \cdot (c \sqcap d) \\ &= (a \cdot (c \sqcap d)) \sqcap (b \cdot (c \sqcap d)) \\ &= (a \cdot c) \sqcap (a \cdot d) \sqcap (b \cdot c) \sqcap (b \cdot d) \\ &= [\min(ac, ad, bc, bd), \max(ac, ad, bc, bd)] \end{aligned}$$

In the last line we assumed that $\cdot$ extends multiplication of real numbers.

Proposition 2.5 *For intervals I, J, K*

$$I \sqcap J < K \iff I < K \text{ and } J < K,$$

$$K < I \sqcap J \iff K < I \text{ and } K < J.$$

Moreover $I = J$ if and only if for all K

$$I < K \Leftrightarrow J < K$$

and

$$K < I \Leftrightarrow K < J.$$

Proof. This is immediate from the definition of the order of intervals. [X]

Proposition 2.6 *The set of interval numbers $\mathcal{I}$ is order-complete with respect to $<$: for $S = \{[a_i, b_i] : i \in I\}$ bounded above, the real number $\sup_i b_i$ is the supremum. If S is instead bounded below, the real number $\inf_i a_i$ is the infimum.* [X]

Remark 2.7 What laws do hold for interval numbers? It turns out that this can, in principle, be decided for many cases. It is an algorithmically decidable question for closed first order formulas over $(\mathcal{I}; <, \sqcap, +, \cdot, -, 0, 1)$ since this structure can be interpreted into $(\mathbb{R}; <, +, \cdot, -, 0, 1)$. (Exercise: write down the necessary formulas.) The latter has a well-known decision method due to Tarski. (For a proper answer to the question, see one of the more modern books on interval analysis.)

3 Continuous functions

If an interval $[a, b]$ is strictly included in $[c, d]$ on both sides, then for any directed set $I_k = [x_k, y_k]$ of intervals such that

$$[a, b] \supseteq \cap_k I_k$$

there is already some $I_{k'}$ with $[c, d] \supseteq I_{k'}$. This follows since

$$\cap_k I_k = [\sup_k x_k, \inf_k y_k],$$

and thus $c < a \leq \sup_k x_k$ and $\inf_k y_k \leq b < d$. Thereby for some k_1, k_2: $c < x_{k_1}$ and $y_{k_2} < d$. Since the set of intervals is directed, $I_{k_1}, I_{k_2} \supseteq I_{k'}$ for some k'. In particular, $x_{k_1} \leq x_{k'}$ and $y_{k'} \leq y_{k_2}$ yielding the desired k'.

This motivates the following general definition for partial orders.

Definition 3.1 Let $(C, \sqsubseteq)$ be any directed complete partial order. Then x is said to be *way below* y (in symbols $x \ll y$) if, and only if, for any directed $A \subseteq D$

$$x \sqsubseteq \sqcup A \Longrightarrow (\exists a \in A)\, x \sqsubseteq a.$$

Taking the trivial directed set $A = \{y\}$ we see that $x \ll y$ implies $x \sqsubseteq y$. The converse is not true for e.g. intervals.

Theorem 3.2 *For intervals we have*

$$[a, b] \ll [c, d] \iff a < c \text{ and } d < b.$$

Proof. The direction $(\Leftarrow)$ follows from the discussion above. As for $(\Rightarrow)$ assume that $[a, b] \ll [c, d]$. Let $I_k = [c - 1/k, d + 1/k]$ for $k = 1, 2, 3, \ldots$. Then $\sqcup_{k \geq 1} I_k = \cap_{k \geq 1} I_k = [c, d]$, so by assumption $I_k \sqsupseteq [a, b]$ for some k. Thus $a \leq c - 1/k < c$ and $d < d + 1/k \leq b$. [X]

Note that $[c, d] = \cap\{[a, b] : a < c, d < b\}$ so $[c, d]$ is the supremum of all intervals way below $[a, b]$.

Definition 3.3 Let $(C, \sqsubseteq)$ be any directed complete partial order. Then C is *continuous* if for any $x \in C$ the set $\{y \in C : y \ll x\}$ is directed, and

$$x = \sqcup\{y \in C : y \ll x\}.$$

If in addition, C has a least element, it is called a *continuous cpo.*

Example 3.4 $\mathcal{I}$ is a continuous directed complete partial order. Moreover any interval can be expressed as an intersection of intervals with rational endpoints, so

$$[a, b] = \sqcup\{[p, q] : [p, q] \ll [a, b], p, q \in \mathbb{Q}\}$$

This suggests another definition.

Definition 3.5 Let $(D, \sqsubseteq)$ be any directed complete partial order. A *base* for D is a subset $B \subseteq D$ such that for each $x \in D$, the set $\text{approx}_B(x) = \{y \in B : y \ll x\}$ is directed, and $x = \sqcup \text{approx}_B(x)$.

Clearly set of intervals with rational endpoint forms a base for $\mathcal{I}$.

Trivially, if D is continuous then $B = D$ is a base for D. Thus one direction of the following proposition is clear. We leave the other direction as an exercise.

Proposition 3.6 *A directed complete partial order D is continuous iff it has a base.* [X]

By Theorem 10 we have the "interpolation property" for intervals

$$I \ll J \Longrightarrow (\exists K)\, I \ll K \ll J.$$

More abstractly we have

Theorem 3.7 *Let D be a directed complete partial order with base B_D. Then*

$$x \ll y \Longrightarrow (\exists z \in B_D)\ x \ll z \ll y.$$

Proof. Let

$$A = \{x \in D : (\exists z \in B_D)\, x \ll z \ll y\}.$$

It can straightforwardly be checked that A is directed using the directedness of the approximation sets $\mathrm{approx}_{B_D}(\cdot)$. We claim that $y = \sqcup A$. We prove the nontrivial relation $\sqsubseteq$. Note that for $a \in \mathrm{approx}_{B_D}(y)$, we have $\mathrm{approx}_{B_D}(a) \subseteq A$, so $a = \sqcup \mathrm{approx}_{B_D}(a) \sqsubseteq \sqcup A$. Thus $y = \sqcup \mathrm{approx}_{B_D}(y) \sqsubseteq \sqcup A$.

Now suppose $x \ll y$. Since $y = \sqcup A$, there is some $u \in A$ with $x \sqsubseteq u$. But then, $u \ll z \ll y$ for some $z \in B_D$. Indeed also $x \ll z$. [X]

For an even stronger version of Theorem 3.7 see [NDT].

Proposition 3.8 *Let D and E be a directed complete partial orders with bases B_D and B_E, respectively. Then $B_D \times B_E$ is a base for $D \times E$.*

Proof. The result follows from the equivalence

$$(x, y) \ll (u, v) \Longleftrightarrow x \ll u \text{ and } y \ll v. \qquad [X]$$

Notice that by the construction of the cartesian product, the n-fold product $\mathcal{I}^n$ consists of vectors $(I_1, \ldots, I_n)$ of intervals, ordered such that $(I_1, \ldots, I_n) \sqsubseteq (J_1, \ldots, J_n)$ if, and only if, $I_k \supseteq J_k$ for each $k = 1, \ldots, n$. By the proposition, the vectors where all intervals have rational endpoints forms a base ("rational boxes").

Theorem 3.9 *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a continuous function. Then the canonical extension $If : \mathcal{I}^n \to \mathcal{I}$ is continuous.*

Proof. The verification is elementary using the characterisation Proposition 2.27 [NDT] of continuity, and the base of rational boxes. [X]

We have a converse to this theorem.

Theorem 3.10 *Let $g : \mathcal{I}^n \to \mathcal{I}$ be a continuous function such that $g(I_1, \ldots, I_n)$ is real for all real $I_1, \ldots, I_n$. Then the restriction $g : \mathbb{R}^n \to \mathbb{R}$ is continuous with respect to the usual topology on real numbers.*

Proof. Let B be the set of intervals with rational end-points. Then B^n is a base for $\mathcal{I}^n$. By Proposition 2.27 of [NDT] we get for real $x_1, \ldots, x_n \in \mathbb{R}$ and rational p, q with $p < g(x_1, \ldots, x_n) < q$ some $(I_1, \ldots, I_n) \in B^n$ with $x_1 \in I_1, \ldots, x_n \in I_n$ and

$$[p, q] \ll g(I_1, \ldots, I_n).$$

Write $g(I_1, \ldots, I_n) = [g_1(I_1, \ldots, I_n), g_2(I_1, \ldots, I_n)]$. For $u_1 \in I_1, \ldots, u_n \in I_n$ we have $g(I_1, \ldots, I_n) \sqsubseteq g(u_1, \ldots, u_n)$ by monotonicity of g. It follows that

$$p < g_1(u_1, \ldots, u_n) = g_2(u_1, \ldots, u_n) < q$$

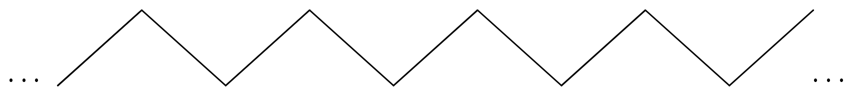
proving the result. [X]

4 Digital Topology

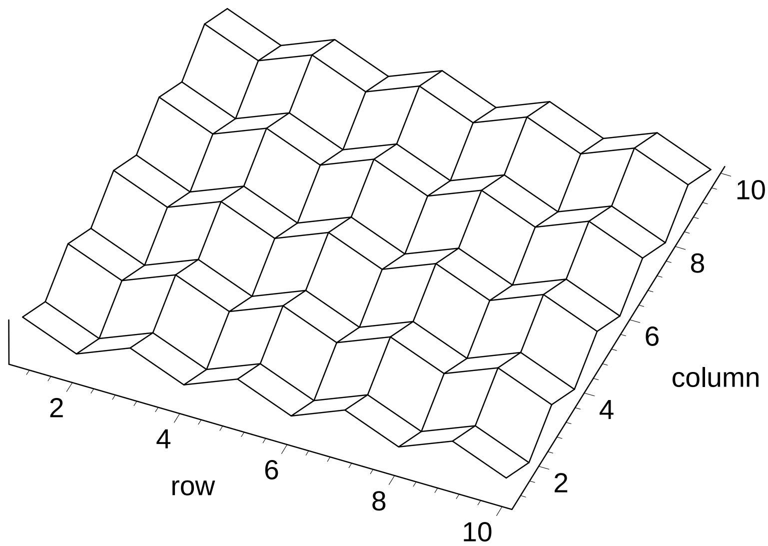
Curves on a computer screen can be studied using the so-called *Khalimsky topology* (see Kiselman [K]). The Khalimsky topology on the integers $\mathbb{Z}$ is the Alexandrov topology [MTD, p.116] of the following partial order. Define $\sqsubseteq_K$ on $\mathbb{Z}$ by

$$m \sqsubseteq_K n \iff (m-n)^2 \leq \frac{1+(-1)^m}{2}.$$

This is less complicated than it looks. Note that for m even: $m \sqsubseteq_K n$ iff $(m-n)^2 \leq 1$ iff $|m-n| \leq 1$. In case m is odd: $m \sqsubseteq_K n$ iff $(m-n)^2 \leq 0$ iff $m = n$. The resulting partial order $(\mathbb{Z}, \sqsubseteq_K)$ is the *Khalimsky line.* Drawing its Hasse-diagram it actually looks more like the edge of a saw:



It is easily checked to be connected. Taking the cartesian product [MTD, p.34] of two copies of this partial order yields the *Khalimsky plane* $\mathbb{Z} \times \mathbb{Z}$. The Alexandrov topology of this partial order gives a connected topology on $\mathbb{Z} \times \mathbb{Z}$. A three-dimensional Hasse-diagram (height=2) of a piece of the Khalimsky plane is given below:



Exercise. Consider the n-fold cartesian product $\mathbb{Z}^n$ of the partial order $(\mathbb{Z}, \sqsubseteq_K)$. (This is the n-dimensional Khalimsky space.) What is its height (maximal length of a chain)?

Embedding as chained intervals. The Khalimsky line can be embedded into the intervals $\mathcal{I}$ by the function $f : \mathbb{Z} \to \mathcal{I}$

$$f(n) = \left[n - \frac{3 + (-1)^n}{2}, n + \frac{3 + (-1)^n}{2}\right]$$

Thus $f(n) = [n-2, n+2]$ for n even, and $f(n) = [n-1, n+1]$ for n odd.

Proposition 4.1 *$f : (\mathbb{Z}, \sqsubseteq) \to (\mathcal{I}, \sqsubseteq)$ is order preserving.* [X]

Note that if allow different scales of the embedded intervals, they form a base $B = \{2^{-k} f(n) : k, n \in \mathbb{Z}\}$ for $\mathcal{I}$.

We have the following characterisation of continuous functions with respect to the Alexandrov topology.

Theorem 4.2 *Let $(X_1, \leq_1)$ and $(X_2, \leq_2)$ be partially ordered sets, and let τ_1 and τ_2 be the corresponding Alexandrov topologies. Then a function $f : X_1 \to X_2$ is continuous $(X_1, \tau_1) \to (X_2, \tau_2)$ if, and only if, $f : (X_1, \leq_1) \to (X_2, \leq_2)$ is monotone.*

Proof. (only if): Let $u \leq_1 v$. Clearly $U = \{y \in Y : f(u) \leq_2 y\}$ is open in τ_2. Thus $f^{-1}(U)$ is open by continuity, and contains u. Hence it contains also v, that is $f(v) \in U$, i.e. $f(u) \leq_2 f(v)$.

(if): left as an easy exercise. [X]

Fixed points. It is easy to see that every continuous function $f : [a, b] \to [a, b]$ has a fixed point. (Draw a picture.) Does the corresponding hold in the digital case? A *Khalimsky interval* is a set of consecutive integers

$$[m, m + \ell]_{\mathbb{Z}} = \{m, m + 1, m + 2, \ldots, m + \ell\}$$

ordered by $\sqsubseteq_K$. By Theorem 4.2 a continuous function $[m, m+\ell]_{\mathbb{Z}} \to [m, m+\ell]_{\mathbb{Z}}$ is simply a monotone function with respect to $\sqsubseteq_K$. If every monotone function on $[m, m + \ell]_{\mathbb{Z}}$ has a fixed point, we say that $[m, m + \ell]_{\mathbb{Z}}$ has the *fixed point property.* Every complete lattice, and hence every finite lattice with 0 and 1, has the fixed point property:

Theorem 4.3 *(Tarski) Let $(L, \leq)$ be a complete lattice. Then for every monotone $f : L \to L$ there is a $y \in L$ with $f(y) = y$, and $y \leq x$ for whenever $f(x) \leq x$. Thus y is the least fixed point of f.*

Proof. Since L is complete the following infimum exists

$$y = \wedge\{x \in L : f(x) \leq x\}.$$

Clearly, if $f(x) \leq x$ then by definition of the infimum $y \leq x$. Monotonicity of f gives $f(y) \leq f(x) \leq x$. Hence $f(y) \leq y$. Again applying monotonicity $f(f(y)) \leq f(y)$, from which we conclude that $f(y)$ is in the set taken infimum of. Thereby $y \leq f(y)$, and $f(y) = y$. [X]

> **Problem*** Does every Khalimsky interval have the fixed point property? (Solution in Chapter 5.)
>
> **Exercise** Suppose $n \geq 2$. Let L be the set of subsets A of $\{0, \ldots, n-1\}$ where $0 < |A| < n$. Define a monotone function $F : L \to L$ by
>
> $$F(A) = \{k + 1 \bmod n : k \in A\}$$
>
> Show that F lacks fixed points. Is L a (complete) lattice?
>
> **Research Problem** Note that every finite partial order with least element $\perp$ has the fixed point property. Open problem: find a characterisation of the partial orders which have the fixed point property. See Björner [B] for interesting partial results and further references.

References

[B] A. Björner. Combinatorics and Topology. Notices of the American Mathematical Society, June 1985, pp. 339 – 345.

[K] C.O. Kiselman: Digital Jordan Curve Theorems. *Discrete Geometry for Computer Imagery*, 9th International Conference, DGCI 2000, Uppsala, Sweden, December 13–15, 2000. (Eds. Gunilla Borgefors, Ingela Nyström, Gabriella Sanniti di Baja.) Lecture Notes in Computer Science **1953**, pp. 46–56. Springer, 2000.

5 Discrete fixed point theorems

A finite poset is *dismantable* if there is a monotone $f : [0, n]_{\mathbb{Z}} \times P \to P$ such that $f(n, \cdot) = id_P$ and $f(0, \cdot)$ constant. This definition is similar to that of a contractible space except that a real interval has been replaced by a Khalimsky interval.

Theorem 5.1 *(Baclawski, Björner (1979)) If P is dismantable, then every monotone $g : P \to P$ has a fixed point.*

Proof: We have for some monotone $f : [0, n]_{\mathbb{Z}} \times P \to P$ that

$$\lambda x.p = f(0, \cdot) \leq f(1, \cdot) \geq f(2, \cdot) \leq \cdots \geq f(n, \cdot) = id_P$$

Let $h_k = f(k, \cdot) \circ g$.

Clearly p is a fixed point of h_0. Show that $h_n = g$ has a fixed point by *induction*:

If z is a fixed point of h_k, then (depending on parity)

$$h_{k+1}(z) \leq h_k(z) = z \text{ or } h_{k+1}(z) \geq h_k(z) = z$$

Since P finite, $h^n_{k+1}(z) = h^{n+1}_{k+1}(z)$ for some n, and thus $h^n_{k+1}(z)$ is a fixed point of of h_{k+1}. [X]

Theorem 5.2 *The Khalimsky interval $[0, m]_{\mathbb{Z}}$ is dismantled by the minimum function*

$$f(k, x) = \min(k, x)$$

(here $f : [0, m]_{\mathbb{Z}} \times [0, m]_{\mathbb{Z}} \to [0, m]_{\mathbb{Z}}$).

Proof: Obviously $f(0, x) = 0$ and $f(m, x) = x$, for all $x \in [0, m]_{\mathbb{Z}}$. So the condition on the endpoints is correct. It remains to show that f is monotone, and to verify this it suffices to check monotonocity in each argument. Since the function is symmetric it is enough to check the first argument. Suppose $n \sqsubseteq n'$. If n is odd, then $n = n'$ so $f(n, x) = f(n', x)$. In case $n = 2\ell$, and $n \neq n'$ we have $n' = 2\ell - 1$ or $n' = 2\ell + 1$. For $n' = 2\ell - 1$: if $x \leq 2\ell - 1$, then $f(n, x) = f(n', x) = x$ and if $x \geq 2\ell$, then

$$f(n, x) = n = 2\ell \sqsubseteq 2\ell - 1 = n' = f(n', x).$$

(Note that $\sqsubseteq$ refers to the Khalimsky ordering.) For the case $n' = 2\ell + 1$: if $x \leq 2\ell$, then $f(n, x) = x = f(n', x)$, and if $x \geq 2\ell + 1$, then

$$f(n, x) = n = 2\ell \sqsubseteq 2\ell + 1 = n' = f(x, n').$$

This shows that f is monotone. [X]

Certain powers of dismantable finite sets are dismantable:

Theorem 5.3 *(Baclawski, Björner 1979): Suppose P is a dismantable finite poset and Q is an arbitrary finite poset. Then the function space P^Q dismantable.*

Proof: If $f : [0,n]_{\mathbb{Z}} \times P \to P$ monotone, then so is

$$F(k,g) = f(k,\cdot) \circ g$$

here $F : [0,n]_{\mathbb{Z}} \times P^Q \to P^Q$. Clearly $F(0,g) = f(0,\cdot) \circ g = (\lambda y.p) \circ g = \lambda x.p$, and $F(n,g) = f(n,\cdot) \circ g = id_P \circ g = g$. Hence $F(0,\cdot)$ is constant, and $F(n,\cdot)$ is the identity. [X]

Taking Q to be the discrete poset $\{1,2\}$ we get immediately:

Corollary 5.4 *The Khalimsky square $[0,n]_{\mathbb{Z}} \times [0,n]_{\mathbb{Z}}$ is dismantable.*

References

K. Baclawski, A. Björner. Fixed points in partially ordered sets. *Advances in Mathematics* 31(1979).

6 Digitalization

Consider the "rounding" function $\delta : \mathbb{R} \to \mathbb{Z}$ given by

$$\delta(x) = \begin{cases} 2n & \text{if } x = 2n \text{ for some } n \in \mathbb{Z} \\ 2n+1 & \text{if } x \in (2n, 2n+2) \text{ for some } n \in \mathbb{Z} \end{cases}$$

(It rounds x to the nearest odd number, unless x is even in which case it cannot decide and does nothing.) The Khalimsky topology on the integers has the remarkable property of making this function continuous! The basic open sets are of the form $U_n = \{2n+1\}$ or $V_n = \{2n-1, 2n, 2n+1\}$. Then $\delta^{-1}(U_n) = (2n, 2n+2)$ and

$$\begin{aligned} \delta^{-1}(V_n) &= (2n-2, 2n) \cup \{2n\} \cup (2n, 2n+2) \\ &= (2n-2, 2n+2). \end{aligned}$$

So clearly δ is continuous. We can extend the discretization function to the plane as well. Define $\delta_2 : \mathbb{R}^2 \to \mathbb{Z}^2$ by letting $\delta_2(x,y) = (\delta(x), \delta(y))$. This is again continuous since the Khalimsky topology on the plane is the product topology of two Khalimsky lines.

Remark It would arguably be more natural to round to the nearest even number. One may also consider rounding to numbers with a fixed number n of decimals $\mathbb{R} \to 10^{-n}\mathbb{Z}$. This requires a change to the Khalimsky topology, which we leave as an easy exercise.

7 Does every real number have a decimal expansion?

This is the English translation the title of a famous paper of L.E.J. Brouwer. (1921). There he shows that this is *not* the case if these notions are to be understood in a constructive sense. We do the argument for the binary number system.

Suppose every real number $x \in [0,1)$ can be assigned a unique binary expansion in the sense that there is a sequence $d_1, d_2, d_3, \ldots \in \{0,1\}$ with $x \in [e_n, e_n + 2^{-n})$ where

$$e_n = \sum_{k=1}^{n} d_k 2^{-k}.$$

The sequence (d_k) is necessarily unique and $x = (0.d_1 d_2 d_3 \cdots)_2$.

Consider a sequence $(a_n)_{n=1}^{\infty}$ of 0 and 1's which is such that, if it at some point it becomes 0, then it stays 0. Intuitively, there is no algorithmic procedure that decides for a general sequence if it ever becomes 0. This intuition is correct, and it can be shown that no Turing machine can do it. (Exercise)

Define a sequence of rational numbers $x_1, x_2, \ldots$

$$x_n = \sum_{k=1}^{n} a_k 2^{-k-1}.$$

It is easily seen that this sequence is increasing and bounded by $1/2$, so it has a limit $x \in [0, 1/2]$. The first digit d_1 in the binary expansion of x is 1 if, and only if, the sequence (a_n) is forever 1. Thus we should not expect a general constructive method for obtaining the digits of a decimal expansion.

We have $(0.011111111\cdots)_2 = (0.1000000\cdots)_2$, so one might argue that the problem can be solved by identifying these expansions, more generally, allowing $x \in [e_n, e_n + 2^{-n}]$. Note that two such intervals may overlap in one point. But the argument can be strengthened. Let $s(n) = a_1 + \cdots + a_n$. Define a new sequence

$$x_n = \frac{1}{2} + \big(\frac{-1}{2}\big)^{s(n)}.$$

Let x be its limit. Notice that if a_n stays 1 forever then the sequence oscillates around $1/2$ and $x = 1/2$. In this case, the first digit in the expansion of x can be 0 or 1. Suppose now that a_n becomes 0 at some point. If a_n becomes 0 first at $n = 2k$, an even number, then for all $m \geq n$

$$x_m = \frac{1}{2} + \big(\frac{-1}{2}\big)^{2k-1} = \frac{1}{2} + -\big(\frac{1}{2}\big)^{2k-1} < \frac{1}{2}.$$

In this second case the first digit of x is 0. If a_n becomes 0 first at $n = 2k+1$, an odd number, then for all $m \geq n$

$$x_m = \frac{1}{2} + \big(\frac{-1}{2}\big)^{2k} = \frac{1}{2} + \big(\frac{1}{2}\big)^{2k} > \frac{1}{2}.$$

In this third case the first digit of x is 1.

In conclusion: if the first digit in the expansion of x is 1 we can exclude the second case, and if the first digit in the expansion of x is 0 we can exclude the third case. Suppose that we can compute the digits of this version of decimal expansion. We are thus able to predict that either A) the sequence does not become 0 at an even position or B) the sequence does not become 0 at an odd position. This is not algorithmically possible!

A solution to the problem is to introduce even more redundancy into the expansions by allowing a negative digit $\overline{1} = -1$ as well. For $d_k \in \{\overline{1}, 0, 1\}$

$$f = (d_n d_{n-1} \cdots d_1 d_0 . d_{-1} d_{-2} \cdots d_{-m})_{\pm 2} = \sum_{k=-m}^{n} d_k 2^k.$$

This number represents the interval $I = f + D = [f - \delta, f + \delta]$, where $\delta = 2^{-m}$ and $D = [-\delta, \delta]$. This interval may be decomposed as chained intervals

$$\begin{aligned} I &= [f - \delta, f] \cup [f - \delta/2, f + \delta/2] \cup [f, f + \delta] \\ &= ((f - 2^{-(m+1)}) + \frac{D}{2}) \cup ((f + 0) + \frac{D}{2}) \cup ((f + 2^{-(m+1)}) + \frac{D}{2}) \end{aligned}$$

By approximating $x \in I$ we may decide which of the components it belongs, and thereby determine the next digit $d = d_{-(m+1)}$. Consider a rational number q approximating x to within $\delta/4$, i.e. $|x - q| \leq \delta/4$. Thus if $q \leq f - \delta/4$, x belongs to the first component, and take $d = \overline{1}$, and if $q \geq f + \delta/4$, x belongs to the last component and take $d = 1$. Otherwise $f - \delta/4 < q < f + \delta/4$, and then x belongs to the intermediate component and take $d = 0$. We thus need only a *finite* amount of information about x to select a correct interval:

$$x \in f + d2^{-(m+1)} + \frac{D}{2}.$$

It follows that if x is a constructively given real number we can compute signed digits $d_n, d_{n-1}, \ldots, d_0, d_{-1}, d_{-2}, \ldots$ such that

$$x = \sum_{k=-\infty}^{n} d_k 2^k.$$

Exercise Compute signed digit expansions of of -37, $1/3$ and π.

References

L.E.J. Brouwer. Besitzt jede reelle Zahl eine Dezimalbruchentwicklung? *Mathematische Annalen* 83(1921), 201-210.

8 Formal spaces

One might argue that points of a topological space are not the most basic objects, but rather the open sets and their relations. We have seen [MTD Prop. 6.2.3] that the open sets form a complete lattice which satisfies the infinite distributive law. Such lattices — *frames* — may be constructed from yet more basic structures called formal spaces. We shall here use a more general version than in [MTD].

Example 8.1 Let $P = \{\langle a,b\rangle \in \mathbb{Q}\times\mathbb{Q} : a < b\}$. A pair $\langle a,b\rangle \in P$ is considered as a symbol for the interval $(a,b)\cap\mathbb{Q}$. For any $U \subseteq P$ define the covering relation

$$\langle a,b\rangle \lhd U \tag{2}$$

if, and only if, for any $x \in (a,b)\cap\mathbb{Q}$ there is $\langle c,d\rangle \in U$ with $x \in (c,d)\cap\mathbb{Q}$. Thus (2) says that the interval (a,b) is covered by the intervals represented by the pairs in U. (We give another definition of covering in Section 8.3 which is better from the constructive point of view.) We easily see that $\langle a,b\rangle \lhd U$ for $\langle a,b\rangle \in U$. Extend the covering relation as follows

$$U \lhd V \Longleftrightarrow_{\mathrm{def}} (\forall p \in U)\, p \lhd V.$$

Then it is clear that

$$p \lhd U, U \lhd V \Longrightarrow p \lhd V.$$

Notice that

$$\langle 1/2, 2/3\rangle \lhd \{\langle 0,2/3\rangle, \langle 1/2,1\rangle\} = U$$

and

$$\langle 1/2, 2/3\rangle \lhd \{\langle 0,1/2\rangle, \langle 1/3,1\rangle\} = V,$$

but that the intersection $U\cap V$ is empty, and does not cover $\langle 1/2,2/3\rangle$. The set of intervals refining some interval in $W \subseteq P$ is $W\downarrow = \{\langle p,q\rangle \in P : (\exists\langle r,s\rangle \in W)\, r \le p < q \le s\}$. We have $\langle 1/2,2/3\rangle \lhd (U\downarrow)\cap(V\downarrow)$, since if $x \in (1/2,2/3)$ is a rational, then $\langle x-\delta, x+\delta\rangle \in (U\downarrow)\cap(V\downarrow)$, for some sufficiently small $\delta > 0$. (For instance, let $\delta = \min(|x-1/2|, |x-2/3|)$.)

Definition 8.2 Let S be a set, and let $\lhd$ be a relation between elements of S and subsets of S, i.e. $\lhd \subseteq S \times \mathcal{P}(S)$. Extend $\lhd$ to a relation between subsets of S:

$$U \lhd V \Longleftrightarrow_{\mathrm{def}} (\forall p \in U)\, p \lhd V.$$

For $U \subseteq S$, let

$$U\downarrow = \{d \in S : (\exists u \in U)\, d \lhd \{u\}\}.$$

Note that $(\cup_{i\in I} U_i)\downarrow = \cup_{i\in I}(U_i\downarrow)$.

Definition 8.3 A *formal space* is a set S (of so-called *basic opens*) together with a relation $\lhd \subseteq S \times \mathcal{P}(S)$, the *covering relation,* satisfying the three conditions

(R) $a \in U$ implies $a \lhd U$,

(T) $a \lhd U$, $U \lhd V$ implies $a \lhd V$,

(L) $a \lhd U$, $a \lhd V$ implies $a \lhd (U\downarrow) \cap (V\downarrow)$.

(R for Reflexivity, T for Transitivity and L for Localization.) We call $(S, \lhd)$ a *weak formal space* if (R) and (T) holds. Any formal space is thus also a weak formal space.

The reader interested in getting to the point, should skip to Definition 8.7. We prepare here for some discussions on frames and closure operators.

Let $(S, \lhd)$ be a weak formal space. Note that by (R),

$$U \subseteq V \Longrightarrow U \lhd V, \tag{3}$$

and by (T), also $\lhd$ is transitive:

$$U \lhd V, V \lhd W \Longrightarrow U \lhd W.$$

Thus $\lhd$ is a preorder of $\mathcal{P}(S)$ extending the relation $\subseteq$. From (R) follows $a \lhd \{a\}$ for any $a \in S$, so

$$U \subseteq (U\downarrow). \tag{4}$$

The set of basic opens covered by U, is

$$\tilde{U} =_{\mathrm{def}} \{a \in S : a \lhd U\}.$$

By (T) follows

$$(U\downarrow) \subseteq \tilde{U}. \tag{5}$$

Clearly by (R)

$$U \subseteq \tilde{U} \tag{6}$$

and by (T)

$$U \lhd V \Longrightarrow \tilde{U} \subseteq \tilde{V} \tag{7}$$

By definition of $\tilde{U}$,

$$\tilde{U} \lhd U.$$

Hence by (7)

$$\tilde{\tilde{U}} \subseteq \tilde{U}$$

and thus by (6)

$$\tilde{\tilde{U}} = \tilde{U}. \tag{8}$$

From (3) and (7) we get

$$U \subseteq V \Longrightarrow \tilde{U} \subseteq \tilde{V}. \tag{9}$$

Properties (6),(8) and (9) states that $\tilde{(\cdot)} : \mathcal{P}(S) \to \mathcal{P}(S)$ is a closure operator on the partial order $(\mathcal{P}(S), \subseteq)$. Any set $U \subseteq S$ such that $\tilde{U} = U$ is called *saturated*. Let $\mathrm{Sat}(S) = \mathrm{Sat}(S, \lhd)$ be the set of saturated subsets of S. Note that for saturated U

$$a \in U \Longleftrightarrow a \lhd U. \tag{10}$$

The direction from right to left uses $\tilde{U} = U$. Then for $U, V \in \mathrm{Sat}(S)$:

$$U \subseteq V \Longleftrightarrow U \lhd V. \tag{11}$$

This shows that $\subseteq$ and $\lhd$ are the same partial orders on $\mathrm{Sat}(S)$. The following is immediate by (4) and (5)

Lemma 8.4 *For saturated U in a weak formal space, $(U\downarrow) = U$.* [X]

Lemma 8.5 *Let $(S, \lhd)$ be a weak formal space. The intersection $\cap$ is the infimum operation in* $\mathrm{Sat}(S)$.

Proof: Let $U, V \in \mathrm{Sat}(S)$. Then $a \in \widetilde{U \cap V}$ implies $a \lhd U \cap V$. Hence $a \lhd U$ and $a \lhd V$ by transitivity, and consequently by (10), $a \in U$ and $a \in V$. Thus $\widetilde{U \cap V} \subseteq U \cap V$. The reverse inclusion is an instance of (6). Hence $U \cap V \in \mathrm{Sat}(S)$ and it is immediate that it is the infimum of U and V. [X]

The structure of the saturated sets is given by:

Theorem 8.6 *(a) If $(S, \lhd)$ is a weak formal space, then $(\mathrm{Sat}(S), \subseteq)$ is a complete lattice.*

(b) If $(S, \lhd)$ is a formal space, then $(\mathrm{Sat}(S), \subseteq)$ is a frame.

Proof: (a): Suppose that U_i $(i \in I)$ is a family of saturated sets. Consider

$$\widetilde{\bigcup_{i\in I} U_i}.$$

This is a saturated set, and it is straightforward, using the closure property of $\widetilde{(\cdot)}$, to verify that it is the supremum of the family. (b): We have to verify the infinite distributive law

$$\bigvee_{i\in I}(U_i \wedge V) = (\bigvee_{i\in I} U_i) \wedge V.$$

Here $\subseteq$ is automatic by the definition of suprema and infima. As for $\supseteq$ suppose,

$$x \in (\bigvee_{i\in I} U_i) \wedge V = \left(\widetilde{\bigcup_{i\in I} U_i}\right) \cap V.$$

Thus $x \lhd \bigcup_{i\in I} U_i$ and $x \lhd V$. By (L) we have the first member of

$$\begin{aligned} x \quad \lhd \quad & \left(\bigcup_{i\in I} U_i\right) \downarrow \cap V \downarrow \\ = \quad & \left(\bigcup_{i\in I} U_i \downarrow\right) \cap V \downarrow \\ = \quad & \bigcup_{i\in I}(U_i \downarrow \cap V \downarrow) \\ = \quad & \bigcup_{i\in I}(U_i \cap V) \end{aligned}$$

The last member follows by Lemma 8.4. We thus have

$$x \in \left(\bigcup_{i\in I}\widetilde{(U_i \cap V)}\right).[\mathtt{X}]$$

Points are now constructed rather than considered as ready-made.

Definition 8.7 Let $S = (S, \lhd)$ be a (weak) formal space. A subset $\alpha \subseteq S$ is called a *point* if

(P1) $(\exists a \in S)\, a \in \alpha$

(P2) $a \in \alpha$, $b \in \alpha$ implies $(\exists c \in \alpha)\, c \in \{a\} \downarrow \cap \{b\} \downarrow$

(P3) $a \in \alpha$, $a \lhd U$ implies $(\exists b \in U)\, b \in \alpha$.

Denote the set of points of the formal space by $\mathrm{Pt}(S)$.

Example 8.8 (continued) Consider the formal space $(P, \lhd)$ of Example 8.1. Let $\alpha \subseteq P$ be a point of this formal space. (P1) means that there is some initial approximation $\langle a, b\rangle \in \alpha$. (P2) says any two approximations a and b has a common refinement x. (P3) means that approximations can be refined. We have

$$\langle a, b\rangle \lhd \{\langle a, (a+b)/2\rangle, \langle (3a+b)/4, (a+3b)/4\rangle, \langle (a+b)/2, b\rangle\}.$$

Thus one of $\langle a, (a+b)/2\rangle$, $\langle (3a+b)/4, (a+3b)/4\rangle$, $\langle (a+b)/2, b\rangle$ belongs to α. (Cf. signed digit representation.)

Example 8.9 Let $(Q, \leq)$ be a poset. Define a cover relation $\lhd \subseteq Q \times \mathcal{P}(Q)$ by

$$a \lhd U \iff (\exists b \in U)\, b \leq a.$$

Then $(Q, \lhd)$ is a formal space (exercise). What are the points of this space? Let $\alpha \subseteq Q$ be a point. The condition (P1) says (again) that there is an initial approximation. Note that $x \in \{y\}\downarrow$ iff $y \leq x$. Thus (P2) states that α is directed. For singleton sets $U = \{b\}$ condition (P3) says that

$$a \in \alpha, b \leq a \Longrightarrow b \in \alpha$$

i.e. that α is downward closed. Conversely, suppose α is downward closed. If $a \in \alpha$ and $a \lhd U$, then $(\exists b \in U)\, b \leq a$, and since α is downward closed, $b \in \alpha$, verifying (P3).

In conclusion: the points of $\mathrm{Pt}(Q)$ are non-void, directed and downward closed sets.

Notice that if the partial order has finite height, then the points are all of the form

$$\{q \in Q : q \leq p\}.$$

Example 8.10 Consider the integers with the Khalimsky order $(\mathbb{Z}, \sqsubseteq)$. Then for each real $x \in \mathbb{R}$ let

$$\begin{aligned}\delta(x) \quad = \quad & \{2m \in \mathbb{Z} : x \in (2m - \frac{2}{3}, 2m + \frac{2}{3})\} \\ & \cup \{2m, 2m+1, 2m+2 \in \mathbb{Z} : x \in (2m+1 - \frac{2}{3}, 2m+1+\frac{2}{3})\}.\end{aligned}$$

This is a point of the formal space $(\mathbb{Z}, \lhd)$ where

$$m \lhd U \iff (\exists n \in U) n \sqsubseteq m.$$

Remark 8.11 Sometimes a more restricted notion of formal space is used where there is a positive way (PP1) of saying that a basic open is cannot be covered by an empty set. Such a formal space consists of an ordinary formal space $(S, \lhd)$ and a set of *positive basic opens* $P \subseteq S$ satisfying the axioms

(PP1) $a \in P$, $a \lhd U$ implies U non-void,[1]

(PP2) $a \lhd U$ implies $a \lhd U \cap P$.

Note that (PP2) says that only positive basic opens matter for covering. This is equivalent to the usual formulation (Sambin) since from $a \lhd U$ and (PP2) follows that $U \cap P$ is non-void.

We leave as an easy exercise in classical logic to prove that (PP1) and (PP2) are equivalent to the condition that

$$a \lhd \emptyset \iff a \notin P.$$

The strength in the constructive formulation is that (PP1) says that an element of U can constructed, not only that U is not empty.

For any $a \in S$, we have $a \lhd \{a\}$ and thus by $a \lhd \{a\} \cap P$. Hence if α is a point, then for $a \in \alpha$, we have by (P3) some $b \in \{a\} \cap P$ with $b \in \alpha$. But this states that $a \in P$. Thus all approximations in a point are positive basic opens.

As a simple minded example we can consider a different way of presenting Example 8.1. Let $S = \mathbb{Q} \times \mathbb{Q}$. Define $\langle a, b\rangle \lhd U$ to be: for each rational x such that $a < x < b$ there exists $\langle c, d\rangle \in U$ with $c < x < d$. Note that $\langle 1, 0\rangle \in S$ and that (trivially) $\langle 1, 0\rangle \lhd \emptyset$! It is straightforward to check that $(S, \lhd)$ is a formal space. Then $P = \{\langle a, b\rangle \in S : a < b\}$ is a set of positive basic opens that satisfies (P4) and (P5). (Exercise: check these claims.)

How does ordinary topologies arise from formal spaces? Let $P = (P, \lhd)$ be a *weak* formal space. For each subset $U \subseteq P$ define

$$U^* = \{\alpha \in \mathrm{Pt}(P) : (\exists a \in U)\, a \in \alpha\}.$$

Theorem 8.12 *For a weak formal space $P = (P, \lhd)$ the sets $\tau = \{U^* : U \subseteq P\}$ constitutes a topology on* $\mathrm{Pt}(P)$.

[1] U non-void means that an element of U can be constructed. Classically, this is the same being non-empty.

Proof: We have $P^* = \mathrm{Pt}(P)$ since every point is non-void. It is easy to see that $\cup_{i\in I} U_i^* = (\cup_{i\in I} U_i)^*$, so τ is closed under arbitrary unions. To show that τ is closed under intersections we show that $U^* \cap V^* = (U\downarrow \cap V\downarrow)^*$: First suppose $\alpha \in U^* \cap V^*$. Thus $a \in \alpha \cap U$, $b \in \alpha \cap V$ for some a and b. Since α is a point (P2) yields $c \in \alpha$ with $c \lhd \{a\}$ and $c \lhd \{b\}$. Thus $c \in U\downarrow \cap V\downarrow$, so $\alpha \in (U\downarrow \cap V\downarrow)^*$. Conversely, let α be a point and assume $c \in \alpha \cap U\downarrow \cap V\downarrow$. Hence there are $a \in U$ and $b \in V$ such that $c \lhd \{a\}$ and $c \lhd \{b\}$. By (P3), and since $c \in \alpha$, we have $a \in \alpha$ and $b \in \alpha$. Thus $\alpha \in U^*$ and $\alpha \in V^*$. [X]

Example 8.13 Let X be a topological space, where $\mathcal{O}(X)$ is the set of open subsets of X. Define for $V \in \mathcal{O}(X)$ and $\mathcal{U} \subseteq \mathcal{O}(X)$ the relation

$$V \lhd \mathcal{U} \Longleftrightarrow_{\mathrm{def}} V \subseteq \bigcup \mathcal{U}.$$

It is readily checked that $(\mathcal{O}(X), \lhd)$ is a formal space. If $\mathcal{O}(X)$ is replaced by a toplogical base $\mathcal{B}$ on X ([MTD, Def. 5.1.3]), then $(\mathcal{B}, \lhd)$ is a more typical formal space. The crucial axiom is (L): Suppose $W \in \mathcal{B}$ and $\mathcal{U}, \mathcal{V} \subseteq \mathcal{V}$ and such that $W \subseteq \cup\mathcal{U}$ and $W \subseteq \cup\mathcal{V}$. Hence for $x \in W$ there exists $U \in \mathcal{U}$, with $x \in U$, and there exists $V \in \mathcal{V}$, with $x \in V$. Since $\mathcal{B}$ is a base there exists $Z \in \mathcal{B}$, with $Z \subseteq U \cap V$ and $x \in Z$. Now clearly $Z \lhd \{U\}$ and $Z \lhd \{V\}$, so $Z \in \mathcal{U}\downarrow \cap \mathcal{V}\downarrow$. Thus $W \lhd \mathcal{U}\downarrow \cap \mathcal{V}\downarrow$.

For the record, we give a (rather artificial) example of a weak formal space.

Example 8.14 Let (S, R) be a set with a binary relation $R \subseteq S \times S$. We regard this as a directed graph. Let $N(a) = \{b \in P : aRb\}$. Define inductively

$$\begin{aligned} a \lhd_0 U \quad &\Leftrightarrow \quad a \in U \\ a \lhd_{n+1U} \quad &\Leftrightarrow \quad a \lhd_n U \text{ or } (\forall b \in N(a))\, b \lhd_n U, \end{aligned}$$

and then let

$$a \lhd U \Longleftrightarrow (\exists n)\, a \lhd_n U.$$

Then $(S, \lhd)$ is a weak formal space, if $N(a)$ is finite for every $a \in S$. Transitivity is proved by induction on n:

$$a \lhd_n U, U \lhd V \Longrightarrow a \lhd V.$$

Consider $S = \{0, 1, 2\}$, and the relation $R = \{(0,1), (0,2), (1,1), (2,2)\}$. Then $0 \lhd \{0\}\downarrow = \{0\}$ and $0 \lhd \{1,2\}\downarrow = \{1,2\}$ but 0 is not covered by the empty set. This shows that the axiom (L) fails in this example.

8.1 Morphisms

A continuous function $f : X \to Y$ induces a frame morphism between open sets going in the opposite direction $f^{-1} : \mathcal{O}(Y) \to \mathcal{O}(X)$. Frame morphisms arise from yet more primitive notions called *approximable mappings* (though these are really relations). A motivating example is the relation

$$a\,R_{(f)}\,b \Longleftrightarrow f[a] \subseteq b \Longleftrightarrow a \subseteq f^{-1}(b) \tag{12}$$

where $a \in \mathcal{O}(X)$ and $b \in \mathcal{O}(Y)$.

For a relation $R \subseteq S \times T$ and $U \subseteq S$, let $U\,R\,b$ mean $(\forall u \in U)\,uRb$. The *inverse image of* V *under the relation* R is, as usual,

$$R^{-1}[V] =_{\mathrm{def}} \{a \in S : (\exists b \in V)\,a\,R\,b\}$$

Notice that $R^{-1}[U] \subseteq R^{-1}[V]$ whenever $U \subseteq V$, and

$$R^{-1}[\cup_{i\in I} U_i] = \cup_{i\in I} R^{-1}[U_i].$$

Definition 8.15 Let $(S, \lhd)$ and $(T, \lhd')$ be formal spaces. A relation $R \subseteq S \times T$ is an *approximable mapping* from $(S, \lhd)$ to $(T, \lhd')$ if

(A1) $a\,R\,b$, $b \lhd' V$ implies $a \lhd R^{-1}[V]$,

(A2) $a \lhd U$, $U\,R\,b$, implies $a\,R\,b$,

(A3) $S \lhd R^{-1}[T]$,

(A4) $a \lhd R^{-1}[U]$, $a \lhd R^{-1}[V]$ implies $a \lhd R^{-1}[(U\downarrow) \cap (V\downarrow)]$,

Remark 8.16 Note that an approximable mapping R satisfies

$$a\,R\,b, b \lhd \{b'\} \Longrightarrow a\,R\,b'.$$

The assumptions imply $a \lhd R^{-1}[\{b'\}]$ using (A1). Trivially, $U\,R\,b'$ for $U = R^{-1}[\{b'\}]$ so by (A2) we get $a\,R\,b'$. Note also that by $b \lhd' \{b\}$, (A1) and (A2)

$$a\,R\,b \Longleftrightarrow a \lhd R^{-1}[\{b\}]$$

Example 8.17 Let $f : X \to Y$ be a continuous function. Consider the open sets as formal spaces $(\mathcal{O}(X), \lhd)$ and $(\mathcal{O}(Y), \lhd)$ (cf. Example 8.13). Then $R = R_{(f)} \subseteq \mathcal{O}(X) \times \mathcal{O}(Y)$, as defined at the beginning of this section, is an approximable mapping. Note that for $V \subseteq \mathcal{O}(Y)$,

$$a \lhd R^{-1}[V] \Longleftrightarrow a \subseteq \bigcup\{f^{-1}(b) : b \in V\} = f^{-1}(\cup V). \tag{13}$$

(A1): From $b \lhd V$ follows $b \subseteq \cup V$. Thus $a\,R\,b$ implies $a \subseteq f^{-1}(b)$, and hence $a \subseteq f^{-1}(b) \subseteq f^{-1}(\cup V)$, i.e. $a \lhd R^{-1}[V]$.

(A2): Suppose $a \lhd U$ and $U\,R\,b$. Thus $f^{-1}(b) \supseteq c$ for all $c \in U$, and $\cup U \supseteq a$. It follows that $f^{-1}(b) \supseteq a$.

(A3): Clear by (13).

(A4): From $a \lhd R^{-1}[U]$ and $a \lhd R^{-1}[V]$ follows $a \subseteq f^{-1}(\cup U)$ and $a \subseteq f^{-1}(\cup V)$. Hence

$$\begin{aligned} a \subseteq f^{-1}(\cup U) \cap f^{-1}(\cup V) &= f^{-1}(\cup\{c \in \mathcal{O}(X) : c \subseteq b \cap b', b \in U, b' \in V\}) \\ &= f^{-1}(\bigcup((U\downarrow) \cap (V\downarrow))) \qquad [\mathtt{X}] \end{aligned}$$

We record some useful facts about approximable mappings.

Lemma 8.18 *Let $R \subseteq S \times T$ be an approximable mapping. Then:*

(a) $U \lhd V$ implies $R^{-1}[U] \lhd R^{-1}[V]$,

(b) $b \lhd R^{-1}[U]$ iff $b \lhd R^{-1}[\tilde{U}]$,

(c) $\widetilde{R^{-1}[U]} = \widetilde{R^{-1}[\tilde{U}]}$.

Proof: (a) Suppose $U \lhd V$ and $a \in R^{-1}[U]$. Thus aRb for some $b \in U$. Therefore $b \lhd V$ and by (A1) $a \lhd R^{-1}[V]$. But $a \in R^{-1}[U]$ was arbitrary, so $R^{-1}[U] \lhd R^{-1}[V]$.

(b) follows from (a) (use $\tilde{U} \lhd U$). (c) follows from (b). $[\mathtt{X}]$

Let **Ftop** be the following category of formal spaces and approximable mappings. For a formal space $(S, \lhd)$ we define an approximable mapping $I \subseteq S \times S$ (the identity) by

$$aIb \Longleftrightarrow a \lhd \{b\}.$$

For approximable mappings $R_1 \subseteq S_1 \times S_2$ and $R_2 \subseteq S_2 \times S_3$ between formal spaces, define the composition

$$a(R_2 \circ R_1)b \Longleftrightarrow a \lhd R_1^{-1}[R_2^{-1}[\{b\}]].$$

This is an approximable mapping $(R_2 \circ R_1) \subseteq S_1 \times S_3$. It is possible to check that this defines a category.

Theorem 8.19 *Let $R \subseteq S \times T$ be an approximable mapping between formal spaces S and T. Then $k = \mathrm{Pt}(R) : \mathrm{Pt}(S) \to \mathrm{Pt}(T)$ defined by*

$$k(\alpha) = \{b \in T : (\exists a \in \alpha)\, a\, R\, b\}$$

is a continuous function. In fact, Pt *defines a functor from the category of formal spaces to the category of topological spaces.*

Proof: Suppose that α is a point in S. We first verify the axioms (P1) – (P3) for $k(\alpha)$ being a point.

(P1): The point α has some element a. We have $S \lhd R[T]$, so $a \lhd R[T]$. By (P3) for α there is some $c \in R[T]$ such that $c \in \alpha$. But then $(\exists b \in T)\, c\, R\, b$ and thus $b \in k(\alpha)$.

(P2): Suppose $b, b' \in k(\alpha)$. Thus for some $a, a' \in \alpha$: $a\, R\, b$ and $a'\, R\, b'$. But since α is a point it contains some c such that $c \lhd \{a\}$ and $c \lhd \{a'\}$. Trivially $\{a\}\, R\, b$ and $\{a'\}\, R\, b'$, so by (A2): $c\, R\, b$ and $c\, R\, b'$. Thus $c \lhd R^{-1}[\{b\}]$ and $c \lhd R^{-1}[\{b'\}]$. By (A4) we get $c \lhd R^{-1}[\{b\}\downarrow \cap \{b'\}\downarrow]$. Now by (P3) for the point α there is $x \in R^{-1}[\{b\}\downarrow \cap \{b'\}\downarrow]$ such that $x \in \alpha$. Hence there is some d: $d \lhd \{b\}$, $d \lhd \{b'\}$, $x\, R\, d$. But this means also that $d \in k(\alpha)$.

(P3): Suppose $b \in k(\alpha)$ and $b \lhd V$. There is thus some $a \in \alpha$ with $a\, R\, b$, and thus by (A1), $b \lhd R^{-1}[U]$. Now since β is a point, there is $d \in R^{-1}[V] \cap \alpha$. From this follows that there is $c \in U$ with $d\, R\, c$, and thus also $c \in k(\alpha)$.

As for the continuity of k note that

$$\begin{aligned}
k^{-1}(V^*) &= \{\alpha \in \mathrm{Pt}(S) : k(\alpha) \in V^*\} \\
&= \{\alpha \in \mathrm{Pt}(S) : (\exists b \in V)(\exists a \in \alpha) a\, R\, b\} \\
&= \{\alpha \in \mathrm{Pt}(S) : \exists a \in \alpha \cap R^{-1}[V]\} \\
&= (R^{-1}[V])^*.
\end{aligned}$$

By Theorem 8.12, $\mathrm{Pt}(S)$ is a topological space for any formal space S. It remains to check the action of Pt on morphisms in **Ftop**, i.e. approximable mappings. It is readily seen that $\mathrm{Pt}(I)(\beta) = \beta$. By using Lemma 8.18 one proves the functoriality condition

$$\mathrm{Pt}(R_2 \circ R_1)(\beta) = \mathrm{Pt}(R_2)(\mathrm{Pt}(R_1)(\beta)). \qquad [\mathtt{X}]$$

Each approximable mapping determines a frame homomorphism, and conversely.

Theorem 8.20 *Let $S = (S, \lhd)$ and $T = (T, \lhd')$ be formal spaces. An approximable mapping $R \subseteq S \times T$ defines a frame homomorphism f_R : $\mathrm{Sat}(S) \to \mathrm{Sat}(T)$ by*

$$f_R(V) = \widetilde{R^{-1}[V]}.$$

Theorem 8.21 *Let $S = (S, \lhd)$ and $T = (T, \lhd')$ be formal spaces. A frame homomorphism $g : \mathrm{Sat}(T) \to \mathrm{Sat}(S)$ determines an approximable mapping $Q_g \subseteq S \times T$ by*

$$aQ_gb \Longleftrightarrow \widetilde{\{a\}} \subseteq g(\widetilde{\{b\}}).$$

Then also $f_{Q_g} = f$.

8.2 Covering compactness

The Cantor space is a well-known example of a compact space, i.e. a space where every covering of the space by open sets has a finite subcover. However regarding the Cantor space as metric space it is not possible to prove this property constructively. Formal spaces gives a way of saving covering compactness for constructivity as was shown by Martin-Löf (1970). The key is to generate the covers inductively.

Let $\Sigma = \{0,1\}$ and denote by Σ^* the set of finite strings over Σ. We consider this set of strings as partial specifications of elements in the Cantor space. Denote by uv the concatenation of strings u and v, and by $u \sqsubseteq w$ that $w = uv$ for some v (i.e. string extension). Define a cover relation $\lhd \subseteq \Sigma^* \times \mathcal{P}(\Sigma^*)$ by

$$u \lhd V \Longleftrightarrow (\exists n \in \mathbb{N})\, u \lhd_n V. \tag{14}$$

where we define inductively

$$\begin{aligned} u \lhd_0 U \quad &\Leftrightarrow \quad \text{for some } w \in U,\ w \sqsubseteq u \\ u \lhd_{n+1} U \quad &\Leftrightarrow \quad u \lhd_n U \text{ or both } u0 \lhd_n U \text{ and } u1 \lhd_n U. \end{aligned}$$

For instance $0 \lhd_2 U = \{00, 010, 011\}$, since we have the following "derivation tree"

$$\cfrac{\cfrac{00 \lhd_0 U}{00 \lhd_1 U} \qquad \cfrac{010 \lhd_0 U \qquad 011 \lhd_0 U}{01 \lhd_1 U}}{0 \lhd_2 U}$$

The following lemma is an easy consequence of the definitions:

Lemma 8.22 *(a) $w \lhd_n U$, $U \subseteq V$ implies $w \lhd_n V$*

(b) $w0 \lhd_m U$, $w1 \lhd_n U$ implies $w \lhd_{\max(m,n)+1} U$.

Lemma 8.23 *(Covering compactness) If $w \lhd U$, then $w \lhd U_0$ already for some finite $U_0 \subseteq U$.*

Proof: We show

$$w \lhd_n U \Longrightarrow (\exists \text{ finite } U_0 \subseteq U)\, w \lhd_n U_0$$

by induction on n. For $n = 0$, $w \lhd_0 U$ means that there is some $u \in U$ which is extended by w. Hence $w \lhd_0 \{u\} \subseteq U$, so we have found a finite subcover. Suppose that the statement is true for n and any w and U. Assume $w \lhd_{n+1} U$. Thus either $w \lhd_n U$, in which case we can apply the induction hypothesis directly, or $w0 \lhd_n U$ and $w1 \lhd_n U$. In the latter case the inductive hypothesis gives finite $U_0 \subseteq U$ and $U_1 \subseteq U$ such that $w0 \lhd_n U_0$ and $w1 \lhd_n U_1$. By Lemma 8.22.(a) we have $w0 \lhd_n U_0 \cup U_1$ and $w1 \lhd_n U_0 \cup U_1$. Thus by definition $w \lhd_{n+1} U_0 \cup U_1$ which completes the inductive step. [X]

Lemma 8.24 *If $w \lhd_n U$, then $wv \lhd_n U$ for any $v \in \Sigma^*$.*

Proof: We prove the statement by induction on n. For $n = 0$ it follows by definition of $\lhd_0$. Suppose the statement is true for n and all w, v and U. Assume $w \lhd_{n+1} U$. If $w \lhd_n U$ we can use the inductive hypothesis directly, otherwise $w0 \lhd_n U$ and $w1 \lhd_n U$. By inductive hypothesis, $w0v' \lhd_n U$ and $w1v' \lhd_n U$ for all $v' \in \Sigma^*$. But this is the same as $wv0 \lhd_n U$ and $wv1 \lhd_n U$ for all $v \in \Sigma^*$. Thus $wv \lhd_n U$ for all $v \in \Sigma^*$ and the induction step is finished. [X]

The next lemma follows from Lemma 8.22.(b).

Lemma 8.25 *$w0 \lhd U$, $w1 \lhd U$ implies $w \lhd U$.*

Lemma 8.26 *(a) $w \lhd_0 U$, $w \lhd_n V$ implies $w \lhd_n (U \downarrow) \cap (V \downarrow)$.*

(b) $w \lhd_m U$, $w \lhd_n V$ implies $w \lhd (U \downarrow) \cap (V \downarrow)$.

Proof: (a) follows easily by induction on n. The base case of (b) is (a). Suppose that the statement holds for m, and all n. Assume $w0 \lhd_n U$ and $w1 \lhd_m U$ and $w \lhd_n V$. The latter implies by Lemma 8.24 that $w0 \lhd_n V$ and $w1 \lhd_n V$. Thus by the inductive hypothesis, $w0 \lhd (U \downarrow) \cap (V \downarrow)$ and $w1 \lhd (U \downarrow) \cap (V \downarrow)$. Thus by Lemma 8.25, $w \lhd (U \downarrow) \cap (V \downarrow)$. [X]

Theorem 8.27 *$(\Sigma^*, \lhd)$ is a formal space.*

Proof: The axiom (R) follows since $a \lhd_0 U$ whenever $a \in U$. (L) is due to Lemma 8.26.(b). The transitivity follows by proving

$$w \lhd_m U, U \lhd V \Longrightarrow w \lhd V$$

by induction on m. Lemma 8.25 is used in the induction step. [X]

8.3 Generating formal spaces

In the previous section we saw an example where the cover relation is generated inductively. It is possible to generalise this method.

Let S be a set and suppose that $\lhd^{(i)}$ is a relation $\lhd^{(i)} \subseteq S \times \mathcal{P}(S)$ such that $(S, \lhd^{(i)})$ is a weak formal space. Then define

$$a \lhd U \iff (\forall i \in I)\, a \lhd^{(i)} U. \tag{15}$$

As subsets of $S \times \mathcal{P}(S)$ we have $\lhd = \cap_{i \in I} \lhd^{(i)}$. It is easily verified that $(S, \lhd)$ is a weak formal space. Now suppose that G is some relation $G \subseteq S \times \mathcal{P}(S)$ such that

(E) $a\, G\, U$ implies $a \lhd^{(i)} U$,

(SL) $a \lhd^{(i)} U$, $a \lhd^{(i)} V$ implies $a \lhd^{(i)} U_G \cap V_G$,

where $U_G = \{a \in S : (\exists b \in U)\, a\, G\, \{b\}\}$. It is easily checked that $\lhd$ satisfies (E) and (SL) as well. But $W_G \subseteq W\downarrow = \{a \in S : (\exists b \in W)\, a \lhd \{b\}\}$, so by (T),

$$a \lhd U, a \lhd V \Longrightarrow a \lhd U\downarrow \cap V\downarrow .$$

Thus $(S, \lhd)$ is a formal space whose cover relation extends G

$$a\, G\, U \Longrightarrow a \lhd U.$$

We summarize and extend this discussion to a theorem.

Theorem 8.28 *Let S be a set and let $G \subseteq S \times \mathcal{P}(S)$ be any relation. Then there exists a weak formal space $(S, \lhd_G)$ satisfying the axioms*

(E) $a\, G\, U$ implies $a \lhd_G U$,

(SL) $a \lhd_G U$, $a \lhd_G V$ implies $a \lhd U_G \cap V_G$.

*If $(S, \lhd)$ is any other weak formal space satisfying these axioms (we call it an G-*extending formal space*) , then $\lhd_G \subseteq \lhd$. Moreover $(S, \lhd_G)$ is a formal space satisfying*

$$a\, G\, U \Longrightarrow a \lhd_G U.$$

Proof: Let $\mathcal{C}$ be the set of relations $R \subseteq S \times \mathcal{P}(S)$ such that (S, R) is a weak formal space satisfying (E) and (SL) (with bRW in place of $b \lhd_G W$). By the above reasoning $\lhd_G = \cap\mathcal{C}$ is again a relation such that $(S, \lhd_G)$ is a formal space satifying these axioms, and by construction it is clearly the smallest such relation. [X]

Example 8.29 Let $\Sigma = \{0, 1\}$ and define generators

$$G = \{(wv, \{w\}), (w, \{w0, w1\}) : w, v \in \Sigma^*\}.$$

Let $\lhd_G$ be the smallest cover extending G as given by the theorem. It is easily seen by induction that $w \lhd_n U$ implies $w \lhd_G U$. Thus $\lhd \subseteq \lhd_G$. Note that $W_G \subseteq W\downarrow = \{w \in \Sigma^* : (\exists u \in W)\, w \lhd \{u\}\}$, where $\lhd$ is the cover relation introduced in (14). Clearly $u\, G\, U$ implies $u \lhd_1 U$, so $\lhd$ defines a covering relation satisfying (E) and (SL). Thus $\lhd_G \subseteq \lhd$, and consequently $\lhd_G = \lhd$.

Induction on covers. How is it possible to prove a property of covers $\lhd_G$ by induction?

Like this: suppose $P(a, U)$ is some property of basic opens a and covers U that we want to establish, i.e. we want to show

$$a \lhd_G U \Longrightarrow P(a, U).$$

Then it is by Theorem 8.28 sufficient to show that the relation $aRU \Leftrightarrow_{\text{def}} P(a, U)$ satisfies the axioms (R), (T), (E) and (SL). Then by the theorem $a \lhd_G U$ implies $P(a, U)$. We give an example below.

8.4 The constructive real line as a formal space

To present the (constructive) real numbers as a formal space, we define a new cover relation for the basic opens

$$P = \{\langle a, b\rangle \in \mathbb{Q} \times \mathbb{Q} : a < b\}.$$

Let $G \subseteq P \times \mathcal{P}(P)$ be the relation

$$\begin{aligned} G \;=\; & \Big\{(\langle p, q\rangle, \{\langle r, s\rangle : p < r < s < q\}) : \langle p, q\rangle \in P\Big\} \\ & \cup \Big\{(\langle p, q\rangle, \{\langle p', s\rangle, \langle r, q\rangle\} : \langle p', s\rangle, \langle r, q'\rangle, \langle p, q\rangle \in P, r < s, p' \le p, q \le q'\Big\} \end{aligned}$$

Let $\lhd_G$ be the smallest G-extending cover according to Theorem 8.28. Thus we have

$$\langle p, q\rangle \lhd_G \{\langle r, s\rangle : p < r < s < q\}$$

i.e. an open interval is covered by the set of its strict open subintervals. Next

$$\langle p, q\rangle \lhd_G \{\langle p', s\rangle, \langle r, q\rangle\}$$

where $p' \leq p$, $r < s$, and $q \leq q'$. Notice that,

$$\langle p, q\rangle G\{\langle r, s\rangle\} \iff r \leq p < q \leq s.$$

Hence U_G is the set of open intervals contained in some interval of U.

We have the following "correctness" lemma for the set of inductively generated covers.

Lemma 8.30 *For* $\langle p, q\rangle \lhd_G U$,

$$(\forall x \in \mathbb{Q})\,[p < x < q \Rightarrow (\exists\langle r, s\rangle \in U)\, r < x < s]. \tag{16}$$

Proof: We prove the lemma by "induction on $\lhd_G$". That is, we define the relation $R \subseteq P \times \mathcal{P}(P)$ to hold $\langle p, q\rangle RU$ iff (16) holds. Then we show that R is a G-generated cover, i.e. that the axioms (R), (T), (E) and (SL) hold. By Theorem 8.28, it follows that $\lhd_G \subseteq R$, i.e. that

$$\langle p, q\rangle \lhd_G U \Longrightarrow \langle p, q\rangle RU,$$

thus proving the lemma.

We proceed to the verification of the axioms.

(R) and (L) we already checked in Example 8.1.

(E): We have $\langle p, q\rangle G\{\langle r, s\rangle : p < r < s < q\} = U$. This follows since for $p < x < q$ we have by the density of rational numbers some r and s such that $p < r < x < s < q$. This shows that $\langle p, q\rangle RU$. We have also $\langle p, q\rangle G\{\langle p', s\rangle, \langle r, q\rangle\} = V$ where $p' \leq p$, $r < s$, and $q \leq q'$. If $p < x < q$, we have $x < s$ or $r < x$. Thus $\langle p, q\rangle RV$. This verifies (E).

(SL): Suppose $\langle p, q\rangle RU$, $\langle p, q\rangle RV$. Thus if $p < x < q$, there are $\langle r, s\rangle \in U$ and $\langle r', s'\rangle \in V$ with $r < x < s$ and $r' < x < s'$. Let $\langle r'', s''\rangle = \langle \max(r, r'), \min(s, s')\rangle$. This contains, as an interval, x and $\langle r'', s''\rangle \in U_G \cap V_G$. This verifies (SL) and concludes the proof. [X]

Theorem 8.31 *The points in* $\mathrm{Pt}(P, \lhd_G)$ *are the* $\alpha \subseteq P$ *such that for some real number* x *and all rational numbers* p, q*:*

$$\langle p, q\rangle \in \alpha \iff p < x < q. \tag{17}$$

Proof: First suppose that α is a point of $(P, \lhd_G)$. We show that (17) holds for some $x \in \mathbb{R}$. Let $\langle p_0, q_0\rangle \in \alpha$. From $\langle p_n, q_n\rangle$ we construct an interval $\langle p_{n+1}, q_{n+1}\rangle$ of two thirds as long: we have

$$\langle p_n, q_n\rangle \lhd_G \{\langle p_n, (p_n + 2q_n)/3\rangle, \langle (2p_n + q_n)/3, q_n\rangle\}.$$

By (P3) either of the intervals in the cover belong to α. We let $\langle p_{n+1}, q_{n+1}\rangle$ be that interval. We thus construct an increasing sequence (p_n) and a decreasing sequence (q_n) with $p_n < q_n$ and

$$q_n - p_n = (q_0 - p_0)\Big(\frac{2}{3}\Big)^n,$$

which is visibly converging to 0 as n grows. Let

$$x = \lim_{n\to\infty} p_n = \lim_{n\to\infty} q_n,$$

which is a real number. Thus if $p < x < q$, there are some n such that $p < p_n \le x \le q_n < q$. But then $\langle p_n, q_n\rangle \lhd_G \{\langle p, q\rangle\}$, so since $\langle p_n, q_n\rangle \in \alpha$, also $\langle p, q\rangle \in \alpha$ by (P3).

Conversely, assume $\langle r, s\rangle \in \alpha$. Then since this interval is covered by $\{\langle r', s'\rangle : r < r' < s' < s\}$ we get by (P3) some $\langle r', s'\rangle \in \alpha$ with $r < r' < s' < s$. Let $\delta = \min(|r' - r|, |s' - s|) > 0$. Now take n so large that $q_n - p_n \le \delta$. By (P2) there exists $\langle u, v\rangle \in \alpha$ such that $r' \le u < v \le s'$ and $p_n \le u < v \le q_n$. Thus

$$q_n \le p_n + \delta < v + \delta \le s' + \delta \le s$$

and

$$p_n \ge q_n - \delta > u - \delta \ge r' - \delta \ge r.$$

Since $p_n < x < q_n$, we thus get $r < x < s$.

Now suppose that $\alpha \subseteq P$ is given by (17). The axioms (P1) and (P2) are easily verified. To verify (P3) we first define the relation $\langle p, q\rangle R U$ to hold if, and only if,

$$\langle p, q\rangle \in \alpha \Longrightarrow (\exists \langle r, s\rangle \in U)\, \langle r, s\rangle \in \alpha.$$

This is a relation $R \subseteq P \times \mathcal{P}(P)$. We show that it satisfies the axioms (R), (T), (E) and (SL).

(R): If $\langle p, q\rangle \in U$, then trivially $\langle p, q\rangle R U$.

(T): Assume $\langle p, q\rangle R U$, and $(\forall \langle r, s\rangle \in U)\, \langle r, s\rangle R V$. Suppose $\langle p, q\rangle \in \alpha$. Then by the first assumption $\exists \langle r, s\rangle \in U$ with $\langle r, s\rangle \in \alpha$. By the second assumption there is $\langle r', s'\rangle \in \alpha \cap V$ which was to be shown.

(E): $\langle p, q\rangle R\{\langle r, s\rangle : p < r < s < q\}$ follows since if $p < x < q$, then there are rational numbers r, s such that $p < r < x < s < q$. To prove $\langle p, q\rangle R\{\langle p', s\rangle, \langle r, q'\rangle\}$ for $r < s$, $p' \le p$ and $p \le q'$, assume $p < x < q$. Then (even constructively):

$$r < x \text{ or } x < s.$$

Thus $p' < x < s$ or $r < x < q'$ verifying the axiom also for the second kind of generator.

(SL): From $\langle p, q\rangle RU$ and $\langle p, q\rangle RV$, and $p < x < q$ follows that there are $r < x < s$ and $r' < x < s'$. Let $r'' = \max(r, r')$ and $s'' = \min(s, s')$. Thus $r'' < x < s''$ and $\langle r'', s''\rangle \in U_G \cap V_G$.

By Theorem 8.28, $\lhd_G \subseteq R$ and thus if $\langle p, q\rangle \lhd_G U$, we have $\langle p, q\rangle RU$, so $\langle p, q\rangle \in \alpha$ implies that for some $\langle r, s\rangle \in U \cap \alpha$. We have just verified the condition (P3). [X]

8.5 Formal spaces and sites

In this section we clarify the relation of formal spaces to an earlier version of point-free topologies known as *sites* or *Grothendieck topologies.* (See Mac Lane and Moerdijk 1992 for background.)

Let $(Q, \leq)$ be a preorder, i.e. set with a reflexive and transitive relation. For a subset $X \subseteq Q$ define the downward closure of X:

$$X_{(\leq)} = \{a \in Q : (\exists x \in X) a \leq x\}.$$

Define the *formal intersection* of X and Y as

$$X \wedge Y = X_{(\leq)} \cap Y_{(\leq)}.$$

Definition 8.32 (Sigstam and Stoltenberg-Hansen) Let $Q = (Q, \leq)$ be a preorder. A *Q-based formal space* is Q together with a cover relation $\lhd$ satisfying

(R) $a \in U$ implies $a \lhd U$,

(T) $a \lhd U$, $U \lhd V$ implies $a \lhd V$,

(QL) $a \lhd U$, $a \lhd V$ implies $a \lhd U \wedge V$,

(QG) $a \leq b$ implies $a \lhd \{b\}$.

Remark 8.33 Suppose that G is a set of generators and that $\leq$ is a partial order such that

$$a\, G\, \{b\} \Longrightarrow a \leq b.$$

Extend G as follows

$$G' = G \cup \{(a, \{b\}) : a \leq b\}.$$

Let $\lhd$ be the minimal cover satisfying R, T, QL, QR and extending G. Let $\lhd'$ be the minimal cover satisfying R, T,GE, GL and extending G. Then it is easy to check that the minimality properties give $\lhd = \lhd'$.

Define $X \cdot a = X \wedge \{a\}$.
We leave the verification of the following as a straightforward exercise.

Proposition 8.34 *For a $(Q, \leq)$-based formal space $(Q, \lhd)$*

(a) $a \lhd U$ *iff* $a \lhd U_{(\leq)}$,

(b) $a \lhd U_{(\leq)}$ *iff* $a \lhd U \cdot a$,

(c) $a \lhd \{a\}_{(\leq)}$,

(d) $a \lhd U$ *and* $b \leq a$ *implies* $b \lhd U \cdot b$

(e) if $a \lhd U$, *and* $(\forall b \in U)\, b \lhd V \cdot b$, *then* $a \lhd V$. [X]

A subset $X \subseteq Q$ is a *sieve on a* if $x \leq a$ for all $x \in X$, and

$$y \in Q, x \in X, y \leq x \Longrightarrow y \in X.$$

Clearly $U \cdot a$ is a sieve on a for *any* $U \subseteq Q$. In particular, $\{a\}_{(\leq)}$ is a sieve. Note $X \subseteq Q$ is a sieve on a iff

$$X \cdot a = X.$$

It is also easy to see that an intersection of two sieves on a is again a sieve on a. Properties (c)-(e) of Proposition 8.34 indicate how the covering relation can be restricted sieves.

Definition 8.35 A *Grothendieck formal space* consists of a preorder $(Q, \leq)$ and a cover relation

$$\lhd \subseteq \{(a, U) : a \in Q, U \subseteq Q \text{ sieve on } a\}$$

that satisfies

(G1) $a \lhd \{a\}_{(\leq)}$,

(G2) $a \lhd U$ and $b \leq a$ implies $b \lhd U \cdot b$

(G3) if $a \lhd U$, and $(\forall b \in U)\, b \lhd V \cdot b$, then $a \lhd V$. [X]

Lemma 8.36 *For a Grothendieck formal space* $(Q, \leq, \lhd)$*, and sieves* U *and* V *on* a

(a) $a \lhd U$*,* $U \subseteq V$ *implies* $a \lhd V$*,*

(b) $a \lhd U$*,* $a \lhd V$ *implies* $a \lhd U \cap V$*.* [X]

For any Grothendieck formal space $(Q, \leq, \lhd)$ we define a $(Q, \leq)$-based formal space $(Q, \leq, \lhd^*)$ by

$$a \lhd^* X \iff_{\text{def}} a \lhd X \cdot a.$$

Proposition 8.37 $(Q, \leq, \lhd^*)$ *is a formal space.*

Remark 8.38 A Grothendieck topology is a further generalisation where the preorder is replaced by a category. (Recall that every preorder can be regarded as a category in a trivial way.) One may thus define topologies on categories, which has proved very useful in e.g. algebraic geometry.

References

P. Martin-Löf. *Notes on Constructive Mathematics.* Almkvist och Wiksell. Stockholm 1970.

P. Martin-Löf. *Formell (punktfri) topologi.* Notes in Swedish from the Stockholm-Uppsala logic seminar 1986.

G. Sambin. Intuitionistic formal spaces.
`URL: www.math.unipd.it/~sambin`

I. Sigstam, V. Stoltenberg-Hansen. Representability of locally compact regular spaces by domains and formal spaces. *Theoretical Computer Science* 179(1997), 319 – 331.

I. Sigstam. Formal spaces and their effective presentations. *Archive for Mathematical Logic* 34 (1995), 211 – 246.

S. Vickers. *Topology via Logic.* Cambridge University Press.

S. Negri. The continuum as a formal space. *Archive for Mathematical Logic* 38(1999), 423 – 447.

S. Mac Lane and I. Moerdijk. *Sheaves in Geometry and Logic.* Springer 1992.

T. Coquand, G. Sambin, J. Smith, S. Valentini. *Inductively generated formal topologies.*

G. Curi. Constructive metrisability in point-free topology.

9 Möbius inversion formula for partial orders

The Möbius inversion formula from number theory and the inclusion-exclusion principle from combinatorics has a common generalisation in terms of partial orders. Our presentation follows Hall (1967) and Rota (1964), with the small difference that we express the results in terms of (generalised) triangular matrices. For a comprehensive treatment of inversion formulas, see Aigner (1997).

Matrices will be real or complex (but in fact any field of characteristic 0 will do). Let T_n be the set of $n \times n$ upper triangular matrices $A = (a_{ij})$. This set is clearly closed under addition and multiplication. The familiar formula

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

gives the element on row i and column j of the product matrix $C = A \cdot B$. The identity matrix $I = (\delta_{ij})$ is the multiplicative unit. Here δ is the Kronecker delta function: $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$. There is a very simple condition for an upper triangular matrix to be invertible: all elements on the diagonal should be non-zero. The main lemma for the Möbius inversion formula is a generalisation of this simple fact.

Generalised matrices. From a set-theoretic point of view an $n \times n$ matrix $A = (a_{ij})$ may be considered as function $(i, j) \mapsto a_{ij}$ defined on the set $\{1, \ldots, n\} \times \{1, \ldots, n\}$. A generalised quadratic matrix A is therefore a function A defined on $P \times P$, where P is some arbitrary set. Such matrices can be added as usual. However the product of matrices may not be defined, since the sum

$$c_{ij} = \sum_{k \in P} a_{ik} b_{kj}$$

may diverge. To generalise the notion of triangular matrix, we shall assume that P is equipped with a partial order $\sqsubseteq$. A generalised matrix A is *upper triangular* if $a_{ij} = 0$ whenever $i \not\sqsubseteq j$. Let $T(P)$ denote the set of upper triangular matrices on $P = (P, \sqsubseteq)$. Clearly, T_n is the set of generalised triangular matrices on $\{1, \ldots, n\}$ with respect to the usual order $\leq$. For A and B in $T(P)$ the i, j element of the product $C = A \cdot B$ is

$$c_{ij} = \sum_{i \sqsubseteq k \sqsubseteq j} a_{ik} b_{kj} \qquad (1)$$

in case the sum is defined. (The sum is empty (=0) if $i \not\sqsubseteq j$.) This is the case when there are only finitely many elements k between i and j. We say P is *locally finite,* if the "interval"

$$[i, j] =_{\text{def}} \{k \in P : i \sqsubseteq k \sqsubseteq j\}$$

is finite for each pair $i, j \in P$. Thus for locally finite P, the set $T(P)$ is closed under multiplication. The identity element for multiplication is given by the Kronecker symbol $I = (\delta_{ij})$.

Lemma 9.1 *Let P be a locally finite partially ordered set. Let $A = (a_{ij}) \in T(P)$ be an upper triangular matrix with respect to P. Then $A = (a_{ij})$ has an inverse in $T(P)$, if and only if, all the elements a_{ii} of the diagonal are non-zero.*

Proof ($\Rightarrow$) Suppse that $I = A \cdot B$, where $B \in T(P)$. Let $i \in P$ be arbitrary. Thus by (1), and the antisymmetry of $\sqsubseteq$,

$$\delta_{ii} = a_{ii} b_{ii}.$$

Since $\delta_{ii} = 1$, we must have $a_{ii} \neq 0$.

($\Leftarrow$) Now suppose that all diagonal elements of the matrix A are non-zero. We define its right inverse B in $T(P)$. Let $j \in P$ be fixed. For $i \not\sqsubseteq j$, let $b_{ij} = 0$. Suppose $i \sqsubseteq j$. By the above we must set $b_{jj} = a_{jj}^{-1}$. For $i \sqsubset j$, the inverse B should by (1) satisfy

$$\sum_{i \sqsubseteq k \sqsubseteq j} a_{ik} b_{kj} = 0.$$

That is $b_{ij} = -a_{ii}^{-1} \sum_{i \sqsubset k \sqsubseteq j} a_{ik} b_{kj}$. Since P is locally finite, there are only finitely many k satisfying $i \sqsubset k \sqsubseteq j$. Suppose that b_{kj} has been defined for all those k. Then the above gives a formula for b_{ij}. [X]

Let $P = (P, \sqsubseteq)$ be a partial order. The *zeta-matrix* or *zeta-function* $Z = (\zeta_{ij})$ of P is the generalised matrix which is 1 above and on the diagonal and 0 elsewhere, i.e. $\zeta_{ij} = 1$ for $i \sqsubseteq j$ and $\zeta_{ij} = 0$ for $i \not\sqsubseteq j$. The inverse of this matrix, which exists by the above lemma, is the *Möbius function* or *Möbius matrix* of the partial order P. We denote it by $M = (\mu_{ij})$. Since it is both right and left inverse to Z we have by the above

$$\mu_{ii} = 1$$

and for $i < j$,

$$\mu_{ij} = -\sum_{i \sqsubset k \sqsubseteq j} \mu_{kj} = -\sum_{i \sqsubseteq k \sqsubset j} \mu_{ik}. \qquad (4)$$

These identities are very useful.

Example. For $P = \{1, 2, 3, 4\}$ partially ordered such that 1 is smallest, 4 is largest and 2 and 3 are unrelated, we have the following zeta and Möbius matrices

$$Z = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad M = Z^{-1} = \begin{pmatrix} 1 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Theorem 9.2 *Let $(P, \sqsubseteq)$ be a locally finite partial order with a smallest element, and let μ be its Möbius function. Let $(x_i)_{i \in P}$ be a family of numbers. Suppose that $(y_j)_{j \in P}$ is defined by*

$$y_j = \sum_{i \sqsubseteq j} x_i \qquad (2)$$

Then

$$x_i = \sum_{j \sqsubseteq i} y_j \mu_{ji} \qquad (3)$$

Proof Consider $x = (x_i)$ and $y = (y_j)$ as row vectors. Form the row vector $u = (u_j)$ by matrix product $u = x \cdot Z$. Since the partial order is locally finite and has least element,

$$u_j = \sum_i x_i z_{ij} = \sum_{i \sqsubseteq j} x_i.$$

Thus $y = u$, so $y = x \cdot Z$. By multiplying by $M = Z^{-1}$ on the right we get $y \cdot M = x \cdot Z \cdot M = x$. From this (3) follows. [X]

To find a useful expression for the Möbius function of a partial order may be non-trivial. Certain construction principles can be useful.

Example For the partial order $I = \{0, 1\}$ with $0 \sqsubset 1$, we have the Möbius matrix

$$M = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

Theorem 9.3 *If* $(P, \sqsubseteq)$ *and* $(Q, \sqsubseteq)$ *are partial orders with Möbius functions* (μ_{ij}) *and* $(\nu_{k\ell})$*, then the Möbius function of the product partial order* $P \times Q$ *is*

$$\theta_{(i,k),(j,\ell)} = \mu_{i,j}\nu_{k,\ell}$$

That is $T = (\theta_{(i,k),(j,\ell)})$ *is the Kronecker product of matrices* $M = (\mu_{i,j})$ *and* $N = (\nu_{k,\ell})$*.*

Proof. A quick proof uses the fact that the zeta-matrix of $P \times Q$ is the Kronecker product of the zeta-matrices for P and Q. Inverses can then be computed in each factor. [X]

Example: the inclusion-exclusion principle. Let S be a finite set and denote by $\mathcal{P}(S)$ the set of its subsets, partially ordered by inclusion $\subseteq$. We claim that the Möbius function for $(\mathcal{P}(S), \subseteq)$ is

$$\mu_{AB} = (-1)^{|B|-|A|} \qquad (A \subseteq B)$$

where $|X|$ is the cardinality of the set X. This is easily verified using that $(\mathcal{P}(S), \subseteq)$ is isomorphic to the partial order $I^{|S|}$ (cf example above) and Theorem 9.3.

Let K be a finite set of objects. Suppose that $P_1, \ldots, P_n$ are properties of these objects. They can be identified with subsets $P_i \subseteq K$. Let $S = \{1, \ldots, n\}$. For any subset $A \subseteq S$ let U_A be set of objects which $k \in K$ lacks exactly the properties P_i indexed by $i \in A$. That is,

$$U_A = \{k \in K : A = \{i \in S : k \notin P_i\}\}$$

Let

$$V_B = \cup_{A \subseteq B} U_A.$$

Thus $k \in V_B$ if and only if $\{i \in S : k \notin P_i\} \subseteq B$. Thus V_B consists of the objects which has all properties not in B. Let $x_A = |U_A|$ and $y_B = |V_B|$. Since $U_A \cap U_B = \emptyset$ for $A \neq B$, we have

$$y_B = \sum_{A \subseteq B} x_A.$$

By the Theorem 9.2 we get

$$x_A = \sum_{B \subseteq A} (-1)^{|A|-|B|} y_B.$$

For $A = S$, this is

$$x_S = \sum_{k=0}^{n}(-1)^{n-k} \sum_{|B|=k} y_B = \sum_{k=0}^{n}(-1)^k \sum_{|B|=n-k} y_B = \sum_{k=0}^{n}(-1)^k \sum_{|B|=k} y_{S\setminus B}.$$

To see that this is indeed the inclusion-exclusion principle, note that x_S is the number of objects which lacks all properties of S. Moreover $y_{S\setminus B}$ is the number of objects having all the properties of B.

Example The classical Möbius inversion formula is obtained by considering the set of positive integers partially ordered by the divisibility relation. The Möbius function is then $\mu_{ij} = \mu(j/i)$. For details see Hall 1967 or any book on number theory.

Euler characteristic. Let P be a finite partial order with smallest element 0 and a largest element 1. Its *Euler characteristic* E is defined as

$$E = 1 + \mu_{01}$$

where μ is the Möbius function for P. Using fact that $M = (\mu_{ij})$ is Z^{-1} we shall obtain a useful identity following Rota (1964). Subtract the identity matrix from the zeta-matrix and obtain the *incidence matrix* $N = Z - I$. Then by a standard matrix identity

$$M = Z^{-1} = (N + I)^{-1} = I - N + N^2 - N^3 + \cdots$$

Note that if $N^k = (n_{ij}^{(k)})$, then $n_{ij}^{(k)}$ is the number of chains in P of length k from i to j. Write $C_k = n_{01}^{(k)}$. By the above matrix identity we thus obtain

$$E = 1 - C_1 + C_2 - C_3 + \cdots$$

The Euler characteristic is involved in the proof of a sufficient condition for the fixed property of partial orders (see Theorems 1.1, 2.1 and 2.3 of Baclawski and Björner 1979).

Exercises

1. Verify using the formula (4) that the Möbius function for $\mathbb{N}$ with the usual order $\leq$ is $\mu_{ii} = 1$, $\mu_{i,i+1} = -1$ and is $= 0$ otherwise.

2. Find the Möbius function for the product partial order $\mathbb{N} \times \mathbb{N}$.

3. Find the Möbius functions for Khalimskys intervals.

4. In the proof of the inversion formula we did not assume that the matrices consisted of real numbers. Check that Theorem 9.2 is indeed valid for any commutative ring with 1, e.g. $\mathbb{Z}$ or polynomial rings over $\mathbb{Z}$.

Literature

Marshall Hall Jr. *Combinatorial Theory.* Blaisdell Publ. Co. 1967.

Gian-Carlo Rota. On the foundations of combinatorial theory, I. Theory of Möbius functions. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete,* 2(1964), 340 – 368.

M. Aigner. *Combinatorial Theory.* Springer 1997.

Kenneth Baclawski and Anders Björner. Fixed points in partially ordered sets. *Advances in Mathematics* 31(1979), 263 – 297.

10 Galois connections

Let $\mathcal{S}$ be the set of bounded, nonempty subsets of $\mathbb{R}$. Thus $\mathcal{S}$ contains sets such as $\{0,1,2\}$ and $(0,1) \cup (1,2)$ but not $(-1,\infty)$ or $\mathbb{N}$. For $X \in \mathcal{S}$ define

$$f(X) = \cap\{I \in \mathcal{I} : X \subseteq I\}$$

the smallest interval containing X. Being bounded is the same as being included in a finite interval, so f is a well-defined monotone function $f : \mathcal{S} \to \mathcal{I}$. Clearly, we have for $X \in \mathcal{S}$ and $I \in \mathcal{I}$:

$$X \subseteq I \iff f(X) \subseteq I.$$

Letting $g : \mathcal{I} \to \mathcal{S}$ be the inclusion function we can rephrase this equivalence as

$$g(I) \sqsubseteq X \iff I \sqsubseteq f(X).$$

Definition 10.1 Let P and Q be partially ordered sets. Let $f : P \to Q$ and $g : Q \to P$ be monotone functions. We then say that f and g are *Galois connected* iff for all $x \in P$ and $y \in Q$

$$g(y) \sqsubseteq x \iff y \sqsubseteq f(x).$$

We derive some important abstract properties of Galois connections.

Theorem 10.2 *Let $f : P \to Q$ and $g : Q \to P$ be Galois connected monotone functions. Then:*

(i) If the set $S \subseteq Q$ has a supremum $\sqcup S$ in Q, then $g(\sqcup S)$ is the supremum of the image set $g[S]$ in P. In particular, if Q has a least element $\bot$, then $g(\bot)$ is the least element of P.

(ii) If the set $T \subseteq P$ has a infimum $\sqcap T$ in P, then $f(\sqcap T)$ is the infimum of the image set $f[T]$ in Q. In particular, if P has a largest element $\top$, then $f(\top)$ is the least element of Q.

Proof. (i): By assumption and the monotonicity of g we have $g(\sqcup S) \sqsupseteq g(y)$ for each $y \in S$, so $g(\sqcup S)$ is an upper bound of $g[S]$. Suppose now that z is an upper bound of $g[S]$. Thus $g(y) \sqsubseteq z$ for each $y \in S$. By the Galois connection $y \sqsubseteq f(z)$ for each $y \in S$. Now $f(z)$ is an upper bound of S. Hence $\sqcup S \sqsubseteq f(z)$. By the Galois connection again, $g(\sqcup S) \sqsubseteq z$. Consequently $g(\sqcup S)$ is the least upper bound of $g[S]$.

(ii): Exercise (dual to the above proof). [X]

We see that if P and Q are directed complete in the theorem, then g is necessarily continuous.

The following theorem gives an alternative characterisation of Galois connections.

Theorem 10.3 *Let $f : P \to Q$ and $g : Q \to P$ be monotone functions. Then f and g are Galois connected iff the following two conditions hold*

(i) $y \sqsubseteq f(g(y))$ for each $y \in Q$.

(ii) $g(f(x)) \sqsubseteq x$ for each $x \in P$.

Proof. The Galois connection of f and g states that for all $y \in Q$ and $x \in P$

$$g(y) \sqsubseteq x \Longleftrightarrow y \sqsubseteq f(x).$$

Now substituting $g(y)$ for x we get (i) (using reflexivity), and substituting $f(x)$ for y we obtain (ii).

Conversely, suppose that f and g satisfy (i) and (ii). From $g(y) \sqsubseteq x$ follows $f(g(y)) \sqsubseteq f(x)$ by monotonicity of f. Then (i) yields $y \sqsubseteq f(x)$. For the opposite direction suppose $y \sqsubseteq f(x)$. Then by monotonicity of g, $g(y) \sqsubseteq g(f(x))$. Hence we get $g(y) \sqsubseteq x$ by applying (ii). [X]

Galois connected functions determine each other in the following manner:

Corollary 10.4 *Let $f, f' : P \to Q$ and $g, g' : Q \to P$ be monotone functions. Then:*

(i) if f and g are Galois connected, and f' and g are Galois connected, then $f = f'$.

(ii) if f and g are Galois connected, and f and g' are Galois connected, then $g = g'$.

Proof. (i): By Theorem 10.3 (ii) for f, g we have $g(f(x)) \sqsubseteq x$. By monotonicity of f' we get $f'(g(f(x)) \sqsubseteq f'(x)$. Now applying Theorem 10.3 (i) for f', g one obtains $f(x) \sqsubseteq f'(g(f(x)) \sqsubseteq f'(x)$. Interchanging the roles of f and f' one gets similarly $f'(x) \sqsubseteq f(x)$. Thus $f = f'$.

(ii): analogous proof. [X]

Corollary 10.5 *Let $f : P \to Q$ and $g : Q \to P$ be Galois connected monotone functions. Then:*

(i) $g(y) = g(f(g(y)))$ *for each* $y \in Q$.

(ii) $f(x) = f(g(f(x)))$ *for each* $x \in P$.

Proof. We have $y \sqsubseteq f(g(y))$. By monotonicity $g(y) \sqsubseteq g(f(g(y)))$. Also $g(f(g(y))) \sqsubseteq g(y)$ by Theorem 10.3. Thus the identity (i) is proved. The identity (ii) is proved by a dual argument. [X]

Abstract interpretation. Assume that the monotone functions $\alpha : C \to A$ and $\gamma : A \to C$ are Galois connected. The partial order A considered as a simplified, or abstract, version of C. α is then the *abstraction operation,* and γ is the *concretization operation.* These are related as $y \sqsubseteq \alpha(\gamma(y))$ and $\gamma(\alpha(x)) \sqsubseteq x$.

Let $h : C \to C$ be a monotone function. A monotone $h^a : A \to A$ is considered as a simplified version of h. Then

h^a is *locally correct* if $\gamma(h^a(\alpha(x))) \sqsubseteq h(x)$ for all $x \in C$,

h^a is *optimal* if $h^a(y) = \alpha(h(\gamma(y)))$ for all $y \in A$,

h^a is *complete* if $\alpha(h(x)) = h^a(\alpha(x))$ for $x \in X$.

Note that $k(y) =_{\text{def}} \alpha(h(\gamma(y))$ is locally correct and optimal.

Semantics of a recursive program is usually defined as the least fixed point of some continuous $h : C \to C$, i.e. as

$$\bigsqcup_{k \geq 0} h^k(\perp).$$

By the halting theorem the properties of the least fixed point are in general undecidable. It is therefore of great interest to find decidable approximations of the least fixed point. This is the aim of abstract interpretations of programs. Let $t = h^a : A \to A$ be a locally correct abstract version of h. Then one easily proves by induction that

$$h^k(x) \sqsupseteq \gamma(t^k(\alpha(x))).$$

Thus letting $x = \perp$

$$\text{lfp}(h) =_{\text{def}} \bigsqcup_{k \geq 0} h^k(\perp) \sqsupseteq \bigsqcup_{k \geq 0} \gamma(t^k(\alpha(\perp))) = \gamma(\bigsqcup_{k \geq 0} t^k(\alpha(\perp))).$$

By the Galois connection

$$\alpha(\mathrm{lfp}(h)) \sqsupseteq \bigsqcup_{k \geq 0} t^k(\alpha(\perp))$$

Often A is a finite partial order so in this case the right hand side terminates after finitely many steps, and has thus decidable properties.

Example Let C be the domain consisting of the elements

$$\{\perp, -(\perp), 0, +(\perp)\} \cup \mathbb{Z}$$

ordered as follows: $\perp$ is the least element, $+(\perp) \sqsubseteq n$ for positive integers n and $-(\perp) \sqsubseteq n$ for negative integers n. Let A be the subdomain of C consisting of the elements $\{\perp, -(\perp), 0, +(\perp)\}$. Let $\gamma : C \to A$ be the inclusion. Define $\alpha(x) = y$ where y largest element in C such that $y \sqsubseteq x$. Thus for instance $\alpha(0) = 0$, $\alpha(7) = +(\perp)$, $\alpha(\perp) = \perp$. It is easy to check that $\alpha(\gamma(x)) = x$ and $\gamma(\alpha(y)) \sqsubseteq y$. Thus α and γ are Galois connected.