POWER DOMAINS AND PREDICATE TRANSFORMERS: A TOPOLOGICAL VIEW

M.B. Smyth
Department of Computer Science
University of Edinburgh
Edinburgh, EH9 3JZ, Scotland

Abstract

The broad theme of the paper is that topological concepts are basic to computer science. Such concepts as "specifications", "predicate transformer", and "nondeterminism" can be greatly illuminated by being formulated in topological terms. The specific tasks we undertake are: to provide a more adequate framework for powerdomain constructions; and to show that the connection between (Dijkstra's) weakest preconditions and the Smyth powerdomain, established by Plotkin for the case of flat domains, actually holds in full generality.

The broad theme of this paper is that topological concepts are basic to computer science. The recognition of this relationship brings both conceptual and technical benefits. Such concepts as "specification", "predicate transformer", and "nondeterminism" can be greatly illuminated by being formulated in topological terms. The topological formulation enables a more adequate technical treatment to be given, by drawing on a well-established body of mathematical knowledge.

One main area of application is that of powerdomain theory. We show that the ideas of [15], [20] are in perfect harmony with topological treatments of multifunctions and spaces of subsets (or "hyperspaces") going back at least to Vietoris [22]. One obstacle to perceiving this has been that the mathematicians have, for the most part, been interested only in Hausdorff spaces. We propose (Definition 5) a finitary notion of "power space" which includes the existing (finitary) powerdomain and hyperspace constructs as special cases, and which is at the same time more direct and accessible (given a minimal acquaintance with topology) than the versions of [15], [20]. But, for reasons of space, we do not develop the power space theory here and, in particular, we consider the possibility of extending it to cover infinitary powerdomains (as in [1], [17]) only in passing. Instead, we consider Dijkstra's predicate transformers. Here, the topological interpretation is even more direct and compelling than in the case of the power domains. It immediately shows us how to generalize the weakest precondition semantics, and its connection with the upper (or Smyth) powerdomain (cf. Plotkin [16]), to arbitrary domains. (The treatment in [6] and [16] is, of course, restricted to flat, or discrete, domains.) The removal of the restriction to flat domains should permit the development of more adequate programming logics.

The key to the work of generalization presented here, as to much recent mathematical work that seeks to escape the limitations of the traditional insistence on Hausdorff

separation, is the use of sober spaces, frames, and related concepts ("pointless topology"). These, along with more standard topological material, are briefly introduced in Section 1.

1. Topology

A) Preliminaries. In this sub-section we recall some rudimentary topological notions which will be used repeatedly in the sequel.

A topology on a set S is a collection of subsets of S that is closed under finite intersection and arbitrary union. A set S together with a topology $\mathcal{T}$ on S is a topological space $(S,\mathcal{T})$; the elements of $\mathcal{T}$ are the open sets of the space. We also use the notation $\Omega(X)$ for the (complete) lattice of open sets of the space X.

A base of the topology $\mathcal{T}$ on S is a subset $\mathcal{B} \subseteq \mathcal{T}$ such that every open set is the union of elements of $\mathcal{B}$. A subbase of $\mathcal{T}$ is a subset $\mathcal{A} \subseteq \mathcal{T}$ such that every open set is the union of finite intersections of elements of $\mathcal{A}$. $\mathcal{T}$ is then the least topology such that $\mathcal{A} \subseteq \mathcal{P}$; any collection $\mathcal{A} \subseteq \mathcal{P}$ S may be taken as the subbase of a (unique) topology.

The topologies on a set S, ordered by inclusion, form a complete lattice: the lub $\bigvee T$, for T a set of topologies, is the topology with subbase $\bigcup T$. The least topology on S is the trivial topology $\{\emptyset,S\}$, while the greatest is $\mathcal{P}S$ (the discrete topology).

Notation. For a poset $(P,\leq)$, $x \in P$, $X \subseteq P$, we write

$\uparrow x$ for $\{y \mid x \leq y\}$

$\uparrow X$ for $\bigcup\{\uparrow x \mid x \in X\}$.

X is $\uparrow$-closed if $X = \uparrow X$. Similarly for $\downarrow x$, $\downarrow X$, $\downarrow$-closed.

Examples. (1) Euclidean space R^n, with base the open rational intervals. We are more interested in non-Hausdorff (indeed, non T_1) spaces, such as:

(2) Alexandroff topology of a poset, consisting of the $\uparrow$-closed sets; and especially

(3) Scott topology of a poset (usually a cpo) $(P,\leq)$. A set $O \subseteq P$ is open iff O is $\uparrow$-closed and, for any directed set $Y \subseteq P$, if $\bigvee Y \in O$ then some element of Y is in O. We are mainly interested in the case that P is an ω-algebraic cpo (there are countably many finite elements, and each element is the sup of a chain of finite elements). Here the Scott topology is very simply described: it has as base the sets $\uparrow a$, a finite.

For any topology $\mathcal{T}$ on S, we have the specialization preorder $\leq_{\mathcal{T}}$ on S, defined by:

$x \leq_{\mathcal{T}} y \equiv_{df} \forall O \in \mathcal{T}.\, x \in O \Rightarrow y \in O$.

If $\mathcal{T},\mathcal{T}'$ are topologies on S, then $\leq_{\mathcal{T} \vee \mathcal{T}'} = \leq_{\mathcal{T}} \cap \leq_{\mathcal{T}'}$.

A subset Q of a space X is compact provided that any family of open sets whose union contains X (so that the family covers X) has a finite subfamily which covers X. (In Bourbaki, Q is allowed to be only quasi-compact under these circumstances, unless X is Hausdorff; but this convention seems unnecessary.)

If X,Y are (topological) spaces, a map f: X -> Y is continuous if the inverse $f^{-1}(O)$ of each set O open in Y is open in X (equivalently, if the inverse of each closed set is closed).

Fact. If D,D' are cpo's, then f: D -> D' is continuous w.r.t. the Scott topologies of D,D' iff f preserves lubs of directed sets.

Miscellaneous notation. We use B_D for the basis (set of finite elements) of an algebraic cpo D; $\mathcal{P}_{fin}(S)$ for the collection of finite subsets of S; Top for the category of topological spaces with continuous functions as morphisms.

B) Computational significance of topological ideas. We think of a topological space as a "data type", with the open sets as the (computable) properties defined on the type. Taking a predicate on a space X to be a continuous map from X into the Boolean cpo B = ff, tt, $\perp$, we have (trivially) that a subset S of X is open iff S is $p^{-1}(tt)$ for some predicate p. (To make more of a theorem out of this: there is an order-isomorphism between $\Omega(X)$ and $[X \to \mathbb{O}]$, where $\mathbb{O}$ is the two-point cpo.)

Another reasonable notion of computable property would be that in which P is considered computable iff the set of (codes, or indices) of (computable) elements satisfying P can be effectively enumerated (so that P is a completely r.e. class, cf. Rogers [19]). The theorem of Rice et al (Rogers p.76) shows, in effect, that in the case of the domain $\mathcal{P}\omega$, the two notions of computable property are equivalent. A generalization of the Rice theorem (Plotkin [18], Sec. 7, p.9) shows that the equivalence holds in any "effectively given" algebraic cpo.

Intuitively, the idea of a computable property is simply this: we have a uniform procedure that, given (a code for) an element x, tells us within a finite time that P(x) holds, whenever that is true. Of course, this is just the idea of semi-decidability.

An idea that will surface from time to time, although we are not going to develop it in detail here, is that a specification of an object (say, a program) is a (finite or countable) list of properties that the object is to satisfy. In view of our identification of properties with open sets, this means that what is specified is always a countable intersection of open sets, in other words a $\mathcal{G}_\delta$-set (see Kuratowski [13]).

The notion of a compact set is a little harder to motivate: but it will have the significance for us of a "finitarily specifiable" set or, alternatively, of a set of results attainable by a boundedly non-deterministic process (we will elaborate on these points in Sec. 2).

Computability/continuity. We are not going to stress "effectiveness" in this paper. But one requirement (for a computationally reasonable space) which we make use of is that there should be a countable base of open sets. Computability concepts will, in

general, be relative not just to the topologies of the spaces involved, but to the particular open bases chosen. It is not strictly correct that arbitrary open sets represent computable properties; the computable properties will, rather, be the basic open sets and "effective" unions of them.

We can now give a simple reason why computable functions should be expected to be continuous. Let f: X -> Y be computable, where X,Y are "effective" spaces (so that, among other things, particular bases are assumed for X,Y). Let B be a basic, hence computable, property (open set) in Y. Thus B is $p^{-1}(tt)$ for some computable p: Y -> $\mathbb{O}$. Then $f^{-1}(B)$ is $(p \cdot f)^{-1}(tt)$, hence (assuming that computable functions compose) a computable property, therefore an open set, in X. So f^{-1} takes basic open sets, hence arbitrary open sets, of Y to open sets of X.

C) Points vs. properties. Pointless topology.

(i) T_0-spaces. If we really think of the (basic) open sets of a space as the fundamental properties of interest in that space, then, presumably points having the same neighbourhoods should not be distinguished. We thus require spaces to have the "T_0 separation property":

Definition 1. A space X is T_0 provided

$\forall x,y \in X\ ((\forall O \in \Omega(X).\ x \overline{\in} O \equiv y \in O) \rightarrow x = y)$.

Equivalently, X is T_0 provided that its specialization preorder is a partial order. Note that for any space X we have the T_0-ification of X, got by identifying points having the same neighbourhood systems. Alternatively - the procedure we shall adopt in Section 2 - one forms the T_0-ification by selecting a distinguished element from each equivalence class in the specialization preorder.

(ii) Sober spaces. A more radical position would be that, since we can be concerned only with the (ascertainable/computable) properties of points, points should be treated as logical constructions out of properties. Points, in this approach, will be mere "bundles of properties". But which bundles are appropriate?

If X is a space with topology $\mathcal{T}$, and $x \in X$, let us write $\mathcal{T}(x)$ for $\{O \in \mathcal{T} \mid x \in O\}$ (more generally, if $\mathcal{B}$ is any base for the topology, we may write $\mathcal{B}(x)$ for the set of basic open neighbourhoods of x). Any subset $\mathcal{F}$ of $\mathcal{T}$ such that $\mathcal{F} = \mathcal{T}(x)$ for some x satisfies the three conditions:

(1) if $U \in \mathcal{F}$, $V \in \mathcal{T}$ and $U \subseteq V$, then $V \in \mathcal{F}$;

(2) if $U,V \in \mathcal{F}$ then $U \cap V \in \mathcal{F}$;

(3) for any family $(U_i)_{i \in I}$ of open sets, if $\bigcup_i U_i \in \mathcal{F}$ then $U_i \in \mathcal{F}$ for some i.

A subset $\mathcal{F}$ of $\mathcal{T}$ satisfying (1) and (2) is a filter in $\mathcal{T}$. A filter satisfying (3) is said to be completely prime; the intuitive meaning of (3) is that a point which possesses the disjunction of the properties U_i, possesses at least one of these properties. Clearly, the notion of a completely prime filter can be formulated for $\mathcal{T}$ an arbitrary complete lattice.

Now, as one may readily check, the statement that a space X is T_0 is equivalent to :

for any completely prime filter in $\Omega(X)$, there is at most one point x such that $\mathcal{F} = \Omega(X)(x)$. Informally: a space is T_0 iff there is at most one point with a given bundle of properties. A sober space is one in which there is a perfect correspondence between points and bundles of properties. That is:

Definition 2. The space X is sober provided, for every completely prime filter $\mathcal{F}$ in $\Omega(X)$, there is exactly one point x such that $\mathcal{F} = \Omega(X)(x)$.

Loosely, we may say that a space is sober iff it is completely determined by its lattice of properties. For sober spaces X,Y, if $\Omega(X)$, $\Omega(Y)$ are isomorphic lattices, then X,Y are homeomorphic spaces.

For any space X we have its soberification (least sober extension), Sobr(X), which we may take as the set of all completely prime filters in $\Omega(X)$ (instead of just those which happen to correspond to points in X), with base for the topology the sets $\Phi_O = \{\mathcal{F} | O \in \mathcal{F}\}$, where O ranges over $\Omega(X)$.

We note in passing that, for a more "effective" treatment of the definitions and constructions considered here, one can work with an arbitrarily chosen countable base $\mathcal{B}$ in place of $\mathcal{J}(=\Omega(X))$.

Examples (1) Every Hausdorff space is sober.

(2) Every algebraic cpo (indeed, continuous poset) is sober. In detail, for D algebraic: if $\mathcal{F}$ is a completely prime filter in $\Omega(D)$, then $O \in \mathcal{F}$ iff $\uparrow a \in \mathcal{F}$ for some $a \in O$, by the third condition. In consequence, the completely prime filters may be identified with the filters of basic opens $\uparrow a$. These filters in turn are in (order-preserving) bijection with the ideals in B_D, and hence with the points of D. One observes here that completion by ideals may be considered as a special case of soberification. That is: for any poset B, the Scott topology on the completion of B coincides with the soberification of the Alexandroff topology on B.

It is interesting that not every cpo is sober in its Scott topology (Johnstone [10]). On the other hand, every sober space is directedly complete in its specialization order.

Several alternative characterizations of the sober spaces are discussed in works such as [3], [7]. The most adequate is in terms of an adjunction between $\underline{\underline{\mathrm{Top}}}$ and a suitable category of lattices - namely, $\underline{\underline{\mathrm{Frm}}}$, the category of frames (= complete Heyting algebras) and maps which preserve finite meets and arbitrary joins. The left half of the adjunction is in effect Ω, the right half is a functor Pt which acts on objects by sending a frame to its space of completely prime filters. A space is sober iff it is Pt(L) for some frame L; there is a corresponding notion of spatial frames, namely those which are values of Ω. The adjunction cuts down to an equivalence (or rather, a duality, since the morphisms in $\underline{\underline{\mathrm{Top}}}$ and $\underline{\underline{\mathrm{Frm}}}$ are in "opposite" directions) between the sober spaces and the spatial frames. Recent work has shown that there may be significant advantages, not least with respect to constructivity,

in avoiding commitment to "points" by working with $\underline{\underline{\mathrm{Frm}}}$ rather than $\underline{\underline{\mathrm{Top}}}$ (a striking example is Johnstone [11]). This viewpoint informs much of what we are doing in this paper; it is not made more explicit, so as to spare the introduction of too much unfamiliar machinery.

Example. What frames are of the form $\Omega(D)$ for D an algebraic cpo? The open sets of D are in bijection with the $\uparrow$-closed subsets of B_D. Now B_D can be any poset, for suitable choice of D (namely the completion of B_D). Thus, adapting the Representation Theorem 4.1.12 of [23] (for elementary event structures) we find that the frames in question are the prime algebraic complete lattices.

2. Power domains and Vietoris topology

In the study of the semantics of nondeterminism one strangely neglected avenue of approach is that of seeing what mathematicians have had to say about continuity notions for many-valued functions, and about spaces of subsets. On investigation, one finds much of relevance there; the power domains, in particular, are closely related to ideas expounded as long ago as 1921 (Vietoris [22], cf. Kuratowski [13]).

For inverses of many-valued (or multi-) functions, we adopt the notation of Berge [2]: if Γ: X -> Y is a multifunction, then $\Gamma^+(S)$ is $\{x \mid \Gamma x \subseteq S\}$ for $S \subseteq Y$, while $\Gamma^-(S)$ is the relational inverse $\{x \mid \Gamma x \cap S \neq \emptyset\}$.

Definition 3. A multifunction Γ: X -> Y is upper semicontinuous (usc) if $\Gamma^+(O)$ is open in X whenever O is open in Y; and lower semicontinuous (lsc) if $\Gamma^-(O)$ is open in X whenever O is open in Y (equivalently, if $\Gamma^+(Q)$ is closed whenever Q is closed). Finally, Γ is continuous if it is both usc and lsc.

Example. The fair merge function FM: $\Sigma^\infty \times \Sigma^\infty$ -> Σ^∞ is lsc but not usc. Say Σ is {0,1}. Taking S as $\uparrow\{01,10\}$, we find that $\langle 0,1\rangle \in FM^+(S)$, but $\langle 00,1\rangle \notin FM^+(S)$; thus $FM^+(S)$ is not open, so FM is not usc. On the other hand, if S is an arbitrary open set $\uparrow B$, where B is a set of finite sequences, then $FM^-(S) = \{\langle x,x'\rangle \mid \exists$ finite initial segments a,a' of x,x' $\wedge \exists b \in B$ such that some merge of a,a' extends b}, and this is clearly open.

Given a notion of continuity for multifunctions Γ: X -> Y, it is natural to ask whether there is a reasonable topology on Y such that Γ is continuous as a multifunction iff it is continuous in the ordinary sense as a function from X to $\mathcal{P}Y$. In the case of the three continuities of Definition, there are indeed easily defined topologies on $\mathcal{P}Y$ which agree in this sense.

We will arrive at these topologies by considering some notions of "properties of subsets" which readily suggest themselves. Given a notion of "property", i.e. a topology, over X we have, then, two obvious derived notions of property over subsets S of X: every element of S has a given property P; or, some element of S has P. Combinations of these are also possible.

Formally:

Definition 4. Given a space X and a subset $\mathcal{S}$ of $\mathcal{P}X$, the upper topology on $\mathcal{S}$ has as a base the collection of sets of the form U_O (O open in X), where $U_O = \{S \mid S \subseteq O\}$; the lower topology has as subbase the L_O, where $L_O = \{S \mid S \cap O \neq \emptyset\}$; while the Vietoris (or convex) topology takes as subbase both the L_O and the U_O.
(The name convex is non-standard; finite is more usual.)

Remark. The Vietoris topology is the (least) common refinement, that is, the lub (in the lattice of topologies), of the upper and lower topologies. The glb of the upper and lower topologies is trivial, in general.

Our definition of the three topologies is more general than those usually given (e.g. [13]) in that we have parameterized on $\mathcal{S}$ (usually a particular collection $\subseteq$ X is fixed); and we give no priority to T_1-spaces.

Why do we not simply take $\mathcal{S}$ to be $\mathcal{P}X$? One reason for restricting the class of sets is to ensure that the resulting space is T_0; we ensure this by picking distinguished elements from the equivalence classes. It is easy to see, for example, that two sets are equivalent with respect to the upper topology iff they have the same $\uparrow$-closure (in the specialization order); it is therefore reasonable to restrict to $\uparrow$-closed sets when considering the upper topology. Similar remarks apply to the other two topologies (details in Theorem 2).

A further restriction (in the case of the upper and convex topologies) arises from the desire to capture the idea of bounded non-determinism. A boundedly non-deterministic process can, we suppose, be represented as a finitely branching tree T such that the possible results of the computation form the "frontier" of T (limits along paths of T). A little more precisely, we suppose that with each point of T is associated a set R(p) of "potential" results, and that the sets occurring along any path from a decreasing sequence having a unique limit point. (The generating trees of [20] are a special case of this. The "set of potential results" associated with a point of one of those trees, labelled with finite element a, is of course $\uparrow$a.) We claim that the frontier F of such a tree T is compact. Indeed, suppose $F \subseteq \bigcup_{\iota \in I} O_\iota$. The set $\{p \in T \mid \exists \iota . R(p) \subseteq O_\iota\}$ must be finite; for if not, König's lemma implies that there is an infinite path $p_0, p_1, \ldots$, such that for all j, ι, $R(p) \not\subseteq O$, which implies that $\lim_j p_j \notin O$ (for all ι). It follows that there is a (finite) cross-section of T for which each associated set is contained in a single O_ι; thus a finite collection of the O_ι suffices to cover this cross-section and hence F. (The justification of the restriction to compact sets is taken up again at the end of this section.)

If Γ: X -> Y is a multifunction, we denote by $\hat{\Gamma}$: X -> $\mathcal{P}$Y the corresponding function.
Theorem 1. Let Y be a space, $\mathcal{S}$ a (non-empty) subset of $\mathcal{P}$Y. Then, for any space X, a multifunction Γ: X -> Y with (multi)values in $\mathcal{S}$ is usc iff $\hat{\Gamma}$: X -> $\mathcal{S}$ is continuous w.r.t. the upper topology on $\mathcal{S}$; similarly for lower semi-continuity w.r.t. the lower topology, and for continuity w.r.t. the convex topology. Moreover, the three

topologies on $\mathcal{S}$ are uniquely determined by the requirement that they agree with the continuity notions for multifunctions, in this sense.

Proof The (sub-)bases of the three topologies on $\mathcal{S}$ are so chosen as to make the first statement of the Theorem trivial (notice that a function is continuous if the inverse image of each subbasic open set is open). For uniqueness, notice that distinct topologies $\mathcal{Y}$, $\mathcal{Y}'$ on a set Z cannot yield the same set of continuous functions with Z as codomain: the identity functions between $(Z,\mathcal{Y})$ and $(Z,\mathcal{Y}')$ cannot both be continuous. □

We now introduce our definition of the three "power spaces" of a (sober) space.

Notation. Let X be a space. For $S \subseteq X$, $\bar{S}$ denotes the closure of S, while conv(S) is $\bar{S} \cap \uparrow S$. Also, CL(X), UC(X) and COMP(X) are the sets of closed, $\uparrow$-closed and compact sets of X respectively; CONV(X) is the set of fixed points of conv. We use $\leq_L$ for the specialization order derived from the lower topology; similarly for $\leq_C$, $\equiv_L$, etc.

Definition 5. The lower power space of X, $PS_L(X)$, is CL(X) taken with the lower topology; the upper power space, $PS_U(X)$, is COMP(X) $\cap$ UC(X) with the upper topology; and the convex power space, $PS_C(X)$ is COMP(X) $\cap$ CONV(X) with the convex topology.

Theorem 2. $PS_L(X)$, $PS_U(X)$ and $PS_C(X)$ are the T_0-ifications of X, COMP(X) and COMP(X) taken with the lower, upper and convex topologies, respectively.

Proof PS_L: Clearly, it suffices to show that $S \equiv_L S'$ (in the lower topology) iff $\bar{S} \equiv_L \bar{S'}$. But, by definition, a point x is in $\bar{S}$ iff every open set containing x meets S. It follows at once that $\bar{S}$ is the largest set equivalent to S and that $S \equiv_L S'$ iff $\bar{S} \equiv_L \bar{S'}$.

PS_U: Evidently, an open set O contains a set S iff $\uparrow S \subseteq O$. Hence $S \equiv_U \uparrow S$, and if S is compact then so is $\uparrow S$. Moreover, $\uparrow S$ is the largest set equivalent to S: since if $x \notin \uparrow S$ then for each $y \in S$ there is an open neighbourhood O_y of y such that $x \notin O_y$, so that, putting $U = \bigcup_{y \in \uparrow S} O_y$, we have $S \subseteq U$ while $x \notin U$. The conclusion follows as before.

PS_C: Since $S \subseteq \text{conv}(S) \subseteq \bar{S}$, $S \equiv_L \text{conv}(S)$; similarly, $S \equiv_U \text{conv}(S)$. Hence, $S \equiv_C \text{conv}(S)$ An easy calculation shows that conv(conv(S)) = conv(S). Further, if $Y \equiv_C S$ then $Y \subseteq \bar{S}$ (since $Y \equiv_L S$) and $Y \subseteq \uparrow S$ (since $Y \equiv_U S$); hence $Y \subseteq \text{conv}(S)$. Finally, if S is compact then conv(S), as the intersection of a closed set with a compact set, is also compact. We have thus shown that the elements of $PS_C(X)$ are the canonical (largest) elements of the $\equiv_C$-equivalence classes in (COMP(X),C). □

The "hyperspace" most usually studied is CL(X) with the Vietoris topology. We have restricted to compact sets as we are interested in modelling bounded non-determinism (but see remarks at end of this section). The standard treatment is, in effect, restricted to T_1-spaces (see [14]). Now, if X is T_1, all sets are $\uparrow$-closed, CONV(X) = CL(X) and, modulo the restriction to compactness, our theory is equivalent to the usual one. But it seems clear that to have a good theory applicable to non-T_1-spaces one needs to work with convex and not just closed sets (this is one of the main contributions of Plotkin [15]).

It has been proposed by de Bakker and Zucker [4] to use, as a power space construct, the Hausdorff metric on the closed subsets of a metric space X. Now it is not difficult to show that, for the compact (and therefore closed) subsets of X, the Hausdorff metric topology coincides with the Vietoris topology. It is true that they do not coincide in the non-compact case, and that de Bakker and Zucker allow arbitrary closed sets. However, there is a question as to which is the best topology to use in the non-compact situation; Michael [14] argues that the Hausdorff metric topology is mathematically less satisfactory than the Vietoris topology.

We will next show that, in case D is an algebraic cpo, the power spaces reduce to the usual power domains over D. Following [20], we shall define the power domains of D as completions of M(D) under suitable orderings, where M(D) is the set of non-empty finite subsets of B_D. For completeness we treat, along with the upper, or Smyth, powerdomain [20], its dual, sometimes known as the Hoare power domain.

Definition 6. Let D be an ω-algebraic cpo. Define the pre-orders $\sqsubseteq_L, \sqsubseteq_U, \sqsubseteq_C$ on M(D) by:

$A \sqsubseteq_L B$ iff $\forall a \in A.\exists b \in B.a \sqsubseteq b$

$A \sqsubseteq_U B$ iff $\forall b \in B.\exists a \in A.a \sqsubseteq b$

$A \sqsubseteq_C B$ iff $A \sqsubseteq_L B \wedge A \sqsubseteq_U B$.

Then the lower (or Hoare), upper (or Smyth), and convex (or Plotkin) power domains of D, denoted $PD_L(D)$, $PD_U(D)$, $PD_C(D)$, are the completions by ideals of M(D), under the respective orderings $\sqsubseteq_L, \sqsubseteq_U, \sqsubseteq_C$.

Actually we find it convenient, most of the time, to work with (equivalence classes of) ω-chains rather than directed ideals. If $(E, \sqsubseteq)$ is a preorder then $(\omega CH(E), \sqsubseteq_L)$, where ωCH(E) is the set of ω-chains of E, is a preorder equivalent to the completion $\bar{E}$ of E. To show that $\bar{E}$ is isomorphic to a cpo D it suffices to show that there is a (pre-) order-preserving and -reflecting surjection of $(\omega CH(E), \sqsubseteq_L)$ onto D. We write [X] for the ideal generated by an ω-chain X. We usually omit the subscript L for the preorder on chains.

Lemma 1. Let D be ω-algebraic, $S \subseteq D$ compact and non-empty. Then the set $U_S = \{A \in M(D) \mid A \sqsubseteq_U S\}$ is $\sqsubseteq_U$-directed; and $C_S = \{A \in M(D) \mid A \sqsubseteq_C S\}$ is $\sqsubseteq_C$-directed. Moreover $\bigcap\{\uparrow A \mid A \in U_S\} = \bigcap\{\uparrow A \mid A \in C_S\} = \uparrow S$.

Proof If O is an open superset of S, we can find an element K_0 of M(D) such that $K_0 \subseteq O$ and $K_0 \sqsubseteq_C S$. For, since S is compact, $\exists A \in M(D).\ A \subseteq O \wedge S \subseteq \uparrow A$; then choose K_0 to be a minimal such A. The last assertion of the lemma follows at once, since $\uparrow S = \bigcap_{S \subseteq O} O$. It also follows that U_S is $\sqsubseteq_U$-directed, since if $A, B \sqsubseteq_U S$ we have $A, B \sqsubseteq_U K_{\uparrow A \cap \uparrow B} \sqsubseteq_U S$.

Finally, suppose $A, B \sqsubseteq_C S$. Write K for $K_{\uparrow A \cap \uparrow B}$. For each $a \in A$ such that $\exists c \in K.a \sqsubseteq c$, augment K by adding to it an element A' chosen as follows. Find $x \in S$ such that $a \sqsubseteq x$. Find $b \in B$ such that $b \sqsubseteq x$. Then choose a' such that $a, b \sqsubseteq a' \sqsubseteq x$. Also, for each $b \in B$ such that $\exists c \in K.b \sqsubseteq c$, augment K by a similarly chosen b'.

Let K' be the result of all these augmentations of K. Then $A,B \sqsubseteq_C K' \sqsubseteq_C S$. □

In defining the power domains, the empty set is usually excluded from consideration. For the comparison of power spaces with power domains we therefore define $PS_L^+(X)$ to be the subspace of the non-empty elements of $PS_L(X)$, and similarly for $PS_U^+(X)$, $PS_C^+(X)$.

Theorem 3. Let D be an ω-algebraic cpo, taken with its Scott topology. Then $PS_L^+(D)$, $PS_U^+(D)$ and $PS_C^+(D)$ are isomorphic, in their specialization orders, with $PD_L(D)$, $PD_U(D)$ and $PD_C(D)$ respectively.

Proof (i) $PD_L(D)$: if I is a (directed) ideal in $(M(D), \sqsubseteq_L)$, let $L(I) = \{a \mid \{a\} \in I\}$. Then L(I) is a $\downarrow$-closed subset of B_D, and indeed L is an isomorphism of $PS_L^+(D)$ onto $(\mathcal{L}, \subseteq)$, where $\mathcal{L}$ is the set of non-empty $\downarrow$-closed subsets of B_D (with L^{-1} as $\mathcal{O}_{fin}$). If $Z \in \mathcal{L}$ then $\bar{Z} = \{x \mid \downarrow x \cap B_D \subseteq Z\}$, and closure is an isomorphism of $(\mathcal{L}, \subseteq)$ onto $(CL(D), \subseteq)$, with inverse $S \mapsto \downarrow S \cap B_D$. Thus $(\bar{\ }) \circ L$ is the required isomorphism of $PD_L(D)$ onto $PS_L^+(D)$ (i.e. $(CL(D), \subseteq)$).

(ii) $PD_U(D)$: For an ω-chain $H = H_0 \sqsubseteq_U H_1 \sqsubseteq_U \ldots$ in $(M(D), \sqsubseteq_U)$, define $\Phi_U(H) = \bigcap_i \uparrow H_i$. Then Φ_U is order-preserving: indeed, if $H \sqsubseteq K$ then for each i there exists j with $\uparrow H_i \supseteq \uparrow K_j$, so that $\bigcap_i \uparrow H_i \supseteq \bigcap_j \uparrow K_j$. On the other hand, suppose $\bigcap_i \uparrow H_i \supseteq \bigcap_j \uparrow K_j$. We consider the generating tree (cf. [20]) whose finite paths are all the sequences $\langle b_0, \ldots, b_n \rangle$, where $b_i \in K_i$ and $b_i \sqsubseteq b_{i+1}$. The cross-sections of this tree are (multisets whose corresponding sets are) the K_j. For each i there must be a cross-section K_j such that $H_i \sqsubseteq_U K_j$; for if not, we could by König's Lemma find an infinite path $b_0 \sqsubseteq b_1 \sqsubseteq \ldots$ with each $b_j \notin \uparrow H_i$, hence $\bigsqcup_j b_j \notin \uparrow H_i$, hence $\bigcap_j K_j \not\subseteq \uparrow X_i$. This shows that Φ_U is order-reflecting. Further, every compact $\uparrow$-closed set Q is $\Phi_U(H)$ for some H: by Lemma 1, we have only to choose an H cofinal with U_Q. Thus Φ_U determines an isomorphism of $PD_U(D)$ onto $PS_U^+(D)$.

(iii) $PD_C(D)$: For an ω-chain $H = H_0 \sqsubseteq_C H_1 \sqsubseteq_C \ldots$, define

$$\Phi(H) = \Phi_U(H) \cap \Phi_L([H]),$$

where $\Phi_L = (\bar{\ }) \circ L$ is the isomorphism considered in (i). First, $\uparrow\Phi(H) = \Phi_U(H)$. For, obviously $\uparrow\Phi(H) \subseteq \Phi_U(H)$. On the other hand, suppose $x \in \Phi_U(H)$. This means (using König's Lemma) that there is a chain $a_0 \sqsubseteq a_1 \sqsubseteq \ldots$ with $a_i \in H_i$ and $\bigsqcup_i a_i \sqsubseteq x$. But then $\bigsqcup_i a_i \in \Phi_U(H) \cap \Phi_L([H])$, and so $x \in \uparrow\Phi(H)$. Similarly, $\overline{\Phi(H)} = \Phi_L([H])$: the left-to-right inclusion is again trivial, while if $a \in \Phi_L([H])$ we have $a \sqsubseteq a_i$ (for some $a_i \in H_i$) and $a_i \sqsubseteq a_{i+1} \sqsubseteq \ldots$ (for suitable $a_{i+k} \in H_{i+k}$), so that $a \sqsubseteq \bigsqcup_i a_i \in \Phi(H)$. Thus $\Phi(H) \leq_C \Phi(K)$ iff $\Phi_U(H) \leq_U \Phi_U(K)$ and $\Phi_L([H]) \leq_L \Phi_L([K])$. At the same time, it is clear that $H \sqsubseteq_C K$ iff $H \sqsubseteq_U K$ & $H \sqsubseteq_L K$ (notice that if $H_i \sqsubseteq_U K_j$ and $H_i \sqsubseteq_L H_K$ then $H_i \sqsubseteq_C K_{\max(j,k)}$) and that $H \sqsubseteq_L K$ iff $[H] \subseteq [K]$. Hence, by (i) and (ii), $H \sqsubseteq_C K$ iff $\Phi(H) \leq_C \Phi(K)$.

For surjectivity, suppose $Q \in PS_C^+(D)$. Let H be an ω-chain cofinal with C_Q (see Lemma 1); then $\Phi_U(H) = \uparrow Q$. Further, it is clear that $\Phi_L([H]) \subseteq \bar{Q}$. To show that $\Phi_L([H]) \supseteq \bar{Q}$, suppose $a \in \bar{Q}$ (a finite). Then $\{a\} \cup H_0 \sqsubseteq_C Q$. Hence, for some j,

$\{a\} \cup \Sigma_0 \sqsubseteq_C \Sigma_j$. Thus $a \in \Phi_L([H])$; we have shown that $\Phi(H) = Q$. □

Plotkin has observed that the powerdomains over an algebraic cpo have a convenient universal characterisation, namely as free continuous semilattices (see [8]). One naturally tries to extend this to power spaces, in terms of free topological semilattices. Unfortunately this does not work, except for the relatively uninteresting lower power space (for details, see [21]). It seems that the justification of the power spaces, in the general case, has to be rather indirect. A little has been said above to justify the choice of compact sets; we can now add something to that in terms of "specifications". A specification, we have suggested, can be taken to be a countable collection of open sets. Since the set of properties to be satisfied is obviously closed under conjunction (intersection) and logical implication (inclusion), we may as well say that a specification is a countably-generated filter of open sets. We shall say that a specification, $\mathcal{F}$, is finitary if the following condition holds: whenever the union O of an increasing sequence $O_0 \subseteq O_1 \subseteq \ldots$ is in $\mathcal{F}$, some O_i is already in $\mathcal{F}$. To say that the filter $\mathcal{F} \subseteq \Omega(X)$ is finitary is thus equivalent to saying that it is itself an open set in the complete lattice $\Omega(X)$, taken with the Scott topology; or, following the ideas of Section 1, that it is computable, in the sense, e.g. that one can effectively enumerate all (the indices of) the properties which belong to it. The special interest of open filters, in the present context, is due to the following remarkable

FACT Let X be a sober space. A set $Q \subseteq X$ is compact iff the set $\mathcal{F}^*(Q) = \{O \in \Omega(X) \mid Q \subseteq O\}$ is an open filter. Moreover, if $\mathcal{F}$ is any open filter in $\Omega(X)$, then $\cap\mathcal{F}$ is compact (and, of course, $\uparrow$-closed), and if O is any open superset of $\cap\mathcal{F}$ then $O \in \mathcal{F}$. Hence the maps $\mathcal{F}^*$, $\cap$ define an order-isomorphism between $(\mathcal{P}S_U(X), \supseteq)$ and $(O\,\mathrm{Filt}(\Omega(X)), \subseteq)$, where $O\,\mathrm{Filter}\,L$, for L a complete lattice with Scott topology, is the collection of open filters in L.
(See Hofmann & Mislove [9], and references given there.)
Open filters provide the link by which we connect the upper power space with weakest precondition semantics, in the next section.

An equally satisfactory description does not seem to be available for the convex power space, in the general case; these matters are explored in [21].

We conclude this section with some brief remarks on the infinitary powerdomains introduced recently by Apt and Plotkin [1], Plotkin [17] for handling unbounded (countable) nondeterminism. Consider first the case of a flat, countable domain $S_\perp$, as in [1]. Then the upper topology on $\mathcal{P}(S_\perp) - \{\emptyset\}$ gives exactly the infinitary upper (or Smyth) powerdomain of $S_\perp$. This upper topology is not sober, nor is the upper domain a cpo. At the same time, the Vietoris topology gives exactly the convex (Plotkin) powerdomain ($\mathcal{P}(S_\perp) - \{\emptyset\}$, Egli-Milner ordering); in this case the topology is sober, and the powerdomain is a cpo. The lower topology and powerdomain are not very interesting: they are the same as in the finite case.

As for general domains, one suggestion is to treat the infinitary power spaces/ domains analogously to the finitary ones, replacing finite sets by countable sets. That is, one observes that the (finitary) convex power space of an algebraic cpo, D, is the soberification of the Vietoris topology on $\mathcal{P}_{fin}(D)$, and similarly for the upper and lower power spaces. For the infinitary construct, then, one could try the soberification of the space of countable subsets. But whether this leads anywhere is not known at present.

3. Predicate Transformers

Recall that we have defined the "upper" inverse f^+ of a (multi-)map f: X -> Y as f^+: $\mathcal{P}Y$ -> $\mathcal{P}X$: S -> $\{x | f(x) \subseteq S\}$. When f is usc, f^+ cuts down to a function from $\Omega(Y)$ to $\Omega(X)$, which we might denote by $\Omega^+(f)$; the point being that, just as Ω is a functor from $\underline{\underline{Top}}$ into $\underline{\underline{Frm}}$, Ω^+ (with $\Omega^+ = \Omega$ on objects) is a functor from the category of spaces and usc maps into a modified category of frames. But we will not dwell on the categorical aspect here.

Since we identify predicates, or properties, with open sets, maps from $\Omega(Y)$ to $\Omega(X)$ are (the appropriate generalization of) predicate transformers in our framework. The upper inverse can be said to correspond to the weakest precondition: $wp(f,S) = f^+(S)$.

In justification of these remarks, consider the predicate transformers as introduced by Dijkstra [6] and their correspondence, investigated by Plotkin [16], with non-deterministic state transformations. Here we are concerned with discrete state sets X,Y. A predicate transformer from Y to X, satisfying Dijkstra's healthiness conditions, is a strict, multiplicative, continuous function from $\mathcal{P}(Y)$ to $\mathcal{P}(X)$. Plotkin observes that there is an order isomorphism between the (cpo of) healthy predicate transformers from Y to X and the domain of non-deterministic state transformations taken as $[X \to PD_U(Y_\perp)]$. Now, the topology of $Y_\perp$ is $\mathcal{P}(Y) \cup \{Y_\perp\}$, while that of X is $\mathcal{P}(X)$. In order to regard a predicate transformer P: $\mathcal{P}(Y) \to \mathcal{P}(X)$ as a map from $\Omega(Y_\perp)$ to $\Omega(X)$, then, we have only to give it a value for the argument $Y_\perp$; naturally, we assume $P(Y_\perp) = X$. Thus, we consider the domain of (healthy) predicate transformers to be the (pointwise ordered) poset of maps $\Omega(Y_\perp) \to \Omega(X)$ which are strict and continuous and preserve finite intersections (including the null intersection). Our claim is that, with this view of predicate transformers, the correspondence with non-deterministic maps can be extended far beyond the case of discrete spaces considered by Dijkstra and Plotkin; indeed it extends to arbitrary sober spaces.

For Y a sober space, the points of $PS_U(Y)$, as well as of Y itself, can be identified with suitable filters in $\Omega(Y)$, by the above FACT. We will be able to treat deterministic and non-deterministic ST's (state transformations) in a uniform way by regarding them as maps from X into the space $Filt(\Omega(Y))$ of filters in $\Omega(Y)$ (with basic open sets the $\Phi_O = \{\mathcal{F} | O \in \mathcal{F}\}$, for $O \in \Omega(Y)$).

Theorem 4. Let X,Y be sober spaces. For a continuous map f: X -> Filt(Ω(Y)), let $\pi(f)$: Ω(Y) -> Ω(X) be defined by $\pi(f)(0) = \{x \mid 0 \in f(x)\}$ ($\pi(f)(0)$ is open in X by continuity of f, since $\pi(f)(0) = \{x \mid f(x) \in \Phi_0\}$). Then π defines an order-isomorphism between [X -> Filt(Ω(Y))] and the poset of PT's (predicate transformers) $p \in [\Omega(Y) \to \Omega(X)]$ which satisfy

(1) p is monotonic and strict, and preserves finite meets. Moreover, π cuts down to an order-isomorphism between [X -> PS_U(Y)] and the poset of PT's satisfying (1) and

(2) p is continuous (i.e. preserves directed sups; equivalently, under our assumption that spaces are second countable, p preserves sups of ω-chains).

It cuts down further to an order-isomorphism between [X -> Y] and the poset of PT's satisfying (1) and

(2') p is completely additive (i.e. preserves arbitrary sups).

Remark. The final part of the theorem (concerning [X -> Y]) is essentially the (well-known) duality result mentioned at the end of Section 1.

Proof of Theorem 4. It is straightforward to check that, for any f: X -> Filt(Ω(Y)), the PT $\pi(f)$ satisfies (i) (for preservation of meet, for example, one uses the fact that, for any filter $\mathcal{F}$, $0 \cap 0' \in \mathcal{F} \equiv 0 \in \mathcal{F} \wedge 0' \in \mathcal{F}$). For any p: Ω(Y) -> Ω(X) satisfying (1), define T(p): X -> Filt(Ω(Y)) by:

$$T(p)(x) = \{0 \mid x \in p(0)\};$$

again, one readily checks that condition (1) implies that T(p)(x) is a filter. To prove the theorem, it suffices to show that (A) T is a right inverse of π (i.e. that $T \circ \pi(f)(x) = f(x)$), and that this remains true on cutting down in the ways indicated; and (B) T is strictly monotonic (i.e. $T(p) \leq T(q)$ iff $p \leq q$).

A) For the right inverse property, we have

$$T \circ \pi(f)(x) = \{0 \mid x \in \pi(f)(0)\} = \{0 \mid 0 \in f(x)\} = f(x).$$

It remains to show that π and T cut down appropriately. Suppose that f: X -> 0 Filt(Ω(Y)) (recall that this codomain is identified with PS_U(Y)), and let $0_1 \subseteq 0_2 \subseteq \ldots$ be an increasing sequence in Ω(Y). Suppose also that $x \in \pi(f)(\bigcup_i 0_i)$. This means that $\bigcup_i 0_i \in f(x)$. Since f(x) is (Scott-)open, $0_i \in f(x)$ for some i; thus $x \in \pi(f)(0_i)$ for some i. This shows that $\pi(f)$ is continuous. One shows similarly that if p satisfies (1) and (2), then T(p) maps X into 0 Filt(Ω(Y)).

Suppose now that f: X -> Y (here we are of course identifying Y with the space of completely prime filters in Ω(Y)). Let $(Q_\iota)_{\iota \in I}$ be a family of open sets in Y. Suppose that $x \in \pi(f)(\bigcup_\iota 0_\iota)$, in other words $\bigcup_\iota 0_\iota \in f(x)$. Since f(x) is completely prime, some $0_\iota \in f(x)$. Thus $x \in \pi(f)(0_\iota)$ for some ι.. This shows that $\pi(f)$ is additive. Again, it is easy to see that if p satisfies conditions (1) and (2'), then $\pi(p)$ maps X into Y.

B) Suppose $p \leq q$, that is $p(0) \subseteq q(0)$ for all $0 \in \Omega(Y)$. Then, for each $x \in X$, $T(p)(x) = \{0 \mid x \in p(0)\} \subseteq \{0 \mid x \in q(0)\} = T(q)(x)$; that is, $T(p) \leq T(q)$. On the other hand, suppose $\neg(p \leq q)$. Then for some $x \in X$, $0 \in Y$ we have $x \in p(0)$ while $x \notin q(0)$. But then $T(p)(x) \not\subseteq T(q)(x)$; that is, $\neg(T(p) \leq T(q))$. Thus strict mono-

tonicity obtains; the theorem is proved.

The significance of this theorem (more precisely, of part (2) of the theorem) is that it gives us an equivalence, in a very general setting, between a denotational semantic using the upper power domain/space and axiomatic semantics in the manner of Dijkstra.

The viewpoint of the upper powerdomain/predicate transformer approach is, of course, that a process passes a test (satisfies a property) iff all its possible computations do so - that is, it must pass the test. Also to be considered is the view which corre ponds to the lower topology (the process may pass the test), and the conjunction of th two (convex topology). Given a notion of successful computation, the resulting specialization orders will give three preorders and equivalence notions for processes. It is interesting to note that (independently of the above) de Nicola and Hennessy [5] have recently developed exactly this approach to the equivalence of processes.

Acknowledgements

Discussions with Gordon Plotkin have been very helpful. The comprehensive treatise [7] has proved to be a continuing, almost inexhaustible, source of inspiration. Financial support has been provided by the (U.K.) SERC.

References

1. Apt, K., Plotkin, G., A Cook's tour of countable non-determinism. Proc. ICALP 1981, Springer-Verlag LNCS 115, pp. 479-494 (1981).
2. Berge, C., Espaces Topologiques: Fonctions Multivoques. Dunod, Paris (1959).
3. Continuous Lattices, Proceedings Bremen 1979, ed. Banaschewski and Hoffman, Springer LN Math. 871 (1981).
4. de Bakker, J., Zucker, J., Denotational semantics of concurrency, Proc. 14th ACM STOC, pp. 153-158 (1982).
5. de Nicola, R., Hennessy, M., Testing equivalences for processes, CSR-123-82, Dept. of Computer Science, Edinburgh (1982).
6. Dijkstra, E., A Discipline of Programming, Prentice-Hall (1976).
7. Gierz, G., Hofmann, K., Keimel, K., Lawson, J., Mislove, M., Scott, D., A Compendium of Continuous Lattices. Springer (1980).
8. Hennessy, M., Plotkin, G., Full abstraction for a simple parallel programming language. Proc. MFCS, Springer LNCS 74, pp. 108-120 (1979).
9. Hofmann, K., Mislove, M., Local compactness and continuous lattices: in [3] (pp, 209-248).
10. Johnstone, P., Scott is not always sober: in [3] (pp. 283-284).
11. Johnstone, P., Tychonoff's theorem without the axiom of choice, Fund. Math. 113, pp. 21-35 (1981).
12. Johnstone, P., Stone Spaces, Cambridge U.P. (198?).
13. Kuratowski, K., Topology. Revised edition, Academic Press and PWN (1966).
14. Michael, E., Topologies on spaces of subsets, Trans. AMS 71,pp.152-182 (1951).
15. Plotkin, G., A powerdomain construction, SIAM J. Comput. 5,pp. 452-487 (1976).
16. Plotkin, G., Dijkstra's predicate transformers and Smyth's powerdomains, Abstract Software Specifications (ed. D. Bjørner) LNCS 86 (1980).
17. Plotkin, G., A powerdomain for countable non-determinism, Proc. ICALP 1982.
18. Plotkin, G., Domains: notes for lecture course, Edinburgh (1981).
19. Rogers, H., Theory of Recursive Functions.
20. Smyth, M., Power domains, JCSS 16 (1978).
21. Smyth, M., Powerdomain and hyperspace. To appear.
22. Vietoris, L., Monatsh. f. Math. u. Phys. 31, pp. 173-204 (1921).
23. Winskel, G., Events in Computation, Thesis, Edinburgh (1980).