The Synthetic Plotkin Powerdomain

Wesley Phoa Paul Taylor

1990

Abstract

Plotkin [1976] introduced a *powerdomain* construction on domains in order to give semantics to a *non-deterministic binary choice* constructor, and later [1979] characterised it as the *free semilattice.* Smyth [1983] and Winskel [1985] showed that it could be interpreted in terms of *modal predicate transformers* and Robinson [1986] recognised it as a special case of Johnstone's [1982] *Vietoris construction*, which itself generalises the *Hausdorff metric* on the set of closed subsets of a metric space. The domain construction involves a curious order relation known as the *Egli-Milner order.*

In this paper we relate the powerdomain directly to the free semilattice, which in a topos is simply the *finite powerset*, *i.e.* the object of (*Kuratowski*-)finite subobjects of an object. We show that the Egli-Milner order coincides (up to "$\neg\neg$") with the intrinsic order induced by a family of "observable predicates."

This problem originally arose in the context of the *Effective topos*, in which the observable predicates are the recursively enumerable subsets. However we find that the results of this paper hold for *any elementary topos*, and so by considering a (pre)sheaf topos (which the Effective topos is not) we may compare them with the classical approach.

Important Note: Much of the credit for the work in this paper is due to Wesley Phoa and Martin Hyland, but I take the blame for its presentation. Comments on it are most welcome. When it is finished it will be submitted as a joint paper with Wesley Phoa, and an announcement will be made on `types`.

1 Introduction

1.1 The Plotkin powerdomain

Plotkin [1976] introduced his powerdomain construction in order to extend denotational semantics in the Scott style to languages involving a binary choice, **or**. The behaviour of a program in such a language may be that:

- it always diverges;
- it always terminates, and with the same output value;
- it always terminates, but there are several (but finitely many) possible output values;
- it sometimes converges and sometimes diverges;

and so to express its denotation we must consider the set of possible outputs. Divergence must be mentioned explicitly as a value if it occurs in order to distinguish the third and fourth cases. The set must be nonempty since there must be some behaviour — divergence if nothing else. Incidentally, by König's lemma, if there are infinitely many possible output values, then divergence must also be possible.

By analogy with the power*set*, Ω^X, one might suppose that the powerdomain would be of the form T^X for some "truthvalues" domain T. There are two objections to this: First, the class of admissible subobjects would then be closed under inverse images, so including "infinite" subobjects. Second, the subobjects themselves would be upwards-closed (on the reasonable assumption that the generic such set is a maximal element of T), but we want $\{\bot\}$ to be admissible.

The central theme of denotational semantics is that each program constructor should correspond to an algebraic operation in the domain. In particular since **or** is a conjunction of nondeterministic behaviours, it must correspond to a binary operation $\Cup$ on the domain. In the natural understanding, this must be commutative, associative, idempotent and computable, so the nondeterministic domain must be a *semilattice* $(A, \Cup)$ in the category of domains. Moreover since every deterministic program is nondeterministic in a trivial way, there is an inclusion of the deterministic domain X into the nondeterministic one. Indeed Hennessy and Plotkin [1979] argued that $(A, \Cup)$ has to be the *free* semilattice on X.

There is another approach to semantics, which is *axiomatic*: we argue about the *properties* of programs. We have already informally said that a program *may* or *must* diverge: these are modalities on propositions concerning its actual behaviours in any particular run. Smyth [1983] showed how a program p (in particular a non-deterministic one) can be interpreted as a *predicate transformer* from post-conditions to the weakest corresponding pre-condition. Winskel [1985] characterised the powerdomain in terms of the properties it could express in a logic which includes these transformers $[p]$ and $\langle p\rangle$ as *unary operators.* Robinson [1986] did something slightly different: he treated the modal predicates $\Box\phi$ and $\Diamond\phi$ as *abstract symbols* and showed that they generate the topology (*i.e.* the lattice of properties) on the powerdomain A as ϕ ranges over the open sets of the base domain X. In fact the point of Robinson's paper was to show that the powerdomain is a special case of Johnstone's [1982] Vietoris monad, which had already been generalised from a construction on metric spaces due originally to Hausdorff.

These axiomatic and topological approaches are very significant in the literature, but for two reasons we have not attempted to make use of them in this paper. First, Johnstone showed that the Vietoris construction and the free semilattice agree only in special cases (admittedly including all those of interest in classical domain theory), and our problem is likely to be as difficult as his. Secondly, the analogy with topology is not strict (in particular we do not assume all joins), so it is not yet clear what a "Σ-frame" should be.

1.2 Synthetic domain theory

(To be written)

1.3 The synthetic Plotkin powerdomain

Throughout we shall use the word "set" to mean an object of a given elementary topos, $\mathcal{E}$. We suppose that we have a category $\mathcal{C}$ of predomains which is a *full reflective* subcategory of the category of sets. Then

- arbitrary limits of predomains exist (which is not true of most of the classical categories of domains) and are constructed "set-theoretically"

- we may perform some type construction with sets (for instance, in our case the Plotkin powerdomain is the free semilattice) and turn the result into a predomain.

Definition 1.1 A *semilattice* is a set $A \in \mathcal{E}$ together with a (global) element $\circledcirc \in A$ and a binary operation $\Cup : A \times A \to A$ which is

- *idempotent*: $a \Cup a = a$,
- *commutative*: $a \Cup b = b \Cup a$,
- *associative*: $a \Cup (b \Cup c) = (a \Cup b) \Cup c$, and
- $\circledcirc$ is the *unit*: $a \Cup \circledcirc = a = \circledcirc \Cup a$.

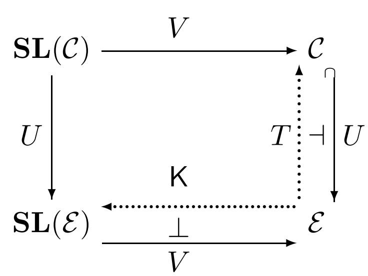
We shall find that $\circledcirc$ is an inessential part of the structure, so we define a *binary semilattice* to be an algebra $(A, \Cup)$ without the unit.

It is easy to see that

$$a \Subset b \overset{\text{def}}{\iff} a \Cup b = b$$

defines a partial order (reflexive, transitive antisymmetric relation), and in fact $\Cup$ is the join for this. However it is important not to consider $(A, \Cup)$ as specifically a *join*-semilattice (or as a meet-semilattice), **because $\Subset$ is not what we shall mean by the intrinsic order on the set** A (see section 2): it is intrinsic to the *semilattice*, not to the *set*.

The definition of a semilattice can be expressed in any category with finite products, so we write $\mathbf{SL}(-)$ for the category of semilattices in any such. Then we have forgetful functors



two of which (we shall show) have left adjoints (indicated by dotted arrows). From K and T, it is a simple categorical argument to derive the other two adjoints.

Proposition 1.2 The left adjoint to $\mathbf{SL}(\mathcal{C}) \to \mathbf{SL}(\mathcal{E})$ is given by the reflector $T : \mathcal{E} \to \mathcal{C}$.

Proof Explicitly, if $(A, \Cup)$ is a (binary) semilattice, then the free $\mathcal{C}$-semilattice on it is $(TA, T\Cup)$. To make this meaningful we need

$$TA \times TA \cong T(A \times A)$$

i.e. T preserves finite products: $\times$ itself is unambiguous because products in a reflective subcategory are always calculated as in the larger category. By functoriality this is a $\mathcal{C}$-semilattice. If $f : (A, \Cup) \to (B, \Cup')$ is a homomorphism into a $\mathcal{C}$-semilattice then the underlying map has a lifting $\bar{f} : TA \to B$ and this is a homomorphism because $\Cup' \circ (\bar{f} \times \bar{f})$ and $\bar{f} \circ T\Cup$ both serve as the unique lifting of $\Cup' \circ (f \times f) = f \circ T\Cup$, again using the fact that T preserves binary products. The argument for the unit, $\circledcirc$, is similar, using the terminal object. $\square$

Theorem 1.3 The left adjoint to $\mathbf{SL}(\mathcal{C}) \to \mathcal{C}$ is given by $T \circ \mathsf{K} \circ U$.

Proof Let $X \in \mathcal{C}$ and $(A, \Cup) \in \mathbf{SL}(\mathcal{C})$. We have to show a natural bijection between maps $f : X \to A$ and homomorphisms $T(\mathsf{K}(X), \cup) \to (A, \Cup)$; it doesn't matter whether we work in $\mathcal{C}$ or $\mathcal{E}$ because the former is a full subcategory of the latter. But $T \circ \mathsf{K} \dashv V \circ U$. $\square$

So in order to construct the synthetic Plotkin powerdomain it suffices

- to define our categories of sets and domains, and show that the latter is a full reflective subcategory of the former and that the reflector preserves finite products,
- to show that the finite powerset affords the free semilattice in the category of sets.

These two topics will be the subject of sections 2 and 3 respectively.

This abstract nonsense, however, tells us little about the concrete structure of the powerdomain, and the main purpose of the paper is to show that the Egli-Milner order is (almost) the intrinsic order relation on it. In other words, the synthetic construction is the same as the concrete one. Section 4 shows one implication, and with the help of modal operators (section 5) we prove a weak form of the converse in section 6.

2 The intrinsic order

As usual, we use Ω to denote the object of truth values in $\mathcal{E}$, and we shall also assume given a sublattice $\Sigma \subset \Omega$ whose elements we shall think of as "computable predicates." In section 6 we shall need to assume that these predicates are $\neg\neg$-closed, *i.e.* $\neg\neg\phi \Rightarrow \phi$.

If we look at a parametric case it will become more reasonable to the intuition why Ω is a very complex object, much larger than the set $2 = \{\mathbf{true}, \mathbf{false}\}$ of decidable truthvalues or even than a typical choice of Σ. A map $\phi : \mathbb{N} \to \Omega$ is a predicate $\phi(n)$ on natural numbers, and as such it may perhaps be primitive recursive, recursively decidable, recursively enumerable, Π^0_2 or worse. In fact the parameter is irrelevant and so using the Kleene bracket notation we can define

$$\Sigma = \{\phi \in \Omega : \exists n.(\{n\}(0)\downarrow \leftrightarrow \phi)\}$$

the object of recursively enumerable predicates.

Although this is the intended application, it is easier to grasp the intuition if you think of "open" instead of "computable" predicates. For this purpose the reader is invited to apply the following definitions to the topos $\mathbf{Set}^{\mathcal{C}^{op}}$ where $\mathcal{C}$ is the category of countably based algebraic lattices and Scott-continuous maps and Σ is (the representable functor on) the two-point lattice. In this case a sieve (*i.e.* a subobject of a representable) is generated by the inclusion of an open set iff its characteristic function factors through Σ.

Given Σ, we can define the "intrinsic order:"

Definition 2.1 For any object $X \in \mathcal{E}$ and $x, y \in X$, write

$$x \sqsubseteq y \overset{\text{def}}{\iff} \forall \phi \in \Sigma^X . \phi(x) \Rightarrow \phi(y)$$

This says that every computable property possessed by x is shared by y, so y is "more defined" than x. Clearly $\sqsubseteq$ is reflexive and transitive, but it need not be antisymmetric.

Examples 2.2

- if $\Sigma = \Omega$ then this order is discrete, *i.e.* $x \sqsubseteq y \iff x = y$.

- if $\Sigma = \{\top, \bot\}$ then the (pre)order is the finest decidable equivalence relation on X.
- in the topological example, (the externalisation of) $\sqsubseteq$ is exactly the specialisation order (on generalised points of representables).
- $\bot \sqsubseteq \top$ in Σ [spell out]

Lemma 2.3 Every function is monotone with respect to this order. $\square$

Unfortunately it is difficult to deduce very much about $\sqsubseteq$ on a power X^I from the order on X without additional assumptions, but we do have the expected result for binary product:

Lemma 2.4 For $x_1, x_2 \in X$ and $y_1, y_2 \in Y$, we have $\langle x_1, y_1\rangle \sqsubseteq \langle x_2, y_2\rangle$ in $X \times Y$ iff $x_1 \sqsubseteq x_2$ in X and $y_1 \sqsubseteq y_2$ in Y. $\square$

Traditional domain theory begins with posets — sets with an *imposed* order relation — and then considers extra conditions such as bottom and joins of chains. The idea here is to follow the same course, but starting from the *intrinsic* order relation on all sets, which is automatically preserved by all functions. Domains are then just *special* sets but with *ordinary* functions.

This point of view is analogous to the topological approach to domain theory, for which Vickers [1989] is an excellent introduction. A map $X \to \Sigma$ plays the rôle of an open set of X and $\sqsubseteq$ is antisymmetric iff X is T_0 in this topology. The point $\bot$ is characterised as being in no open set save the whole space, and sobriety is analogous to (but stronger than) directed-completeness. Note, however, that the class of Σ-subsets is in general not closed under arbitrary unions.

Definition 2.5 A ***Σ-space*** is an object X for which $\sqsubseteq$ is antisymmetric; it is ***focal***[1] if it has a least element $\bot$ in this order.

Examples 2.6

- If $\Sigma = \Omega$, every object is a Σ-space, but only the terminal object is focal.
- If $\Sigma = \{\top, \bot\}$, an object is a Σ-space iff (the equality predicate on) it is decidable, and again only the terminal object is a focal Σ-space.
- In a Scott topos, every representable object is a Σ-space, and is focal iff it has a bottom in the specialisation order.
- In the Effective topos, all Σ-spaces are modest sets (but not conversely) and hence definable by partial equivalence relations on $\mathbb{N}$.

It is not difficult to see that X is a Σ-space iff the map

$$\epsilon_X : X \to \Sigma^{\Sigma^X} \qquad \text{by} \qquad x \mapsto \lambda f. fx$$

is mono. This suggests forming the epi-mono factorisation of ϵ_X: we shall show that this does in fact give the reflection of X into the full subcategory of Σ-spaces.

Lemma 2.7 Let $p : X \to Y$. Then

[1] For topological spaces, this term is due to Peter Freyd.

- the induced map $\Sigma^p : \Sigma^Y \to \Sigma^X$ is split epi iff p factors into ϵ_X.
- if Σ^p is mono and X is focal then Y is focal and p preserves $\bot$. $\square$

Proposition 2.8 Let $X \stackrel{p_X}{\to} TX \stackrel{e_X}{\to} \Sigma^{\Sigma^X}$ be the epi-mono factorisation of ϵ_X. Then T defines the reflection into the full subcategory of Σ-spaces, and also preserves the property of being focal. $\square$

In order to be able to construct the powerdomain we need another property:

Proposition 2.9 T preserves finite products. $\square$

So much for the synthetic analogue of posets; for (pre)domains we need some kind of either directed-completeness or sobriety. There are several different candidates for this, some of which are considered by the first author in [1990], but in this paper we prefer not to be drawn into this discussion. However in the proofs of the previous results the important property was being epi *with respect to maps into* Σ, and by isolating this we obtain easily a good notion, due to Martin Hyland, which suffices for our purposes (in fact we shall make no further use of it).

Definition 2.10 $p : X \to Y$ is called Σ-***epi*** if it induces a mono $\Sigma^p : \Sigma^Y \to \Sigma^X$ and Σ-***anodyne*** if this is an isomorphism. The object X is Σ-***replete*** if the only Σ-anodyne maps $p : X \to Y$ are isomorphisms.

Proposition 2.11 Every object X has a Σ-replete reflection, SX, and S preserves finite products. $\square$

In the topological example, a representable is Σ-replete iff it is sober, and in this case the specialisation order has directed joins.In the Effective Topos Σ-replete also implies that ω-sequences have joins, although the proof makes crucial use of Markov's Principle and Church's Thesis.

3 The finite powerset

In order to construct free algebras it is in general necessary to assume that the topos $\mathcal{E}$ has a natural numbers object $\mathbb{N}$ (since that is itself a free model). However the powerset Ω^X of a set $X \in \mathcal{E}$ is already the free internally-complete $\bigcup$-semilattice on X, even when $\mathcal{E}$ itself fails to have infinitary colimits or a natural numbers object.

Since Ω^X has I-indexed joins for all $I \in \mathcal{E}$, in particular it has nullary and binary ones, usually written $\emptyset$ and $U \cup V$ respectively, so it is a (finitary) $\cup$-semilattice.

Notation 3.1 Let $\mathsf{K}(X) \subset \Omega^X$ denote the smallest subset which

- contains the empty set $\emptyset \in \Omega^X$
- contains the singletons $\{\} : X \hookrightarrow \Omega^X$ and
- is closed under binary unions $\cup : \Omega^X \times \Omega^X \to \Omega^X$.

So,

to prove properties of $\mathsf{K}(X)$ we consider the class $L \subset \mathsf{K}(X)$ of sets which possess the property and show that it includes $\emptyset$ and singletons and is closed under binary unions.

If $U \in \mathsf{K}(X)$ for some X, we say U is ***Kuratowski-finite.*** On the assumption that the topos $\mathcal{E}$ has a natural numbers object $\mathbb{N}$, a set is Kuratowski-finite iff locally[2] it has an enumeration

$$U = \{x_1, \ldots, x_n\}$$

possibly including repetitions for some $n \in \mathbb{N}$, *i.e.* there is a surjection $[n] \twoheadrightarrow U$. Hence the class of Kuratowski-finite sets is closed under quotients, although not under subobjects. For an account of this characterisation, the reader is referred to Johnstone [1977]. Although it is useful intuition, we prefer not to make our proofs rely on it as it is more complicated to express categorically.

Proposition 3.2 $\mathsf{K}(X)$ is the *free* semilattice on X.

Proof Let $(A, \Cup, \circledcirc)$ be any semilattice; we are going to construct the structure map $\alpha : \mathsf{K}(A) \to A$. Consider the set

$$C = \left\{ \langle U, a \rangle \in \Omega^A \times A : \ (\forall u \in U. u \Subset a) \ \wedge \ \big(\forall b \in A. (\forall u \in U. u \Subset b) \Rightarrow a \Subset b\big) \right\}$$

and let

$$D = \left\{ U \in \Omega^A : \exists a \in A. \langle U, a \rangle \in C \right\}$$

Then by antisymmetry of $\Subset$, the projection $\pi_0 : C \twoheadrightarrow D$ is an isomorphism; also

- $\langle \{\}, \mathsf{id} \rangle : A \to \Omega^A \times A$ factors through C,
- $\langle \emptyset, \circledcirc \rangle \in C$ and
- if $\langle U, a \rangle, \langle V, b \rangle \in C$ then $\langle U \cup V, a \Cup b \rangle \in C$

Hence $\mathsf{K}(A) \subset D$ and the components of

$$\alpha : \mathsf{K}(A) \subset D \cong C \subset \Omega^A \times A \xrightarrow{\pi_1} A$$

are semilattice homomorphisms. Moreover $\alpha \circ \{\} = \mathsf{id}$ because

$$\alpha \{a\} = \pi_1 \langle \{a\}, a \rangle = a$$

Hence if we are given any function $f : X \to A$ we may factor it through $\{\} : X \hookrightarrow \mathsf{K}(X)$ by the semilattice homomorphism

$$\tilde{f} \stackrel{\text{def}}{=\!=} \alpha \circ \mathsf{K}(f) \qquad \text{where} \qquad \mathsf{K}(f)(U) \stackrel{\text{def}}{=\!=} \{f(u) : u \in U\}$$

(so essentially $\tilde{f}(U) = \biguplus \{f(u) : u \in U\}$). This factorisation is unique, since given two such we may form their equaliser $E \subset \mathsf{K}(X)$, which is a sub-semilattice containing X and hence the whole. $\square$

[2] The number n is not a constant, but is parametrised by $v \in V$, where V is some *supported* object (see next footnote). The indices i of the enumeration are similarly functions $i : V \to \mathbb{N}$ such that $\forall v. 1 \leq i(v) \leq n(v)$. For example if $\mathcal{E} = \mathbf{Set}^G$ for some group G, any finite set with a G-action is Kuratowski-finite, but (constant) numerals $[n]$ and their quotients carry the trivial action.

The following simple but important result is true of the free functor of any finitary algebraic theory:

Lemma 3.3 The functor $\mathsf{K} : \mathcal{E} \to \mathcal{E}$ preserves surjectivity.

Proof Let $f : Y \twoheadrightarrow X$ in $\mathcal{E}$, *i.e.*

$$\forall x \in X . \exists y \in Y . f(y) = x$$

Consider the set

$$L = \{U \in \mathsf{K}(X) : \exists V \in \mathsf{K}(Y) . \mathsf{K}(f)(V) = U\}$$

- It contains the singletons because for $U = \{x\}$ we are given $\exists y \in Y . f(y) = x$, so put $V = \{y\}$ and then $\mathsf{K}(f)(V) = \{fy\} = U$.
- It contains the empty set because $\mathsf{K}(f)(\emptyset) = \emptyset$
- It is closed under unions because if $U_1 = \mathsf{K}(f)(V_1)$ and $U_2 = \mathsf{K}(f)(V_2)$ then $U_1 \cup U_2 = \mathsf{K}(f)(V_1) \cup \mathsf{K}(f)(V_2) = \mathsf{K}(f)(V_1 \cup V_2)$.

and so $L = \mathsf{K}(X)$, *i.e.* $\forall U \in \mathsf{K}(X) . \exists V \in \mathsf{K}(Y) . \mathsf{K}(f)(V) = U$. □

Corollary 3.4 ("Weak Axiom of Finite Choice") Let $U \subset X$ be finite (*i.e.* $U \in \mathsf{K}(X)$) and let $\phi(x, f)$ be a predicate on $X \times F$ such that

$$\forall u \in U . \exists f \in F . \phi(u, f)$$

Then there is a finite set of pairs $V \subset U \times F$ such that

$$\forall u \in U . \exists f \in F . \langle u, f \rangle \in V \quad \text{and} \quad \forall \langle u, f \rangle \in V . \phi(u, f)$$

Proof Apply the Proposition to the projection

$$\pi_0 : \{\langle u, f \rangle \in U \times F : \phi(u, f)\} \twoheadrightarrow U$$

and consider $U \in \mathsf{K}(U)$. □

Notation 3.5 Let $\mathsf{K}^+(X) \subset \Omega^X$ be generated by the singletons and $\cup$ (*not* $\emptyset$). By a *binary semilattice* we mean an algebra $(A, \Cup)$ with an idempotent, commutative and associative binary operation (but no unit).

Proposition 3.6

- $\mathsf{K}^+(X)$ is the free binary semilattice on X,
- any $U \in \mathsf{K}^+(X)$ is *supported*,[3] *i.e.* $\exists u \in U . \top$, and
- $\mathsf{K}(X) = \mathsf{K}^+(X) + \{\emptyset\}$ (the *disjoint* union).

[3]Being *supported* is the internal way of saying that a set has an element; diagrammatically, $U \twoheadrightarrow 1$. It need not be *inhabited*, *i.e.* have a *global* element $1 \to U$.

Proof The first part is exactly similar to what we did before. The subset $L \subset \mathsf{K}^+(X)$ of supported sets includes the singletons and is closed under $\cup$ so is all of it. Finally $\mathsf{K}^+(X)+\{\emptyset\}$ carries a $(\Cup, \circledcirc)$-semilattice structure, so there are mediators $\mathsf{K}(X) \leftrightarrows \mathsf{K}^+(X) + \{\emptyset\}$; the universal properties (coproduct and free semilattice) make these mutually inverse. $\square$

So the finite powerset, like the Hausdorff and Vietoris constructions but unlike the full powerset Ω^X, falls into two parts. This means that, given a Kuratowski-finite set, there is a constructive procedure to determine whether it is empty or inhabited. The Plotkin construction only defined the larger part anyway because the empty set of process behaviours is not meaningful in denotational semantics.

4 The Egli-Milner order

Since the order on $A \times A$ is pointwise, we have

Lemma 4.1 If $a_1 \sqsubseteq a_2$ and $b_1 \sqsubseteq b_2$ in a semilattice $(A, \Cup)$ then $a_1 \Cup b_1 \sqsubseteq a_2 \Cup b_2$. $\square$

Here it is important to remember the distinction between the two order relations: the similar result for $\Subset$ is trivial.

Let S be a Kuratowski-finite set; informally, we can think of it as the word $s_1 \Cup s_2 \Cup \cdots \Cup s_n$ for some $n \in \mathbb{N}$ (where the s_i are not necessarily distinct). Now suppose that T is another finite set and the relation

$$\big(\forall s \in S.\exists t \in T.s \sqsubseteq t\big) \quad \wedge \quad \big(\forall t \in T.\exists s \in S.s \sqsubseteq t\big)$$

holds; this is called the **Egli-Milner order**, written $S \sqsubseteq_{\mathrm{EM}} T$. Then for each i we have some $t'_i \in T$ with $s_i \sqsubseteq t'_i$. Similarly T is the word $t_1 \Cup \cdots \Cup t_m$ and we have $s'_j \sqsubseteq t_j$ with $s'_j \in S$. Then

$$(s_1 \Cup \cdots \Cup s_n) = (s_1 \Cup \cdots \Cup s_n) \Cup (s'_1 \Cup \cdots \Cup s'_m) \sqsubseteq (t'_1 \Cup \cdots \Cup t'_n) \Cup (t_1 \Cup \cdots \Cup t_m) = (t_1 \Cup \cdots \Cup t_m)$$

using the semilattice equations for the equalities and $\sqsubseteq$-monotonicity of $\Cup$ for the inequality.

Now each of the authors who have discussed the Egli-Milner order have given motivations for it (from Computer Science), which one may or may not find convincing. However a little consideration of pure category theory shows how it is forced upon us. For each object $X \in \mathcal{E}$ we have

$$[\sqsubseteq] \stackrel{\text{def}}{=\!=} \{\langle s, t\rangle \in X \times X : s \sqsubseteq t\}$$

which internalises the order relation. We write $p, q : [\sqsubseteq] \rightrightarrows X$ for the projections, and of course one is pointwise less than the other.

Now apply the functor K. What is this order[4] $\mathsf{K}[\sqsubseteq] \rightrightarrows \mathsf{K}X$? An instance of it is a finite set V of pairs $\langle s, t\rangle$ with $s \sqsubseteq t$; then let

$$S \stackrel{\text{def}}{=\!=} \mathsf{K}(p)(V) = \{s \in X : \exists t \in X.\langle s, t\rangle \in V\}$$

and

$$T \stackrel{\text{def}}{=\!=} \mathsf{K}(q)(V) = \{t \in X : \exists s \in X.\langle s, t\rangle \in V\}$$

[4]In fact $\mathsf{K}[\sqsubseteq] \to \mathsf{K}(X) \times \mathsf{K}(X)$ is not mono, but this doesn't matter; shortly we shall show that its image is $[\sqsubseteq_{\mathrm{EM}}]$.

so we have $S \sqsubseteq_{\text{EM}} T$. We shall now give a purely categorical proof that it implies the Σ-order. The first result (like preservation of surjectivity) is true of the free functor of any finitary algebraic theory.

Lemma 4.2 The functor K preserves the (pointwise) $\sqsubseteq$ relation.

Proof We are given $p, q : Y \rightrightarrows X$ satisfying $\forall y \in Y.p(y) \sqsubseteq q(y)$. Consider the set

$$L = \{V \in \mathsf{K}(Y).\mathsf{K}(p)(V) \sqsubseteq \mathsf{K}(q)(V)\}$$

Then

- $\mathsf{K}(p)(\{y\}) = \{py\} \sqsubseteq \{qy\} = \mathsf{K}(q)(\{y\})$ by monotonicity of $\{\} : X \to \mathsf{K}(X)$,
- $\mathsf{K}(p)(\emptyset) = \emptyset = \mathsf{K}(q)(\emptyset)$ and
- if $\mathsf{K}(p)(V_1) \sqsubseteq \mathsf{K}(q)(V_1)$ and $\mathsf{K}(p)(V_2) \sqsubseteq \mathsf{K}(q)(V_2)$ then using the Corollary,

$$\mathsf{K}(p)(V_1 \cup V_2) = \mathsf{K}(p)(V_1) \cup \mathsf{K}(p)(V_2) \sqsubseteq \mathsf{K}(q)(V_1) \cup \mathsf{K}(q)(V_2) = \mathsf{K}(q)(V_1 \cup V_2)$$

so $L = \mathsf{K}(Y)$, *i.e.* $\forall V \in \mathsf{K}(Y).\mathsf{K}(p)(V) \sqsubseteq \mathsf{K}(q)(V)$. □

Lemma 4.3 If $S, T \in \mathsf{K}(X)$ with $S \sqsubseteq_{\text{EM}} T$ then there is some $V \in \mathsf{K}[\sqsubseteq]$ with $\mathsf{K}(p)(V) = S$ and $\mathsf{K}(q)(V) = T$.

Proof We use the weak axiom of finite choice with the finite set S and the predicate $s \sqsubseteq t$ on $S \times T$ to find $V_1 \in \mathsf{K}(S \times T)$ with

$$\forall s \in S.\exists t \in T.\langle s, t\rangle \in V_1$$

and similarly $V_2 \in \mathsf{K}(S \times T)$ with

$$\forall t \in T.\exists s \in S.\langle s, t\rangle \in V_2$$

Then $V_1, V_2 \in \mathsf{K}[\sqsubseteq]$ with

$$\mathsf{K}(p)(V_2) \subset \mathsf{K}(p)(V_1) = S \qquad \text{and} \qquad \mathsf{K}(q)(V_1) \subset \mathsf{K}(q)(V_2) = T$$

Finally put $V = V_1 \cup V_2$. □

Proposition 4.4 For $S, T \in \mathsf{K}(X)$, if $S \sqsubseteq_{\text{EM}} T$ then $S \sqsubseteq T$ in $\mathsf{K}(X)$. □

Corollary 4.5 $\sqsubseteq$ is not necessarily antisymmetric, but if X has a least element $\bot$ in this order then $\mathsf{K}^+(X)$ has a least element $\{\bot\}$.

Proof

- Let $X = \Sigma \times \Sigma$ and consider the finite sets

  $$S \stackrel{\text{def}}{=} \{\langle\bot,\bot\rangle, \langle\top,\bot\rangle, \langle\top,\top\rangle\} \qquad \text{and} \qquad T \stackrel{\text{def}}{=} \{\langle\bot,\bot\rangle, \langle\bot,\top\rangle, \langle\top,\top\rangle\}$$

  Then we have both $S \sqsubseteq_{\text{EM}} T$ and $T \sqsubseteq_{\text{EM}} S$, so by the Proposition $S \sqsubseteq T$ and $T \sqsubseteq S$ in $\mathsf{K}(X)$. However neither is a subset of the other, so they're certainly not equal.

- Any $T \in \mathsf{K}^+(X)$ is supported, *i.e.* $\exists y \in T.\bot \sqsubseteq y$, so $\{\bot\} \sqsubseteq_{\text{EM}} T$ and hence $\{\bot\} \sqsubseteq T$. □

5 Modalities

We want to derive a property of $\sqsubseteq$ on X (which is defined in terms of maps $\phi : X \to \Sigma$) from $\sqsubseteq$ on $\mathsf{K}(X)$ (which is defined in terms of $\psi : \mathsf{K}(X) \to \Sigma$). Therefore we need a way of generating computable properties of finite sets from those of elements.

Lemma 5.1 Let $\phi(x)$ be a Σ-predicate in $x \in X$. Then

$$\Diamond\,\phi(U) \stackrel{\text{def}}{=\!=} \exists u \in U.\phi(u) \quad \text{and} \quad \Box\,\phi(U) \stackrel{\text{def}}{=\!=} \forall u \in U.\phi(u)$$

are Σ-predicates in $U \in \mathsf{K}(X)$.

Proof Treating Σ as respectively an $\vee$- and an $\wedge$-semilattice, these predicates are the mediators from $\mathsf{K}(X)$, the free semilattice, of the maps $\phi : X \to \Sigma$. $\Box$

$\Box\,\phi$ concerns *inevitable* behaviour of a process (containment in Johnstone's topological setting, where he writes "$t(\phi)$") and $\Diamond\,\phi$ *possible* behaviour (non-empty intersection, "$m(\phi)$"). In the rest of our discussion of the modal operators, the predicates to which they are applied are not necessarily computable, unless explicitly stated. In fact we shall simply find $\Box_S$ a convenient abbreviation for $\forall s \in S$, and similarly $\Diamond_S$, $\Box_T$ and $\Diamond_T$, but this notation already illustrates that when we use the modal operators for several variables, we more or less end up using quantifiers anyway.

Lemma 5.2 $\Box\top = \top$, $\quad \Box(\phi \wedge \psi) = \Box\,\phi \wedge \Box\,\psi \quad$ and $\quad \Diamond \bigvee_{i \in I} \phi_i = \bigvee_{i \in I} \Diamond\,\phi_i$. $\Box$

Definition 5.3 A family $\{\phi_i : i \in I\}$ of predicates is *directed* if

- $\exists i \in I.\top$,
- $\forall i, j \in I.\exists k \in I.\phi_i \Rightarrow \phi_k \;\wedge\; \phi_j \Rightarrow \phi_k$.

In this case we write $\bigvee^{\uparrow} \phi_i$ for their join[5]. These two axioms are of course the nullary and binary forms of the more general

$$\forall U \in \mathsf{K}(I).\exists j \in I.\forall i \in U.\phi_i \Rightarrow \phi_j$$

which is shown to be equivalent by the same methods as before.

Lemma 5.4 $\Box$ is *continuous*, *i.e.* if $\{\phi_i : i \in I\}$ is a directed family of predicates then

$$\Box \bigvee^{\uparrow}_{i \in I} \phi_i = \bigvee^{\uparrow}_{i \in I} \Box\,\phi_i$$

Proof ($\Leftarrow$ follows from monotonicity of $\Box$.) For $U \in \mathsf{K}(X)$ we must show

$$\forall u \in U.\exists i \in I.\phi_i(u) \vdash \exists j \in I.\forall u \in U.\phi_j(u)$$

i.e. a "uniformity" result. For this we use the "weak axiom of finite choice" to obtain a finite set $V \subset U \times I$ such that

$$\forall u \in U.\exists i \in I.\langle u, i\rangle \in V \qquad \text{and} \qquad \forall \langle u, i\rangle \in V.\phi_i(u)$$

[5] Not necessarily a Σ-predicate.

So by the general statement of directedness of I we have $j \in I$ with

$$\forall \langle u, i \rangle \in V. \phi_i \Rightarrow \phi_j$$

So $\exists j \in I. \forall u \in U. \phi_j(u)$ as required. $\square$

Remark 5.5 It seems that the dual result, cocontinuity of $\lozenge$, can only be proved by contradiction. This is a pity, because it is what we really want to use.

Finally there are two properties which relate the two modalities:

Lemma 5.6 $\square\, \phi \wedge \lozenge\, \psi \Rightarrow \lozenge(\phi \wedge \psi)$ and $\square(\phi \vee \psi) \Rightarrow \square\, \phi \vee \lozenge\, \psi$.

Proof The first is obvious; for the second show that the set of finite sets satisfying it contains $\emptyset$ and the singletons and is closed under $\cup$. $\square$

Johnstone defines the *Vietoris locale* $\mathsf{V}(A)$ of an arbitrary locale A as the free frame generated by symbols $\{\square\, a, \lozenge\, a : a \in A\}$ subject to these six relations. He shows that this is part of a monad defined on the category of locales, and that every algebra for this monad carries a (localic) semilattice structure. However the correspondence between the Vietoris and free semilattice constructions is only exact in special cases, so we do not expect it to hold in our setting.

Lemma 5.7 $\mathsf{K}^+(X) \subset \mathsf{K}(X)$ is characterised by the imposition of either of the equivalent additional relations

$$\square \perp = \perp \qquad \text{or} \qquad \lozenge \top = \top$$

Proof The second is $\exists x \in U. \top$, which is just the definition of being inhabited, whilst the first, $\perp \iff \forall x \in U. \perp$, is clearly equivalent. $\square$

In the context of locales or Σ-predicates we do not consider negation, but of course it is defined for general predicates and we need to know how the modal operators relate to it. It is an easy exercise in natural deduction to show that $\neg\neg(\phi \wedge \psi) \iff (\neg\neg\phi) \wedge (\neg\neg\psi)$.

Lemma 5.8 $\neg \lozenge \equiv \square \neg$ and $\neg\neg \square \equiv \square \neg\neg$.

Proof The first follows immediately from the definitions as quantifiers, whilst the second holds because $\square$ is really finite conjunction. Let $L \subset \mathsf{K}(X)$ be the class of finite sets U for which $\neg\neg \square\, \phi(U) \equiv \square \neg\neg\phi(U)$. Then L contains $\emptyset$, singletons and binary unions. $\square$

6 Sigma implies not not Egli-Milner

As we said in section 2, we need an additional assumption:

$$\text{every } \phi \in \Sigma \text{ is } \neg\neg\text{-closed, } i.e.\ \neg\neg\phi \Rightarrow \phi$$

In the Effective Topos, where ϕ is of the form $\exists n. f(n) = 1$ for some $f : \mathbb{N} \to 2$, this assumption is precisely ***Markov's principle***; intuitively, it says that if a process doesn't diverge then eventually it converges. Although forcing *all* predicates $\phi \in \Omega$ to be $\neg\neg$-closed makes Ω Boolean, this condition does not even make Σ Boolean.[6]

[6] The reader is invited to find a lattice Σ of regular ("pinhole-free") open subsets of $\mathbb{R}$.

The converse argument is beset with negations, and the best way to understand them is by introducing a relation which says positively that not every property of s is shared by t:

$$x \mathrel{\sqsubseteq\!\!\!\!|}\, t \stackrel{\text{def}}{\iff} \exists\phi \in \Sigma^X.\phi(s) \wedge \neg\phi(t)$$

Clearly we have $s \mathrel{\sqsubseteq\!\!\!\!|}\, t \Rightarrow \neg(s \sqsubseteq t)$, but in fact

Lemma 6.1 $s \sqsubseteq t$ iff $\neg(s \mathrel{\sqsubseteq\!\!\!\!|}\, t)$.

Proof It is convenient to introduce $N(s) \stackrel{\text{def}}{=} \big\{\phi \in \Sigma^X : \phi(s)\big\}$, the set of *neighbourhoods* or *properties* of s. Then the right hand side is

$$\neg\exists\phi \in N(s).\neg\phi(t)$$

which, since $\neg\exists \equiv \forall\neg$, is just

$$\forall\phi \in N(s).\neg\neg\phi(t)$$

But $\phi(t) \in \Sigma$ and is by hypothesis $\neg\neg$-closed, so this is just $s \sqsubseteq t$. □

Corollary 6.2 $\sqsubseteq$ is $\neg\neg$-closed, *i.e.* $\neg\neg(S \sqsubseteq T) \Rightarrow S \sqsubseteq T$. □

Hence the best converse of section 4 we can expect is $S \sqsubseteq T \Rightarrow \neg\neg(S \sqsubseteq_{\text{EM}} T)$. It is convenient to show this in the form $\neg(S \sqsubseteq_{\text{EM}} T) \Rightarrow \neg(S \sqsubseteq T)$: a classical "argument by contradiction." Incidentally, all functions reflect $\mathrel{\sqsubseteq\!\!\!\!|}$, but the best transitivity result we have is

$$x \mathrel{\sqsubseteq\!\!\!\!|}\, z \Rightarrow \forall y.\neg\neg(x \mathrel{\sqsubseteq\!\!\!\!|}\, y \vee y \mathrel{\sqsubseteq\!\!\!\!|}\, z)$$

We introduce

$$S \not\sqsubseteq_{\text{EM}} T \stackrel{\text{def}}{\iff} \exists s \in S.\forall t \in T.s \mathrel{\sqsubseteq\!\!\!\!|}\, t \quad \vee \quad \exists t \in T.\forall s \in S.s \mathrel{\sqsubseteq\!\!\!\!|}\, t$$

Suppose informally that the first disjunct holds for a particular $s \in S$. Writing $T = \{t_1, \ldots, t_m\}$, there are computable predicates $\phi_j \in \Sigma^X$ such that $\phi_j(s)$ but $\neg\phi_j(t_j)$. Then with $\phi = \phi_1 \wedge \cdots \wedge \phi_m$ we have $\phi(s)$ but $\neg\exists t \in T.\phi(t)$. Then $\psi = \Diamond\,\phi$ is satisfied by S but not by T. The other part is similar, with ϕ as the disjunction and $\Box\,\phi$. More formally,

Lemma 6.3 If $S \not\sqsubseteq_{\text{EM}} T$ then $S \mathrel{\sqsubseteq\!\!\!\!|}\, T$.

Proof The first predicate (fixing s) is

$$\Box_T \bigvee\!\!\!\uparrow_{\phi \in N(s)} \neg\phi(T) \iff \bigvee\!\!\!\uparrow_{\phi \in N(s)} \Box_T\,\neg\phi(T) \iff \bigvee\!\!\!\uparrow_{\phi \in N(s)} \neg\Diamond_T\,\phi(T)$$

by continuity of $\Box$ and then $\Box\,\neg \equiv \neg\,\Diamond$. Recall that the former used the weak axiom of finite choice, and it is easy to check that $N(s)$ is a filter. Then

$$\exists\phi \in \Sigma^X.\exists s \in S.\phi(s) \wedge \neg\,\Diamond\,\phi(T)$$

whence the result follows by putting $\psi = \Diamond\,\phi$.

Using the ideal

$$M(t) \stackrel{\text{def}}{=} \big\{\phi \in \Sigma^X.\neg\phi(t)\big\}$$

the second predicate (fixing t) is

$$\Box_S \bigvee^{\uparrow}_{\phi\in M(t)} \phi(S) \iff \bigvee^{\uparrow}_{\phi\in M(t)} \Box_S\, \phi(S)$$

Then

$$\exists\phi \in \Sigma^X.\exists t \in T.\neg\phi(t) \wedge \Box_S\, \phi(S)$$

from which we deduce $\neg\,\Box\,\phi(T) \wedge \Box\,\phi(S)$, so we put $\psi = \Box\,\phi$. $\Box$

A classical argument would now be complete, but we have to reason constructively, and negation is a delicate thing, so there is more work to be done and we must be careful. The negated Egli-Milner relations do not behave quite as well as $\not\sqsubseteq$, but we do have

Lemma 6.4 $\neg(S \not\sqsubseteq_{\mathrm{EM}} T)$ iff $\neg\neg(S \sqsubseteq_{\mathrm{EM}} T)$.

Proof $\neg(S \not\sqsubseteq_{\mathrm{EM}} T)$ is of the form

$$\neg\,\Diamond_S\,\Box_T\, s \not\sqsubseteq t \quad \wedge \quad \neg\,\Diamond_T\,\Box_S\, s \not\sqsubseteq t$$

whilst, by the first lemma, we have already expressed $\neg\neg(S \sqsubseteq_{\mathrm{EM}} T)$ in the form

$$\neg\neg\,\Box_S\,\Diamond_T\,\neg s \not\sqsubseteq t \quad \wedge \quad \neg\neg\,\Box_T\,\Diamond_S\,\neg s \not\sqsubseteq t$$

Then

$$\neg\,\Diamond\,\Box \equiv \Box\,\neg\,\Box \equiv \Box\,\neg\neg\neg\,\Box \equiv \Box\,\neg\,\Box\,\neg\neg \equiv \Box\,\neg\neg\,\Diamond\,\neg \equiv \neg\neg\,\Box\,\Diamond\,\neg$$

from the relationships between modal operators and negation.[7] $\Box$

Theorem 6.5 $S \sqsubseteq T$ iff $\neg\neg(S \sqsubseteq_{\mathrm{EM}} T)$.

Proof We have shown that

$$S \sqsubseteq T \iff \neg(S \not\sqsubseteq T) \Rightarrow \neg(S \not\sqsubseteq_{\mathrm{EM}} T) \iff \neg\neg(S \sqsubseteq_{\mathrm{EM}} T) \Rightarrow \neg\neg(S \sqsubseteq T) \iff S \sqsubseteq T$$

$\Box$

7 Bibliography

J.L. Bell Toposes and local set theories, Oxford logic guides 14, Oxford University Press, 1988.

M.P. Fourman, The Logic of Topoi, in: J. Barwise, ed., Handbook of Mathematical Logic, North-Holland, 1977, 1053–1090.

M. Hennessy and G.D. Plotkin, Full Abstraction for a Simple Parallel Programming Language, in J. Becvar, ed., Proc. MFCS, Lecture Notes in Computer Science 74, Springer, 1979, 108–120.

R. Hindley and J. Seldin, eds., To H.B. Curry: essays in combinatory logic, lambda calculus and formalisms, Academic Press, 1980

J.M.E. Hyland, The effective topos, in: A.S. Troelstra & D. van Dalen,, eds., Brouwer centenary symposium, North Holland, 1982.

[7]This formula, though terse and unorthodox, precisely captures the active part of the argument.

J.M.E. Hyland, P.T. Johnstone and A.M. Pitts, Tripos theory, Proc. Camb. Philos. Soc. 88 (1980) 205–232.

P.T. Johnstone, Topos Theory, Acedemic Press, 1977.

P.T. Johnstone, Stone Spaces, Cambridge studies in advanced mathematics 3, Cambridge University Press, 1983.

P.T. Johnstone, The Vietoris Monad on the Category of Locales, in: R.-E. Hoffmann, ed., Continuous Lattices and Related Topics, Universität Bremen Mathematik-Arbeitspapier 27 (1982) 162–179.

A. Kock, Synthetic differential geometry, LMS lecture notes, Cambridge University Press, 1981.

J. Lambek, From λ-calculus to cartesian closed categories, in: Hindley & Seldin.

J. Lambek and P.J. Scott, Introduction to higher order categorical logic, Cambridge studies in advanced mathematics 7, Cambridge University Press, 1986.

M. Makkai and G. Reyes, First order categorical logic, Lecture notes in Mathematics 611, Springer, 1977.

W.K.-S. Phoa, Effective Domains and Intrinsic Structure, in: Logic in Computer Science (Philadelphia, 1990), to appear.

G.D. Plotkin, A Powerdomain Construction, SIAM J. Comp. 5 (1976) 452–487.

G.D. Plotkin, Dijkstra's predicate transformers and Smyth's powerdomain, in: D. Bjørner, ed., Abstract Software, Lecture Notes in Computer Science 86, Springer, 1979.

E.P. Robinson, A Modal Language for Power-Domains, manuscript.

E.P. Robinson, Powerdomains, Modalities and the Vietoris Monad, Cambridge University Computer Laboratory Technical Report 98, 1986.

G. Rosolini, Continuity and effectiveness in topoi, Ph. D. thesis, Carnegie-Mellon University, 1986.

G. Rosolini, Categories and effective computation, in: D. Pitt, ed., Category Theory and Computer Science (Edinburgh, 1987), Lecture Notes In Computer Science 240, Springer, 1987.

D.S. Scott, Relating theories of the λ-calculus, in Hindley & Seldin.

M.B. Smyth, Powerdomains and Predicate Transformers: a Topological view, in: J. Diaz, ed., Automata, Languages and Programming, Lecture Notes in Computer Science 154, Springer, 1983, 662–675.

S.J. Vickers, Topology *via* Logic, Cambridge University Press, 1989.

G. Winskel, Note on Powerdomains and Modality, Theor. Comp. Sci. 36 (1985) 127–137.