Semilattices, Domains, and Computability

Dana S. Scott

University Professor Emeritus
Carnegie Mellon University
Visiting Scholar
University of California, Berkeley
Visiting Fellow
Magdalen College, Oxford, Trinity Term 2010
Visiting Lecturer
University of Edinburgh, July 2010

Algebraic Lattices:
The Prime Examples

- The ***powerset*** of a set.
- The lattice of ***subgroups*** of a group.
- The lattice of ***ideals*** of a ring.

What is a Lattice?

$0 \leq x \leq 1$ — **Bounded**

$x \leq x$

$x \leq y \;\&\; y \leq z \Rightarrow x \leq z$

$x \leq y \;\&\; y \leq x \Rightarrow x = y$

Partially Ordered Set

$x \vee y \leq z \Leftrightarrow x \leq z \;\&\; y \leq z$

$z \leq x \wedge y \Leftrightarrow z \leq x \;\&\; z \leq y$

With sups & With infs

What is a Semilattice?

$0 \leq x \leq 1$	**Bounded**
$x \leq x$	**Partially**
$x \leq y \,\&\, y \leq z \Rightarrow x \leq z$	**Ordered**
$x \leq y \,\&\, y \leq x \Rightarrow x = y$	**Set**
$x \vee y \leq z \Leftrightarrow x \leq z \,\&\, y \leq z$	**With sups**

What is a Complete Semiattice?

$$\bigvee_{i\in I} x_i \leq y \Leftrightarrow (\forall i \in I)\ x_i \leq y$$

What is a Complete Lattice?

$$y \leq \bigwedge_{i\in I} x_i \Leftrightarrow (\forall i \in I)\ y \leq x_i$$

Note: A complete semilattice is a complete lattice:

$$\bigwedge_{i\in I} x_i = \bigvee \{y \mid (\forall i \in I)\ y \leq x_i\}$$

The Equational Axiomatization of Semilattices

$$0 \vee x = x \qquad 1 \vee x = 1 \qquad x \vee x = x$$

$$x \vee y = y \vee x$$

$$x \vee (y \vee z) = (x \vee y) \vee z$$

Definition: $x \leq y \Leftrightarrow x \vee y = y$

Algebraic Lattices:
The Abstract Definition

Definition: An element u of a complete lattice is ***finite*** (or, ***compact***) provided that whenever we have $u \leq \bigvee_{i\in I} x_i$, then $u \leq \bigvee_{i\in J} x_i$ for some ***finite*** $J \subseteq I$.

Definition: A complete lattice is ***algebraic*** iff every element is the sup of its finite subelements.

Note: **The finite elements of the lattice of subgroups of a group are exactly the finitely generated subgroups. And the lattice is thus algebraic.**

Semilattice Completion

Theorem: The finite elements of a complete lattice form a subsemilattice — provided the unit element is finite.

Definition: The ***ideals*** of semilattice are the subsets closed under finite sups and subelements.

Theorem: The ideals of semilattice form an algebraic lattice with a finite unit element.

Theorem: Every algebraic lattice with a finite unit element is isomorphic to the ideal lattice of its semilattice of finite elements.

Topological Connections

Theorem: Every algebraic lattice becomes a ***T_0-topological space*** with a basis for the open sets consisting of sets $\uparrow u = \{ x \mid u \leq x \}$ for u finite.

Theorem: The lattice of open subsets of the ***Cantor Discontinuum*** is an algebraic lattice with the finite elements being the compact opens.

Theorem: The ***continuous functions*** between algebraic lattices are exactly the functions preserving ***directed sups***. They can also be characterized by the equation:

$$F(x) = \bigvee \{ F(u) \mid u \leq x \ \&\ u \text{ finite} \}.$$

What are Scott-Ershov Domains?

Definition: A ***domain*** is an algebraic lattice ***minus*** a finite unit; ***equivalently ...***

A ***domain*** is any ***closed subset*** of an algebraic lattice; ***equivalently ...***

A ***domain*** is the completion of a semilattice by ***proper ideals***.

Note: Every algebraic lattice is a domain.

(Hint: Add an extra unit element at the top.)

Theorem: Domains form a ***category*** with the continuous functions as the ***mappings***.

Back to Semilattices!

Definition: For $\mathcal{A} = \langle A, 0, 1, \vee \rangle$ a given semilattice,

let $||\mathcal{A}||$ be the set of ***proper ideals*** of $\mathcal{A}$; that is,

$||\mathcal{A}|| = \{X \subseteq A \mid 0 \in X \,\&\, 1 \notin X \,\&\, \forall a,b \in A[a,b \in X \Leftrightarrow a \vee b \in X]\}$.

Theorem: $||\mathcal{A}||$ is a domain with finite elements of the form

$\downarrow a = \{x \in A \mid a \vee x = a\}$; if additionally, $\mathcal{A}$ satisfies

$$\forall a,b \in A[a = 1 \text{ or } b = 1 \Leftrightarrow a \vee b = 1],$$

then $||\mathcal{A}||$ is an algebraic lattice.

Note: Intuitively 0 indicates no information and 1 too much information or an inconsistency.

The Countable Case

Theorem: The completion $||\mathcal{A}||$ of a ***countable*** semilattice $\mathcal{A} = \langle A, 0, 1, \vee \rangle$ can be thought of as adding ***limit points*** to $\mathcal{A}$ of increasing sequences $a_0 \leq a_1 \leq a_2 \leq \ldots \leq a_n \leq \ldots$ of elements of A, where we define $\mathbf{lim}_{n\to\infty}\, a_n \leq \mathbf{lim}_{m\to\infty}\, b_m$ to mean that ***each*** a_n ***is*** $\leq$ ***some*** b_m.

Note: **Of course, limits prove to be sups in $||\mathcal{A}||$, and we can identify the elements of A with the limits of the constant sequences. However, from this point of view, in order to prove that $||\mathcal{A}||$ is (directed) complete, it is probably easier to relate limits to ideals.**

A Universal Semilattice

Definition: Let $\mathcal{P} = \langle P, 0, 1, \vee \rangle$ be the ***semilattice*** of (equivalence classes of) ***propositional formulae*** with generators $\xi_0, \xi_1, \xi_2, \ldots, \xi_n, \ldots$.

Note: **We will use the usual notation for other propositional operators, so $\mathcal{P}$ may also be considered a Boolean algebra.**

Theorem: $\|\mathcal{P}\|$ as a domain is isomorphic to the domain of ***proper open subsets*** of the Cantor set.

Main Theorem: ***Every*** domain with a countable number of finite elements can be ***isomorphically embedded*** into $\|\mathcal{P}\|$.

Outline of a Proof

Theorem: Every ***countable Boolean algebra*** can be isomorphically embedded into $\mathcal{P}$.

Hint: It is easy to show that a finite Boolean algebra can be embedded into $\mathcal{P}$. And then the embedding can be continued to any finite superalgebra. Next note that a countable algebra is the union of a countable chain of finite algebras.

Theorem: Every ***countable semilatice*** can be isomorphically embedded into $\mathcal{P}$.

Hint: Every semilattice $\mathcal{A} = \langle A, 0, 1, \vee \rangle$ can be embedded into the powerset lattice of $A \backslash \{1\}$ by the mapping $\rho(a) = \{x \mid a \not\leq x\}$.

Theorem: If a semilattice $\mathcal{A}$ is a subsemilattice of a semilattice $\mathcal{B}$, then $\|\mathcal{A}\|$ is a ***subdomain*** of $\|\mathcal{B}\|$.

Simplifying the Notation

(Step 1) $<P, 0, 1, \vee>$ is the semilattice of ***propositional formulae*** with generators $\xi_0, \xi_1, \xi_2, \ldots, \xi_n, \ldots$.

(Step 2) $\mathbb{S}$ is the family of all ***subsemilattices*** of P ; thus

$$\mathbb{S} = \{A \subseteq P \mid 0,1 \in A \;\&\; \forall a,b \in A [a \vee b \in A]\}.$$

Note: $\mathbb{S}$ is an algebraic lattice with a countable number of finite elements. (Why?)

(Step 3) For $A \in \mathbb{S}$, let $\|A\| = \{\downarrow(X \cap A) \mid X \in \|\mathcal{P}\|\}$.

Note: $\|A\|$ is a subdomain of $\|P\| = \|\mathcal{P}\|$, and every countably based domain is isomorphic one such. The semilattice structure of $\|P\|$ is defined by $X \vee Y = \{x \vee y \mid x \in X \;\&\; y \in Y\}$.

Gödel Numbering & Pairing

Theorem. There is a numbering of the elements of P so that all Boolean operations are ***primitive recursive***.

Theorem. Under this numbering, there is a primitive recursive ***pairing operation*** $\langle\!\langle p,q \rangle\!\rangle$ on P with a recursive range where:

(i) $\langle\!\langle 0,0 \rangle\!\rangle = 0$;

(ii) $\langle\!\langle p,q \rangle\!\rangle = 1 \Leftrightarrow p = 1$ or $q = 1$;

(iii) $\langle\!\langle p_0,q_0 \rangle\!\rangle \vee \langle\!\langle p_1,q_1 \rangle\!\rangle = \langle\!\langle p_0 \vee p_1, q_0 \vee q_1 \rangle\!\rangle$;

(iv) $\langle\!\langle p_0,q_0 \rangle\!\rangle \leq \langle\!\langle p_1,q_1 \rangle\!\rangle \Leftrightarrow p_1 = 1$ or $q_1 = 1$ or $[p_0 \leq p_1$ & $q_0 \leq q_1]$.

Hint: Define Boolean injections $\sigma_0, \sigma_1 : P \rightarrowtail P$ **by** $\sigma_0(\xi_n) = \xi_{2n}$ **and** $\sigma_1(\xi_n) = \xi_{2n+1}$. **Then define** $\langle\!\langle p,q \rangle\!\rangle = \sigma_0(p) \vee \sigma_1(q)$.

Another Construction of $\mathcal{P}$

(Step 1) For any set S, let $F(S)$ denote the collection of all the ***finite subsets*** of S.

(Step 2) $F(S)$ may be regarded as a ***vector space*** over the field {0,1}, where the ***zero vector***, 0, is the empty set, and where ***vector addition***, +, is the symmetric difference of sets.
A ***basis*** for the space $F(S)$ consists of the singleton subsets.

(Step 3) Let $P = F(F(\mathbb{N}))$, and define a ***bilinear multiplication*** on P by the stipulation $\{s\}\cdot\{t\} = \{s \cup t\}$ for $s,t \in F(\mathbb{N})$. Let $1 = \{0\}$.

Theorem: The algebra $\langle P, 0, 1, +, \cdot \rangle$ is the ***free Boolean ring*** (with unit) on the generators $\{\{n\}\}$ for $n \in \mathbb{N}$. It can be made into a semilattice by defining $x \vee y = x + y + x\cdot y$.

Note: **Using $P = F(F(\mathbb{N}))$ gives us another Gödel numbering.**

Computable Domains and Mappings

Definition. The ***computable*** elements of $\mathbb{S}$ are those which are ***recursively enumerable*** subsets of P.

Definition. The ***computable*** elements of $||A||$ are those which are ***recursively enumerable*** subsets of P.

Definition. The ***computable*** mappings $F{:}||A||\rightarrow||B||$ are those which are continuous and where the relationship $\downarrow b \subseteq F(\downarrow a)$ between finite elements of $||A||$ and $||B||$ is ***recursively enumerable***.

Domain Products

Definitions. (i) $X \times Y = \{\langle\!\langle p,q \rangle\!\rangle \mid p \in X \ \&\ q \in Y\}$;

(ii) $H = \{\langle\!\langle p,q \rangle\!\rangle \mid [p = 0 \ \&\ q = 0] \text{ or } [p \neq 0 \ \&\ q \neq 0]\}$;

(iii) $A \times_s B = (A \times B) \cap H$.

Lemma. (i) If $A, B \in \mathbb{S}$, then $H, (A \times B), (A \times_s B) \in \mathbb{S}$.

(ii) If $X, Y \in \|P\|$, then $(X, Y) = \downarrow(X \times Y) \in \|P\|$.

Theorem. If $A, B \in \mathbb{S}$, then $\|A \times B\|$ is isomorphic to the ***product*** of the domains $\|A\|$ and $\|B\|$, while $\|A \times_s B\|$ is isomorphic to the ***smash product***.

Hint: Let $X = \{p \mid \langle\!\langle p,0 \rangle\!\rangle \in Z\}$ and $Y = \{q \mid \langle\!\langle 0,q \rangle\!\rangle \in Z\}$, for any $Z \in \|A \times B\|$. Then $X \in \|A\|, Y \in \|B\|$, and $\downarrow(X \times Y) = Z$.

Domain Sums

Definition. Let $\zeta_n = \neg\xi_0 \vee \neg\xi_1 \vee \neg\xi_2 \vee \ldots \vee \neg\xi_{n-1} \vee \xi_n$.

Definition.

$$A_0 + A_1 + A_2 + \ldots + A_n = \{0\} \cup \bigcup_{i \leq n} \{ \langle\!\langle p, \zeta_i \rangle\!\rangle \mid p \in A_i \}.$$

Definition.

$$A_0 +_c A_1 +_c A_2 +_c \ldots +_c A_n = (A_0 + A_1 + A_2 + \ldots + A_n) \cap H.$$

Theorem. For $A_0, A_1, A_2, \ldots, A_n \in \mathbb{S}$, $\|A_0 + A_1 + A_2 + \ldots + A_n\|$ is isomorphic to the ***separated sum*** of the domains $\|A_i\|$.

Theorem. For $A_0, A_1, A_2, \ldots, A_n \in \mathbb{S}$, $\|A_0 +_c A_1 +_c A_2 +_c \ldots +_c A_n\|$ is isomorphic to the ***coalesced sum*** of the domains $\|A_i\|$.

Lifting and Dropping

Definitions. (i) $A_\perp = \{0\} \cup \{ \langle\!\langle p, 0 \rangle\!\rangle \vee \xi_1 \mid p \in A \}$.

(ii) $A^\top = \{1\} \cup \{ \langle\!\langle p, 0 \rangle\!\rangle \wedge \xi_1 \mid p \in A \}$.

Theorem. For $A \in \mathbb{S}$, we have $A_\perp, A^\top \in \mathbb{S}$, and the domain $\|A_\perp\|$ is like $\|A\|$ but with a ***new bottom element***, and $\|A^\top\|$ is like $\|A\|$ but with a ***new top element***.

Note: **All the operations of products, sums, lifts and drops on $\mathbb{S}$ need to be checked for continuity and computability.**

Function Spaces

Theorem. Under the numbering of P, there is a primitive recursive operation $(p \Rightarrow q)$ on P, defined when $p \neq 1$, such that:

(i) $(p \Rightarrow 1) = 1$;

(ii) $\bigvee_{i<k} (p_i \Rightarrow q_i) = 1 \;\Rightarrow\; \exists r \neq 1.\ \bigvee\{q_i \mid p_i \leq r\} = 1$; and

(iii) $(r \Rightarrow s) \leq \bigvee_{i<k} (p_i \Rightarrow q_i) \Leftrightarrow \bigvee_{i<k} (p_i \Rightarrow q_i) = 1$ or $s \leq \bigvee\{q_i \mid p_i \leq r\}$.

Definitions.

(i) $(A \Rightarrow B) = \{\bigvee_{i<k}(p_i \Rightarrow q_i) \mid \forall i < k\,[p_i \in A \backslash \{1\}\ \&\ q_i \in B]\}$;

(ii) $(A \Rightarrow_S B) = \{0,1\} \cup \{\bigvee_{i<k}(p_i \Rightarrow q_i) \mid \forall i < k\,[p_i \in A \backslash \{0,1\}\ \&\ q_i \in B \backslash \{0,1\}]\}$;

Theorem. If $A, B \in \mathbb{S}$, then $(A \Rightarrow B), (A \Rightarrow_S B) \in \mathbb{S}$, and $||A \Rightarrow B||$ is isomorphic to the domain of ***continuous functions*** from $||A||$ to $||B||$ and $||A \Rightarrow_S B||$ gives ***strict continuous functions***.

Embedding $\mathbb{S}$ into $\|P\|$

Note: The finite elements of $\mathbb{S}$ are the finite subsemilattices of P, and P is the (non-finite) unit element of $\mathbb{S}$. The semilattice operation on $\mathbb{S}$ is $A \vee B$.

Lemma. For finite $A, B \in \mathbb{S}$, we have

(i) $\bigvee_{p \in A \setminus \{1\}} (p \Rightarrow p) = \bigvee_{q \in B \setminus \{1\}} (q \Rightarrow q) \Leftrightarrow A = B$; and

(ii) $\bigvee_{r \in (A \vee B) \setminus \{1\}} (r \Rightarrow r) = \bigvee_{p \in A \setminus \{1\}} (p \Rightarrow p) \vee \bigvee_{q \in B \setminus \{1\}} (q \Rightarrow q)$.

Theorem. The domain $\mathbb{S}$ is isomorphic to a subdomain of $\|P \Rightarrow_S P\|$ by a computable embedding.

Recursive Domain Equations

Theorem. All the operations $(A \times B)$, $(A \times_s B)$, $(A + B)$, $(A +_c B)$, $A_\perp$, $A^\top$, $(A \Rightarrow B)$, and $(A \Rightarrow_s B)$ map $\mathbb{S}$ to $\mathbb{S}$ and are ***continuous and computable***. Hence, so are any ***compositions*** of these mappings.

Note: **The standard Fixed-Point Theorem can then be applied to obtain recursively defined domains.**

Definition. $\mathbb{N}_\perp = \{0,1\} \cup \{\zeta_n \mid n \in \mathbb{N}\}$.

Theorem. $\mathbb{N}_\perp \in \mathbb{S}$, and $\| \mathbb{N}_\perp \|$ is isomorphic to the ***flat domain of integers***.

Note: **A typical example of a recursively defined domain is given by $D = \mathbb{N}_\perp +_c (D \Rightarrow D)_\perp$. This constructs a model of the λ-calculus closely related to recursive function theory.**

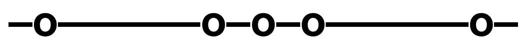
Some Additional Examples

Potentially infinite:

$B = B + B$ binary sequences

$S = \mathbb{N}_\bot \times_s S_\bot$ sequences of integers

$L = \mathbb{N}_\bot \times_s (L \times L)_\bot$ labelled trees



Another lambda-calculus domain:

$A =$ given

$B = B \times (A \times B)$ fixed point

$C = A \times B \cong (A \times B) \times (A \times B) = C \times C$ defined & isomorphed

$D = D \Rightarrow C$ fixed point

$D \times D = (D \Rightarrow C) \times (D \Rightarrow C) \cong D \Rightarrow (C \times C) \cong D \Rightarrow C = D$ isomorphism

$D \Rightarrow D = D \Rightarrow (D \Rightarrow C) \cong (D \times D) \Rightarrow C \cong D \Rightarrow C = D$ isomorphism

$\|P\|$ as a λ-Calculus Model

Definitions.

(i) $\mathbf{Id}(Z) = \downarrow\{\bigvee_{i<k} q_i \mid \forall i<k[q_i \in Z]\}$; and

(ii) $F(X) = \mathbf{Id}(\{q \mid (p \Rightarrow q) \in F \;\&\; p \in X\})$; and

(iii) $\lambda X.\Phi(X) = \mathbf{Id}(\{(p \Rightarrow q) \mid q \in \Phi(\downarrow p) \;\&\; p \neq 1\})$, where

$F, X \in \|P\|$ and $\Phi : \|P\| \rightarrow \|P\|$ is continuous.

Note: **It is possible that $\mathbf{Id}(Z) = P$, if Z is inconsistent.**

However, for F, X, Φ as above, both

$F(X)$ and $\lambda X.\Phi(X)$ are consistent.

Equilogical Spaces

Remember: • The space $||P||$ is not only universal for domains, but it contains as subspaces all countably based T_0-spaces.

• Moreover, by passing to partial equivalence relations (PERs) and equivalence-preserving continuous mappings, we obtain a cartesian closed category (and more).

• It contains the two previous categories and has an intrinsic notion of computable function and computable element. (But a certain subcategory may be better.)

• In this way we have a semantics for a notion of computability at higher types.

Martin-Löf Type Theory

Definition. A ***family of types*** consists of a PER $\mathcal{A}$ and a mapping $\mathcal{B} : ||P|| \to$ PER, where for all $X_0, X_1 \in ||P||$ we have

$$X_0 \; \mathcal{A} \; X_1 \Rightarrow \mathcal{B}(X_0) = \mathcal{B}(X_1).$$

Definition. A ***product*** of a family of types is the PER defined by:

$$F_0 \, (\prod X{:}\mathcal{A}.\, \mathcal{B}(X)) \; F_1 \Leftrightarrow \forall \, X_0, X_1 [X_0 \; \mathcal{A} \; X_1 \Rightarrow F_0(X_0) \; \mathcal{B}(X_0) \; F_1(X_1) \,].$$

Definition. A ***sum*** of a family of types is the PER defined by:

$$Z_0 \, (\sum X{:}\mathcal{A}.\, \mathcal{B}(X)) \; Z_1 \Leftrightarrow \exists \; X_0, X_1, Y_0, Y_1 [\, X_0 \; \mathcal{A} \; X_1 \;\&\; Y_0 \; \mathcal{B}(X_0) \; Y_1 \;\&$$

$$Z_0 = (X_0, Y_0) \;\&\; Z_1 = (X_1, Y_1) \,].$$

Note: It must be proved that these definitions actually do produce PERs.

Systems of Dependent Types

Theorem. Given families of types where always

$$X_0 \mathcal{A} X_1 \Rightarrow \mathcal{B}(X_0) = \mathcal{B}(X_1) \text{ and}$$

$$X_0 \mathcal{A} X_1 \;\&\; Y_0 \mathcal{B}(X_0) Y_1 \Rightarrow \mathcal{C}(X_0,Y_0) = \mathcal{C}(X_1,Y_1) \text{ and}$$

$$X_0 \mathcal{A} X_1 \;\&\; Y_0 \mathcal{B}(X_0) Y_1 \;\&\; Z_0 \mathcal{C}(X_0,Y_0) Z_1 \Rightarrow \mathcal{D}(X_0,Y_0,Z_0) = \mathcal{D}(X_1,Y_1,Z_1),$$

then this ***iterated*** products of sums of ... is a PER:

$$\prod X{:}\mathcal{A}. \sum Y{:}\ \mathcal{B}(X). \prod Z{:}\ \mathcal{C}(X,Y).\ \mathcal{D}(X,Y,Z).$$

Note: Of course, properties of sums and products have to be established showing they follow the usual rules of type theory.

Extensional Identity Types

Definition. Given a PER $\mathcal{A}$ we define:

$$U \ \mathrm{Id}_{\mathcal{A}}(X,Y) \ V \Leftrightarrow U \ \mathcal{A} \ X \ \mathcal{A} \ Y \ \mathcal{A} \ V \ .$$

Proposition. Given a PER $\mathcal{A}$, then $\mathrm{Id}_{\mathcal{A}}(X,Y)$ is a PER and

$$X_0 \ \mathcal{A} \ X_1 \ \& \ Y_0 \ \mathcal{A} \ Y_1 \Rightarrow \mathrm{Id}_{\mathcal{A}}(X_0,Y_0) = \mathrm{Id}_{\mathcal{A}}(X_1,Y_1).$$

Example: **In case** $F \ (\prod X{:}\mathcal{A}. \prod Y{:}\mathcal{A}. \ \mathcal{A}) \ F$**, we can regard** F **as a binary operation of type** $\mathcal{A}$**. Then, if the following type is inhabited, we can say** F **is an associative operation:**

$$\prod X{:}\mathcal{A}. \prod Y{:}\mathcal{A}. \prod Z{:}\mathcal{A}. \ \mathrm{Id}_{\mathcal{A}}(\ F(F(X)(Y))(Z), \ F(X)(F(Y)(Z)) \ ).$$

Why Domain Theory?

The aim of Domain Theory is:

(a) To provide one convenient category having many familiar examples;

(b) To permit some new space constructions, including function spaces;

(c) To allow for the solution of recursive domain equations, including for the λ-calculus; and

(d) To give one sound basis for some notions of higher-type computability.

Why Semilattices?

Semilattice theory:

(a) Has a very elementary definition;

(b) Has a universal space with very easy computable structure;

(c) Has a very direct way to pass to completions; and

(d) Has a category construction needing a minimum of set theory and abstract algebra.

THE END

dana.scott@cs.cmu.edu

[redacted]