STONE DUALITY IN UNEXPECTED PLACES

Michael Mislove*
Tulane University

Oxford Duality Workshop
June 2012

*: Work supported by the US ONR

OVERVIEW

- Domains as computational models
  - *de facto* models for programming semantics
  - Many CCCs, can model most constructs
  - Applications outside programming language semantics
    - Useful tools for topology, fractal geometry, integration…

- Probabilistic computation is a problem
  - *Probabilistic power domain* forms monad, but no known invariant CCC
  - No distributive law wrt *power domains* - nondeterminism models

- Alternative model of *random variables*
  - *Coin algebra domain* yields monad on *BCD (Goubault-Larrecq & Varacca)*
  - Side-steps issues around probabilistic power domain

- *Stone duality* reveals structure of random variable monad
  - Applicable to probabilistic transition systems
  - Classical & quantum information

DOMAINS

Directed Complete Partial Orders (DCPOs)

- Partial orders in which directed sets have suprema
- Maps preserve sups of directed sets
- Scott Topology:

$$U \text{ Scott open iff } U = \uparrow U \;\&\; \sup D \in U \Rightarrow D \cap U \neq \emptyset$$

- Scott continuous maps are exactly those preserving directed suprema
- DCPO is a CCC with products, sums, etc.

Domains support *approximation:* $x \ll y$ iff $y \leq \sup D \Rightarrow x \leq d \in D$

- Domain: $\downarrow y = \{ x \mid x \ll y \}$ directed & $y = \sup \downarrow y \quad (\forall y)$
- *Examples:*
  - A any set $\Rightarrow A^\infty = A^* \cup A^\omega$; $s \ll t$ iff s is finite
  - X locally compact $\Rightarrow (\{C \subseteq X \mid C \text{ compact}\}, \supseteq)$; $C \ll C'$ iff $C' \subseteq C^\circ$
- DOM - Not a CCC ; has many CCC full subcategories

FUNDAMENTAL APPLICATION

Lambda Calculus - prototypical programming language

(Lambek) Models of typed lambda calculus are cartesian closed categories.
(Scott) Models of the un- / uni-typed lambda calculus are *reflexive objects* in CCCs

$$[X \to X] \rightarrowtail X \twoheadrightarrow [X \to X]$$

- Fixed point combinator implies models have fixed point property

Scott's $D_\infty \cong [D_\infty \to D_\infty]$*-Model:* Lives in category of (embedding) (T_0-)injective spaces

- Every T_0-space is embeddable in a power of Sierpinski space
- *Continuous lattices* are retracts of powers of Sierpinski space
- D_∞*-Model* obtained as *bilimit* if such spaces

Moggi's (Strong) Monadic Semantics over *C, a* CCC of domains

- Monads on *C* give meaning to *computational effects*, nondeterminism, etc.
- Want monads to compose - requires *distributive law* (Beck)

PROBABILITY AND COMPUTATION

Probability arises in many places:

- Randomized algorithms
  - Prime testing

- Stochastic process calculi
  - Include probabilistic choice $P +_{1/2} Q$, etc.
  - Useful in specification and verification
  - Models for Systems Biology

- Cryptography and crypto-protocols
  - One-way and trap-door functions
    - Lead to probabilistic reasoning about chances of finding key
  - Crypto-protocols employ random choices
    - Also involve *nondeterminism*

- Classical and quantum information

DOMAINS AND PROBABILITY

Modeled by *Valuations:* $\mu : O(X) \to [0,1]$ satisfying:

i) $\mu(\varnothing) = 0$

ii) $\mu(U \cup V) + \mu(U \cap V) = \mu(U) + \mu(V)$

iii) $U \leq V \Rightarrow \mu(U) \leq \mu(V)$, and

iv) D directed $\Rightarrow \mu(\bigcup D) = \sup \{ \mu(U) \mid U \in D \}$

$V(X)$ - valuations in pointwise order;

$V_1(X)$ - valuations with total mass 1 - probability measures on X

Theorem (Lawson) Valuations on distributive continuous lattices correspond to Borel measures

Jones' Splitting Lemma: All valuations are directed sups of *simple valuations* $\sum r_i \, \delta_{x_i}$

- Simple valuations on a domain form a basis

V and V_1 form monads on DCPO & DOM

THE MONAD THAT WON'T PLAY NICE

Problems: - *No known V-invariant CCC of domains*
- *No distributive law for V and any nondeterminism monad* (N.D. Gautam. 1957)

Solutions:

Do nothing: (Morgan, *et al,* 1992) Added probabilistic choice to CSP models
Result: Nondeterministic choice is no longer idempotent.

Form monad from composition: (M, 2000; Tix, 2000; Keimel, Plotkin & Tix, 2005)
$Pow_X = \langle P_X \circ V \rangle$ yields monad where all laws of each still hold.

- Probabilistic choice and nondeterministic choice are related.
- P_L and P_U take *COH* into *BCD*, the CCC of bounded complete domains.
  So, Pow_L and Pow_U leave *BCD* invariant.
- *Question:* Is *RB* or *FS* an exponential ideal of *COH?*

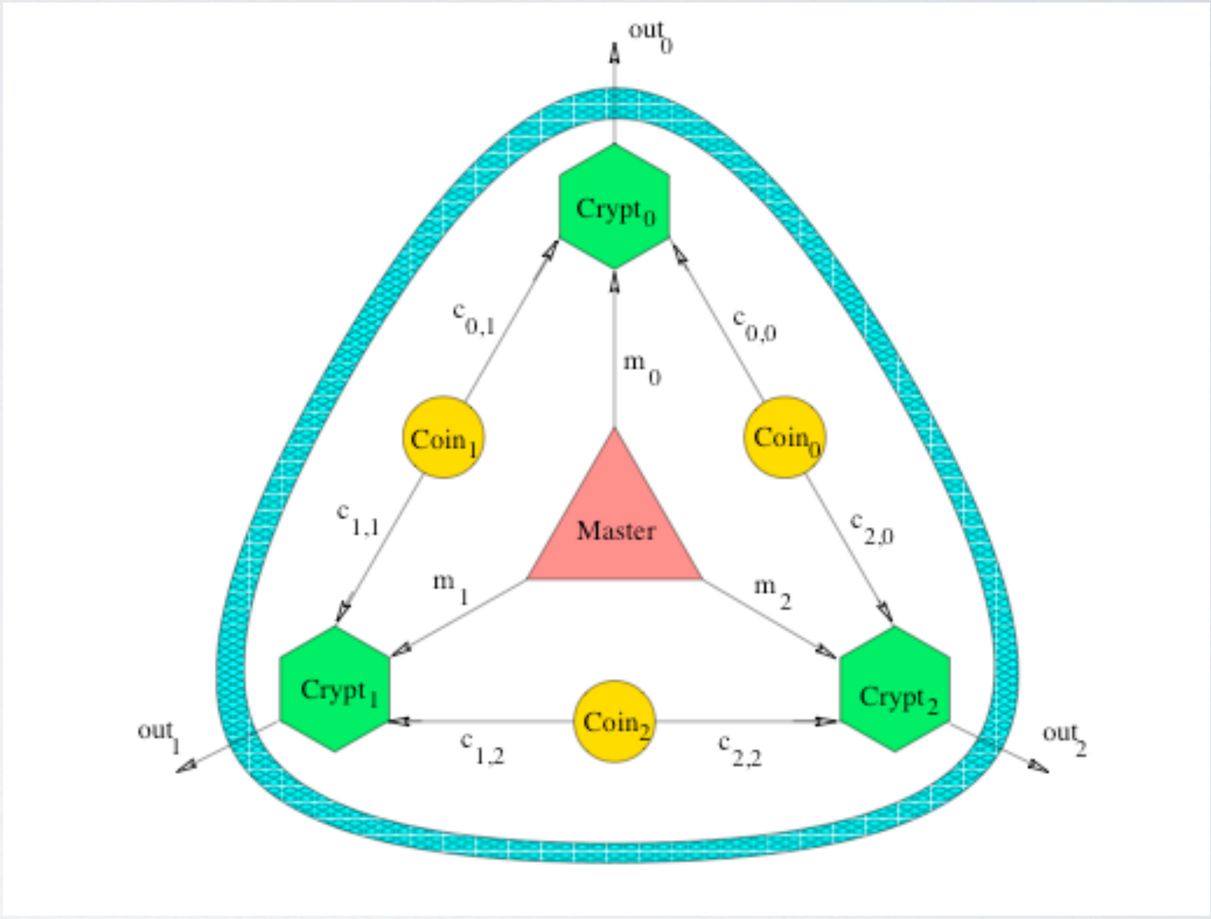
Divide and ~~Conquer~~ Pacify: Use random variables to confine domain of V_1;
Yields distributive law (hence monad); weakens laws of probability: $P +_r P \neq P$

FLIPPING COINS

Chaum's Dining Cryptographers
- *Master & Cryptographers*

- *Nondeterminism:* Master; Adversary
- *Probabilistic choice:* Cryptographers' coin flips

Model: Trace distributions on events in protocol run - $\Sigma\, r_i\, \delta_{s(i)}$, *s(i) trace*
Must support nondeterminism and probabilistic choice



Problem: Probability measure is on *D*.
- $V_1(D)$ is not well-behaved even if *D* is a trace model.
- Jung & Tix: $V_1(D)$ is in RB if *D* is a tree.

Solution: Probability measure is on fixed domain A^∞ where V_1 is well-behaved.

RANDOM VARIABLES

X - measure space;
μ (probability) measure on X

- supp μ - complement of largest open set U with $\mu(U) = 0$
- X domain implies supp μ Scott closed;
- supp $\sum_{i \in I} r_i \delta_{s(i)} = \downarrow\{ s(i) \mid i \in I \}$

- μ is *concentrated on* A iff $\mu(B) = 0 \quad (\forall B \subset X \setminus A,\ B$ measurable)
- $\sum r_i \delta_{s(i)}$ = concentrated on $\{ s(i) \mid i \in I \}$

Useful fact:
If $\{0,1\}^\infty = \{0,1\}^* \cup \{0,1\}^\omega$, then

- $A \subset \{0,1\}^\infty$ Scott closed implies $\exists\ \pi_A : \{0,1\}^\infty \to A$ continuous

True for any tree-like domain, in particular, for traces domain.

RANDOM VARIABLES

X, Y - measure spaces;
μ (probability) measure on X,
Random variable: $f : X \to Y$ measurable function.

Usual approach:
Push μ forward using f:
$f(\mu)(A) = \mu(f^{-1}(A))$ if $A \subset Y$ is measurable.
This is just action of $V_1 : \mathrm{Meas} \to \mathrm{Meas}$ (Giry monad)

Alternative view: E..g., $X = \{0,1\}^\infty$ ($= \{0,1\}^* \cup \{0,1\}^\omega$) - flips of a coin

Leave μ *on X; f* gives outcomes in Y of random choices (*Oracle*)
Measures are confined to X - for domains X and Y:
- order only applied to $V_1(X)$
- require $f : X \to Y$ to be Scott continuous

CONTINUOUS RANDOM VARIABLES

$\{0,1\}^\infty = \{0,1\}^* \cup \{0,1\}^\omega$ - ideal completion of full binary tree

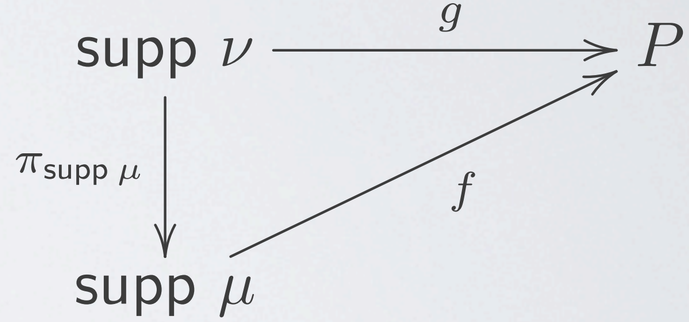
Random variable $f : \{0,1\} \to P$ *- outcome of coin flip; give* $\{0,1\}$ *probability distribution*

Over course of computation, outcomes of flips define f : supp $\mu \to P$,

supp $\mu \subset \{0,1\}^\infty$ Scott closed, assume f Scott continuous

Rand($\{0,1\}^\infty$, P) $\equiv \{(\mu, f) \mid f : \text{supp } \mu \to P \text{ Scott continuous}\}$

$(\mu, f) \leq (\nu, g)$ *iff* $\pi_{\text{supp } \mu}(\nu) = \mu$ & $f \circ \pi_{\text{supp } \mu}|_{\text{supp } \nu} \leq g$



$r(\mu, f) + (1\text{-}r)(\nu, g) = (r\mu 0 + (1\text{-}r)\nu 1, f0 + g1)$, *where*

- $\mu 0 = \mu$ transported to (supp μ)$0 \equiv \{ x0 \mid x \in \text{supp } \mu\}$
- $f0 : (\text{supp } \mu)0 \to P$ *by* $f0(x0) = f(x)$, *etc.*
- Note: $(\mu, f) \leq r(\mu, f) + (1\text{-}r)(\mu, f)$

Defines endofunctor on *BCD:*

$$(\mu, f), (\mu', f') \leq (\nu, g) \Rightarrow (\mu, f) \vee (\mu', f') = (\pi|_x(\nu), f \vee f')$$

RANDOM VARIABLE MONAD

Problem: Rand($\{0,1\}^\infty$, -) is not a monad

Call $\Sigma\, r_i \,\delta_{x_i}$ *flat* if $\{\, x_i \mid i \in I \,\}$ is an antichain; μ is *flat* iff $\mu = \sup \Sigma\, r_i \,\delta_{x_i}$ flat, iff $\mathrm{tr}_n(\mu)$ flat

ΘRand($\{0,1\}^\infty$, P) - flat random variables concentrated on compact subsets;

- assume f defined only on $Max(supp\ \mu)$

Theorem: *(Goubault-Larrecq & Varacca, LICS 2011)*
If P is a BCD domain, then so is ΘRand($\{0,1\}^\infty$, P), where

$$(\mu, f) \leq (\nu, g) \text{ iff } \pi_{\mathrm{supp}\ \mu}(\nu) = \mu \ \&\ f \circ \pi_{\mathrm{supp}\ \mu} | \ \mathrm{supp}\ \nu \leq g$$

In fact, ΘRand($\{0,1\}^\infty$, P) *forms a monad on BCD, CCC of domains*

Question: *What does it mean for* μ *to be flat?*

USING STONE DUALITY

$\{0,1\}^\infty$ as completion of full binary tree is "bottom up" construction.

Use Stone Duality to give "top down" construction:

$C = \{0,1\}^\omega$ Cantor set - Stone space.

Define $\mathbf{C}(C)$ = { $\boldsymbol{P}$ | $\boldsymbol{P}$ partitions C into clopen sets}
- $\boldsymbol{P} \leq \boldsymbol{Q}$ iff $\boldsymbol{Q}$ *refines* $\boldsymbol{P}$

Stone duality implies $C \cong \mathsf{Max}\ \mathrm{Id}(\mathbf{C}(C), \leq) \cong \mathbf{lim}(\boldsymbol{P}, i_{\boldsymbol{QP}})_{\boldsymbol{P} \in \mathbf{C}(C)}$

$\{0,1\}^\infty$ special case - { $\{0,1\}^n$ | n ≥ 0} cofinal in $\mathbf{C}(C)$

Advantages over $C \cong \mathsf{Max}\ \mathrm{K}\Omega(C, \leq)$:

1) Scott-closed subsets are retracts of $\mathrm{Id}(\mathbf{C}(C), \leq)$
2) Scott-continuous mappings $f : \mathrm{Id}(\mathbf{C}(C), \leq) \longrightarrow P$ defined via ``layers'' $\boldsymbol{P}$

FACTS ABOUT $V_1(\{0,1\}^\infty)$

Theorem: (V. Fedorchuk, 1981)
$V_1 : \mathrm{COMP} \to \mathrm{AffCOMP}$ is pro-continuous

Thus $V_1(\{0,1\}^\omega) \cong \lim(V_1(\{0,1\}^n), V_1(\pi_n))$

$\{0,1\}^n$ finite $\Rightarrow$ $V_1(\{0,1\}^n)$ flat $\Rightarrow$ $V_1(\{0,1\}^\omega)$ flat.

Lemma: $\mu \in V_1(\{0,1\}^\infty)$ *maximal flat iff* μ *concentrated on* $A \subset \{0,1\}^\omega$ *compact*

Theorem: *Let* $(\mu, f) \in \Theta\mathrm{Rand}(\{0,1\}^\infty, P)$. *Then*

1) i) μ *is concentrated on compact antichain in* $\{0,1\}^\infty$

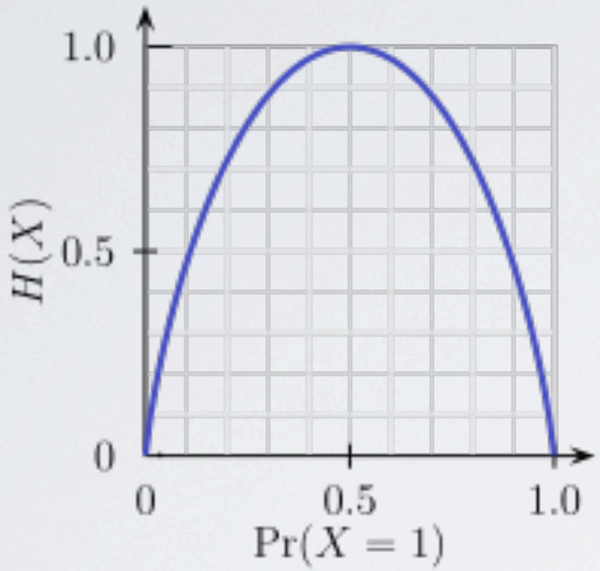
ii) $\mu = \pi^\omega{}_X(\nu)$, *some* $\nu \in V_1(\{0,1\}^\omega)$ *flat,* X *Scott closed.*

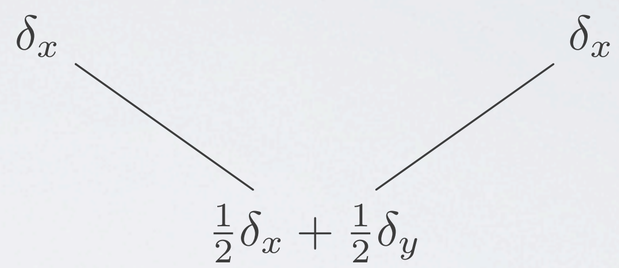
2) *supp* $\mu \subset \{0,1\}^\omega$ *implies* $f = \sup_n f_n$ *with* $f_n : \pi_n(\{0,1\}^\omega) \to P$ *Scott continuous.*

Proof: Ad 1i) $\mu(w) > 0 \Rightarrow \mu = r\delta_w + \nu$ *and* $\nu(\uparrow w) = 0 \ldots$ □

MUSINGS ON INFORMATION THEORY

$H : V_1(\{0,1\}) \to [0, 1]^{op}$ entropy function:





Supports embedding $i_n : V_1(\{0,1\}^n) \to V_1(\{0,1\}^{n+1})$ for $\pi_n : \{0,1\}^{n+1} \to \{0,1\}^n$

Allows to choose $\nu \in V_1(\{0,1\}^\omega)$ "optimal" with $\pi^\omega{}_n(\nu) = \mu$;

A CONTINUOUS IMAGE

$\mathbb{I}[0,1] = (\{ [a,b] \mid a \leqslant b\}, \supseteq)$ - interval domain

$\mathbb{I}_b[0,1] = (\{ [m/2^n,(m+1)/2^n] \mid m \leqslant 2^n\text{-}1\}, \supseteq)$ - "binary" interval domain

$\varphi : \{0,1\}^\infty \to \mathbb{I}_b[0,1]$ Scott continuous quotient map

$V_1(\varphi) : V_1(\{0,1\}^\infty) \to V_1(\mathbb{I}_b[0,1])$ continuous

Example: $\{0,1\}^\omega$ compact group; μ Haar measure

- $\mu = \sup \mu_n$, μ_n uniform distribution on $\{0,1\}^n$

Proposition: $V_1(\varphi)(\mu)$ is Lebesgue measure on [0,1].

Proof: Order $\{0,1\}^\omega$ lexicographically. $\varphi|_{\{0,1\}^\omega}$ becomes order-isomorphism onto [0,1].

For $x \in \{0,1\}^n$, $\{x\} \times \{0,1\}^{\omega+|x|}$ maps to $[x, 1]$. []