A Strongly Effective Domain Model for the Calculus of Constructions

Dieter Spreen
University of Siegen

“Models, Proofs, Constructions”, Munich, August 11/12, 2010

Calculus of Constructions

(Coquand/Huet; *here:* notation by Hyland/Pitts)

Well-formed expressions are divided in 3 levels:

Terms, Orders, Operators

Metavariables:

Orders: K, L, M, ...

Operators: S, T, U, ...

Terms: s, t, u, ...

Order constant: Type

(Types = Operators of Order "Type")

Metavariables: A, B, C, ...

The rules of the calculus allow the derivation of *Judgements*.

Structural Judgements:

$$\Gamma \vdash K : \mathrm{Order}, \qquad \Gamma \vdash S : K, \qquad \Gamma \vdash S : A$$

Equality Judgements:

$$\Gamma \vdash K = L : \mathrm{Order}, \quad \Gamma \vdash S = T : K, \quad \Gamma \vdash s = t : A$$

All judgements are made with respect to a *Context* Γ (Declaration of variables)

Contexts are built according to the following rules:

- $()$ context
- $$\frac{\Gamma \text{ context}}{\Gamma, X : \text{Order context}} \quad (X \notin \mathrm{dom}(\Gamma))$$
- $$\frac{\Gamma \vdash K : \text{Order}}{\Gamma, Y : K \text{ context}} \quad (Y \notin \mathrm{dom}(\Gamma))$$
- $$\frac{\Gamma \vdash S : \text{Type}}{\Gamma, x : S \text{ context}} \quad (x \notin \mathrm{dom}(\Gamma))$$

Judgements can be derived by *general* rules:

- equality rules
- substitution
- assumption
- weakening

and *specific* rules

- Type $\dfrac{}{() \vdash \mathsf{Type} : \mathsf{Order}}$

Orders and Types are closed under "quantification" over both Orders and Types.

- Product clauses ("Types over Types")

Formation	$$\frac{\Gamma, x : A \vdash C : \mathrm{Type}}{\Gamma \vdash \Pi x : A.C : \mathrm{Type}}$$	
Introduction	$$\frac{\Gamma, x : A \vdash s : C}{\Gamma \vdash \lambda x : A.s : \Pi x : A.C}$$	(abstraction)
Eliminiation	$$\frac{\Gamma \vdash t : \Pi x : A.C \quad \Gamma \vdash u : A}{\Gamma \vdash tu : C[u/x]}$$	(application)
Equality	$$\frac{\Gamma \vdash u : A \quad \Gamma, x : A \vdash s : C}{\Gamma \vdash (\lambda x : A.s)u = s[u/x] : C[u/x]}$$ $$\frac{\Gamma \vdash t : \Pi x : A.C}{\Gamma \vdash \lambda x : A.tx = t : \Pi x : A.C}$$	

- Sum clauses ("Types over Types")

Formation
$$\frac{\Gamma, x : A \vdash C : \mathrm{Type}}{\Gamma \vdash \Sigma x : A.C : \mathrm{Type}}$$

Introduction
$$\frac{\Gamma \vdash s : A \quad \Gamma \vdash t : C[s/x]}{\Gamma \vdash \langle s, t\rangle : \Sigma x : A.C}$$

Elimination
$$\frac{\Gamma \vdash s : \Sigma x : A.C \quad \Gamma, x : A, y : C \vdash t : B[\langle x, y\rangle/z]}{\Gamma \vdash E(s, (x, y).t) : B[s/z]}$$

Equality
$$\frac{\Gamma \vdash s : A \quad \Gamma \vdash u : C[s/x] \quad \Gamma, x : A, y : C \vdash t : B[\langle x, y\rangle/z]}{\Gamma \vdash E(\langle s, u\rangle, (x, y).t) = t[s/x, u/y] : B[\langle s, u\rangle/z]}$$

$$\frac{\Gamma \vdash s : \Sigma x : A.C \quad \Gamma, z : \Sigma x : A.C \vdash t : B}{\Gamma \vdash E(s, (x, y).t[\langle x, y\rangle/z]) = t[s/z] : B[s/z]}$$

CC has λ^2 as a subsystem.

Coquand, Gunter and Winskel (model of λ^2):

$$\text{Types} \xrightarrow{[\![\cdot]\!]} \text{dI-domains}$$

here:

$$\begin{array}{ccc} \text{Types} & \xrightarrow{[\![\cdot]\!]} & \begin{array}{c}\text{canonical representations}\\ \text{of dI-domains}\end{array} \\ & & \Big\| \;\text{Winskel} \\ & & \text{stable event structures} \end{array}$$

$$\text{Terms} \xrightarrow{[\![\cdot]\!]} \begin{array}{c}\text{elements of the}\\ \text{corresponding dI-domain}\end{array}$$

Advantage: *There is a natural substructure relation such that stable event structures form a domain that is similar to a dI-domain.*

Definition

Let $(D, \sqsubseteq, \perp)$ be a Scott domain with set of compact elements D^0.

1. D is a dI-domain if the following Axioms d and I are satisfied:

   Axiom d: $(\forall x, y, x)[\{x, y, z\}\uparrow \text{ (bounded) } \Rightarrow$
   $$x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z).$$

   Axiom I: Each compact element dominates only finitely many elements.

2. An element $p \in D^0$ is *completely prime* if for all bounded $X \subseteq D$,
   $$p \sqsubseteq \bigsqcup X \Rightarrow (\exists x \in X) p \sqsubseteq x.$$

Definition

Let D_1, D_2 be Scott domains. A map $f\colon D_1 \to D_2$ is said to be

1. *continuous*, if it is monotone and preserves least upper bounds of directed subsets.
2. *stable*, if it is continuous and preserves greatest lower bounds of bounded pairs of elements, i.e. for all $x, y \in D_1$,

$$x \uparrow y \Rightarrow f(x \sqcap y) = f(x) \sqcap f(y).$$

Note that for stable maps $f\colon D_1 \to D_2$ we have that for all $x' \in D_2^0$ there is a least $x \in D_1^0$ such that $x' \sqsubseteq f(x)$.

Definition

$$\mathrm{trace}(f) = \{\, (x, x') \in D_1^0 \times D_2^0 \mid x \text{ least with } x' \sqsubseteq f(x) \,\}.$$

Posets are categories with an arrow ι_x^y from x to y, excactly if $x \sqsubseteq y$. Greatest lower bounds of bounded pairs correspond to pullbacks in this case.

$$
\begin{tikzcd}
x \sqcap y \arrow[r, dash] \arrow[d, dash] & y \arrow[d, dash] \\
x \arrow[r, dash] & z
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
X \times_Z Y \arrow[r, "f"'] \arrow[d, "g"] & X \arrow[d, "h"'] \\
Y \arrow[r, "k"] & Z
\end{tikzcd}
$$

Definition

Let $\mathbf{C}_1, \mathbf{C}_2$ be categories with pullbacks. A functor $F\colon \mathbf{C}_1 \to \mathbf{C}_2$ is *stable*, if it preserves directed limits and pullbacks.

Definition

Let D_1, D_2 be Scott domains. A pair (e, p) of stable maps $e\colon D_1 \to D_2$ and $p\colon D_2 \to D_1$ is a *stable embedding/projection* if

- $p \circ e = \mathrm{id}_{D_1}$
- $e \circ p \sqsubseteq \mathrm{id}_{D_2}$.

Note that each component of such a pair uniquely determines the other one.

Let $\mathbf{SD^e}$ be the category of all Scott domains with stable embeddings, D be a Scott domain and $F\colon D \to \mathbf{SD^e}$ be a stable functor.

For $x, y \in D$ with $x \sqsubseteq y$ we write $F_{x,y}$ for the embedding $F(\iota_x^y)\colon F(x) \to F(y)$ and F_{xy}^R for the corresponding projection.

Definition

A family $f = (f_d)_{d \in D}$ with $f_d \in F(d)$ is said to be

1. *monotone* if
$$x \sqsubseteq y \Rightarrow F_{xy}(f_x) \sqsubseteq f_y.$$
2. *continuous* if it is monotone and for all directed $S \subseteq D$,
$$f_{\bigsqcup S} = \bigsqcup \{ F_{x,\bigsqcup S}(f_x) \mid x \in S \}.$$
3. *stable* if it is continuous and for all $x, y \in D$ with $x \uparrow y$
$$F^R_{x \sqcap y, x}(f_x) \sqcap F^R_{x \sqcap y, y}(f_y) = f_{x \sqcap y}.$$

As in the case of stable maps, for each $x' \in \bigcup \{ F(x)^0 \mid x \in D \}$ there is a least $x_0 \in D^0$ such that $x' \in F(x_0)^0$ and $x' \sqsubseteq f_{x_0}$. Let

$$\mathrm{trace}(f) = \{ (x, x') \in (\textstyle\sum_{x \in D} F(x))^0 \mid x \text{ least with } x' \sqsubseteq f_x \}.$$

Definition

1. An *event structure* $E = (E, \mathrm{Con}, \vdash)$ is given by
   - a set E of *events*,
   - a nonempty predicate $\mathrm{Con} \subseteq \mathcal{P}_{fin}(E)$, called *consistency*, such that
   $$X \in \mathrm{Con} \wedge Y \subseteq X \Rightarrow Y \in \mathrm{Con},$$
   - a relation $\vdash \subseteq \mathrm{Con} \times E$, called *enabling relation*.
2. An event structure E is *stable* if for $e \in E$ and $X, Y \subseteq E$
$$X \vdash e \wedge Y \vdash e \wedge X \cup Y \cup \{e\} \in \mathrm{Con} \Rightarrow X = Y.$$

Every stable event structure gives rise to a dI-domain and vice versa.

Definition

1. A *proof* τ of an event e is a set of events defined recursively by
   - $\emptyset \vdash e \Rightarrow \tau = \emptyset$.
   - If $\tau_1, \ldots, \tau_n$ are proofs of $e_1, \ldots, e_n$ and $\{e_1, \ldots, e_n\} \vdash e$, then $\tau_1 \cup \{e_1\} \cup \cdots \cup \tau_n \cup \{e_n\}$ is a proof of e.
2. A *state* x is a subset of E which is
   - *finitely consistent*, i.e., $(\forall X \subseteq_f x) X \in \mathrm{Con}$.
   - *safe*, i.e., x contains proof of e, for all $e \in x$.

Proposition

1. *Let $\mathcal{S}^+(E)$ be the set of all states of E. Then $(\mathcal{S}^+(E), \subseteq)$ is a dI-domain.*

2. *Let D be a dI-domain and $\mathcal{S}^-(D)$ be the set of its complete primes. Moreover, for $X \subseteq_f \mathcal{S}^-(D)$ and $p \in \mathcal{S}^-(D)$ let*

   - *$X \in \mathrm{Con}$ if X is bounded*
   - *$X \vdash p$ if X is the set of complete primes immediately below p.*

   Then $(\mathcal{S}^-(D), \mathrm{Con}, \vdash)$ is a stable event structure with

$$D \cong \mathcal{S}^+(\mathcal{S}^-(D)).$$

Set

$$\mathcal{W} = \{\, E \subseteq \omega \mid E \text{ is stable event structure} \,\}.$$

Definition

Let A, $B \in \mathcal{W}$. $A \trianglelefteq B$ if

- $A \subseteq B$
- $\mathrm{Con}_A = \mathrm{Con}_B \cap \mathcal{P}_{fin}(A)$

  (No new consistent subsets of A w.r.t. Con_B)
- $\vdash_A \subseteq \vdash_B$
- $(\forall e \in A)(\forall X \in \mathrm{Con}_B) X \vdash_B e \Rightarrow X \subseteq A \wedge X \vdash_A e$

  ($\vdash_B$ allows no additional enablings w.r.t. A).

Proposition

$(\mathcal{W}, \trianglelefteq)$ *is a locally distributive stable* ω*-bifinite domain, i.e.,*

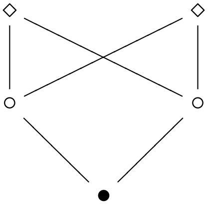
- ω*-algebraic*
- $\{x, y\}\uparrow \Rightarrow x \sqcap y$ *exists*
- *every principal ideal is distributive*
- $x \uparrow \bigsqcup X \Rightarrow x \sqcap \bigsqcup X = \bigsqcup \{ x \sqcap z \mid z \in X \}$*, for all* $x \in \mathcal{W}$ *and all directed subsets* X *of* $\mathcal{W}$
- $(U{\downarrow})^{\infty}(X)$ *is finite, for all finite sets* X *of compact elements of* $\mathcal{W}$*.*

$$(U{\downarrow})^{\infty}(X) = \bigcup_{n\in\omega} (U{\downarrow})^{n}(X)$$

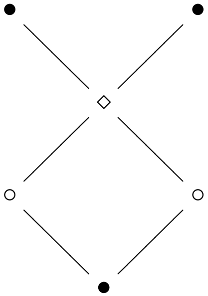
$$(U{\downarrow})(X) = \bigcup \{ \mathrm{MUB}(Y) \mid Y \subseteq_f {\downarrow} X \}.$$

Thus $\mathcal{W}$ is nearly a dI-domain:

Here, a finite bounded set can have *finitely many* minimal upper bounds, whereas in a dI-domain it has *exactly one* minimal upper bound.



now
finitely many minimal upper bounds



dI
exactly one minimal upper bound

Since ω-bifinite domains are algebraic, they are completely determined by their compact elements

Proposition

Let D be an algebraic domain and D^0 be the subset of its compact elements. Set

$$\mathcal{R}^-(D) = (D^0, \sqsubseteq \restriction D^0)$$
$$\mathcal{R}^+(D) = (\textit{ideal completion of } D^0, \subseteq).$$

Then

$$D \cong \mathcal{R}^+(\mathcal{R}^-(D)).$$

$$\mathcal{B} = \{ A \subseteq \omega \mid A \text{ algebraic base of a stable locally distributive } \omega\text{-bifinite domain} \}$$

Definition

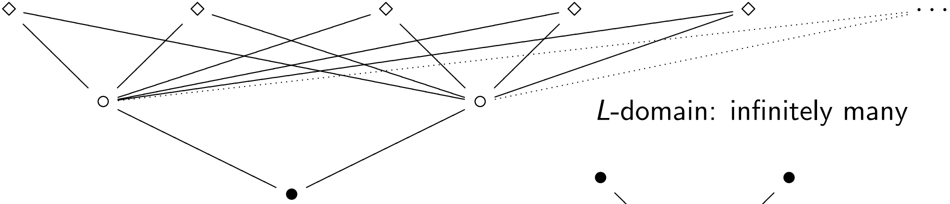
Let A, $C \in \mathcal{B}$. $A \Subset C$ if

- $A \subseteq C$
- $(\forall a, b \in A) a \sqsubseteq_A b \Leftrightarrow a \sqsubseteq_C b$
- $(\forall a \in A)(\forall b \in C) b \sqsubseteq_C a \Rightarrow b \in A$
- $(\forall X \subseteq_f A) \mathrm{MUB}_C(X) \subseteq A$

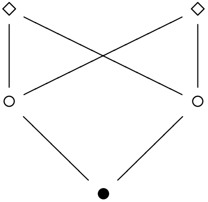
Proposition

$(\mathcal{B}, \Subset)$ is a locally distributive ω-algebraic L-domain that satisfies Berry's finiteness condition, i.e., $\downarrow\{A\}$ is finite, for all $A \in \mathcal{B}^0$.

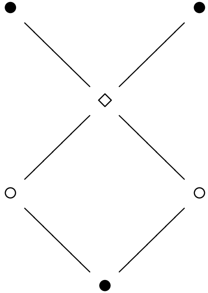
Hence $\mathcal{B}$ is nearly a dI-domain.



L-domain: infinitely many



ω-bifinite: finitely many



dI: exactly one

minimal upper bound(s)

Intended Interpretation

- Type expression α with free variables in Γ by a stable map

$$[\![\alpha]\!]_\Gamma : [\![\Gamma]\!] \to \mathcal{W}$$

- Term expression t of Type α with free variables in Γ by a stable family

$$\big([\![t]\!]_\Gamma(x)\big)_{x \in [\![\Gamma]\!]} \ \text{with} \ [\![t]\!]_\Gamma(x) \in \mathcal{S}^+([\![\alpha]\!]_\Gamma(x))$$

- Order expression σ with free variables in Γ by a stable map

$$[\![\sigma]\!]_\Gamma : [\![\Gamma]\!] \to \mathcal{B}$$

- Operator expression T of Order σ with free variables in Γ by a stable family

$$\big([\![T]\!]_\Gamma(x)\big)_{x \in [\![\Gamma]\!]} \ \text{with} \ [\![T]\!]_\Gamma(x) \in \mathcal{R}^+([\![\sigma]\!]_\Gamma(x))$$

Let

ω**dLI**	category of locally distributive ω-algebraic L-domains with Berry's axiom I
$\omega\mathbf{Bif}_\wedge$	category of locally distributive stable ω-bifinite domains
DI	category of dI-domains

always with stable maps as morphisms

Proposition

Let $D \in \omega\mathbf{dLI}$.

1. $F : D \to \mathcal{W}$ *stable* $\Rightarrow \mathcal{S}^+ \circ F : D \to \mathbf{DI}$ *stable functor*
2. $F : D \to \mathcal{B}$ *stable* $\Rightarrow \mathcal{R}^+ \circ F : D \to \omega\mathbf{Bif}_\wedge$ *stable functor*

$$[\![\Gamma]\!] = \ ?$$

- $[\![()]\!] =$ one-point domain
- $[\![\Gamma, X : \mathsf{Order}]\!] = [\![\Gamma]\!] \times \mathcal{B}$
- $[\![\Gamma, X : K]\!] = ?$
- $[\![\Gamma, x : A]\!] = ?$

Suppose $\Gamma \vdash K : \mathrm{Order}.$
Then

$$\mathcal{R}^+ \circ [\![K]\!]_\Gamma : [\![\Gamma]\!] \to \omega\mathbf{Bif}_\wedge$$

is a stable functor. Construct

$$\sum\nolimits_{[\![\Gamma]\!]} \mathcal{R}^+ \circ [\![K]\!]_\Gamma = \{ (x, y) \mid x \in [\![\Gamma]\!] \wedge y \in \mathcal{R}^+([\![K]\!]_\Gamma(x)) \}$$

$$(x, y) \sqsubseteq (x', y') \Leftrightarrow x \sqsubseteq_{[\![\Gamma]\!]} x' \wedge y \sqsubseteq_{\mathcal{R}^+([\![K]\!]_\Gamma(x'))} y'$$

[Note: $\mathcal{R}^+([\![K]\!]_\Gamma(x)) \subseteq \mathcal{R}^+([\![K]\!]_\Gamma(x'))$]

- $[\![\Gamma, X : K]\!] = \sum_{[\![\Gamma]\!]} \mathcal{R}^+ \circ [\![K]\!]_\Gamma$

$$\frac{\Gamma, x : A \vdash C : \mathrm{Type}}{\Gamma \vdash \Pi x : A.C : \mathrm{Type}}$$

Suppose

- $[\![C]\!]_{\Gamma,x:A} : \sum_{[\![\Gamma]\!]} \mathcal{S}^+ \circ [\![A]\!]_\Gamma \to \mathcal{W}$ is stable
- $[\![A]\!]_\Gamma : [\![\Gamma]\!] \to \mathcal{W}$ is stable.

Let $z \in [\![\Gamma]\!]$ be fixed. Then

- $[\![A]\!]_\Gamma(z) \in \mathcal{W}$
- $\lambda d.[\![C]\!]_{\Gamma,x:A}(z, d) : \mathcal{S}^+([\![A]\!]_\Gamma(z)) \to \mathcal{W}$ stable.

Set

$$\prod_{\mathcal{S}^+([\![A]\!]_\Gamma(z))} \lambda d.\mathcal{S}^+ \circ [\![C]\!]_{\Gamma,x:A}(z,d) =$$

$$\{\, (f_d)_{d \in \mathcal{S}^+([\![A]\!]_\Gamma(z))} \mid (f_d) \text{ stable family: } f_d \in \mathcal{S}^+([\![C]\!]_{\Gamma,x:A}(z,d)) \,\}$$

$$f \sqsubseteq g \Leftrightarrow \ \mathrm{trace}(f) \subseteq \mathrm{trace}(g)$$

Lemma

$$\Big(\prod_{\mathcal{S}^+([\![A]\!]_\Gamma(z))} \lambda d.\mathcal{S}^+ \circ [\![C]\!]_{\Gamma,x:A}(z,d), \sqsubseteq\Big) \in \mathbf{DI}.$$

Thus, there is a stable event structure

$$\Pi_{[\![A]\!]_\Gamma(z)} [\![C]\!]^z_{\Gamma,x:A} \tag{1}$$

in $\mathcal{W}$ such that

$$\mathcal{S}^+(\Pi_{[\![A]\!]_\Gamma(z)} [\![C]\!]^z_{\Gamma,x:A}) \overset{F_z}{\rightleftarrows} \prod_{\mathcal{S}^+([\![A]\!]_\Gamma(z))} \lambda d.\mathcal{S}^+ \circ [\![C]\!]_{\Gamma,x:A}(z,d).$$

Note that (1) can be constructed from $[\![A]\!]_\Gamma$ and $[\![C]\!]_{\Gamma,x:A}$ such that

$$\Pi([\![A]\!]_\Gamma, [\![C]\!]_{\Gamma,X;A}) : z \in [\![\Gamma]\!] \mapsto \Pi_{[\![A]\!]_\Gamma(z)} [\![C]\!]^z_{\Gamma,x:A}$$

is stable. Define

- $[\![\Pi x : A.C]\!]_\Gamma = \Pi([\![A]\!]_\Gamma, [\![C]\!]_{\Gamma,X;A})$

$$\frac{\Gamma, x : A \vdash s : C}{\Gamma \vdash \lambda x : A.s : \Pi x : A.C}$$

Suppose

- $[\![A]\!]_\Gamma : [\![\Gamma]\!] \to \mathcal{W}$ is stable
- $[\![C]\!]_{\Gamma,x:A} : \sum_{[\![\Gamma]\!]} \mathcal{S}^+ \circ [\![A]\!]_\Gamma \to \mathcal{W}$ is stable
- $\big([\![s]\!]_\Gamma(z,d)\big)_{(z,d)\in\sum_{[\![\Gamma]\!]} \mathcal{S}^+\circ[\![A]\!]_\Gamma}$ is a stable family such that

$$[\![s]\!]_\Gamma(z,d) \in \mathcal{S}^+([\![C]\!]_{\Gamma,x:A}(z,d)).$$

Fix $z \in [\![\Gamma]\!]$. Then

$$\left([\![s]\!]_\Gamma^z(d)\right)_{d\in\mathcal{S}^+([\![A]\!]_\Gamma(z))} = \left([\![s]\!]_\Gamma(z,d)\right)_{d\in\mathcal{S}^+([\![A]\!]_\Gamma(z))}$$

is a stable family such that

$$\begin{array}{cc} \left([\![s]\!]_\Gamma^z(d)\right)_{d\in\dots} & \in \prod_{\mathcal{S}^+([\![A]\!]_\Gamma(z))} \lambda d.\mathcal{S}^+([\![C]\!]_{\Gamma,x:A}(z,d)) \\ & \Big\downarrow F_z^{-1} \\ & \mathcal{S}^+(\Pi_{[\![A]\!]_\Gamma(z)}[\![C]\!]^z_{\Gamma,x:A}) \\ & \Big\| \\ & \mathcal{S}^+([\![\Pi x:A.C]\!]_\Gamma(z)) \end{array}$$

Note that

$$\mathrm{curry}([\![s]\!]_\Gamma) : z \in [\![\Gamma]\!] \mapsto F_z^{-1}(\left([\![s]\!]_\Gamma^z(d)\right)_{d\in\dots})$$

is stable. Define

- $[\![\lambda x:A.s]\!]_\Gamma = \mathrm{curry}([\![s]\!]_\Gamma)$

Advantages of this model:

- Conceptually much easier than other models which make heavy use of category theory.
- Recursion can be dealt with without any extra effort.
- Disjoint unions and definitions by cases can easily be added.
- Effectively given: all operations are computable in a strong sense: their traces are effectively enumerable.