Proofs and Computations

Helmut Schwichtenberg

Mathematisches Institut, LMU, München

22. August 2010

Computing with partial continuous functionals

- Proofs in mathematics: on abstract, "higher type" objects.
- Therefore an analysis of computational aspects of such proofs must be based on a theory of computation in higher types.
- Such a theory has been provided by Scott (1970) and Ershov (1977). Basic concept: partial continuous functional F.
- Since F can be seen as a limit of its finite approximations U we get for free the notion of a computable functional: it is given by a recursive enumeration of finite approximations.
- The price to pay for this simplicity is that functionals are now partial, in stark contrast to the view of Gödel (1958).
- However, the total functionals can be defined as a dense subset of the partial ones, w.r.t. the Scott topology.

TCF, a "theory of computable functionals"

- The partial continuous functionals are the intended range of its (typed) variables.
- Terms: T^+, an extension of Gödel's T and Plotkin's PCF.
- (Co)inductively defined predicates (with param.); only $\to, \forall$.
- $\mathrm{Eq}(r, s)$ (Leibniz), $\exists$, $\land$, $\lor$ inductively defined. $\mathbf{F} := \mathrm{Eq}(\mathtt{ff}, \mathtt{tt})$.
- Natural deduction style (rules $\to^{\pm}$, $\forall^{\pm}$). $\mathbf{F} \to A$ provable.

Properties

- TCF can reflect on the computational content of proofs, along the lines of the Brouwer-Heyting-Kolmogorov interpretation.
- Main difference to Martin-Löf type theory (or Coq, Agda): Partial continuous functionals are first class citizens.

Finitary algebras as non-flat Scott information systems

- An algebra ι is given by its constructors.
- Examples:

$$0^{\mathbf{N}}, \mathrm{S}^{\mathbf{N}\to\mathbf{N}} \quad \text{for } \mathbf{N} \text{ (unary natural numbers)},$$
$$1^{\mathbf{P}}, S_0^{\mathbf{P}\to\mathbf{P}}, S_1^{\mathbf{P}\to\mathbf{P}} \quad \text{for } \mathbf{P} \text{ (Cantor algebra)},$$
$$0^{\mathbf{D}} \text{ (axiom) and } \mathrm{C}^{\mathbf{D}\to\mathbf{D}\to\mathbf{D}} \text{ (rule) for } \mathbf{D} \text{ (derivations)}.$$

- Examples of "tokens" ($*$: special symbol; no information):

$$\mathrm{S}^n 0 \ (n \geq 0),\ \mathrm{S}^2 * \ (\text{in } \mathbf{N}),$$
$$S_0 S_1 S_0 S_0 1,\ S_0 S_1 S_0 S_0 * \ (\text{in } \mathbf{P}),$$
$$\mathrm{C}(\mathrm{C}0*)(\mathrm{C}*0) \ (\text{in } \mathbf{D}).$$

- A token is total if it contains no $*$.
- In $\mathbf{D}$: total token $\sim$ finite (well-founded) derivation.

Finitary algebras: consistency, entailment, ideals

By example. For **D** (derivations):

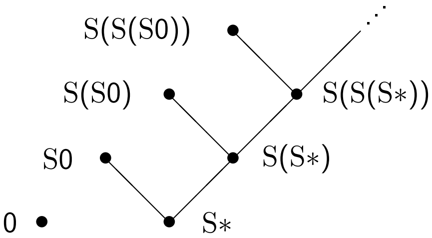
- $\{\mathrm{C}0*, \mathrm{C}*0\}$ is "consistent", written $\mathrm{C}0* \uparrow \mathrm{C}*0$.
- $\{\mathrm{C}0*, \mathrm{C}*0\} \vdash \mathrm{C}00$ ("entails").
- Ideals: consistent and "deductively closed" sets of tokens.

Examples of ideals:

- $\{\mathrm{C}0*, \mathrm{C}**\}$.
- $\{\mathrm{C}00, \mathrm{C}0*, \mathrm{C}*0, \mathrm{C}**\}$, and generally the deductive closure of a finite (well-founded) derivation.
- $\{\mathrm{C}**, \mathrm{C}(\mathrm{C}**)*, \mathrm{C}*(\mathrm{C}**), \mathrm{C}(\mathrm{C}**)(\mathrm{C}**), \dots\}$ ("cototal").
- Locally correct, but possibly non well-founded derivations (Mints 1978).

An ideal x is cototal if every constructor tree $P(*) \in x$ has a "predecessor" $P(\mathrm{C}\vec{*}) \in x$.

Tokens and entailment for **N**



Why non-flat?

- Continuous maps $f\colon |\mathbf{N}| \to |\mathbf{N}|$ (see below) are monotone: $x \subseteq y \to fx \subseteq fy$.
- Easy: every constructor gives rise to a continuous function.
- Want: constructors have disjoint ranges and are injective (cf. the Peano axioms $\mathrm{S}x \neq 0$ and $\mathrm{S}x = \mathrm{S}y \to x = y$).
- This holds for non-flat algebras, but not for flat ones:

There constructors must be strict (i.e., $\mathrm{C}\vec{x}\emptyset\vec{y} = \emptyset$), hence

$$\text{In } \mathbf{P}\text{:} \quad \mathrm{S}_1\emptyset = \emptyset = \mathrm{S}_2\emptyset,$$
$$\text{In } \mathbf{D}\text{:} \quad \mathrm{C}\emptyset\{0\} = \emptyset = \mathrm{C}\{0\}\emptyset.$$

The Scott-Ershov model of partial continuous functionals

- Let $\mathbf{A} = (A, \mathrm{Con}_A, \vdash_A)$, $\mathbf{B} = (B, \mathrm{Con}_B, \vdash_B)$ be information systems (Scott). Function space: $\mathbf{A} \to \mathbf{B} := (C, \mathrm{Con}, \vdash)$, with

$$C := \mathrm{Con}_A \times B,$$

$$\{(U_i, b_i)\}_{i \in I} \in \mathrm{Con} := \forall_{J \subseteq I}(\bigcup_{j \in J} U_j \in \mathrm{Con}_A \to \{b_j\}_{j \in J} \in \mathrm{Con}_B),$$

$$\{(U_i, b_i)\}_{i \in I} \vdash (U, b) := (\{\, b_i \mid U \vdash_A U_i \,\} \vdash_B b).$$

- Partial continuous functionals of type ρ: the ideals in $\mathbf{C}_\rho$.

$$\mathbf{C}_\iota := (\mathrm{Tok}_\iota, \mathrm{Con}_\iota, \vdash_\iota), \qquad \mathbf{C}_{\rho \to \sigma} := \mathbf{C}_\rho \to \mathbf{C}_\sigma.$$

  $|\mathbf{C}_\rho|$ is defined to be the set of ideals in $\mathbf{C}_\rho$.
- $f \in |\mathbf{C}_\rho|$: limit of formal neighborhoods $U \in \mathrm{Con}_{\rho \to \sigma}$.
- $f \in |\mathbf{C}_\rho|$ computable: r.e. limit.

A common extension T^+ of Gödel's T and Plotkin's PCF

- Terms of T^+ are built from (typed) variables and constants:

$$M, N ::= x^\rho \mid \mathrm{C}^\rho \mid D^\rho \mid (\lambda_{x^\rho} M^\sigma)^{\rho\to\sigma} \mid (M^{\rho\to\sigma} N^\rho)^\sigma.$$

  (constructors C or defined constants D, see below)
- Every defined constant D comes with a system of computation rules $D\vec{P}_i(\vec{y}_i) = M_i$ with $\mathrm{FV}(M_i) \subseteq \vec{y}_i$.
- $\vec{P}_i(\vec{y}_i)$: "constructor patterns", i.e., lists of applicative terms built from constructors and distinct variables, with each constructor C occurring in a context $\mathrm{C}\vec{P}$ (of base type). We assume that $\vec{P}_i$ and $\vec{P}_j$ for $i \neq j$ are non-unifiable.

Examples:

- Predecessor $\mathrm{P}\colon \mathbf{N} \to \mathbf{N}$, defined by $\mathrm{P}0 = 0$, $\mathrm{P}(\mathrm{S}n) = n$,
- Gödel's primitive recursion operators $\mathcal{R}^\tau_{\mathbf{N}}\colon \mathbf{N} \to \tau \to (\mathbf{N} \to \tau \to \tau) \to \tau$ with computation rules $\mathcal{R}0fg = f$, $\mathcal{R}(\mathrm{S}n)fg = gn(\mathcal{R}nfg)$, and
- the least-fixed-point operators Y_ρ of type $(\rho \to \rho) \to \rho$ defined by the computation rule $Y_\rho f = f(Y_\rho f)$.

Corecursion operators

Recall $\mathcal{R}_{\mathbf{N}}^{\tau} \colon \mathbf{N} \to \tau \to (\mathbf{N} \to \tau \to \tau) \to \tau$ with computation rules $\mathcal{R}0fg = f$, $\mathcal{R}(\mathrm{S}n)fg = gn(\mathcal{R}nfg)$. Corecursion operators:

$$^{\mathrm{co}}\mathcal{R}_{\mathbf{N}}^{\tau} \colon \tau \to (\tau \to \mathbf{U} + (\mathbf{N} + \tau)) \to \mathbf{N},$$
$$^{\mathrm{co}}\mathcal{R}_{\mathbf{P}}^{\tau} \colon \tau \to (\tau \to \mathbf{U} + (\mathbf{P} + \tau) + (\mathbf{P} + \tau)) \to \mathbf{P},$$
$$^{\mathrm{co}}\mathcal{R}_{\mathbf{D}}^{\tau} \colon \tau \to (\tau \to \mathbf{U} + (\mathbf{D} + \tau) \times (\mathbf{D} + \tau)) \to \mathbf{D},$$

Conversion: For $f \colon \rho \to \tau$ and $g \colon \sigma \to \tau$ we denote $\lambda_x(\mathcal{R}_{\rho+\sigma}^{\tau} xfg)$ of type $\rho + \sigma \to \tau$ by $[f, g]$.

$$^{\mathrm{co}}\mathcal{R}_{\mathbf{N}}^{\tau} NM \mapsto [\lambda\_0, \lambda_x(\mathrm{S}([\mathrm{id}^{\mathbf{N}\to\mathbf{N}}, \lambda_y(^{\mathrm{co}}\mathcal{R}_{\mathbf{N}}^{\tau} yM)]x))](MN),$$
$$^{\mathrm{co}}\mathcal{R}_{\mathbf{P}}^{\tau} NM \mapsto [\lambda\_1, \lambda_x(S_0([\mathrm{id}, P_{\mathbf{P}}]x)), \lambda_x(S_1([\mathrm{id}, P_{\mathbf{P}}]x))](MN),$$
$$^{\mathrm{co}}\mathcal{R}_{\mathbf{D}}^{\tau} NM \mapsto [\lambda\_0, \lambda_x(\mathrm{C}([\mathrm{id}, P_{\mathbf{D}}]x_1)([\mathrm{id}, P_{\mathbf{D}}]x_2))](MN).$$

Denotational semantics

For every closed term $\lambda_{\vec{x}} M$ of type $\vec{\rho} \to \sigma$ we inductively define a set $[\![\lambda_{\vec{x}} M]\!]$ of tokens of type $\vec{\rho} \to \sigma$.

$$\frac{U_i \vdash b}{(\vec{U}, b) \in [\![\lambda_{\vec{x}} x_i]\!]}(V), \qquad \frac{(\vec{U}, V, c) \in [\![\lambda_{\vec{x}} M]\!] \qquad (\vec{U}, V) \subseteq [\![\lambda_{\vec{x}} N]\!]}{(\vec{U}, c) \in [\![\lambda_{\vec{x}}(MN)]\!]}(A).$$

For every constructor C and defined constant D:

$$\frac{\vec{V} \vdash \vec{b^*}}{(\vec{U}, \vec{V}, \mathrm{C}\vec{b^*}) \in [\![\lambda_{\vec{x}} \mathrm{C}]\!]}(\mathrm{C}), \qquad \frac{(\vec{U}, \vec{V}, b) \in [\![\lambda_{\vec{x}, \vec{y}} M]\!] \qquad \vec{W} \vdash \vec{P}(\vec{V})}{(\vec{U}, \vec{W}, b) \in [\![\lambda_{\vec{x}} D]\!]}(D),$$

with one rule (D) for every computation rule $D\vec{P}(\vec{y}\,) = M$. Note:

$(\vec{U}, b)$ denotes $(U_1, \dots (U_n, b) \dots)$,

$(\vec{U}, V) \subseteq [\![\lambda_{\vec{x}} M]\!]$ means $(\vec{U}, b) \in [\![\lambda_{\vec{x}} M]\!]$ for all $b \in V$.

Denotational semantics (continued)

Theorem

- *For every term M, $[\![\lambda_{\vec{x}} M]\!]$ is an ideal.*
- *If a term M converts to M' by $\beta\eta$-conversion or application of a computation rule, then $[\![M]\!] = [\![M']\!]$.*

Let

$$[\![M]\!]_{\vec{x}}^{\vec{u}} := \bigcup_{\vec{U} \subseteq \vec{u}} [\![M]\!]_{\vec{x}}^{\vec{U}} \quad \text{with} \quad [\![M]\!]_{\vec{x}}^{\vec{U}} := \{\, b \mid (\vec{U}, b) \in [\![\lambda_{\vec{x}} M]\!] \,\}.$$

A consequence of (A) is continuity of application:

$$c \in [\![MN]\!]_{\vec{x}}^{\vec{u}} \leftrightarrow \exists_{V \subseteq [\![N]\!]_{\vec{x}}^{\vec{u}}} ((V, c) \in [\![M]\!]_{\vec{x}}^{\vec{u}}).$$

Inductive and coinductive definitions

- Computational content of Ir, with I inductively defined: what was needed to put r into I.
- Example: Even is inductively defined by the clauses

$$\mathrm{Even}(0), \qquad \forall_n(\mathrm{Even}(n) \to \mathrm{Even}(\mathrm{S}(\mathrm{S}n))).$$

  A generation tree for $\mathrm{Even}(6)$ consists of a single branch with nodes $\mathrm{Even}(0)$, $\mathrm{Even}(2)$, $\mathrm{Even}(4)$ and $\mathrm{Even}(6)$.
- Computational content of Jr, with J coinductively defined: how to continue after putting r into J.
- Example: St ("t is a stream") is coinductively defined by the clause

$$St \to t = \mathrm{nil} \vee St_0 \vee St_1.$$

An abstract theory of sets of nodes

Nodes a, b, c are total ideals in $\mathbf{P}$, viewed as lists of $0, 1$.
Let t be a variable of an unspecified type α ("set of nodes").
Language:

- a relation of arity $(\mathbf{P}, \alpha)$, written $a \in t$,
- a function of type $\alpha \to \mathbf{P} \to \alpha$, written t_a ("t's subtree at a")
- a function of type $\mathbf{P} \to \alpha \to \alpha$, written at ("a plus t").

Define

$$\mathrm{Tree}(t) := \forall_{a \in t} \forall_{n \le |a|} \bar{a}n \in t \quad \text{"}t \text{ is upward closed"},$$

$$\mathrm{Inf}(t) := \forall_n \exists_{a \in t} |a| = n \quad \text{"}t \text{ is infinite"},$$

$$\mathrm{UEU}(t) := \forall_n \exists_{m \ge n} \forall_{a,b \in t} (|a| = |b| = m \to \bar{a}n = \bar{b}n)$$

"t satisfies the uniform effective uniqueness condition",

$$C_t a := \exists_{n \ge |a|} \forall_{b \in t} (|b| = n \to \bar{b}|a| = a) \quad \text{"}a \text{ covers the paths in } t\text{"}.$$

Properties

$$\begin{aligned} &b \in t_a \leftrightarrow ab \in t, \\ &ab \in at \leftrightarrow b \in t, \\ &\exists_t \forall_a (a \in t \leftrightarrow A) \quad \text{for } A\ \Sigma\text{-formula}. \end{aligned}$$

Covering nodes are in t:

$$\mathrm{Tree}(t) \to \mathrm{Inf}(t) \to C_t a \to a \in t.$$

Covering nodes are "fertile":

$$\mathrm{Tree}(t) \to \mathrm{Inf}(t) \to C_t a \to \mathrm{Inf}(t_a).$$

The uniform effective uniqueness property is inherited to t_a:

$$\mathrm{UEU}(t) \to \mathrm{UEU}(t_a).$$

Nodes covering the paths in t can be extended

Lemma (Extension)

$\mathrm{Tree}(t) \to \mathrm{Inf}(t) \to \mathrm{UEU}(t) \to C_t a \to C_t(a0) \vee C_t(a1)$.

Proof.

Let t be an infinite tree. Assume $\mathrm{UEU}(t)$ and $C_t a$. Then we have $n \geq |a|$ such that $\forall_{b \in t}(|b| = n \to a \preceq b)$. By $\mathrm{UEU}(t)$ for $n+1$ we have $m \geq n+1$ such that

$$\forall_{b,c \in t}(|b| = |c| = m \to \overline{b}(n+1) = \overline{c}(n+1)).$$

Since t is infinite we have $b \in t$ such that $|b| = m$. Then $\overline{b}n \in t$ since t is a tree and $m \geq n+1$, hence $a \preceq \overline{b}n$ by assumption. Let $i := (b)_{|a|}$. We show $C_t(ai)$. Take m. Clearly $m \geq |ai|$. Let $c \in t$ with $|c| = m$. We show $ai \preceq c$. Since $|b| = |c| = m$ we have $\overline{b}(|a|+1) = \overline{c}(|a|+1)$. Hence

$$ai = \overline{b}(|a|+1) = \overline{c}(|a|+1) \preceq c. \qquad \square$$

Computational content if the Extension lemma

$$\mathrm{Tree}(t) \to \mathrm{Inf}(t) \to \mathrm{UEU}(t) \to C_t a \to C_t(a0) \vee C_t(a1).$$

Relative to realizers for its assumptions on t. Let inf_t and ueu_t be witnesses for t's infinity and $\mathrm{UEU}(t)$, i.e., for all k

$$\mathrm{inf}_t(k) \in t \wedge |\mathrm{inf}_t(k)| = k, \qquad |a| = |b| = \mathrm{ueu}_t(k) \to \bar{a}k = \bar{b}k.$$

Given a, let n witness $C_t a$. Let $m := \mathrm{ueu}_t(n+1)$ and $b := \mathrm{inf}_t(m)$. Then $i := (b)_{|a|}$ determines which of the two alternatives is proved. In each case m is the required witness for $C_t(ai)$. Hence

$$h_t(a, \mathrm{inf}_t, \mathrm{ueu}_t, n) = \begin{cases} \mathrm{inl}(m) & \text{if } (b)_{|a|} = 0, \\ \mathrm{inr}(m) & \text{if } (b)_{|a|} = 1. \end{cases}$$

Computational and non-computational logical connectives

Idea: fine tune the computational content of proofs, by switching on and off the computational effect of logical connectives.

- Example: in $\forall_n(\mathrm{Even}(n) \to \mathrm{Even}(\mathrm{S}(\mathrm{S}n)))$ only the premise $\mathrm{Even}(n)$ should be computationally relevant, not the $\forall_n$.
- Following Ulrich Berger (1993) we distinguish between a computational $\forall^{\mathrm{c}}$ and non-computational ("uniform") $\forall^{\mathrm{nc}}$.
- Similarly: $\to^{\mathrm{c}}$ and $\to^{\mathrm{nc}}$.

Streams

We coinductively define a predicate S of arity (α) by

$$\forall_t^{\mathrm{nc}}(St \to^{\mathrm{c}} \mathrm{Eq}(t, \mathrm{nil}) \vee St_0 \vee St_1).$$

The greatest-fixed-point (or coinduction) axiom for S is

$$\forall_t^{\mathrm{nc}}(Qt \to^{\mathrm{c}} \forall_t^{\mathrm{nc}}(Qt \to^{\mathrm{c}} \mathrm{Eq}(t, \mathrm{nil}) \vee (St_0 \vee Qt_0) \vee (St_0 \vee Qt_1)) \to^{\mathrm{c}} St).$$

The types are, with $\iota := \tau(St) = \mathbf{P}$, $\tau := \tau(Qt)$:

$$\iota \to \mathbf{U} + \iota + \iota \quad \text{(type of destructor for } \mathbf{P}\text{)},$$
$$\tau \to (\tau \to \mathbf{U} + (\iota + \tau) + (\iota + \tau)) \to \iota \quad \text{(type of } {}^{\mathrm{co}}\mathcal{R}_\iota^\tau\text{)}.$$

Converting reals into streams

Theorem

$\forall^{\mathrm{nc}}_t (Rt \to^{\mathrm{c}} St)$, *where* $Rt := \mathrm{Tree}(t) \wedge \mathrm{Inf}(t) \wedge \mathrm{UEU}(t)$.

Proof.

Use coinduction with R for Q. Suffices: $Rt \to Rt_0 \vee Rt_1$. From Rt we obtain $\mathrm{UEU}(t)$. From Rt and $C_t(\mathrm{nil})$ we have $C_t 0$ or $C_t 1$, by the Extension lemma. Assume $C_t 0$. Then Rt_0, since $\mathrm{Tree}(t_0) \wedge \mathrm{Inf}(t_0) \wedge \mathrm{UEU}(t_0)$ (cf. "Properties" above). □

Extracted term: recall $\tau(Rt) = \rho := (\mathbf{N} \to \iota) \times (\mathbf{N} \to \mathbf{N})$.

$$^{\mathrm{co}}\mathcal{R}^{\rho}_{\mathbf{P}}(\mathrm{inf}_t, \mathrm{ueu}_t)^{\rho} g_t^{\rho \to \mathbf{U} + (\iota + \rho) + (\iota + \rho)},$$

with g_t defined from inf_t, ueu_t and the content h_t of the Extension lemma.

Conclusion

- Terms in T^{+} ($\supset \mathrm{T}, \mathrm{PCF}$): denotational semantics.
- TCF, a theory of computable functionals.
- Witnesses of coinductively defined predicates: cototal ideals.
- Example: abstract real $\mapsto$ stream, from $\vdash \forall_t^{\mathrm{nc}}(Rt \to^{\mathrm{c}} St)$.

References

- U. Berger, Uniform Heyting arithmetic. APAL 133 (2005).
- U. Berger, From coinductive proofs to exact real arithmetic. CSL 2009.
- J. Berger and H. Ishihara, Brouwer's fan theorem and unique existence in constructive analysis. MLQ 51 (2005).
- T. Coquand and P. Schuster, Unique paths as formal points. Submitted, June 2010.
- D. Ratiu and H.S., Decorating proofs. To appear, Mints volume (S. Feferman and W. Sieg, eds.), 2010.
- H.S., A direct proof of the equivalence between Brouwer's fan theorem and König's lemma with a uniqueness hypothesis. JUCS 11 (2005).
- H.S. and S.S. Wainer, Proofs and Computations. To appear, Perspectives in Mathematical Logic, 2010.