Computational content of proofs

Helmut Schwichtenberg

Mathematisches Institut, LMU, München

Pohlers-Fest, Münster, 19. Juli 2008

Computable functionals of finite types

- Gödel 1958: “Über eine bisher noch nicht benützte Erweiterung des finiten Standpunkts”, namely computable finite type functions.
- Need partial continuous functionals as their intendend domain (Scott 1969). The total ones then appear as a dense subset (Kreisel 1959, Ershov 1972).
- Type theory of Martin-Löf 1983 deals with total (structural recursive) functionals only. Fresh start, based on (a simplified form of) information systems (Scott 1982).

Atomic coherent information systems (acis's)

- Acis: $(A, \smile, \geq)$ such that $\smile$ (consistent) is reflexive and symmetric, $\geq$ (entails) is reflexive and transitive and $a \smile b \to b \geq c \to a \smile c$.
- Formal neighborhood: $U \subseteq A$ finite and consistent. We write $U \geq a$ for $\exists_{b \in U} b \geq a$, and $U \geq V$ for $\forall_{a \in V} U \geq a$.
- Function space: Let $\mathbf{A} = (A, \smile_A, \geq_A)$ and $\mathbf{B} = (B, \smile_B, \geq_B)$ be acis's. Define $\mathbf{A} \to \mathbf{B} = (C, \smile, \geq)$ by

$$
\begin{aligned}
C &:= \mathrm{Con}_A \times B, \\
(U, b) \smile (V, c) &:= U \smile_A V \to b \smile_B c, \\
(U, b) \geq (V, c) &:= V \geq_A U \wedge b \geq_B c.
\end{aligned}
$$

$\mathbf{A} \to \mathbf{B}$ is an acis again.

Ideals, Scott topology

- Ideal: $x \subseteq A$ consistent and deductively closed. $|\mathbf{A}|$ is the set of ideals (points, objects) of $\mathbf{A}$.
- $|\mathbf{A}|$ carries a natural topology, with cones $\tilde{U} := \{\, z \mid z \supseteq U \,\}$ generated by the formal neighborhoods U as basis.

Theorem (Scott 1982)

The continuous maps $f \colon |\mathbf{A}| \to |\mathbf{B}|$ and the ideals $r \in |\mathbf{A} \to \mathbf{B}|$ are in a bijective correspondence.

Free algebras

are given by their constructors. Examples

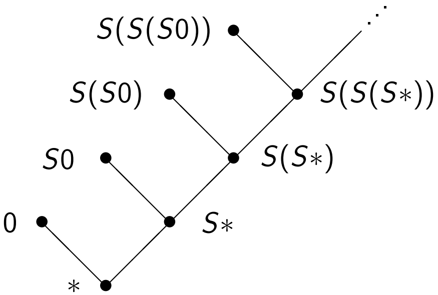
- Natural numbers: 0, S.
- Binary trees: nil, C.
- Unit $\mathbf{U}$: $\mathbf{u}$.
- Booleans $\mathbf{B}$: $\mathtt{tt}$, $\mathtt{ff}$.
- Signed digits $\mathbf{SD}$: -1, 0, $+1$.
- Lists of signed digits $\mathbf{L}(\mathbf{SD})$: nil, $d :: l$.

We always require a nullary constructor.

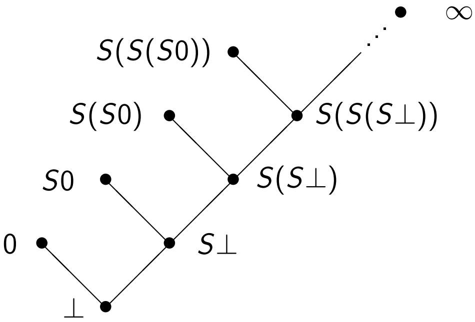
Turning free algebras into information systems

- Commonly done by adding $\bot$: "flat cpo".
- Problem 1: Constructors are not injective:
  $C(\bot, b) = \bot = C(a, \bot)$.
- Problem2 : Constructors do not have disjoint ranges:
  $C_1(\bot) = \bot = C_2(\bot)$.
- Solution: Use as atoms constructor expressions involving a symbol $*$, meaning "no information".

Example: atoms and entailment for **N**



Example: ideals for **N**



Total and cototal ideals

For a base type ι, the total ideals are defined inductively:

- 0 is total (0 being the nullary constructor), and
- If $\vec{z}$ are total, then so is $\mathrm{C}\vec{z}$.

The cototal ideals x are those of the form $\mathrm{C}\vec{z}$ with C a constructor of ι and $\vec{z}$ cototal. – For example, in **L**(**SD**),

- the total ideals are the finite and
- the cototal ideals are the finite or infinite

lists of signed digits ($\sim$ an interval with rational end points or a stream real, both in $[-1, 1]$).

Totality in higher types, density

- An ideal r of type $\rho \to \sigma$ is total iff for all total z of type ρ, the result $|r|(z)$ of applying r to z is total.
- Density theorem (Kreisel 1959, Ershov 1972, U. Berger 1993): Assume that all base types are finitary. Then for every $U \in \mathrm{Con}_\rho$ we can find a total x such that $U \subseteq x$.

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

- Terms $M, N ::= x^\rho \mid C \mid D \mid (\lambda_{x^\rho} M^\sigma)^{\rho\to\sigma} \mid (M^{\rho\to\sigma} N^\rho)^\sigma$.
- Constants D defined by computation rules. Examples:
  Recursion $\mathcal{R}_{\mathbf{N}}^\tau \colon \mathbf{N} \to (\mathbf{U} \times \tau \times \mathbf{N} \to \tau) \to \tau$.

$$\mathcal{R}0xy = x, \quad \mathcal{R}(\mathrm{S}n)xy = yn(\mathcal{R}nxy).$$

  Corecursion $\mathcal{C}_{\mathbf{N}}^\tau \colon \tau \to (\tau \to \mathbf{U} + \tau + \mathbf{N}) \to \mathbf{N}$.

$$\mathcal{C}xy = [\textbf{case } yx \textbf{ of } 0 \mid \lambda_z(\mathrm{S}[\textbf{case } z^{\tau+\mathbf{N}} \textbf{ of } \lambda_u(\mathcal{C}uy) \mid \lambda_n n])].$$

  Case of type $\rho + \sigma \to (\rho \to \tau) \to (\sigma \to \tau) \to \tau$:

$$[\textbf{case } (\mathrm{inl}(M))^{\rho+\sigma} \textbf{ of } \lambda_x N(x) \mid \lambda_y K(y)] = N(M),$$
$$[\textbf{case } (\mathrm{inr}(M))^{\rho+\sigma} \textbf{ of } \lambda_x N(x) \mid \lambda_y K(y)] = K(M).$$

Denotational semantics

- Define $(\vec{U}, b) \in [\![\lambda_{\vec{x}} M]\!]$:

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

  For every constructor C and defined constant D

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

  with one rule (D) for every computation rule $D\vec{P}(\vec{y}) = M$.
- $[\![M]\!]_{\vec{x}}^{\vec{U}} := \{\, b \mid (\vec{U}, b) \in [\![\lambda_{\vec{x}} M]\!] \,\}$ and $[\![M]\!]_{\vec{x}}^{\vec{u}} := \bigcup_{\vec{U} \subseteq \vec{u}} [\![M]\!]_{\vec{x}}^{\vec{U}}$.

Properties

- $[\![\lambda_{\vec{x}} M]\!]$ is an ideal, i.e., consistent and deductively closed.
- (Monotonicity) If $\vec{v} \supseteq \vec{u}$, $b \geq c$ and $b \in [\![M]\!]_{\vec{x}}^{\vec{u}}$, then $c \in [\![M]\!]_{\vec{x}}^{\vec{v}}$.
- (Substitution) $[\![M(z)]\!]_{\vec{x},z}^{\vec{u},[\![N]\!]_{\vec{x}}^{\vec{u}}} = [\![M(N)]\!]_{\vec{x}}^{\vec{u}}$.
- (Beta) $[\![(\lambda_y M(y))N]\!]_{\vec{x}}^{\vec{u}} = [\![M(N)]\!]_{\vec{x}}^{\vec{u}}$.
- (Eta) $[\![\lambda_y (My)]\!]_{\vec{x}}^{\vec{u}} = [\![M]\!]_{\vec{x}}^{\vec{u}}$ if $y \notin \mathrm{FV}(M)$.

Preservation of values

Theorem (Substitution of constructor terms)

$(\vec{U}, \vec{V}, b) \in [\![\lambda_{\vec{x},\vec{y}} M(\mathrm{C}\vec{y}\,)]\!] \leftrightarrow (\vec{U}, \mathrm{C}\vec{V}, b) \in [\![\lambda_{\vec{x},z} M(z)]\!]$, *with the same height and D-height.*

Corollary (Preservation of values under computation rules)

For every computation rule $D\vec{P}(\vec{y}\,) = M$ *of a defined constant* D, $[\![\lambda_{\vec{y}}(D\vec{P}(\vec{y}\,))]\!] = [\![\lambda_{\vec{y}} M]\!]$.

Head reduction

Define $M \succ_1 N$, M head-reduces to N:

$$(\lambda_x M(x))N \succ_1 M(N),$$

$$\frac{M \succ_1 M'}{MN \succ_1 M'N},$$

$$D\vec{P}(\vec{N}) \succ_1 M(\vec{N}) \quad \text{for } D\vec{P}(\vec{y}) = M(\vec{y}) \text{ a computation rule,}$$

$$\frac{N \succ_1 N'}{MN \succ_1 MN'} \quad \text{for } M \text{ in head normal form.}$$

Operational semantics

Define $M \in [a]$, for M closed:

- For a of base type ι, $M \in [a]$ iff $\exists_{N \geq a} M \succeq N$.
- $M \in [(U, b)]$ iff $M \succeq \lambda_x M'$ or M in head normal form, and $\forall_{N \in [U]} MN \in [b]$.

Write $M \in [U]$ for $\forall_{a \in U} M \in [a]$ (operational interpretation of formal neighborhoods, Martin-Löf 1983). – Plotkin (1977) proved: Whenever an atom b belongs to the value of a closed term M, then M head-reduces to an atom entailing b. Here we have more generally:

Theorem (Adequacy)

$$(\vec{U}, b) \in [\![\lambda_{\vec{x}} M]\!] \to \lambda_{\vec{x}} M \in [(\vec{U}, b)].$$

Formulas, predicates, clauses: general definition

Let X be a fixed predicate variable. Formulas $A, B, C, D \in \mathrm{F}$, predicates $P, Q, I \in \mathrm{Preds}$ and constructor formulas (or clauses) $K \in \mathrm{KF}_X$ are generated inductively:

$$\frac{\vec{A}, \vec{B}_0, \dots, \vec{B}_{n-1} \in \mathrm{F}}{\forall_{\vec{x}}(\vec{A} \to (\forall_{\vec{y}_\nu}(\vec{B}_\nu \to X(\vec{s}_\nu)))_{\nu<n} \to X(\vec{t}\,)) \in \mathrm{KF}_X} \quad (n \geq 0)$$

$$\frac{K_0, \dots, K_{k-1} \in \mathrm{KF}_X \quad (k \geq 1)}{\mu_X(K_0, \dots, K_{k-1}) \in \mathrm{Preds}} \qquad \frac{P \in \mathrm{Preds}}{P(\vec{r}\,) \in \mathrm{F}} \qquad \frac{C \in \mathrm{F}}{\{\, \vec{x} \mid C \,\} \in \mathrm{Preds}}$$

$$\frac{A, B \in \mathrm{F}}{A \to B \in \mathrm{F}} \qquad \frac{A \in \mathrm{F}}{\forall_{x^\rho} A \in \mathrm{F}}.$$

We always require a nullary clause.

Logic of inductive definitions LID

LID is the (extensional) system in minimal logic for $\to$ and $\forall$, whose formulas are those in F above, and whose axioms are, for each inductively defined predicate, introduction or closure axioms, together with an elimination or least fixed point axiom.

Example

Totality $T_{\mathbf{N}}$ is inductively defined by

$$T_{\mathbf{N}}(0),$$
$$\forall_n(T_{\mathbf{N}}(n) \to T_{\mathbf{N}}(\mathrm{S}n)),$$
$$\forall_{n \in T}\big(A(0) \to \forall_{n \in T}(A(n) \to A(\mathrm{S}n)) \to A(n^{\mathbf{N}})\big).$$

Further examples of inductively defined predicates

- Leibniz equality. $\mathrm{Eq}^+ \colon \forall_x \mathrm{Eq}(x,x)$,
  $\mathrm{Eq}^- \colon \forall_{x,y}(\mathrm{Eq}(x,y) \to \forall_x C(x,x) \to C(x,y))$.
- Existence. $\exists^+ \colon \forall_x(A \to \exists_x A)$.
  $\exists^- \colon \exists_x A \to \forall_x(A \to C) \to C$ with $x \notin \mathrm{FV}(C)$.
- Conjunction. $\wedge^+ \colon A \to B \to A \wedge B$.
  $\wedge^- \colon A \wedge B \to (A \to B \to C) \to C$.

Properties of Leibniz equality

Recall $\mathrm{Eq}^+ \colon \forall_x \mathrm{Eq}(x,x)$,
$\mathrm{Eq}^- \colon \forall_{x,y}(\mathrm{Eq}(x,y) \to \forall_x C(x,x) \to C(x,y))$.

Lemma (Compatibility of Eq)

$\forall_{x,y}\left(\mathrm{Eq}(x,y) \to A(x) \to A(y)\right)$.

Proof.
Use Eq^- with $C(x,y) := A(x) \to A(y)$. $\square$

Using compatibility of Eq one easily proves symmetry and transitivity.

Decidable prime formulas, falsity

Using Leibniz equality, we can lift a boolean term r to a prime formula $\mathrm{Eq}(r, \mathtt{tt})$. Define falsity by $\mathbf{F} := \mathrm{Eq}(\mathtt{ff}, \mathtt{tt})$.

Theorem (Ex Falso Quodlibet)

$\mathbf{F} \to A$.

Proof.

We first show $\mathbf{F} \to \mathrm{Eq}(x^\rho, y^\rho)$. Notice: from $\mathrm{Eq}(\mathtt{ff}, \mathtt{tt})$ we obtain $\mathrm{Eq}[\mathbf{if}\ \mathtt{tt}\ \mathbf{then}\ x\ \mathbf{else}\ y][\mathbf{if}\ \mathtt{ff}\ \mathbf{then}\ x\ \mathbf{else}\ y]$ by compatibility. Hence $\mathrm{Eq}(x^\rho, y^\rho)$.
Now use induction on $A \in \mathrm{F}$. *Case* $I(\vec{s}\,)$. Let K_i be the nullary clause, with final conclusion $I(\vec{t}\,)$. By IH from $\mathbf{F}$ we can derive all parameter premises. Hence $I(\vec{t}\,)$. From $\mathbf{F}$ we also obtain $\mathrm{Eq}(s_i, t_i)$. Hence $I(\vec{s}\,)$ by compatibility. Cases $A \to B$ and $\forall_x A$: obvious. □

Embedding PA^ω

- Define $\neg A := A \to \mathbf{F}$, $\tilde{\exists}_x A := \neg\forall_x \neg A$ weak (or "classical") existence.
- Decidable equality for finitary base types: $=_\iota : \iota \to \iota \to \mathbf{B}$.
- A is stable if $\neg\neg A \to A$.
- $\forall_{p \in T}(\neg\neg\mathrm{Eq}(p, \mathtt{tt}) \to \mathrm{Eq}(p, \mathtt{tt}))$ by boolean induction.

Lemma (Stability)

If A has a stable end conclusion, then $\neg\neg A \to A$.

Cototality

Cototality $T^{\infty}_{\mathbf{N}}$ is coinductively defined by the clause

$$\forall^{\mathrm{U}}_{n}(T^{\infty}_{\mathbf{N}}(n) \to n{=}0 \lor \exists_{m}(n{=}\mathrm{S}m \land T^{\infty}_{\mathbf{N}}(m)))$$

and the greatest fixed point axiom

$$\begin{aligned}&\forall^{\mathrm{U}}_{n}(A(n) \to \\ &\quad \forall^{\mathrm{U}}_{n}(A(n) \to n{=}0 \lor \exists_{m}[n{=}\mathrm{S}m \land (A(m) \lor T^{\infty}_{\mathbf{N}}(m))]) \to \\ &\quad T^{\infty}_{\mathbf{N}}(n)).\end{aligned}$$

The greatest fixed point axiom is called coinduction.

Why extract computational content from proofs?

- Proofs are machine checkable $\Rightarrow$ no logical errors.
- Program on the proof level $\Rightarrow$ maintenance becomes easier. Possibility of program development by proof transformation (Goad 1980).
- Discover unexpected content:
  - U. Berger 1993: Tait's proof of the existence of normal forms for the typed λ-calculus $\Rightarrow$ "normalization by evaluation".
  - Content in weak (or "classical") existence proofs, of

    $$\tilde{\exists}_x A := \neg \forall_x \neg A,$$

    via proof interpretations: (refined) A-translation or Gödel's Dialectica interpretation.

Soundness

For every proof M in LID we can define its extracted term $[\![M]\!]$ (modified realizability interpretation: Kreisel 1959, Seisenberger 2003). In particular this needs to be done for the axioms.

Theorem

Let M be a derivation of A from assumptions $u_i\colon C_i$ $(i < n)$. Then we can find a derivation of $[\![M]\!]$ $\mathbf{r}$ A from assumptions $\bar{u}_i\colon x_{u_i}$ $\mathbf{r}$ C_i.

Proof.

Induction on A. $\square$

Recursion operator $= [\![T_{\mathbf{N}}^{\mathrm{fp}}]\!]$

Fixed point axiom for totality

$$T_{\mathbf{N}}^{\mathrm{fp}} \colon \forall_n (T_{\mathbf{N}}(n) \to A(0) \to \forall_n (T_{\mathbf{N}}(n) \to A(n) \to A(\mathrm{S}n)) \to A(n^{\mathbf{N}})).$$

Its extracted term is the structural recursion operator

$$\mathcal{R}_{\mathbf{N}}^{\tau} \colon \mathbf{N} \to \tau \to (\mathbf{N} \to \tau \to \tau) \to \tau,$$

since $\tau(T_{\mathbf{N}}(n)) := \varepsilon$.

Corecursion operator $= [\![(T^\infty_{\mathbf{N}})^{\mathrm{fp}}]\!]$

Fixed point axiom for cototality

$$(T^\infty_{\mathbf{N}})^{\mathrm{fp}} \colon \forall^{\mathsf{U}}_n (A(n) \to \forall^{\mathsf{U}}_n (A(n) \to n{=}0 \lor \exists_m [n{=}\mathrm{S}m \land (A(m) \lor T^\infty_{\mathbf{N}}(m))]) \to T^\infty_{\mathbf{N}}(n)).$$

Its extracted term is the corecursion operator

$$\mathcal{C}^\tau_{\mathbf{N}} \colon \tau \to (\tau \to \mathbf{U} + \tau + \mathbf{N}) \to \mathbf{N},$$

since $\tau(T^\infty_{\mathbf{N}}(n)) := \mathbf{N}$ and $\tau(\forall^{\mathsf{U}}_x B) := \tau(B)$.

Decorating proofs

Goal: Insertion of uniformity marks (Berger 2005) into a proof.

- The sequent $\mathrm{Seq}(M)$ of a proof M consists of its context and its end formula.
- The uniform proof pattern $\mathrm{UP}(M)$ of a proof M is the result of changing in M all occurrences of $\to, \forall, \exists, \wedge$ in its formulas into their uniform counterparts $\to^{\mathsf{U}}, \forall^{\mathsf{U}}, \exists^{\mathsf{U}}, \wedge^{\mathsf{U}}$, except the uninstantiated formulas of axioms and theorems.
- A formula D extends C if D is obtained from C by changing some connectives into one of their more informative versions, according to the following ordering: $\to^{\mathsf{U}} \leq \to$, $\forall^{\mathsf{U}} \leq \forall$, $\exists^{\mathsf{U}} \leq \exists^{\mathsf{L}}, \exists^{\mathsf{R}} \leq \exists$ and $\wedge^{\mathsf{U}} \leq \wedge^{\mathsf{L}}, \wedge^{\mathsf{R}} \leq \wedge$.
- A proof N extends M if (1) $\mathrm{UP}(M) = \mathrm{UP}(N)$, and (2) each formula in N extends the corresponding one in M. In this case $\mathrm{FV}([\![N]\!])$ is essentially (i.e., up to extensions of assumption formulas) a superset of $\mathrm{FV}([\![M]\!])$.

Decoration algorithm

Theorem (Ratiu, S)

For every uniform proof pattern U and every extension of its sequent $\mathrm{Seq}(U)$ we can find a decoration M_∞ of U such that

(a) $\mathrm{Seq}(M_\infty)$ *extends the given extension of* $\mathrm{Seq}(U)$*, and*

(b) M_∞ *is optimal in the sense that any other decoration M of U whose sequent $\mathrm{Seq}(M)$ extends the given extension of $\mathrm{Seq}(U)$ has the property that M also extends M_∞.*