Invariance axioms for realizability

Helmut Schwichtenberg

Mathematisches Institut, LMU, München

May 7, 2016

Kolmogorov 1932: "Zur Deutung der intuitionistischen Logik"

- Proposed to view a formula A as a computational problem, of type $\tau(A)$, the type of a potential solution or "realizer" of A.
- Example: $\forall_n \exists_{m>n} \mathrm{Prime}(m)$ has type $\mathbf{N} \to \mathbf{N}$.

The fact that nested implications may occur in A requires the concept of higher type computable functionals.

Computation in higher types

Fundamental property of computation:

evaluation must be finite.

- Principle of finite support. If $\mathcal{H}(\Phi)$ is defined with value n, then there is a finite approximation Φ_0 of Φ such that $\mathcal{H}(\Phi_0)$ is defined with value n.
- Monotonicity principle. If $\mathcal{H}(\Phi)$ is defined with value n and Φ' extends Φ, then also $\mathcal{H}(\Phi')$ is defined with value n.
- Effectivity principle. An object is computable just in case its set of finite approximations is (primitive) recursively enumerable (or equivalently, Σ^0_1-definable).

- Gödel (1958): "Über eine noch nicht benützte Erweiterung des finiten Standpunkts". Higher type term system T.
- Platek (1966): "Foundations of recursion theory".
- Scott (1969): LCF "Logic for Computable Functions". LCF's term language has arithmetic, booleans and recursion in higher types. LCF is based on classical logic.
- Plotkin (1977): Higher type term system PCF, with partiality.
- Martin-Löf (1984): constructive type theory. Formulas are types. Functionals are total.
- Proposal here: a constructive theory of computation in higher types, based on the Scott (1970) - Ershov (1977) model of partial continuous functionals.

points, ideals, abstract objects

$\uparrow\downarrow$

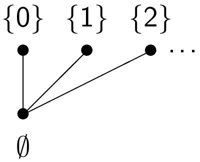
finite approximations

(Finitary) algebras viewed as “non-flat Scott information systems”.

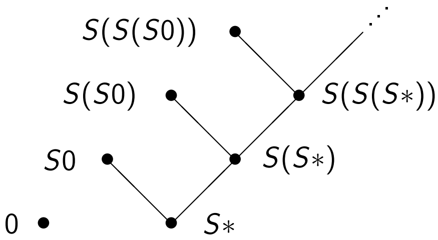
- An algebra ι is given by its constructors.
- Example: $0^{\mathbf{N}}, S^{\mathbf{N} \to \mathbf{N}}$ for $\mathbf{N}$ (unary natural numbers)
- Examples of “tokens”: $S^n 0$ ($n \geq 0$), $S^2 *$ (in $\mathbf{N}$) ($*$: special symbol; no information).
- A token is total if it contains no $*$.

Flat or non flat algebras?

- Flat:



- Non flat:



Non flat!

- Continuous maps 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: $Sx \neq 0$ and $Sx = Sy \to x = y$).
- 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

in **P**:	$S_1\emptyset = \emptyset = S_2\emptyset$	(overlapping ranges),
in **D**:	$\mathrm{C}\emptyset\{0\} = \emptyset = \mathrm{C}\{0\}\emptyset$	(not injective).

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 $\mathbf{C}_\rho$ (ideals are consistent and deductively closed sets of tokens).

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

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

TCF (theory of computable functionals), a variant of HA^ω with variables ranging over arbitrary partial continuous functionals.

- Existence axioms: by terms, built from constants for (partial) computable functionals, given by defining equations (computation rules, pattern matching conditions apply)
- Inductively (and coinductively) defined predicates. Totality for ground types inductively defined.
- Induction := elimination (or least-fixed-point) axiom for a totality predicate. (Coinduction := greatest-fixed-point axiom for a coinductively defined predicate.)
- Minimal logic: $\to, \forall$ only. $=^{\mathrm{d}}$ (Leibniz), $\exists$, $\vee$, $\wedge$ inductively defined (Russell, Martin-Löf).
- $\bot := (\mathrm{False} =^{\mathrm{d}} \mathrm{True})$. Ex-falso-quodlibet: $\bot \to A$ provable.

Definition ($a \in [\![\lambda_{\vec{x}} M]\!]$)

Case $\lambda_{\vec{x},y,\vec{z}} M$ with $\vec{x}$ free in M, but not y.

$$\frac{(\vec{U}, \vec{W}, a) \in [\![\lambda_{\vec{x},\vec{z}} M]\!]}{(\vec{U}, V, \vec{W}, a) \in [\![\lambda_{\vec{x},y,\vec{z}} M]\!]}(K).$$

Case $\lambda_{\vec{x}} M$ with $\vec{x}$ the free variables in M.

$$\frac{U \vdash a}{(U, a) \in [\![\lambda_x x]\!]}(V), \quad \frac{(\vec{U}, V, a) \in [\![\lambda_{\vec{x}} M]\!] \quad (\vec{U}, V) \subseteq [\![\lambda_{\vec{x}} N]\!]}{(\vec{U}, a) \in [\![\lambda_{\vec{x}} (MN)]\!]}(A).$$

For every constructor C and defined constant D:

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

with one rule (D) for every defining equation $D\vec{P}(\vec{x}) = M$.

Predicates and formulas

$$P, Q ::= X \mid \{\,\vec{x} \mid A\,\} \mid \mu_X(\forall_{\vec{x}_i}((A_{i\nu})_{\nu<n_i} \to X\vec{r}_i))_{i<k}$$
$$A, B ::= P\vec{r} \mid A \to B \mid \forall_x A$$

Examples

$$\begin{aligned}
\mathrm{Total} &:= \mu_X(X0, \forall_n(Xn \to X(Sn))) \\
\mathrm{Ex}_Y &:= \mu_X(\forall_x(Yx \to X)) \\
\mathrm{Or}_{Y,Z} &:= \mu_X(Y \to X,\ Z \to X)
\end{aligned}$$

Define $\tau(C)$ for predicates and formulas C. Given $X \mapsto \xi$.

$$\tau(X) := \xi$$
$$\tau(\{\, \vec{x} \mid A \,\}) := \tau(A)$$
$$\tau(\underbrace{\mu_X(\forall_{\vec{x}_i}(\vec{A}_i \to X\vec{r}_i))_{i<k}}_{I}) := \underbrace{\mu_\xi(\tau(\vec{x}_i) \to \tau(\vec{A}_i) \to \xi)_{i<k}}_{\iota_I}$$

ι_I is the algebra associated with I.

$$\tau(P\vec{r}\,) := \tau(P)$$
$$\tau(A \to B) := (\tau(A) \to \tau(B))$$
$$\tau(\forall_{x^\rho} A) := (\rho \to \tau(A))$$

Examples of ι_I. Recall

$$\begin{aligned} \mathrm{Total} &:= \mu_X(X0, \forall_n(Xn \to X(Sn))) \\ \mathrm{Ex}_Y &:= \mu_X(\forall_x(Yx \to X)) \\ \mathrm{Or}_{Y,Z} &:= \mu_X(Y \to X,\ Z \to X) \end{aligned}$$

Then

ι_{Total} algebra with constructors $\mathrm{O}\colon \iota_{\mathrm{Total}}$, $\mathrm{C}\colon \mathbf{N} \to \iota_{\mathrm{Total}} \to \iota_{\mathrm{Total}}$

$\iota_{\mathrm{Ex}_Y} := \rho \times \zeta$

$\iota_{\mathrm{Or}_{Y,Z}} := \zeta + \eta$

Realizability. Given $X\colon(\vec\rho) \mapsto X^{\mathbf{r}}\colon(\tau(X), \vec\rho)$.

$$
\begin{aligned}
X^{\mathbf{r}} &:= \text{as given}\\
\{\, \vec y \mid A \,\}^{\mathbf{r}} &:= \{\, x, \vec y \mid x \mathrel{\mathbf{r}} A \,\}\\
I^{\mathbf{r}} &:= \mu^{\mathrm{nc}}_{X^{\mathbf{r}}}(\forall_{\vec y_i, \vec x_i}((x_{i\nu} \mathrel{\mathbf{r}} A_{i\nu})_{\nu<n_i} \to \mathrm{C}_i \vec y_i \vec x_i \mathrel{\mathbf{r}} X \vec r_i))_{i<k}\\
&\qquad \text{for } I := \mu_X(\forall_{\vec y_i}((A_{i\nu})_{\nu<n_i} \to X \vec r_i))_{i<k}
\end{aligned}
$$

$$
\begin{aligned}
x \mathrel{\mathbf{r}} P\vec r &:= P^{\mathbf{r}} x \vec r\\
x \mathrel{\mathbf{r}} (A \to B) &:= \forall_y (y \mathrel{\mathbf{r}} A \to xy \mathrel{\mathbf{r}} B)\\
x \mathrel{\mathbf{r}} \forall_y A &:= \forall_y (xy \mathrel{\mathbf{r}} A)
\end{aligned}
$$

Examples. Recall

$$\mathrm{Total} := \mu_X(X0, \forall_n(Xn \to X(Sn))),$$
$$\iota_{\mathrm{Total}} \text{ with constructors } \mathrm{O}\colon \iota_{\mathrm{Total}},\ \mathrm{C}\colon \mathbf{N} \to \iota_{\mathrm{Total}} \to \iota_{\mathrm{Total}}$$

Then

$$\mathrm{Total}^{\mathbf{r}} := \mu^{\mathrm{nc}}_{X^{\mathbf{r}}}(\mathrm{O}\ \mathbf{r}\ X0, \forall_{n,x}(x\ \mathbf{r}\ Xn \to \mathrm{C}(n,x)\ \mathbf{r}\ X(Sn))).$$

With $x_0 := \mathrm{O}$, $x_{n+1} := \mathrm{C}(n, x_n)$ we have

$$x_n\ \mathbf{r}\ \mathrm{Total}\ n$$

Recall

$$\begin{aligned} \mathrm{Ex}_{Y} &:= \mu_X(\forall_y(Yy \to X)) \\ \mathrm{Or}_{Y,Z} &:= \mu_X(Y \to X,\ Z \to X) \end{aligned}$$

Then

$$\begin{aligned} \mathrm{Ex}^{\mathbf{r}}_{Y^{\mathbf{r}}} &:= \mu^{\mathrm{nc}}_{X^{\mathbf{r}}}(\forall_{y,x}(x \mathrel{\mathbf{r}} Yy \to (y,x) \mathrel{\mathbf{r}} X)), \\ \mathrm{Or}^{\mathbf{r}}_{Y^{\mathbf{r}},Z^{\mathbf{r}}} &:= \mu^{\mathrm{nc}}_{X^{\mathbf{r}}}(\forall_y(y \mathrel{\mathbf{r}} Y \to \mathrm{Inl}(y) \mathrel{\mathbf{r}} X),\ \forall_z(z \mathrel{\mathbf{r}} Z \to \mathrm{Inr}(z) \mathrel{\mathbf{r}} X)). \end{aligned}$$

- Add μ^{nc}-clause in the definition of predicates.
- Witnesses in μ^{nc}-predicates ignored: they are already there.
- Add axioms:

$$A \leftrightarrow \exists_x (x \mathbf{r} A) \qquad \text{(invariance under realizability)}$$

- Then (Troelstra): AC, IP derivable. Realizers are identities.
- Soundness theorem:

$$M \vdash A \quad \text{implies} \quad \vdash \mathrm{et}(M) \mathbf{r} A.$$

- Decoration (for fine tuning): $\forall^{\mathrm{nc}}, \to^{\mathrm{nc}}, X^{\mathrm{nc}}, \mu^{\mathrm{nc}}$
- Correct proof: ignore $^{\mathrm{nc}}$-decorations in n.c. subproofs
- $A \mapsto A^{\mathrm{nc}}$ (in final conclusion $\mu, X \mapsto \mu^{\mathrm{nc}}, X^{\mathrm{nc}}$)
- Variants of $\exists$, $\vee$ etc., e.g.

$$\begin{aligned}
\mathrm{ExL}_Y &:= \mu_X(\forall_x(Yx \to^{\mathrm{nc}} X)) \\
\mathrm{OrU} &:= \mu_X(Y \to^{\mathrm{nc}} X,\ Z \to^{\mathrm{nc}} X) \\
\mathrm{OrNC} &:= \mu_X^{\mathrm{nc}}(Y \to^{\mathrm{nc}} X,\ Z \to^{\mathrm{nc}} X)
\end{aligned}$$

- Properties of **r** for $\exists^{\mathrm{l}}$ etc., e.g. $(x\ \mathbf{r}\ \exists^{\mathrm{l}}_x A) \leftrightarrow A^{\mathrm{nc}}$
- $\vdash (A \to^{\mathrm{nc}} B) \leftrightarrow (A^{\mathrm{nc}} \to B)$
- Decoration algorithm