Invariance axioms for realizability

Helmut Schwichtenberg

Mathematisches Institut, LMU, München

JAIST, 25. August 2016

Kolmogorov 1932: "Zur Deutung der intuitionistischen Logik"

- 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 $\mathbf{N} \to \mathbf{N}$.

Proposal: express this view as

invariance under realizability

of formulas A:

$$A \leftrightarrow \text{there is a solution of problem } A$$

- A may have nested implications.
- Hence a solution is a higher type computable functional ("modified realizability").

- 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

Examples of computable functionals

- Fixed point operator $Y\colon (\rho \to \rho) \to \rho$ defined by

$$Yf = f(Yf)$$

- Recursion operator $\mathcal{R}^{\tau}_{\mathbf{N}}\colon \mathbf{N} \to \tau \to (\mathbf{N} \to \tau \to \tau) \to \tau$ defined by

$$\begin{aligned} \mathcal{R}0mf &= m, \\ \mathcal{R}(Sn)mf &= fn(\mathcal{R}nmf). \end{aligned}$$

- Corecursion operator ${}^{\mathrm{co}}\mathcal{R}^{\tau}_{\mathbf{N}}\colon \tau \to (\tau \to \mathbf{U} + (\mathbf{N} + \tau)) \to \mathbf{N}$

Definition (Types).

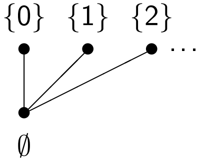
$$\rho, \sigma ::= \alpha \mid \rho \to \sigma \mid \mu_\xi((\rho_{i\nu})_{\nu<n_i} \to \xi)_{i<k}$$

Examples

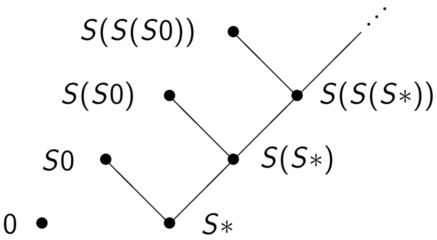
$$\begin{aligned}
\mathbf{U} &:= \mu_\xi \xi && \text{(unit)},\\
\mathbf{B} &:= \mu_\xi(\xi, \xi) && \text{(booleans)},\\
\mathbf{N} &:= \mu_\xi(\xi, \xi \to \xi) && \text{(natural numbers, unary)},\\
\mathbf{P} &:= \mu_\xi(\xi, \xi \to \xi, \xi \to \xi) && \text{(positive numbers, binary)},\\
\mathbf{D} &:= \mu_\xi(\xi, \xi \to \xi \to \xi) && \text{(binary trees, or derivations)},\\
\mathbf{L}(\alpha) &:= \mu_\xi(\xi, \alpha \to \xi \to \xi) && \text{(lists)},\\
\alpha \times \beta &:= \mu_\xi(\alpha \to \beta \to \xi) && \text{(product)},\\
\alpha + \beta &:= \mu_\xi(\alpha \to \xi, \beta \to \xi) && \text{(sum)}.
\end{aligned}$$

(Finitary) algebras viewed as "non-flat Scott information systems". Why?

- Flat:



- Non flat: "tokens" for **N** are



Problem for flat algebras

- Continuous functions 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

$$\begin{array}{lll} \text{in } \mathbf{P}\text{:} & S_0\emptyset = \emptyset = S_1\emptyset & \text{(overlapping ranges),} \\ \text{in } \mathbf{D}\text{:} & \mathrm{C}\emptyset\{0\} = \emptyset = \mathrm{C}\{0\}\emptyset & \text{(not injective).} \end{array}$$

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: $\mathbf{A} \to \mathbf{B} := (C, \mathrm{Con}, \vdash)$:

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

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

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

- Partial continuous functionals of type ρ: the "ideals" in $\mathbf{C}_\rho$ (ideals are consistent and deductively closed sets of tokens).

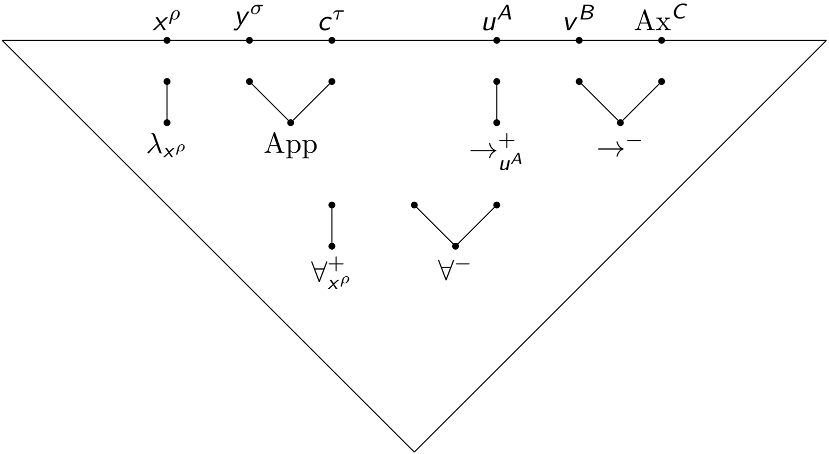
$$\mathbf{C}_\iota := (C_\iota, \mathrm{Con}_\iota, \vdash_\iota), \qquad \mathbf{C}_{\rho \to \sigma} := \mathbf{C}_\rho \to \mathbf{C}_\sigma.$$

- $f \in |\mathbf{C}_\rho|$: 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.

Proof terms in natural deduction



The realizability interpretation transforms such a proof term directly into an object term.

Decoration

Proofs can be transformed and/or "decorated", for efficiency of the extracted program.

- A related concept of "proof irrelevance" has been studied by Pfenning and (in Agda) by Abel/Scherer (2012).

We decorate

- connectives: $\to^{\mathrm{c}}, \forall^{\mathrm{c}}$ and $\to^{\mathrm{nc}}, \forall^{\mathrm{nc}}$, and
- least-fixed-point operators: $\mu^{\mathrm{c}}, \mu^{\mathrm{nc}}$.

Distinguish two sorts of predicate variables

- computationally relevant ones $X, Y, Z \dots$, and
- non-computational ones $X^{\mathrm{nc}}, Y^{\mathrm{nc}}, Z^{\mathrm{nc}} \dots$.

Definition (Predicates and formulas).

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

$$A, B ::= P\vec{r} \mid A \to^{\mathrm{c/nc}} B \mid \forall_x^{\mathrm{c/nc}} A$$

Write $\to$, $\forall$, μ for $\to^{\mathrm{c}}$, $\forall^{\mathrm{c}}$, μ^{c}. Examples

$$\begin{aligned}
\mathrm{Total}_{\mathbf{N}} &:= \mu_X(X0, \forall_n^{\mathrm{nc}}(Xn \to X(Sn))) \\
\mathrm{ExD}_Y &:= \mu_X(\forall_x(Yx \to X)) \\
\mathrm{ExL}_Y &:= \mu_X(\forall_x(Yx \to^{\mathrm{nc}} X)) \\
\mathrm{CupU}_{Y,Z} &:= \mu_X(Y \to^{\mathrm{nc}} X,\ Z \to^{\mathrm{nc}} X) \\
\mathrm{CupNc}_{Y,Z} &:= \mu_X^{\mathrm{nc}}(Y \to X,\ Z \to X)
\end{aligned}$$

Abbreviations

$$\begin{aligned}
\exists_x^{\mathrm{d}} A &:= \mathrm{ExD}_{\{x \mid A\}} \\
\exists_x^{\mathrm{l}} A &:= \mathrm{ExL}_{\{x \mid A\}} \\
A \vee^{\mathrm{u}} B &:= \mathrm{CupU}_{\{\mid A\},\{\mid B\}} \\
A \vee^{\mathrm{nc}} B &:= \mathrm{CupNc}_{\{\mid A\},\{\mid B\}}
\end{aligned}$$

Axioms

We have introduction and elimination axioms for inductively defined predicates I. Example:

$$\mathrm{Even} := \mu_X(X0, \forall^{\mathrm{nc}}_n(Xn \to X(S(Sn))))$$

Introduction axioms

$$\mathrm{Even}(0), \qquad \forall^{\mathrm{nc}}_n(\mathrm{Even}(n) \to \mathrm{Even}(S(Sn)))$$

Elimination axioms

$$\forall^{\mathrm{nc}}_n(\mathrm{Even}(n) \to P0 \to \forall^{\mathrm{nc}}_m(\mathrm{Even}(m) \to Pm \to P(S(Sm))) \to Pn).$$

Computationally relevant (c.r.) and non-computational (n.c.) predicates and formulas

To every predicate or formula C assign its final predicate $\mathrm{fp}(C)$

$$
\begin{aligned}
\mathrm{fp}(X) &:= X, \quad \mathrm{fp}(X^{\mathrm{nc}}) := X^{\mathrm{nc}} & \mathrm{fp}(P\vec{r}\,) &:= \mathrm{fp}(P) \\
\mathrm{fp}(\{\, \vec{x} \mid A \,\}) &:= \mathrm{fp}(A) & \mathrm{fp}(A \to^{\mathrm{c/nc}} B) &:= \mathrm{fp}(B) \\
\mathrm{fp}(I) &:= I, \quad \mathrm{fp}(I^{\mathrm{nc}}) := I^{\mathrm{nc}} & \mathrm{fp}(\forall_x^{\mathrm{c/nc}} A) &:= \mathrm{fp}(A)
\end{aligned}
$$

C is non-computational (n.c.) if its final predicate $\mathrm{fp}(C)$ is of the form X^{nc} or I^{nc}. Else: computationally relevant (c.r.).

Logic with decorations

Introduction and elimination rules for $\to^{\mathrm{c/nc}}$, $\forall^{\mathrm{c/nc}}$.

- In n.c. parts of a derivation (i.e., with an n.c. end formula) decorations are ignored.
- If M^B is a derivation and u^A not a "computational assumption variable" ($u^A \notin \mathrm{CA}(M)$), then $(\lambda_{u^A} M^B)^{A \to^{\mathrm{nc}} B}$ is a derivation.
- If M^A is a derivation, x is not free in any formula of a free assumption variable of M and x not a "computational object variable" ($x \notin \mathrm{CV}(M)$), then $(\lambda_x M^A)^{\forall^{\mathrm{nc}}_x A}$ is a derivation.

Computational assumption variables $\mathrm{CA}(M^A)$

For A n.c. let $\mathrm{CA}(M^A) := \emptyset$. Assume A c.r.

$$
\begin{aligned}
&\mathrm{CA}(c^A) := \emptyset \quad (c^A \text{ an axiom}),\\
&\mathrm{CA}(u^A) := \{u\},\\
&\mathrm{CA}((\lambda_{u^A} M^B)^{A \to B}) := \mathrm{CA}((\lambda_{u^A} M^B)^{A \to^{\mathrm{nc}} B}) := \mathrm{CA}(M) \setminus \{u\},\\
&\mathrm{CA}((M^{A \to B} N^A)^B) := \mathrm{CA}(M) \cup \mathrm{CA}(N),\\
&\mathrm{CA}((M^{A \to^{\mathrm{nc}} B} N^A)^B) := \mathrm{CA}(M),\\
&\mathrm{CA}((\lambda_x M^A)^{\forall_x A}) := \mathrm{CA}((\lambda_x M^A)^{\forall_x^{\mathrm{nc}} A}) := \mathrm{CA}(M),\\
&\mathrm{CA}((M^{\forall_x A(x)} r)^{A(r)}) := \mathrm{CA}((M^{\forall_x^{\mathrm{nc}} A(x)} r)^{A(r)}) := \mathrm{CA}(M).
\end{aligned}
$$

Computational object variables $\mathrm{CV}(M^A)$

For A n.c. let $\mathrm{CV}(M^A) := \emptyset$. Assume A c.r.

$$\begin{aligned}
&\mathrm{CV}(c^A) := \emptyset \quad (c^A \text{ an axiom}),\\
&\mathrm{CV}(u^A) := \emptyset,\\
&\mathrm{CV}((\lambda_{u^A} M^B)^{A\to B}) := \mathrm{CV}((\lambda_{u^A} M^B)^{A\to^{\mathrm{nc}} B}) := \mathrm{CV}(M),\\
&\mathrm{CV}((M^{A\to B} N^A)^B) := \mathrm{CV}(M) \cup \mathrm{CV}(N),\\
&\mathrm{CV}((M^{A\to^{\mathrm{nc}} B} N^A)^B) := \mathrm{CV}(M),\\
&\mathrm{CV}((\lambda_x M^A)^{\forall_x A}) := \mathrm{CV}((\lambda_x M^A)^{\forall_x^{\mathrm{nc}} A}) := \mathrm{CV}(M) \setminus \{x\},\\
&\mathrm{CV}((M^{\forall_x A(x)} r)^{A(r)}) := \mathrm{CV}(M) \cup \mathrm{FV}(r),\\
&\mathrm{CV}((M^{\forall_x^{\mathrm{nc}} A(x)} r)^{A(r)}) := \mathrm{CV}(M).
\end{aligned}$$

Type $\tau(C)$ of predicates and formulas C

Given $X \mapsto \xi$. For C n.c. let $\tau(C) := \circ$. Assume C is c.r.

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

Call ι_I the algebra associated with I.

$$\tau(P\vec{r}\,) := \tau(P),$$
$$\tau(A \to B) := \begin{cases} \tau(A) \to \tau(B) & \text{if } A \text{ is c.r.} \\ \tau(B) & \text{if } A \text{ is n.c.} \end{cases} \qquad \tau(A \to^{\mathrm{nc}} B) := \tau(B),$$
$$\tau(\forall_{x^\rho} A) := (\rho \to \tau(A)), \quad \tau(\forall^{\mathrm{nc}}_{x^\rho} A) := \tau(A).$$

Examples of ι_I. Recall

$$\begin{aligned}
\mathrm{Total}_{\mathbf{N}} &:= \mu_X(X0, \forall^{\mathrm{nc}}_n(Xn \to X(Sn))) \\
\mathrm{ExD}_Y &:= \mu_X(\forall_x(Yx^\rho \to X)) \\
\mathrm{ExL}_Y &:= \mu_X(\forall_x(Yx^\rho \to^{\mathrm{nc}} X)) \\
\mathrm{CupD}_{Y,Z} &:= \mu_X(Y \to X,\ Z \to X) \\
\mathrm{CupU}_{Y,Z} &:= \mu_X(Y \to^{\mathrm{nc}} X,\ Z \to^{\mathrm{nc}} X)
\end{aligned}$$

Then

$$\begin{aligned}
\iota_{\mathrm{Total}_{\mathbf{N}}} &:= \mathbf{N} \\
\iota_{\mathrm{ExD}_Y} &:= \rho \times \zeta \qquad \iota_{\mathrm{ExL}_Y} := \rho \\
\iota_{\mathrm{CupD}_{Y,Z}} &:= \zeta + \eta \qquad \iota_{\mathrm{CupU}_{Y,Z}} := \mathbf{B}
\end{aligned}$$

Realizability: $C^{\mathbf{r}}$ (n.c.) for predicates and formulas C

Given $X\colon (\vec{\rho}) \mapsto X^{\mathbf{r}}\colon (\tau(X), \vec{\rho})$. For C n.c. let $C^{\mathbf{r}} := C$.
Assume C is c.r. We define $C^{\mathbf{r}}\colon (\tau(C), \vec{\sigma}\,)$. Write $z \mathrel{\mathbf{r}} C$ for $C^{\mathbf{r}} z$.

$$X^{\mathbf{r}} \text{ given}, \qquad \{\, \vec{x} \mid A \,\}^{\mathbf{r}} := \{\, z, \vec{x} \mid z \mathrel{\mathbf{r}} A \,\}.$$

For $I := \mu_X(\forall^{\mathrm{c/nc}}_{\vec{y}_i}((A_{i\nu})_{\nu<n_i} \to^{\mathrm{c/nc}} X\vec{r}_i))_{i<k}$ define $I^{\mathbf{r}}$ by

$$I^{\mathbf{r}} := \mu^{\mathrm{nc}}_{X^{\mathbf{r}}}(\forall_{\vec{x}_i,\vec{z}_i}((z_{i\nu} \mathrel{\mathbf{r}} A_{i\nu})_{\nu<n_i} \to \mathrm{C}_i\vec{x}_i\vec{z}_i \mathrel{\mathbf{r}} X\vec{r}_i))_{i<k}$$

with the understanding that for

- for c.r. $A_{i\nu}$ followed by $\to$: $z_{i\nu} \mathrel{\mathbf{r}} A_{i\nu}$ and $z_{i\nu}$ is in $\mathrm{C}_i\vec{x}_i\vec{z}_i$,
- X in $A_{i\nu}$ followed by $\to^{\mathrm{nc}}$: $z_{i\nu} \mathrel{\mathbf{r}} A_{i\nu}$ but $z_{i\nu}$ is not in $\mathrm{C}_i\vec{x}_i\vec{z}_i$,
- else we keep $A_{i\nu}$ and there is no $z_{i\nu}$.

Only x_{ij} with a computational $\forall_{x_{ij}}$ occur as arguments in $\mathrm{C}_i\vec{x}_i\vec{z}_i$.
Here C_i is the i-th constructor of the algebra ι_I generated from the constructor types $\tau(K_i)$ with K_i the i-th clause of I.

Realizability (ctd.): $C^{\mathbf{r}}$ (n.c.) for formulas C

For c.r. formulas let

$$\begin{aligned}
z \,\mathbf{r}\, P\vec{r} &:= P^{\mathbf{r}}(z, \vec{r}\,) \\
z \,\mathbf{r}\, (A \to B) &:= \begin{cases} \forall_x (x \,\mathbf{r}\, A \to zx \,\mathbf{r}\, B) & \text{if } A \text{ is c.r.} \\ A \to z \,\mathbf{r}\, B & \text{if } A \text{ is n.c.} \end{cases} \\
z \,\mathbf{r}\, (A \to^{\mathrm{nc}} B) &:= A \to z \,\mathbf{r}\, B \\
z \,\mathbf{r}\, \forall_x A &:= \forall_x (zx \,\mathbf{r}\, A) \\
z \,\mathbf{r}\, \forall_x^{\mathrm{nc}} A &:= \forall_x (z \,\mathbf{r}\, A)
\end{aligned}$$

Example: Even and $\mathrm{Even}^{\mathbf{r}}$

For $\mathrm{Even} := \mu_X(X0, \forall^{\mathrm{nc}}_n(Xn \to X(S(Sn))))$ with $\iota_{\mathrm{Even}} = \mathbf{N}$:

$$\mathrm{Even}^{\mathbf{r}} := \mu^{\mathrm{nc}}_{X^{\mathbf{r}}}(0 \mathbin{\mathbf{r}} X0, \forall_{n,m}(m \mathbin{\mathbf{r}} Xn \to Sm \mathbin{\mathbf{r}} X(S(Sn))))$$

Introduction axioms:

$$(\mathrm{Even}^{\mathbf{r}})^+_0 \colon 0 \mathbin{\mathbf{r}} \mathrm{Even}(0),$$
$$(\mathrm{Even}^{\mathbf{r}})^+_1 \colon \forall_{n,m}(m \mathbin{\mathbf{r}} \mathrm{Even}(n) \to Sm \mathbin{\mathbf{r}} \mathrm{Even}(S(Sn)))$$

Elimination axiom:

$$\begin{aligned}(\mathrm{Even}^{\mathbf{r}})^- \colon \forall_{n,m}(m \mathbin{\mathbf{r}} \mathrm{Even}(n) \to Q^{\mathrm{nc}}00 \to\ & \\ & \forall_{n,m}(m \mathbin{\mathbf{r}} \mathrm{Even}(n) \to Q^{\mathrm{nc}}mn \to Q^{\mathrm{nc}}(Sm, S(Sn))) \to \\ & Q^{\mathrm{nc}}mn).\end{aligned}$$

Further examples

Recall

$$
\begin{aligned}
\mathrm{ExD}_Y &:= \mu_X(\forall_x(Yx^\rho \to X)) \\
\mathrm{ExL}_Y &:= \mu_X(\forall_x(Yx^\rho \to^{\mathrm{nc}} X)) \\
\mathrm{CupD}_{Y,Z} &:= \mu_X(Y \to X,\ Z \to X) \\
\mathrm{CupU}_{Y,Z} &:= \mu_X(Y \to^{\mathrm{nc}} X,\ Z \to^{\mathrm{nc}} X)
\end{aligned}
$$

Then

$$
\begin{aligned}
\mathrm{ExD}^{\mathbf{r}}_{Y^{\mathbf{r}}} &:= \mu^{\mathrm{nc}}_{X^{\mathbf{r}}}(\forall_{x,z}(z\ \mathbf{r}\ Yx \to (x,z)\ \mathbf{r}\ X)) \\
\mathrm{ExL}^{\mathbf{r}}_{Y} &:= \mu^{\mathrm{nc}}_{X^{\mathbf{r}}}(\forall_x(Yx \to x\ \mathbf{r}\ X)) \\
\mathrm{CupD}^{\mathbf{r}}_{Y^{\mathbf{r}},Z^{\mathbf{r}}} &:= \mu^{\mathrm{nc}}_{X^{\mathbf{r}}}(\forall_y(y\ \mathbf{r}\ Y \to \mathrm{Inl}(y)\ \mathbf{r}\ X),\ \forall_z(z\ \mathbf{r}\ Z \to \mathrm{Inr}(z)\ \mathbf{r}\ X)) \\
\mathrm{CupU}^{\mathbf{r}}_{Y,Z} &:= \mu^{\mathrm{nc}}_{X^{\mathbf{r}}}(Y \to \mathtt{tt}\ \mathbf{r}\ X,\ Z \to \mathtt{ff}\ \mathbf{r}\ X)
\end{aligned}
$$

Realizers for decorated $\exists$

$$
\begin{aligned}
(x, z)\ \mathbf{r}\ \exists^{\mathrm{d}}_x A &\leftrightarrow z\ \mathbf{r}\ A \quad \text{for } A \text{ c.r.}\\
x\ \mathbf{r}\ \exists^{\mathrm{l}}_x A &\leftrightarrow A^{\mathrm{nc}}\\
z\ \mathbf{r}\ \exists^{\mathrm{r}}_x A &\leftrightarrow \exists^{\mathrm{nc}}_x (z\ \mathbf{r}\ A) \quad \text{for } A \text{ c.r.}
\end{aligned}
$$

Non-computational variant C^{nc} of C: have X^{nc} and I^{nc}, and

$$
\begin{aligned}
\{\, \vec{x} \mid A \,\}^{\mathrm{nc}} &:= \{\, \vec{x} \mid A^{\mathrm{nc}} \,\}\\
(P\vec{r}\,)^{\mathrm{nc}} &:= P^{\mathrm{nc}}\vec{r}\\
(A \to^{\mathrm{c/nc}} B)^{\mathrm{nc}} &:= A \to B^{\mathrm{nc}}\\
(\forall^{\mathrm{c/nc}}_x A)^{\mathrm{nc}} &:= \forall_x A^{\mathrm{nc}}
\end{aligned}
$$

Invariance axioms

For c.r. formulas A we take as axioms

$$\mathrm{Inv}_A \colon A \leftrightarrow \exists^{\mathrm{l}}_z (z \;\mathbf{r}\; A)$$

They are realized by identities:

$$(\lambda_z z) \;\mathbf{r}\; (A \to \exists^{\mathrm{l}}_z (z \;\mathbf{r}\; A)),$$
$$(\lambda_z z) \;\mathbf{r}\; (\exists^{\mathrm{l}}_z (z \;\mathbf{r}\; A) \to A).$$

Consequences are choice and independence of premise.

Choice

From the invariance axioms we can derive

$$\forall_x \exists^{\mathrm{l}}_y A(y) \to \exists^{\mathrm{l}}_f \forall_x A(fx) \quad \text{for } A \text{ n.c.}$$
$$\forall_x \exists^{\mathrm{d}}_y A(y) \to \exists^{\mathrm{d}}_f \forall_x A(fx) \quad \text{for } A \text{ c.r.}$$

Proof.
By the invariance axioms it suffices to find a realizer.

$$(\lambda_f f) \mathbf{\ r\ } (\forall_x \exists^{\mathrm{l}}_y A(y) \to \exists^{\mathrm{l}}_f \forall_x A(fx))$$
$$\forall_f (f \mathbf{\ r\ } \forall_x \exists^{\mathrm{l}}_y A(y) \to f \mathbf{\ r\ } \exists^{\mathrm{l}}_f \forall_x A(fx))$$
$$\forall_f (\forall_x (fx \mathbf{\ r\ } \exists^{\mathrm{l}}_y A(y)) \to \forall_x A(fx))$$
$$\forall_f (\forall_x A(fx) \to \forall_x A(fx)). \qquad \square$$

Independence of premise

Assume $x \notin \mathrm{FV}(A)$. From the invariance axioms we can derive

$$
\begin{array}{ll}
(A \to \exists^{\mathrm{l}}_x B) \to \exists^{\mathrm{l}}_x (A \to B) & \text{for } A, B \text{ n.c.} \\
(A \to^{\mathrm{nc}} \exists^{\mathrm{l}}_x B) \to \exists^{\mathrm{l}}_x (A \to B) & \text{for } B \text{ n.c.} \\
(A \to \exists^{\mathrm{d}}_x B) \to \exists^{\mathrm{d}}_x (A \to B) & \text{for } A \text{ n.c., } B \text{ c.r.} \\
(A \to^{\mathrm{nc}} \exists^{\mathrm{d}}_x B) \to \exists^{\mathrm{d}}_x (A \to B) & \text{for } B \text{ c.r.}
\end{array}
$$

Proof.

By the invariance axioms it suffices to find a realizer. For A, B n.c.

$$
\begin{array}{l}
(\lambda_x x) \,\mathbf{r}\, ((A \to \exists^{\mathrm{l}}_x B) \to \exists^{\mathrm{l}}_x (A \to B)) \\
\forall_x (x \,\mathbf{r}\, (A \to \exists^{\mathrm{l}}_x B) \to x \,\mathbf{r}\, \exists^{\mathrm{l}}_x (A \to B)) \\
\forall_x ((A \to x \,\mathbf{r}\, \exists^{\mathrm{l}}_x B) \to x \,\mathbf{r}\, \exists^{\mathrm{l}}_x (A \to B)) \\
\forall_x ((A \to B) \to A \to B).
\end{array}
$$

□

Extracted terms

For derivations M^A with A n.c. let $\mathrm{et}(M^A) := \varepsilon$. Otherwise

$$
\begin{aligned}
\mathrm{et}(u^A) &:= z_u^{\tau(A)} \quad (z_u^{\tau(A)} \text{ uniquely associated to } u^A),\\
\mathrm{et}((\lambda_{u^A} M^B)^{A\to B}) &:= \begin{cases} \lambda_{z_u}^{\tau(A)} \mathrm{et}(M) & \text{if } A \text{ is c.r.}\\ \mathrm{et}(M) & \text{if } A \text{ is n.c.}\end{cases}\\
\mathrm{et}((M^{A\to B} N^A)^B) &:= \begin{cases} \mathrm{et}(M)\mathrm{et}(N) & \text{if } A \text{ is c.r.}\\ \mathrm{et}(M) & \text{if } A \text{ is n.c.}\end{cases}\\
\mathrm{et}((\lambda_{x^\rho} M^A)^{\forall_x A}) &:= \lambda_x^\rho \mathrm{et}(M),\\
\mathrm{et}((M^{\forall_x A(x)} r)^{A(r)}) &:= \mathrm{et}(M) r,\\
\mathrm{et}((\lambda_{u^A} M^B)^{A\to^{\mathrm{nc}} B}) &:= \mathrm{et}(M),\\
\mathrm{et}((M^{A\to^{\mathrm{nc}} B} N^A)^B) &:= \mathrm{et}(M),\\
\mathrm{et}((\lambda_{x^\rho} M^A)^{\forall_x^{\mathrm{nc}} A}) &:= \mathrm{et}(M),\\
\mathrm{et}((M^{\forall_x^{\mathrm{nc}} A(x)} r)^{A(r)}) &:= \mathrm{et}(M).
\end{aligned}
$$

Extracted terms for the axioms.

- Let I be c.r.

$$\mathrm{et}(I_i^+) := \mathrm{C}_i, \qquad \mathrm{et}(I^-) := \mathcal{R},$$

  where both C_i and $\mathcal{R}$ refer to the algebra ι_I associated with I.
- For the invariance axioms we take identities.

The term extracted from a proof in $\mathrm{TCF} + \mathrm{Inv} + \mathrm{Ax}^{\mathrm{nc}}$ is a solution of the problem posed by the proven formula.
($\mathrm{Ax}^{\mathrm{nc}}$ is an arbitrary set of n.c. formulas viewed as axioms).

Theorem (Soundness)

Let M be a derivation of a formula A from assumptions $u_i \colon C_i$ ($i < n$). Then we can derive

$$\begin{cases} \mathrm{et}(M) \mathbf{\ r\ } A & \textit{if } A \textit{ is c.r.} \\ A & \textit{if } A \textit{ is n.c.} \end{cases}$$

from assumptions

$$\begin{cases} z_{u_i} \mathbf{\ r\ } C_i & \textit{if } C_i \textit{ is c.r.} \\ C_i & \textit{if } C_i \textit{ is n.c.} \end{cases}$$

All derivations are in $\mathrm{TCF} + \mathrm{Inv} + \mathrm{Ax}^{\mathrm{nc}}$. Proof by induction on M.

Conclusion

Framework TCF for constructive analysis.

- Invariance axioms ($\Rightarrow$ AC, IP) helpful; realized by identities.
- Expressive term language T^+ (arbitrary defining equations, e.g. for fixed point operators, corecurion).
- Realizability interpretation provides extracted terms expressing computational content of proofs.
- From $M\colon A$ obtain $M^S\colon (\mathrm{et}(M)\ \mathbf{r}\ A)$. The soundness proof M^S can be automatically generated and checked.
- Decorations for fine tuning and efficiency.