Constructive Proofs of Completeness, Extra-intuitionistic Principles, and Delimited Control Operators

Danko Ilik

based on work with Hugo Herbelin

Lyon, January 6, 2011

Completeness Proofs as Programs

Research theme

Definition (Completeness)

ϕ is **true** iff ϕ is **provable**

Application:

- Automatic switching between model theoretic and proof theoretic reasoning (in Coq)

Theoretical questions:

- Algorithm behind Gödel's completeness proof
- Normalisation-by-evaluation for classical logic
- Constructive proof of completeness for Kripke models

Talk Outline

Constructive Completeness for Intuitionistic Logic

Delimited Control Operators in Logic

Talk Outline

Constructive Completeness for Intuitionistic Logic

Delimited Control Operators in Logic

Constructive Completeness for Intuitionistic Logic

Kinds of semantics:

- Reformulation of derivation rules: BHK, Kleene's realisability, Algebraic semantics
- More independent: Beth, Kripke
  - cf. Boolean semantics and classical derivation systems

Completeness for Kripke semantics:

- Gödel-Kreisel's meta-mathematical results (Kreisel 1962)
- Classical Henkin-style proof (Kripke 1965)
- Proof using the Fan Theorem (Veldman 1976)
- Normalisation-by-evaluation gives a proof, but **without** $\vee, \exists$

Gödel-Kreisel's Meta-mathematical Results

Strong Completeness, Weak Completeness, Markov's Principle, and Double-negation Shift for Σ^0_1-formulae

$$(\forall \mathcal{M}.\, \mathcal{M} \models \phi) \longrightarrow\ \vdash \phi \qquad \text{(SC)}$$

$$\nvdash \phi \longrightarrow \neg(\forall \mathcal{M}.\, \mathcal{M} \models \phi) \qquad \text{(WC)}$$

For A_0-decidable,

$$\neg\neg\exists n A_0(n) \to \exists n A_0(n), \qquad \text{(MP)}$$

$$\forall \alpha \neg\neg\exists n A_0(\alpha, n) \to \forall \alpha \exists n A_0(\alpha, n), \qquad (\mathrm{DNS}^{\Sigma}_{+})$$

$$\forall \alpha \neg\neg\exists n A_0(\alpha, n) \to \neg\neg\forall \alpha \exists n A_0(\alpha, n), \qquad (\mathrm{DNS}^{\Sigma})$$

Theorem (Gödel-Kreisel)

- $MP + WC \to SC$
- $SC \to DNS^{\Sigma}_{+} \to MP$
- $WC \to DNS^{\Sigma}$

Kripke Models

Start with a structure $\mathcal{K} = (K, \leq, D, \Vdash, \Vdash_\perp)$, where $\leq$ is a partial order on K, and extend $\Vdash$ to non-atomic formulas:

$\mathbf{w} \Vdash$	
$A \wedge B$	$w \Vdash A$ and $w \Vdash B$
$A \vee B$	$w \Vdash A$ or $w \Vdash B$
$A \to B$	for any $w' \geq w$, if $w' \Vdash A$ then $w' \Vdash B$
$\forall x P(x)$	for any $w' \geq w$ and any $a \in D(w')$, $w' \Vdash P(a)$
$\exists x P(x)$	there is $a \in D(w)$ such that $w \Vdash P(a)$
$\perp$	$w \Vdash_\perp$

Theorem (Completeness)

$(\forall \mathcal{K}.\ \forall w \in K.\ w \Vdash \Gamma \to w \Vdash A) \longrightarrow \Gamma \vdash A$

Prove the more general:

Theorem (Completeness for $\mathcal{U}$)

There is a so called "universal" model $\mathcal{U}$ such that
$\forall \Gamma \in \mathcal{U}.\ \Gamma \Vdash A \longrightarrow \Gamma \vdash A$

Proof.

$\mathcal{U} := (U, \leq, \Vdash, \Vdash_\bot)$, where

- U is the set of contexts, assigning formulas to free variables
- $\Gamma_1 \leq \Gamma_2 := \Gamma_1 \subseteq \Gamma_2$
- $\Gamma \Vdash P := \Gamma \vdash P$
- $\Gamma \Vdash \bot := \Gamma \Vdash_\bot$

□

For **full** intuitionistic logic – with $\vee$ and $\exists$ – Veldman used the Fan Theorem:

$$(\forall \alpha.\exists n.A(\overline{\alpha} n) \rightarrow \exists N.\forall \alpha.\exists k \leq N.A(\overline{\alpha} k) \qquad \text{(FAN)}$$

where

$$\alpha : \mathbb{N} \rightarrow \mathbf{2}$$

$$n, k, N : \mathbb{N}$$

$$\overline{\alpha} n : \mathbf{2}^*$$

and A is decidable i.e.

$$A : \mathbf{2}^* \rightarrow \mathbf{2}$$

Kripke Models

Theorem (Completeness for $\mathcal{U}$)

There is a so called "universal" model $\mathcal{U}$ such that
$\forall \Gamma \in \mathcal{U}.\ \Gamma \Vdash A \longrightarrow \Gamma \vdash A$

is a special case of Berger-Schwichtenberg's – but without $\vee, \exists$

Theorem (Normalisation-by-evaluation)

$\downarrow^A_\Gamma$ ("*reify*") : $\Gamma \Vdash A \longrightarrow \Gamma \vdash^{nf} A$
$\uparrow^A_\Gamma$ ("*reflect*") : $\Gamma \vdash^{ne} A \longrightarrow \Gamma \Vdash A$

$$\downarrow^\tau := a \mapsto a \qquad \tau\text{-atomic}$$
$$\downarrow^{\tau\to\sigma} := S \mapsto \lambda a. \downarrow^\sigma \cdot (S \cdot \uparrow^\tau \cdot a) \qquad a\text{-fresh}$$

$$\uparrow^\tau := a \mapsto a \qquad \tau\text{-atomic}$$
$$\uparrow^{\tau\to\sigma} := e \mapsto S \mapsto \uparrow^\sigma \cdot (e(\downarrow^\tau \cdot S))$$

Completeness/NBE for $\lambda^{\rightarrow\vee}$

What the problem is

Theorem (NBE)

$\downarrow^{A}_{\Gamma}$ ("*reify*") : $\Gamma \Vdash A \longrightarrow \Gamma \vdash^{nf} A$
$\uparrow^{A}_{\Gamma}$ ("*reflect*") : $\Gamma \vdash^{ne} A \longrightarrow \Gamma \Vdash A$

Proof of case $\uparrow^{A\vee B}$.

Given a derivation $\Gamma \vdash^{\mathrm{ne}} A \vee B$, decide: $\Gamma \Vdash A$ **or** $\Gamma \Vdash B$? □

Shift ($\mathscr{S}$) and *Reset* (#) Delimited Control Operators

Examples

$$\# V \to V$$

$$\# F[\mathscr{S} k.p] \to \# p\{k := \lambda x.\# F[x]\}$$

Shift ($\mathscr{S}$) and *Reset* (#) Delimited Control Operators

Examples

$$\#V \to V$$

$$\#F[\mathscr{S}k.p] \to \#p\{k := \lambda x.\#F[x]\}$$

$$
\begin{aligned}
& 1 + \#(2 + \mathscr{S}k.k(k4)) \\
\to & 1 + \#((\lambda a.\#(2+a))((\lambda a.\#(2+a))4)) \\
\to^{+} & 1 + \#(\#(\#8)) \\
\to^{+} & 9
\end{aligned}
$$

Completeness/NBE for $\lambda^{\to\vee}$

Solution of Danvy: use *shift* and *reset*

Theorem (NBE – Danvy)

$\downarrow^{A}_{\Gamma}$ ("*reify*"): $\Gamma \Vdash A \longrightarrow \Gamma \vdash^{nf} A$
$\uparrow^{A}_{\Gamma}$ ("*reflect*"): $\Gamma \vdash^{ne} A \longrightarrow \Gamma \Vdash A$

Proof of case $\uparrow^{A\vee B}$.

Given a derivation $\mathtt{e}$ of $\Gamma \vdash^{\mathrm{ne}} A \vee B$, decide: $\Gamma \Vdash A$ **or** $\Gamma \Vdash B$, by

$$\mathscr{S} k.\ \mathtt{case}\ \mathtt{e}\ \mathtt{of}\ (\mathtt{x}.\#k(\mathrm{left} \uparrow^{A}_{\mathtt{x}:A,\Gamma} \mathtt{x}))\ (\mathtt{y}.\#k(\mathrm{right} \uparrow^{B}_{\mathtt{y}:B,\Gamma} \mathtt{y}))$$

□

Completeness/NBE for $\lambda^{\to\vee}$

Solution of Danvy: is it a proof?

- We are convinced the **program** computes correctly
- There should be a corresponding completeness **proof** for Kripke model
- Type-and-effect system: types $A \to B$ become $A/\alpha \to B/\beta$, what is the logical meaning?

Completeness for Intuitionistic Predicate Logic (IQC)

Extracting a notion of model from Danvy's solution

Like with Kripke models, start with a structure $(K, \leq, D, \Vdash_{\mathbf{s}}, \Vdash^{(\cdot)}_{\perp})$, and extend **strong forcing** ($\Vdash_{\mathbf{s}}$) to non-atomic formulas:

$\mathbf{w} \Vdash_{\mathbf{s}}$	
$A \wedge B$	$w \Vdash A$ and $w \Vdash B$
$A \vee B$	$w \Vdash A$ or $w \Vdash B$
$A \to B$	for any $w' \geq w$, if $w' \Vdash A$ then $w' \Vdash B$
$\forall x P(x)$	for any $w' \geq w$ and any $a \in D(w')$, $w' \Vdash P(a)$
$\exists x P(x)$	there is $a \in D(w)$ such that $w \Vdash P(a)$

where the non-s-annotated $\Vdash$ is **(non-strong) forcing**:

$$w \Vdash A := \forall \mathbf{C}. \forall w_1 \geq w. (\forall w_2 \geq w_1 . w_2 \Vdash_s A \to w_2 \Vdash^{\mathbf{C}}_{\perp}) \to w_1 \Vdash^{\mathbf{C}}_{\perp}$$

Completeness for IQC via Kripke-style Models

Theorem (NBE)

$\downarrow^A_\Gamma$ ("*reify*") : $\Gamma \Vdash A \longrightarrow \Gamma \vdash^{nf} A$
$\uparrow^A_\Gamma$ ("*reflect*") : $\Gamma \vdash^{ne} A \longrightarrow \Gamma \Vdash A$

Proof of case $\uparrow^{A \vee B}$.

Given a derivation e of $\Gamma \vdash^{\mathrm{ne}} A \vee B$, prove $\Gamma \Vdash A \vee B$ i.e.

$$\forall C.\ \forall \Gamma_1 \geq \Gamma.\ (\forall \Gamma_2 \geq \Gamma_1.\ \Gamma_2 \Vdash_S A \text{ or } \Gamma_2 \Vdash_s B \to \Gamma_2 \vdash^C_\perp) \to \Gamma_1 \vdash^C_\perp$$

by

$$C \mapsto \Gamma_1 \mapsto k \mapsto \texttt{ case e of } (\texttt{x}.k(\text{left} \uparrow^A_{\texttt{x}:A,\Gamma_1} \texttt{x}))\ (\texttt{y}.k(\text{right} \uparrow^B_{\texttt{y}:B,\Gamma_1} \texttt{y}))$$

□

Conclusion of Part I

Contribution:

- New notion of model for Intuitionistic logic
- β-Normalises λ-calculus with sum
- Formalised in Coq
- But, not as simple as Kripke models

More details in my thesis: `www.lix.polytechnique.fr/~danko`

Talk Outline

Constructive Completeness for Intuitionistic Logic

Delimited Control Operators in Logic

Delimited control operators in Logic

- Should allow us to give a constructive proof of completeness for Kripke semantics (Danvy's NBE functional program)
- Herbelin: delimited control allows to derive Markov's Principle (Herbelin 2010) and the Double Negation Shift
- Allow to simulate any monadic computational effect (Filinski 1994)

Proof term λ-calculus with $\mathscr{S}$ and

Proof terms:

$$p, q, r ::= a \mid \iota_1 p \mid \iota_2 p \mid \mathsf{case}\ p\ \mathsf{of}\ \left(a.q \| b.r\right) \mid (p, q) \mid \pi_1 p \mid \pi_2 p \mid \lambda a.p \mid$$
$$\mid pq \mid \lambda x.p \mid pt \mid (t, p) \mid \mathsf{dest}\ p\ \mathsf{as}\ (x.a)\ \mathsf{in}\ q \mid \#p \mid \mathscr{S} k.p$$

Proof term λ-calculus with $\mathscr{S}$ and

Proof terms:

$$
\begin{aligned}
p, q, r ::= a \mid \iota_1 p \mid \iota_2 p \mid \mathsf{case}\ p\ \mathsf{of}\ \left(a.q \| b.r\right) \mid (p, q) \mid \pi_1 p \mid \pi_2 p \mid \lambda a.p \mid \\
\mid pq \mid \lambda x.p \mid pt \mid (t, p) \mid \mathsf{dest}\ p\ \mathsf{as}\ (x.a)\ \mathsf{in}\ q \mid \# p \mid \mathscr{S} k.p
\end{aligned}
$$

Values:

$$
V ::= a \mid \iota_1 V \mid \iota_2 V \mid (V, V) \mid (t, V) \mid \lambda a.p \mid \lambda x.p
$$

Proof term λ-calculus with $\mathscr{S}$ and

Proof terms:

$$p, q, r ::= a \mid \iota_1 p \mid \iota_2 p \mid \mathsf{case}\ p\ \mathsf{of}\ \left(a.q \| b.r\right) \mid (p, q) \mid \pi_1 p \mid \pi_2 p \mid \lambda a.p \mid$$
$$\mid pq \mid \lambda x.p \mid pt \mid (t, p) \mid \mathsf{dest}\ p\ \mathsf{as}\ (x.a)\ \mathsf{in}\ q \mid \# p \mid \mathscr{S} k.p$$

Values:

$$V ::= a \mid \iota_1 V \mid \iota_2 V \mid (V, V) \mid (t, V) \mid \lambda a.p \mid \lambda x.p$$

Pure evaluation contexts:

$$P ::= [\,] \mid \mathsf{case}\ P\ \mathsf{of}\ \left(a_1.p_1 \| a_2.p_2\right) \mid \pi_1 P \mid \pi_2 P \mid \mathsf{dest}\ P\ \mathsf{as}\ (x.a)\ \mathsf{in}\ p \mid$$
$$Pq \mid (\lambda a.q) P \mid Pt \mid \iota_1 P \mid \iota_2 P \mid (P, p) \mid (V, P) \mid (t, P)$$

Proof term λ-calculus with $\mathscr{S}$ and

Proof terms:

$$p, q, r ::= a \mid \iota_1 p \mid \iota_2 p \mid \mathsf{case}\ p\ \mathsf{of}\ \left(a.q \| b.r\right) \mid (p, q) \mid \pi_1 p \mid \pi_2 p \mid \lambda a.p \mid$$
$$\mid pq \mid \lambda x.p \mid pt \mid (t, p) \mid \mathsf{dest}\ p\ \mathsf{as}\ (x.a)\ \mathsf{in}\ q \mid \# p \mid \mathscr{S} k.p$$

Values:

$$V ::= a \mid \iota_1 V \mid \iota_2 V \mid (V, V) \mid (t, V) \mid \lambda a.p \mid \lambda x.p$$

Pure evaluation contexts:

$$P ::= [\,] \mid \mathsf{case}\ P\ \mathsf{of}\ \left(a_1.p_1 \| a_2.p_2\right) \mid \pi_1 P \mid \pi_2 P \mid \mathsf{dest}\ P\ \mathsf{as}\ (x.a)\ \mathsf{in}\ p \mid$$
$$Pq \mid (\lambda a.q) P \mid Pt \mid \iota_1 P \mid \iota_2 P \mid (P, p) \mid (V, P) \mid (t, P)$$

Reduction: (Call-by-value strategy)

$$(\lambda a.p) V \to p\{V / a\} \qquad \mathsf{case}\ \iota_i V\ \mathsf{of}\ \left(a_1.p_1 \| a_2.p_2\right) \to p_i\{V / a_i\}$$
$$(\lambda x.p) t \to p\{t / x\} \qquad \mathsf{dest}\ (t, V)\ \mathsf{as}\ (x.a)\ \mathsf{in}\ p \to p\{t / x\}\{V / a\}$$
$$\pi_i(V_1, V_2) \to V_i \qquad \# P[\mathscr{S} k.p] \to \# p\{(\lambda a.\# P[a]) / k\}$$
$$\# V \to V \qquad E[p] \to E[p'] \text{ when } p \to p'$$

Typing/Logical system MQC$^+$

The usual rules of MQC (minimal predicate logic), potentially annotated,

$$\frac{\cdots \vdash^{+}_{T} \cdots}{\cdots \vdash^{+}_{T} \cdots}$$

plus rules for reset and shift:

$$\frac{\Gamma \vdash^{+}_{T} p : T}{\Gamma \vdash^{+}_{\diamond} \#p : T}$$

$$\frac{\Gamma, k : A \Rightarrow T \vdash^{+}_{T} p : T}{\Gamma \vdash^{+}_{T} \mathcal{S} k.p : A}$$

T denotes a $\{\Rightarrow, \forall\}$-free formula ("Σ-formula")

Deriving MP and DNS

Markov's Principle (predicate logic version):

$$\neg\neg S \Rightarrow S, \quad \text{for } S \text{ a } \Sigma\text{-formula}$$

$$\lambda a.\#\bot_E(a(\lambda b.\,\mathscr{S} k.b))$$

Deriving MP and DNS

Markov's Principle (predicate logic version):

$$\neg\neg S \Rightarrow S, \quad \text{for } S \text{ a } \Sigma\text{-formula}$$

$$\lambda a.\#\bot_E(a(\lambda b.\mathscr{S}k.b))$$

Double Negation Shift (predicate logic version):

$$\forall x(\neg\neg A(x)) \Rightarrow \neg\neg(\forall x A(x))$$

$$\lambda a.\lambda b.\#b(\lambda x.\mathscr{S}k.axk)$$

Equiconsistency of MQC^{+} with MQC

By the call-by-value continuation-passing-style translation (related to Glivenko's double-negation translation)

$$A^T := (A_T \Rightarrow T) \Rightarrow T$$

$$\begin{aligned}
A_T &:= A && \text{if } A \text{ is a atomic} \\
(A \Box B)_T &:= A_T \Box B_T && \text{for } \Box = \vee, \wedge \\
(A \Rightarrow B)_T &:= A_T \Rightarrow B^T \\
(\exists A)_T &:= \exists A_T \\
(\forall A)_T &:= \forall A^T
\end{aligned}$$

Relationship to Classical and Intuitionistic Logic

Theorem (Equiconsistency)

Given a derivation of $\Gamma \vdash^{+} A$*, which uses* $\mathscr{S}$ *and* $\#$ *for the* Σ*-formula* T*, we can build a derivation of* $\Gamma_T \vdash^{m} A^T$*.*

Theorem (Glivenko's Theorem extended to quantifiers)

$$\vdash^{+} \neg\neg A \longleftrightarrow DNS \vdash^{i} A^{\perp} \longleftrightarrow \vdash^{c} A$$

Properties of MQC$^+$

Theorem (Subject Reduction)

If $\Gamma \vdash^+_\diamond p : A$ *and* $p \to q$*, then* $\Gamma \vdash^+_\diamond q : A$.

Theorem (Progress)

If $\vdash^+_\diamond p : A$*,* p *is not a value, and* p *is not of form* $P[\mathscr{S} k.p']$*, then* p *reduces in one step to some proof term* r.

Theorem (Normalisation)

For every closed proof term p_0*, such that* $\vdash^+ p_0 : A$*, there is a finite reduction path* $p_0 \to p_1 \to \ldots \to p_n$ *ending with a value* p_n.

Corollary (Disjunction and Existence Properties)

If $\vdash^+ A \vee B$*, then* $\vdash^+ A$ *or* $\vdash^+ B$.
If $\vdash^+ \exists x A(x)$*, then there exists a closed term* t *such that* $\vdash^+ A(t)$.

Conclusion of Part II

- Contribution:
  - A typing system for delimited control which remains intuitionisitc (DP and EP) while deriving MP, DNS
  - But, only one use of MP is allowed
- Future work:
  - Annotating a derivation by a context Δ, like in (Herbelin 2010):

$$\frac{\Gamma \vdash^{+}_{\alpha:T,\Delta} p : T}{\Gamma \vdash^{+}_{\Delta} \#_{\alpha} p : T}$$

$$\frac{\Gamma, k : A \Rightarrow T \vdash^{+}_{\alpha:T,\Delta} p : T}{\Gamma \vdash^{+}_{\alpha:T,\Delta} \mathcal{S}_{\alpha} k.p : A}$$

  - Connection to Fan Theorem, Open Induction, and other principles of Intuitionistic Reverse Mathematics
  - A logical study of computational effects

Kripke and Kripke-style Models

To show their equivalence, and hence completeness for standard Kripke models, the following should be provable for our models:

$$\frac{\forall C.\, \forall w_1 \geq w.\, (\forall w_2 \geq w_1.\, w_2 \Vdash A + w_2 \Vdash B \to w_2 \Vdash_{\perp}^{C}) \to w_1 \Vdash_{\perp}^{C}}{w \Vdash A + w \Vdash B}$$

This is possible if we add some arithmetic and make the rule for shift "polymorphic":

$$\frac{\Gamma, \forall n' (A(n') \Rightarrow T(n')) \vdash_{T(-)}^{+} T(n)}{\Gamma \vdash_{T(-)}^{+} A(n)}$$

But, that system has yet to be studied. In particular, are there any complications when including arithmetic?