Constructive completeness proofs and delimited control

PhD thesis defence

Danko Ilik

École Polytechnique – INRIA – Université Paris Diderot

thesis directed by Hugo Herbelin

Paris, October 22, 2010

Constructive Mathematics and Computer Science

- The Curry-Howard correspondence:
  - proofs are programs;
  - theorems are specifications.
- Constructive type theory and the Coq proof assistant
- Coq is a tool for developing formal proofs:
  - of theorems in Constructive Mathematics;
  - of correctness of programs with respect to a specification.

Completeness theorems as programs

- A formalised Completeness theorem – a tool to switch between model theoretic and proof theory arguments inside Coq
- Conections between Completeness and Normalisation-by-Evaluation

Outline

Boolean completeness

Classical NBE

Intuitionistic NBE

Delimited control in Logic

Outline

Boolean completeness

Classical NBE

Intuitionistic NBE

Delimited control in Logic

Completeness for standard semantics

Theorem (Gödel 1930)

*A is **valid** if and only if A is **derivable***

A - derivable: there is a derivation tree for A in classical 1st-order logic

A - valid: Tarski's truth definition:

$$
\begin{array}{rcl}
\mathcal{M} \vDash A \wedge B & := & \mathcal{M} \vDash A \text{ and } \mathcal{M} \vDash B \\
\mathcal{M} \vDash A \vee B & := & \mathcal{M} \vDash A \text{ or } \mathcal{M} \vDash B \\
\mathcal{M} \vDash A \rightarrow B & := & \mathcal{M} \vDash A \text{ implies } \mathcal{M} \vDash B \\
\mathcal{M} \vDash \exists x A(x) & := & \text{exists } t \text{ with } \mathcal{M} \vDash A(t) \\
\mathcal{M} \vDash \forall x A(x) & := & \text{for any } t, \mathcal{M} \vDash A(t) \\
\mathcal{M} \vDash \bot & := & \text{false}
\end{array}
$$

Is it constructive?

Theorem (McCarty 1996)

No? *– Completeness implies Markov's Principle (MP)*

Is it constructive?

Theorem (McCarty 1996)

No? *– Completeness implies Markov's Principle (MP)*

Theorem (Krivine 1996)

Yes? *– Gödel's proof is constructive, if we allow one more model – the model that validates* $\bot$

What is the algorithm behind Krivine's proof?

- Krivine's proof carried out in *classical* 2nd-order arithmetic
- From the form of the statement, he concludes there is a proof in intuitionistic 2nd-order arithmetic
- Formalisation in Phox (PA_2) by Raffalli; algorithm extracted but "unreadable"
- Proof unwound in (Berardi-Valentini 2004): main ingredient a constructive ultra-filter theorem

Constructive Ultra-filter Theorem

$\mathscr{B}$	countable Boolean algebra
Filter	subset of $\mathscr{B}$ which is inhabited, $\leq$-closed and $\wedge$-closed
$b \in \uparrow X$	$= \exists a_1, \ldots, a_n \in X.\ a_1 \wedge \cdots \wedge a_n \leq b$
X-complete	$(\dot{\neg} c \in X \longrightarrow \dot{\bot} \in X) \longrightarrow c \in X$, for all $c \in \mathscr{B}$

Constructive Ultra-filter Theorem

$\mathscr{B}$	countable Boolean algebra
Filter	subset of $\mathscr{B}$ which is inhabited, $\leq$-closed and $\wedge$-closed
$b \in \uparrow X$	$= \exists a_1, \ldots, a_n \in X.\ a_1 \wedge \cdots \wedge a_n \leq b$
X-complete	$(\dot{\neg} c \in X \longrightarrow \dot{\bot} \in X) \longrightarrow c \in X$, for all $c \in \mathscr{B}$

Theorem (Berardi-Valentini 2004)

Every filter F can be extended to a complete filter $Z(F)$, so that $F \sim Z(F)$ $(\bot \in F \longleftrightarrow \bot \in Z(F))$

Proof.

$$
\begin{aligned}
F_0 &:= F \\
F_{n+1} &:= \uparrow(F_n \cup \{b \mid \ulcorner b \urcorner = n, F_n \sim \uparrow(F_n \cup \{b\})\}) \\
Z &:= \bigcup_{n \in \mathbb{N}} F_n
\end{aligned}
$$

From Ultra-filter theorem to Completeness

Instantiate $\mathscr{B}$ with the Lindenbaum Boolean algebra:

$$a \leq b := a \vdash b$$

$$a \wedge b := \vdash \neg(a \Rightarrow \neg b)$$

If X is a set of axioms, then

$$a \in Z(\uparrow X)$$

means

$$\exists n. \exists \Gamma \subseteq F_n(\uparrow X). \Gamma \vdash a,$$

which implies,

$$\exists \Gamma \subseteq X. \Gamma \vdash a.$$

Computational content

Reflection:

$$(a \Rightarrow b) \in Z \longrightarrow a \in Z \longrightarrow b \in Z$$

$$m \mapsto n \mapsto \max(m, n)$$

Reification:

$$(a \in Z \longrightarrow b \in Z) \longrightarrow (a \Rightarrow b) \in Z$$

$$\text{let } c := (a \Rightarrow b) \text{ in } Z\text{-complete}$$

Z-complete is a kind of meta-level $\neg\neg_E$:

$$((c \in Z \longrightarrow \bot \in Z) \longrightarrow \bot \in Z) \longrightarrow c \in Z$$

Conclusion

Contribution:

- detailed Henkin-style argument formalised in Type Theory;
- generalisation to setoids of the Ultra-filter Theorem.

Future work:

- develop a proof/algorithm not parametrised by an enumeration (using delimited control);
- finish the Coq formalisation.

Outline

Classical Completeness via Kripke-style Models

Motivation

Get a completeness theorem for **computational** classical calculi – reduction relation should be preserved.

Follow Normalization-by-Evaluation (NBE) methodology (Berger-Schwichtenberg 1991):

Theorem (Soundness/Evaluation)

$\Gamma \vdash A \longrightarrow \forall w, w \Vdash \Gamma \longrightarrow w \Vdash A$

Theorem (Completeness/Reification)

$(\forall w, w \Vdash \Gamma \longrightarrow w \Vdash A) \longrightarrow \Gamma \vdash^{nf} A$

Corollary (NBE)

The composition (Completeness ∘ Soundness) normalizes proof terms into η-long β-normal form.

Standard Kripke models

Start with a structure $(K, \leq, D, \Vdash, \Vdash_\bot)$, 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 $w \Vdash P(a)$

Kripke-style models (Call-by-value variant)

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

$w \Vdash_{\mathbf{s}}$	
$A \wedge B$	$w \Vdash A$ 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**:

$$w \Vdash A := \forall w_1 \geq w. \underbrace{(\forall w_2 \geq w_1. w_2 \Vdash_{\mathbf{s}} A \to w_2 \Vdash_{\bot})}_{\text{"refutation"}\, w_1 : A \Vdash} \to w_1 \Vdash_{\bot}$$

Completeness for Kripke-style models and $LK_{\mu\tilde{\mu}}$

Theorem (Soundness)

$c:(\Gamma \vdash \Delta) \implies$ *for any* w, $w \Vdash \Gamma$ *and* $w : \Delta \Vdash$ *implies* $w \Vdash_{\perp}$

$\Gamma \vdash t : A|\Delta \implies$ *for any* w, $w \Vdash \Gamma$ *and* $w : \Delta \Vdash$ *implies* $w \Vdash A$

$\Gamma|e : A \vdash \Delta \implies$ *for any* w, $w \Vdash \Gamma$ *and* $w : \Delta \Vdash$ *implies* $w : A \Vdash$

Theorem (Completeness)

$(\Gamma, \Delta) \Vdash A \implies$ *there is a term* t *such that* $\Gamma \vdash_{cf} t : A|\Delta$

$(\Gamma, \Delta) : A \Vdash \implies$ *there is an ev. context* e *such that* $\Gamma|e : A \vdash_{cf} \Delta$

Proof.

Make a Universal model $\mathcal{U}$ from the derivation system:

- worlds are pairs (Γ, Δ)
- strong forcing is cut-free derivability of atoms: $(\Gamma, \Delta) \Vdash_s X := \exists t.\ \Gamma \vdash_{cf} t : X|\Delta$
- exploding nodes are cuts: $(\Gamma, \Delta) \Vdash_{\perp} := \exists c.\ c : (\Gamma \vdash_{cf} \Delta)$

Conclusion

- New notion of model for classical logic
- Not as simple as Boolean models
- But, reduction is preserved
- Dual notion of model that gives call-by-**name** normalization strategy
- Proofs formalised in Coq

Outline

Boolean completeness

Classical NBE

Intuitionistic NBE

Delimited control in Logic

Completeness of Intuitionistic Logic for Kripke models

- Kripke models are a standard semantics for intuitionistic logic
- But, there is no (simple) constructive proof with $\vee, \exists$:
  - classical Henkin-style proofs (Kripke 1965)
  - using Fan Theorem (Veldman 1976)
  - a constructive proof would imply MP (Kreisel 1962)
- On the other hand, a well-typed functional program for NBE of $\lambda^{\rightarrow\vee}$ (Danvy 1996)
  - using delimited-control operators *shift* and *reset* (Danvy-Filinski 1989)

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

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 delimited control operators shift ($\mathcal{S}$) and reset (#)

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 $\Gamma \vdash^{\mathrm{ne}} A \vee B$, decide: $\Gamma \Vdash A$ **or** $\Gamma \Vdash B$, by

$$\mathcal{S}k.\ \vee_E\ e\ (x \mapsto \#k(\text{left} \uparrow^A_{x:A,\Gamma} x))\ (y \mapsto \#k(\text{right} \uparrow^B_{y:B,\Gamma} y))$$

□

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

Solution of Danvy: Issues

- 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?
- Typing via classical logic

Completeness for Intuitionistic Predicate Logic (IQC)

Extracting a notion of model from Danvy's solution

Like with Kripke models, start with a structure $(K, \leq, D, \Vdash_{\mathbf{s}}, \Vdash^{(\cdot)}_{\bot})$, 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**:

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

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.

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

by

$$k \mapsto \ \vee_E\ e\ (x \mapsto k(\text{left} \uparrow^A_{x:A,\Gamma} x))\ (y \mapsto k(\text{right} \uparrow^B_{y:B,\Gamma} y))$$

□

Conclusion

- Contribution:
  - New notion of model for Intuitionistic logic
  - β-Normalises λ-calculus with sum
  - But, not as simple as Kripke models
  - Formalised in Coq
- Future work:
  - Find a good logical system for delimited control that can prove completeness for standard Kripke models

Outline

Boolean completeness

Classical NBE

Intuitionistic NBE

Delimited control 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:

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

Values:

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

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 $\mathcal{S}$ and

Proof terms:

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

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)

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

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):

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

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

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)

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

$$A_T := A \quad \text{if } A \text{ is a atomic}$$

$$(A \Box B)_T := A_T \Box B_T \quad \text{for } \Box = \vee, \wedge$$

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

$$(\exists A)_T := \exists A_T$$

$$(\forall A)_T := \forall A^T$$

Relationship to classical and intuitionistic logic

Theorem (Equiconsistency)

Given a derivation of $\Gamma \vdash^{+} A$*, which uses* $\mathcal{S}$ *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

- 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