Pedagogical formal and functionnal systems

Vincent Demange

CPR, Cédric, Cnam

27/06/2013

Introduction to formal pedagogy

Published works

- L. Colson and D. Michel. *Pedagogical natural deduction systems : the propositional case*. JUCS, 13(10) :1396–1410, 2007.
- L. Colson and D. Michel. *Pedagogical Second-Order Propositional Calculi*. JLC, 18(4) :669–695, 2008.
- L. Colson and D. Michel. *Pedagogical second-order λ-calculus*. TCS, 410 :4190–4203, 2009.
- L. Colson and V. Demange. *Investigations on a Pedagogical Calculus of Constructions*. JUCS, *to appear*, 2013.

Introduction to formal pedagogy

Basics : the pedagogical constraint

Poincaré criterion

> *«A definition by postulate has value **only if** there exists an example.»* [Henri Poincaré – Last Thoughts (1913)]

Good postulate

Let x be a natural number such that $x^2 - 1 = 0$ holds.

$\triangleright\, x := 1$ suits

Bad postulate

Let y be a natural number verifying $y^2 + 1 = 0$.

$\triangleright$ no such y

Called "pedagogical" because of usual teaching practice

Outline of the investigation

1. Summary of the previous works
2. First attempts toward a pedagogical CC
3. A formal definition and some examples
4. Toward a Pedagogical Calculus of Constructions

Summary of the previous works

The formal pedagogical constraint

Informal Poincaré criterion

> *«A definition by postulate has value **only if** there exists an example.»* [Henri Poincaré – Last Thoughts (1913)]

Formal Poincaré criterion (example)

If $\top$ is a type and o a term of type $\top$:

- $\Gamma := \{f : (\alpha \to \alpha) \to \alpha, g : \top \to \beta\}$ ▷ defines α, β, f, g
- $\sigma := [\alpha \mapsto \top, \beta \mapsto \top, f \mapsto \lambda h^{\top \to \top}.o, g \mapsto \lambda x^{\top}.x]$ example :

$$\vdash \lambda h^{\top \to \top}.o : (\top \to \top) \to \top$$

$$\vdash \lambda x^{\top}.x \quad : \top \to \top$$

Summary of the previous works

The formal pedagogical constraint

Informal Poincaré criterion

> *«A definition by postulate has value **only if** there exists an example.»* [Henri Poincaré – Last Thoughts (1913)]

Formal Poincaré criterion

Used environments must be exemplifiable : $\Gamma \vdash t : A \quad \Rightarrow \quad \vdash \sigma \cdot \Gamma$

where :

$$\frac{}{\vdash \sigma \cdot \emptyset}\ (\mathsf{ex}_1) \qquad \frac{\vdash \sigma \cdot \Gamma \quad \vdash \sigma(x) : \sigma(A)}{\vdash \sigma \cdot (\Gamma, x : A)}\ (\mathsf{ex}_2)$$

i.e. $\vdash \sigma \cdot (x_1 : A_1, \ldots, x_n : A_n) := \forall i \quad \vdash \sigma(x_i) : \sigma(A_i)$

Summary of the previous works

Simply typed λ-calculus

Morphology $\alpha \mid A \to B$

Syntax $x \mid \lambda x^A.u \mid u\ v$

$$\frac{x : F \in \Gamma}{\Gamma \vdash x : F}\ (\text{var})$$

$$\frac{\Gamma, x : A \vdash u : B}{\Gamma \vdash \lambda x^A.u : A \to B}\ (\text{abs}) \qquad \frac{\Gamma \vdash u : A \to B \quad \Gamma \vdash v : A}{\Gamma \vdash u\ v : B}\ (\text{app})$$

Summary of the previous works

Pedagogical simply typed λ-calculus [Colson and Michel (2007)]

Morphology $\alpha \mid A \to B$

Syntax $x \mid \lambda x^A.u \mid u\ v$

$$\frac{x : F \in \Gamma \quad \vdash \sigma \cdot \Gamma}{\Gamma \vdash x : F}\ (\text{var})$$

$$\frac{\Gamma, x : A \vdash u : B}{\Gamma \vdash \lambda x^A.u : A \to B}\ (\text{abs}) \qquad \frac{\Gamma \vdash u : A \to B \quad \Gamma \vdash v : A}{\Gamma \vdash u\ v : B}\ (\text{app})$$

Results

- satisfies the Poincaré criterion

Summary of the previous works

Pedagogical simply typed λ-calculus [Colson and Michel (2007)]

Morphology $\alpha \mid A \to B$

Syntax $x \mid \lambda x^A.u \mid u\ v$

No starting rule

$$\frac{x : F \in \Gamma \quad \vdash \sigma \cdot \Gamma}{\Gamma \vdash x : F}\ (\text{var})$$

$$\frac{\Gamma, x : A \vdash u : B}{\Gamma \vdash \lambda x^A.u : A \to B}\ (\text{abs}) \qquad \frac{\Gamma \vdash u : A \to B \quad \Gamma \vdash v : A}{\Gamma \vdash u\ v : B}\ (\text{app})$$

Results

- satisfies the Poincaré criterion

Summary of the previous works

Pedagogical simply typed λ-calculus [Colson and Michel (2007)]

Morphology $\alpha \mid A \to B \mid \top$

Syntax $x \mid \lambda x^A.u \mid u\ v \mid o$

$$\frac{\vdash \sigma \cdot \Gamma}{\Gamma \vdash o : \top}\ (\text{ax}) \qquad \frac{x : F \in \Gamma \quad \vdash \sigma \cdot \Gamma}{\Gamma \vdash x : F}\ (\text{var})$$

$$\frac{\Gamma, x : A \vdash u : B}{\Gamma \vdash \lambda x^A.u : A \to B}\ (\text{abs}) \qquad \frac{\Gamma \vdash u : A \to B \quad \Gamma \vdash v : A}{\Gamma \vdash u\ v : B}\ (\text{app})$$

Results

- satisfies the Poincaré criterion
- all formulas exemplified by $\top$
- initial and pedagogical systems (syntactically) equivalents

Summary of the previous works

Pedagogical simply typed λ-calculus [Colson and Michel (2007)]

Example of derivation

$$\dfrac{\dfrac{\dfrac{}{\vdash \sigma \cdot (f : A \to B, g : B \to C, x : A)}\,(\text{var})}{\vdots}}{\dfrac{}{f : A \to B, g : B \to C, x : A \vdash g\ (f\ x) : C}\,(\text{app}^\star)}$$

$$\dfrac{}{\vdash \lambda f^{A \to B}.\lambda g^{B \to C}.\lambda x^{A}.g\ (f\ x) : (A \to B) \to (B \to C) \to (A \to C)}\,(\text{abs}^\star)$$

Summary of the previous works

Pedagogical simply typed λ-calculus [Colson and Michel (2007)]

Example of derivation

$$\frac{}{\vdash \sigma \cdot (f : A \to B, g : B \to C, x : A)}\ (\mathsf{ex}_2)$$

$$\sigma := [A, B, C \mapsto \top\,;\ f, g \mapsto \lambda y^{\top}.y\,;\ x \mapsto o]$$

Summary of the previous works

Pedagogical simply typed λ-calculus [Colson and Michel (2007)]

Example of derivation

$$\dfrac{\dfrac{\dfrac{}{y : \top \vdash y : \top}\,(\text{var})}{\vdash \lambda y^{\top}.y : \top \to \top}\,(\text{abs})}{\vdash \sigma \cdot (f : A \to B, g : B \to C)}\,(\text{ex}_2) \qquad \dfrac{}{\vdash o : \top}\,(\text{ax})$$

$$\dfrac{\vdash \sigma \cdot (f : A \to B, g : B \to C)\ \ \vdash o : \top}{\vdash \sigma \cdot (f : A \to B, g : B \to C, x : A)}\,(\text{ex}_2)$$

$$\sigma := [A, B, C \mapsto \top\,;\ f, g \mapsto \lambda y^{\top}.y\,;\ x \mapsto o]$$

Summary of the previous works

Pedagogical simply typed λ-calculus [Colson and Michel (2007)]

Example of derivation

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash o : \top}\,(\mathsf{ax})}{\vdash \sigma'(y : \top)}\,(\mathsf{ex}_2)}{y : \top \vdash y : \top}\,(\mathsf{var})}{\vdash \lambda y^{\top}.y : \top \to \top}\,(\mathsf{abs})}{\vdash \sigma \cdot (f : A \to B, g : B \to C)}\,(\mathsf{ex}_2) \qquad \dfrac{}{\vdash o : \top}\,(\mathsf{ax})$$

$$\dfrac{\vdash \sigma \cdot (f : A \to B, g : B \to C) \qquad \vdash o : \top}{\vdash \sigma \cdot (f : A \to B, g : B \to C, x : A)}\,(\mathsf{ex}_2)$$

$$\sigma := [A, B, C \mapsto \top\,;\ f, g \mapsto \lambda y^{\top}.y\,;\ x \mapsto o]$$
$$\sigma' := [y \mapsto o]$$

Summary of the previous works

System F [Girard (1972), Reynolds (1974)]

Morphology $\alpha \mid A \to B \mid \forall \alpha.A$

Syntax $x \mid \lambda x^A.u \mid u\ v \mid \Lambda \alpha.u$

$$\frac{x : F \in \Gamma}{\Gamma \vdash^{\mathsf{f}} x : F}\ (\text{var})$$

$$\frac{\Gamma, x : A \vdash^{\mathsf{f}} u : B}{\Gamma \vdash^{\mathsf{f}} \lambda x^A.u : A \to B}\ (\text{abs})$$

$$\frac{\Gamma \vdash^{\mathsf{f}} u : A \to B \quad \Gamma \vdash^{\mathsf{f}} v : A}{\Gamma \vdash^{\mathsf{f}} u\ v : B}\ (\text{app})$$

$$\frac{\Gamma \vdash^{\mathsf{f}} u : B \quad \alpha \notin \mathcal{V}(\Gamma)}{\Gamma \vdash^{\mathsf{f}} \Lambda \alpha.u : \forall \alpha.B}\ (\text{Abs})$$

$$\frac{\Gamma \vdash^{\mathsf{f}} u : \forall \alpha.B}{\Gamma \vdash^{\mathsf{f}} u\ V : B[\alpha \leftarrow V]}\ (\text{App})$$

Summary of the previous works

Weakly pedagogical System F [Colson and Michel (2008)]

Morphology $\alpha \mid A \to B \mid \forall \alpha.A \mid \top$

Syntax $x \mid \lambda x^A.u \mid u\ v \mid \Lambda\alpha.u \mid o$

$$\frac{\vdash^{\mathsf{fw}} \sigma \cdot \Gamma}{\Gamma \vdash^{\mathsf{fw}} o : \top}\ (\mathsf{ax}) \qquad \frac{x : F \in \Gamma \quad \vdash^{\mathsf{fw}} \sigma \cdot \Gamma}{\Gamma \vdash^{\mathsf{fw}} x : F}\ (\mathsf{var})$$

$$\frac{\Gamma, x : A \vdash^{\mathsf{fw}} u : B}{\Gamma \vdash^{\mathsf{fw}} \lambda x^A.u : A \to B}\ (\mathsf{abs}) \qquad \frac{\Gamma \vdash^{\mathsf{fw}} u : A \to B \quad \Gamma \vdash^{\mathsf{fw}} v : A}{\Gamma \vdash^{\mathsf{fw}} u\ v : B}\ (\mathsf{app})$$

$$\frac{\Gamma \vdash^{\mathsf{fw}} u : B \quad \alpha \notin \mathcal{V}(\Gamma)}{\Gamma \vdash^{\mathsf{fw}} \Lambda\alpha.u : \forall \alpha.B}\ (\mathsf{Abs}) \qquad \frac{\Gamma \vdash^{\mathsf{fw}} u : \forall \alpha.B}{\Gamma \vdash^{\mathsf{fw}} u\ V : B[\alpha \leftarrow V]}\ (\mathsf{App})$$

Results

- satisfies the Poincaré criterion

Summary of the previous works

Weakly pedagogical System F [Colson and Michel (2008)]

Morphology $\alpha \mid A \to B \mid \forall \alpha.A \mid \top$

Syntax $x \mid \lambda x^A.u \mid u\ v \mid \Lambda\alpha.u \mid o$

$$\frac{\vdash^{\mathsf{fw}} \sigma \cdot \Gamma}{\Gamma \vdash^{\mathsf{fw}} o : \top}\ (\mathsf{ax}) \qquad \frac{x : F \in \Gamma \quad \vdash^{\mathsf{fw}} \sigma \cdot \Gamma}{\Gamma \vdash^{\mathsf{fw}} x : F}\ (\mathsf{var})$$

$$\frac{\Gamma, x : A \vdash^{\mathsf{fw}} u : B}{\Gamma \vdash^{\mathsf{fw}} \lambda x^A.u : A \to B}\ (\mathsf{abs}) \qquad \frac{\Gamma \vdash^{\mathsf{fw}} u : A \to B \quad \Gamma \vdash^{\mathsf{fw}} v : A}{\Gamma \vdash^{\mathsf{fw}} u\ v : B}\ (\mathsf{app})$$

$$\frac{\Gamma \vdash^{\mathsf{fw}} u : B \quad \alpha \notin \mathcal{V}(\Gamma)}{\Gamma \vdash^{\mathsf{fw}} \Lambda\alpha.u : \forall \alpha.B}\ (\mathsf{Abs}) \qquad \frac{\Gamma \vdash^{\mathsf{fw}} u : \forall \alpha.B}{\Gamma \vdash^{\mathsf{fw}} u\ V : B[\alpha \leftarrow V]}\ (\mathsf{App})$$

Results

- satisfies the Poincaré criterion
- no subject reduction property : $\vdash^{\mathsf{fw}} (\Lambda\alpha.\lambda x^{\alpha}.x)\ \bot : \bot \to \bot$ but $\not\vdash^{\mathsf{fw}} \lambda x^{\bot}.x : \bot \to \bot$

$\triangleright \bot := \forall \alpha.\alpha$

Summary of the previous works

Pedagogical System F [Colson and Michel (2009)]

Pre-Morphology $\alpha \mid A \to B \mid \forall \alpha.A \mid \top$

Syntax $x \mid \lambda x^A.u \mid u\ v \mid \Lambda\alpha.u \mid o$

$$\frac{\vdash^{\mathsf{fp}} \sigma \cdot \Gamma}{\Gamma \vdash^{\mathsf{fp}} o : \top}\ (\mathsf{ax}) \qquad \frac{x : F \in \Gamma \quad \vdash^{\mathsf{fp}} \sigma \cdot \Gamma}{\Gamma \vdash^{\mathsf{fp}} x : F}\ (\mathsf{var})$$

$$\frac{\Gamma, x : A \vdash^{\mathsf{fp}} u : B}{\Gamma \vdash^{\mathsf{fp}} \lambda x^A.u : A \to B}\ (\mathsf{abs}) \qquad \frac{\Gamma \vdash^{\mathsf{fp}} u : A \to B \quad \Gamma \vdash^{\mathsf{fp}} v : A}{\Gamma \vdash^{\mathsf{fp}} u\ v : B}\ (\mathsf{app})$$

$$\frac{\Gamma \vdash^{\mathsf{fp}} u : B \quad \alpha \notin \mathcal{V}(\Gamma)}{\Gamma \vdash^{\mathsf{fp}} \Lambda\alpha.u : \forall \alpha.B}\ (\mathsf{Abs}) \qquad \frac{\Gamma \vdash^{\mathsf{fp}} u : \forall \alpha.B \quad \vdash^{\mathsf{fp}} \sigma \cdot V}{\Gamma \vdash^{\mathsf{fp}} u\ V : B[\alpha \leftarrow V]}\ (\mathsf{App})$$

Summary of the previous works

Pedagogical System F [Colson and Michel (2009)]

Main results

- every well-formed sub-type can be exemplified :
  - Poincaré criterion always satisfied :
    $\Gamma \vdash^{\mathsf{fp}} u : A \quad \Rightarrow \quad \vdash^{\mathsf{fp}} \sigma \cdot \Gamma$
  - usefulness of functions :
    $\Gamma \vdash^{\mathsf{fp}} f : A \to B$ with A closed $\quad \Rightarrow \quad A$ is inhabited
  - negationless second-order propositional calculus
- expressive power compared to System F :
  - at logical side :
    $\exists t \quad \Gamma \vdash^{\mathsf{f}} t : F \quad \Leftrightarrow \quad \exists t' \quad \Gamma^{\gamma} \vdash^{\mathsf{fp}} t' : F^{\gamma}$
    where F^{γ} is F with occurrences of variables α replaced by $\alpha \vee \gamma$ (γ fresh)
  - at computational side :
    $\Gamma \vdash^{\mathsf{f}} t : A \quad \Rightarrow \quad \Gamma^{\delta} \vdash^{\mathsf{fp}} \overline{t} : A^{\delta}$
    where A^{δ} is a *double-negation* version of A ($\bot$ replaced by δ)
    and $\overline{t}$ is a CPS version of t (δ fresh)

Summary of the previous works

Pedagogical System F [Colson and Michel (2009)]

Main results

logic	computation
formula	datatype
proof	program
simplification	computation
direct proof	result
proof checking	type checking
exemplifiability	utility

First attempts toward a pedagogical CC

Calculus of Constructions [Coquand and Huet (1985)]

Motivations

The Calculus of Constructions :

- uniform presentation of previous systems
- interdependence between morphology and syntax
  - ▷ reduction of constraints number
- first step towards pedagogical pure type systems (PTS)
  - ▷ especially Type : Type [Martin-Löf (1971)]

First attempts toward a pedagogical CC

Calculus of Constructions [Coquand and Huet (1985)]

$$\frac{}{\emptyset\ \mathsf{wf}^{\mathsf{c}}}\ (\text{c-env}_1) \qquad \frac{\Gamma \vdash^{\mathsf{c}} A : \kappa \quad x \notin \mathsf{dom}(\Gamma)}{\Gamma, x : A\ \mathsf{wf}^{\mathsf{c}}}\ (\text{c-env}_2)$$

$$\frac{\Gamma\ \mathsf{wf}^{\mathsf{c}}}{\Gamma \vdash^{\mathsf{c}} \mathsf{Prop} : \mathsf{Type}}\ (\text{c-ax}) \qquad \frac{\Gamma, x : A, \Gamma'\ \mathsf{wf}^{\mathsf{c}}}{\Gamma, x : A, \Gamma' \vdash^{\mathsf{c}} x : A}\ (\text{c-var})$$

$$\frac{\Gamma, x : A \vdash^{\mathsf{c}} u : B : \kappa}{\Gamma \vdash^{\mathsf{c}} \lambda x^A.u : \forall x^A.B}\ (\text{c-abs}) \qquad \frac{\Gamma \vdash^{\mathsf{c}} u : \forall x^A.B \quad \Gamma \vdash^{\mathsf{c}} v : A}{\Gamma \vdash^{\mathsf{c}} u\ v : B[x \leftarrow v]}\ (\text{c-app})$$

$$\frac{\Gamma, x : A \vdash^{\mathsf{c}} B : \kappa}{\Gamma \vdash^{\mathsf{c}} \forall x^A.B : \kappa}\ (\text{c-prod}) \qquad \frac{\Gamma \vdash^{\mathsf{c}} u : A \quad A \simeq A' \quad \Gamma \vdash^{\mathsf{c}} A' : \kappa}{\Gamma \vdash^{\mathsf{c}} u : A'}\ (\text{c-conv})$$

κ denotes Prop or Type

First attempts toward a pedagogical CC

Naive transposition

Formal Poincaré criterion

$\Gamma \equiv x_1 : A_1, \ldots, x_n : A_n$ can be exemplified by terms $t_1, \ldots, t_n$ if

$$\begin{array}{c} \vdash t_1 : A_1 \\ \vdash t_2 : A_2[x_1 \leftarrow t_1] \\ \vdots \\ \vdash t_n : A_n[x_1, \ldots, x_{n-1} \leftarrow t_1, \ldots, t_{n-1}] \end{array}$$

Abbreviation : $\vdash \sigma \cdot \Gamma$ with $\sigma := [x_1 \mapsto t_1, \ldots, x_n \mapsto t_n]$

First idea

Substitutes the well-formedness of an environment by its exemplifiability

$\triangleright \Gamma$ wf replaced by $\vdash \sigma \cdot \Gamma$

First attempts toward a pedagogical CC

Naive transposition

$$\frac{\vdash^{\mathsf{n}} \sigma \cdot \Gamma}{\Gamma \vdash^{\mathsf{n}} o : \top : \mathsf{Prop} : \mathsf{Type}}\ (\text{n-ax}) \qquad \frac{\vdash^{\mathsf{n}} \sigma \cdot (\Gamma, x : A, \Gamma')}{\Gamma, x : A, \Gamma' \vdash^{\mathsf{n}} x : A}\ (\text{n-var})$$

But

- "exemplifiable" does not imply "well-formed" :
  - $x_1 : \mathsf{Type}$ $\quad \triangleright \sigma := [x_1 \mapsto \mathsf{Prop}]$
  - $x_1 : \mathsf{Prop}, x_2 : (\lambda H^{\top \to x_1}.\top)\ (\lambda y^{\top}.y)$ $\quad \triangleright \sigma := [x_1 \mapsto \top; x_2 \mapsto o]$
  - etc.
- no subject reduction $\quad \triangleright \bot \to \bot$ inhabited

First attempts toward a pedagogical CC

Calculus of Constructions [Coquand and Huet (1985)]

$$\frac{}{\emptyset\ \mathsf{wf}^{\mathsf{c}}}\ (\text{c-env}_1) \qquad \frac{\Gamma \vdash^{\mathsf{c}} A : \kappa \quad x \notin \mathrm{dom}(\Gamma)}{\Gamma, x : A\ \mathsf{wf}^{\mathsf{c}}}\ (\text{c-env}_2)$$

$$\frac{\Gamma\ \mathsf{wf}^{\mathsf{c}}}{\Gamma \vdash^{\mathsf{c}} \mathsf{Prop} : \mathsf{Type}}\ (\text{c-ax}) \qquad \frac{\Gamma, x : A, \Gamma'\ \mathsf{wf}^{\mathsf{c}}}{\Gamma, x : A, \Gamma' \vdash^{\mathsf{c}} x : A}\ (\text{c-var})$$

$$\frac{\Gamma, x : A \vdash^{\mathsf{c}} u : B : \kappa}{\Gamma \vdash^{\mathsf{c}} \lambda x^A.u : \forall x^A.B}\ (\text{c-abs}) \qquad \frac{\Gamma \vdash^{\mathsf{c}} u : \forall x^A.B \quad \Gamma \vdash^{\mathsf{c}} v : A}{\Gamma \vdash^{\mathsf{c}} u\ v : B[x \leftarrow v]}\ (\text{c-app})$$

$$\frac{\Gamma, x : A \vdash^{\mathsf{c}} B : \kappa}{\Gamma \vdash^{\mathsf{c}} \forall x^A.B : \kappa}\ (\text{c-prod}) \qquad \frac{\Gamma \vdash^{\mathsf{c}} u : A \quad A \simeq A' \quad \Gamma \vdash^{\mathsf{c}} A' : \kappa}{\Gamma \vdash^{\mathsf{c}} u : A'}\ (\text{c-conv})$$

κ denotes Prop or Type

First attempts toward a pedagogical CC

Calculus of Constructions [Coquand and Huet (1985)]

$$\frac{}{\emptyset\ \mathsf{wf}^{\mathsf{c}}}\ (\text{c-env}_1) \qquad \frac{\Gamma \vdash^{\mathsf{c}} A : \kappa \quad x \notin \mathrm{dom}(\Gamma)}{\Gamma, x : A\ \mathsf{wf}^{\mathsf{c}}}\ (\text{c-env}_2)$$

$$\frac{\Gamma\ \mathsf{wf}^{\mathsf{c}}}{\Gamma \vdash^{\mathsf{c}} \mathsf{Prop} : \mathsf{Type}}\ (\text{c-ax}) \qquad \frac{\Gamma, x : A, \Gamma'\ \mathsf{wf}^{\mathsf{c}}}{\Gamma, x : A, \Gamma' \vdash^{\mathsf{c}} x : A}\ (\text{c-var})$$

$$\frac{\Gamma, x : A \vdash^{\mathsf{c}} u : B : \kappa}{\Gamma \vdash^{\mathsf{c}} \lambda x^A.u : \forall x^A.B}\ (\text{c-abs}) \qquad \frac{\Gamma \vdash^{\mathsf{c}} u : \forall x^A.B \quad \Gamma \vdash^{\mathsf{c}} v : A}{\Gamma \vdash^{\mathsf{c}} u\ v : B[x \leftarrow v]}\ (\text{c-app})$$

$$\frac{\Gamma, x : A \vdash^{\mathsf{c}} B : \kappa}{\Gamma \vdash^{\mathsf{c}} \forall x^A.B : \kappa}\ (\text{c-prod}) \qquad \frac{\Gamma \vdash^{\mathsf{c}} u : A \quad A \simeq A' \quad \Gamma \vdash^{\mathsf{c}} A' : \kappa}{\Gamma \vdash^{\mathsf{c}} u : A'}\ (\text{c-conv})$$

(c-prod) responsible of vacuity

κ denotes Prop or Type

First attempts toward a pedagogical CC

Poincarean Calculus of Constructions – CCr

Strategy change

- keep Γ wf judgements
- avoid empty types as soon as possible

Radical idea

Constrain (only) the type formation rule :

$$\frac{\Gamma, x : A \vdash^{\mathsf{c}} \quad B : \kappa}{\Gamma \vdash^{\mathsf{c}} \forall x^{A}.B : \kappa}\ \text{(c-prod)}$$

First attempts toward a pedagogical CC

Poincarean Calculus of Constructions – CCr

Strategy change

- keep Γ wf judgements
- avoid empty types as soon as possible

Radical idea

Constrain (only) the type formation rule :

$$\frac{\Gamma, x : A \vdash^{\mathsf{r}} u : B : \kappa}{\Gamma \vdash^{\mathsf{r}} \forall x^{A}.B : \kappa}\ \text{(r-prod)}$$

First attempts toward a pedagogical CC

Poincarean Calculus of Constructions – CCr

Theorems

- respectful of the Poincaré criterion
  - ▷ relies on strong normalization of CC
- subject reduction property holds
  - ▷ Coq proof adapted from [Barras (1996)]
- usefulness of functions
  - ▷ $\vdash^{\mathsf{r}} f : \forall x^A.B \quad \Rightarrow \quad \exists u \quad \vdash^{\mathsf{r}} u : A$
- terms of Gödel system T can be interpreted in CC_{r}
  - ▷ usual way : recursion from iteration (and trick for cartesian products)

But

- does not contain natively simply typed λ-calculus
  - ▷ $\nexists u \quad A\ B\ C : \mathrm{Prop} \vdash^{\mathsf{r}} u : (A \to B) \to (B \to C) \to (A \to C)$
- does not prove symmetry of Leibniz equality
  - ▷ $\nexists u \quad A : \mathrm{Prop}, x\ y\ z : A \vdash^{\mathsf{r}} u : x =_A y \to y =_A z \to x =_A z$

First attempts toward a pedagogical CC

Poincarean Calculus of Constructions – CCr

Observation CCr seems too much constrained

Goal increase expressive power

Idea exemplifiable types should be usable

▷ similar to pedagogical system F

Definition : converse of the Poincaré criterion

$\mathsf{CC}_\star$, sub-system of CC, meets the *converse of the Poincaré criterion* if :

$$\vdash^\star \sigma \cdot \Gamma \qquad \Rightarrow \quad \Gamma\ \mathsf{wf}^\star$$

First attempts toward a pedagogical CC

Poincarean Calculus of Constructions – CCr

Observation CCr seems too much constrained

Goal increase expressive power

Idea exemplifiable types should be usable

▷ similar to pedagogical system F

Definition : converse of the Poincaré criterion

$\mathrm{CC}_\star$, sub-system of CC, meets the *converse of the Poincaré criterion* if :

$$\vdash^\star \sigma \cdot \Gamma \text{ and } \Gamma \,\mathsf{wf}^c \quad \Rightarrow \quad \Gamma \,\mathsf{wf}^\star$$

Beware

Exemplifiable types need not be well-formed

A formal definition and some examples

Pedagogical sub-system of the Calculus of Constructions

Definition : $CC_\star$ pedagogical sub-system of CC

- $CC_\star$ sub-system of CC

$$\triangleright\, \Gamma \vdash^\star u : A \quad \Rightarrow \quad \Gamma \vdash^{\mathsf{c}} u : A$$

- Subject reduction property holds for $CC_\star$

$$\triangleright\, \Gamma \vdash^\star u : A \text{ and } u \rightsquigarrow u' \quad \Rightarrow \quad \Gamma \vdash^\star u' : A$$

- $CC_\star$ meets Poincaré criterion and its converse

$$\triangleright\, \Gamma\, \mathsf{wf}^\star \quad \Leftrightarrow \quad \vdash^\star \sigma \cdot \Gamma \text{ and } \Gamma\, \mathsf{wf}^{\mathsf{c}}$$

A formal definition and some examples

Calculus of Constructions [Coquand and Huet (1985)]

$$\frac{}{\emptyset\ \mathsf{wf}^{\mathsf{c}}}\ (\text{c-env}_1) \qquad \frac{\Gamma \vdash^{\mathsf{c}} A : \kappa \quad x \notin \mathsf{dom}(\Gamma)}{\Gamma, x : A\ \mathsf{wf}^{\mathsf{c}}}\ (\text{c-env}_2)$$

$$\frac{\Gamma\ \mathsf{wf}^{\mathsf{c}}}{\Gamma \vdash^{\mathsf{c}} \mathsf{Prop} : \mathsf{Type}}\ (\text{c-ax}) \qquad \frac{\Gamma, x : A, \Gamma'\ \mathsf{wf}^{\mathsf{c}}}{\Gamma, x : A, \Gamma' \vdash^{\mathsf{c}} x : A}\ (\text{c-var})$$

$$\frac{\Gamma, x : A \vdash^{\mathsf{c}} u : B : \kappa}{\Gamma \vdash^{\mathsf{c}} \lambda x^A.u : \forall x^A.B}\ (\text{c-abs}) \qquad \frac{\Gamma \vdash^{\mathsf{c}} u : \forall x^A.B \quad \Gamma \vdash^{\mathsf{c}} v : A}{\Gamma \vdash^{\mathsf{c}} u\ v : B[x \leftarrow v]}\ (\text{c-app})$$

$$\frac{\Gamma, x : A \vdash^{\mathsf{c}} B : \kappa}{\Gamma \vdash^{\mathsf{c}} \forall x^A.B : \kappa}\ (\text{c-prod}) \qquad \frac{\Gamma \vdash^{\mathsf{c}} u : A \quad A \simeq A' \quad \Gamma \vdash^{\mathsf{c}} A' : \kappa}{\Gamma \vdash^{\mathsf{c}} u : A'}\ (\text{c-conv})$$

κ denotes Prop or Type

A formal definition and some examples

Second order λ-calculus – λ^2

$$\frac{}{\emptyset\,\mathsf{wf}^2}\ (\ \mathsf{env}_1)$$

$$\frac{\Gamma \vdash^2 A : \kappa \quad x \notin \mathsf{dom}(\Gamma)}{\Gamma, x : A\,\mathsf{wf}^2}\ (\ \mathsf{env}_2)$$

$$\frac{\Gamma\,\mathsf{wf}^2}{\Gamma \vdash^2 \mathsf{Prop} : \mathsf{Type}}\ (\ \mathsf{ax})$$

$$\frac{\Gamma, x : A, \Gamma'\,\mathsf{wf}^2}{\Gamma, x : A, \Gamma' \vdash^2 x : A}\ (\ \mathsf{var})$$

$$\frac{\Gamma, x : A \vdash^2 u : B : \mathsf{Prop}}{\Gamma \vdash^2 \lambda x^A.u : \forall x^A.B}\ (\ \mathsf{abs})$$

$$\frac{\Gamma \vdash^2 u : \forall x^A.B \quad \Gamma \vdash^2 v : A}{\Gamma \vdash^2 u\ v : B[x \leftarrow v]}\ (\ \mathsf{app})$$

$$\frac{\Gamma, x : A \vdash^2 B : \mathsf{Prop}}{\Gamma \vdash^2 \forall x^A.B : \mathsf{Prop}}\ (\ \mathsf{prod})$$

A formal definition and some examples

With explicit total exemplifications – λ_e^2

Goal

Obtain a pedagogical version of λ^2

$\triangleright$ in the sense of the previous definition

First idea

Keep examples explicit : $\Gamma \vdash_\sigma u : A$ and $\Gamma\ \mathsf{wf}_\sigma$ where

- $\Gamma \equiv x_1 : A_1, \ldots, x_n : A_n$
- $\sigma \equiv [x_1 \mapsto t_1, \ldots, x_n \mapsto t_n]$ or in short $\sigma \equiv [t_1, \ldots, t_n]$

A formal definition and some examples

Second order λ-calculus – λ^2

$$\frac{}{\emptyset\ \mathsf{wf}^2}\ (\ \mathsf{env_1})$$

$$\frac{\Gamma \vdash^2 A : \kappa \qquad x \notin \mathrm{dom}(\Gamma)}{\Gamma, x : A\ \mathsf{wf}^2}\ (\ \mathsf{env_2})$$

$$\frac{\Gamma\ \mathsf{wf}^2}{\Gamma \vdash^2 \mathsf{Prop} : \mathsf{Type}}\ (\ \mathsf{ax})$$

$$\frac{\Gamma, x : A, \Gamma'\ \mathsf{wf}^2}{\Gamma, x : A, \Gamma' \vdash^2 x : A}\ (\ \mathsf{var})$$

$$\frac{\Gamma, x : A \vdash^2 \quad u : B : \mathsf{Prop}}{\Gamma \vdash^2 \lambda x^A.u : \forall x^A.B}\ (\ \mathsf{abs})$$

$$\frac{\Gamma \vdash^2 u : \forall x^A.B \quad \Gamma \vdash^2 v : A}{\Gamma \vdash^2 u\ v : B[x \leftarrow v]}\ (\ \mathsf{app})$$

$$\frac{\Gamma, x : A \vdash^2 \quad B : \mathsf{Prop}}{\Gamma \vdash^2 \forall x^A.B : \mathsf{Prop}}\ (\ \mathsf{prod})$$

A formal definition and some examples

With explicit total exemplifications – λ^2_e

$$\frac{}{\emptyset\ \mathsf{wf}^{2e}_{\emptyset}}\ (\text{e-env}_1) \qquad \frac{\Gamma \vdash^{2e}_{\sigma} A : \kappa \qquad x \notin \mathrm{dom}(\Gamma)}{\Gamma, x : A\ \mathsf{wf}^{2e}_{\sigma :: a}}\ (\text{e-env}_2)$$

$$\frac{\Gamma\ \mathsf{wf}^{2e}_{\sigma}}{\Gamma \vdash^{2e}_{\sigma} \mathsf{Prop} : \mathsf{Type}}\ (\text{e-ax}) \qquad \frac{\Gamma, x : A, \Gamma'\ \mathsf{wf}^{2e}_{\sigma}}{\Gamma, x : A, \Gamma' \vdash^{2e}_{\sigma} x : A}\ (\text{e-var})$$

$$\frac{\Gamma, x : A \vdash^{2e}_{\sigma :: a} u : B : \mathsf{Prop}}{\Gamma \vdash^{2e}_{\sigma} \lambda x^A.u : \forall x^A.B}\ (\text{e-abs}) \qquad \frac{\Gamma \vdash^{2e}_{\sigma} u : \forall x^A.B \quad \Gamma \vdash^{2e}_{\sigma} v : A}{\Gamma \vdash^{2e}_{\sigma} u\ v : B[x \leftarrow v]}\ (\text{e-app})$$

$$\frac{\Gamma, x : A \vdash^{2e}_{\sigma :: a} B : \mathsf{Prop}}{\Gamma \vdash^{2e}_{\sigma} \forall x^A.B : \mathsf{Prop}}\ (\text{e-prod})$$

A formal definition and some examples

With explicit total exemplifications – λ_e^2

$$\frac{}{\emptyset \,\mathsf{wf}^{2e}_{\emptyset}}\ (\text{e-env}_1) \qquad \frac{\Gamma \vdash^{2e}_{\sigma} A : \kappa \quad \vdash^{2e}_{\emptyset} a : \sigma(A) \quad x \notin \mathrm{dom}(\Gamma)}{\Gamma, x : A \,\mathsf{wf}^{2e}_{\sigma :: a}}\ (\text{e-env}_2)$$

$$\frac{\Gamma \,\mathsf{wf}^{2e}_{\sigma}}{\Gamma \vdash^{2e}_{\sigma} o : \top : \mathsf{Prop} : \mathsf{Type}}\ (\text{e-ax}) \qquad \frac{\Gamma, x : A, \Gamma' \,\mathsf{wf}^{2e}_{\sigma}}{\Gamma, x : A, \Gamma' \vdash^{2e}_{\sigma} x : A}\ (\text{e-var})$$

$$\frac{\Gamma, x : A \vdash^{2e}_{\sigma :: a} u : B : \mathsf{Prop}}{\Gamma \vdash^{2e}_{\sigma} \lambda x^A.u : \forall x^A.B}\ (\text{e-abs}) \qquad \frac{\Gamma \vdash^{2e}_{\sigma} u : \forall x^A.B \quad \Gamma \vdash^{2e}_{\sigma} v : A}{\Gamma \vdash^{2e}_{\sigma} u\ v : B[x \leftarrow v]}\ (\text{e-app})$$

$$\frac{\Gamma, x : A \vdash^{2e}_{\sigma :: a} B : \mathsf{Prop} \quad \vdash^{2e}_{\emptyset} t : \sigma(\forall x^A.B)}{\Gamma \vdash^{2e}_{\sigma} \forall x^A.B : \mathsf{Prop}}\ (\text{e-prod})$$

A formal definition and some examples

With explicit total exemplifications – λ_e^2

Theorems

- λ_e^2 (*almost*) a pedagogical sub-system of CC
- examples contained as sub-derivations

$$\triangleright\, \Gamma \Vdash^{2e}_{\sigma} A : \kappa \quad \Rightarrow \quad \exists a \quad \Vdash^{2e}_{\emptyset} a : \sigma(A) \text{ sub-derivation}$$

- exchange of exemplifications :

$$\triangleright\, \Gamma \Vdash^{2e}_{\sigma} w : C \text{ and } \Gamma \,\mathrm{wf}^{2e}_{\rho} \quad \Rightarrow \quad \Gamma \Vdash^{2e}_{\rho} w : C$$

But

λ_e^2 not exactly sub-system of CC because :

- exemplifications are explicit
- addition of two symbols o and $\top$

A formal definition and some examples

With explicit total exemplifications – λ_e^2

Theorems

- λ_e^2 (*almost*) a pedagogical sub-system of CC
- examples contained as sub-derivations

$$\triangleright\, \Gamma \Vdash^{2e}_{\sigma} A : \kappa \quad \Rightarrow \quad \exists a \quad \Vdash^{2e}_{\emptyset} a : \sigma(A) \text{ sub-derivation}$$

- exchange of exemplifications :

$$\triangleright\, \Gamma \Vdash^{2e}_{\sigma} w : C \text{ and } \Gamma \,\mathrm{wf}^{2e}_{\rho} \quad \Rightarrow \quad \Gamma \Vdash^{2e}_{\rho} w : C$$

But

λ_e^2 not exactly sub-system of CC because :

- exemplifications are explicit
- addition of two symbols o and $\top$

Second idea

Relax constraints on exemplifications by making them implicit

A formal definition and some examples

With explicit total exemplifications – λ_e^2

$$\frac{}{\emptyset\ \mathsf{wf}^{2e}_{\emptyset}}\ (\text{e-env}_1) \qquad \frac{\Gamma \Vdash^{2e}_{\sigma} A : \kappa \quad \Vdash^{2e}_{\emptyset} a : \sigma(A) \quad x \notin \mathrm{dom}(\Gamma)}{\Gamma, x : A\ \mathsf{wf}^{2e}_{\sigma :: a}}\ (\text{e-env}_2)$$

$$\frac{\Gamma\ \mathsf{wf}^{2e}_{\sigma}}{\Gamma \Vdash^{2e}_{\sigma} o : \top : \mathsf{Prop} : \mathsf{Type}}\ (\text{e-ax}) \qquad \frac{\Gamma, x : A, \Gamma'\ \mathsf{wf}^{2e}_{\sigma}}{\Gamma, x : A, \Gamma' \Vdash^{2e}_{\sigma} x : A}\ (\text{e-var})$$

$$\frac{\Gamma, x : A \Vdash^{2e}_{\sigma :: a} u : B : \mathsf{Prop}}{\Gamma \Vdash^{2e}_{\sigma} \lambda x^A.u : \forall x^A.B}\ (\text{e-abs}) \qquad \frac{\Gamma \Vdash^{2e}_{\sigma} u : \forall x^A.B \quad \Gamma \Vdash^{2e}_{\sigma} v : A}{\Gamma \Vdash^{2e}_{\sigma} u\ v : B[x \leftarrow v]}\ (\text{e-app})$$

$$\frac{\Gamma, x : A \Vdash^{2e}_{\sigma :: a} B : \mathsf{Prop} \quad \Vdash^{2e}_{\emptyset} t : \sigma(\forall x^A.B)}{\Gamma \Vdash^{2e}_{\sigma} \forall x^A.B : \mathsf{Prop}}\ (\text{e-prod})$$

A formal definition and some examples

With implicit total exemplifications – λ_t^2

$$\frac{}{\emptyset\ \mathsf{wf}^{2t}}\ (\text{t-env}_1) \qquad \frac{\Gamma \vdash^{2t} A : \kappa \qquad x \notin \mathrm{dom}(\Gamma)}{\Gamma, x : A\ \mathsf{wf}^{2t}}\ (\text{t-env}_2)$$

$$\frac{\Gamma\ \mathsf{wf}^{2t}}{\Gamma \vdash^{2t} o : \top : \mathsf{Prop} : \mathsf{Type}}\ (\text{t-ax}) \qquad \frac{\Gamma, x : A, \Gamma'\ \mathsf{wf}^{2t}}{\Gamma, x : A, \Gamma' \vdash^{2t} x : A}\ (\text{t-var})$$

$$\frac{\Gamma, x : A \vdash^{2t} \quad u : B : \mathsf{Prop}}{\Gamma \vdash^{2t} \lambda x^A.u : \forall x^A.B}\ (\text{t-abs}) \qquad \frac{\Gamma \vdash^{2t} u : \forall x^A.B \quad \Gamma \vdash^{2t} v : A}{\Gamma \vdash^{2t} u\ v : B[x \leftarrow v]}\ (\text{t-app})$$

$$\frac{\Gamma, x : A \vdash^{2t} \quad B : \mathsf{Prop} \quad \sigma\ \mathsf{mot}_\Gamma\ \forall x^A.B}{\Gamma \vdash^{2t} \forall x^A.B : \mathsf{Prop}}\ (\text{t-prod})$$

where $\sigma\ \mathsf{mot}_\Gamma\ C$ abbreviates :

(a) σ exemplifies Γ, i.e. $\vdash^{2t} \sigma \cdot \Gamma$

(b) and there is term t such that $\vdash^{2t} t : \sigma(C)$

A formal definition and some examples

With implicit total exemplifications – λ_t^2

Theorems

- λ_t^2 equivalent to λ_e^2 : $\Gamma \vdash^{2t} t : A \quad \Leftrightarrow \quad \exists \sigma \quad \Gamma \vdash_{\sigma}^{2e} t : A$
- λ_t^2 (*almost*) a pedagogical sub-system of CC

But

λ_t^2 not exactly sub-system of CC because :

- addition of two symbols o and $\top$

A formal definition and some examples

With implicit total exemplifications – λ_t^2

Theorems

- λ_t^2 equivalent to λ_e^2 : $\Gamma \vdash^{2t} t : A \quad \Leftrightarrow \quad \exists \sigma \quad \Gamma \vdash_{\sigma}^{2e} t : A$
- λ_t^2 (*almost*) a pedagogical sub-system of CC

But

λ_t^2 not exactly sub-system of CC because :

- addition of two symbols o and $\top$

Last idea

Have partial exemplifications to restore the CC_r's behaviour :

$\Gamma \vdash^{r} \mathsf{Id} : \mathsf{True} : \mathsf{Prop}$

$\triangleright$ with $\mathsf{Id} := \lambda A^{\mathsf{Prop}}.\lambda x^{A}.x$ and $\mathsf{True} := \forall A^{\mathsf{Prop}}.A \to A$

A formal definition and some examples

With implicit total exemplifications – λ_t^2

$$\frac{}{\emptyset\ \mathsf{wf}^{2t}}\ (\text{t-env}_1) \qquad \frac{\Gamma \vdash^{2t} A : \kappa \quad x \notin \mathrm{dom}(\Gamma)}{\Gamma, x : A\ \mathsf{wf}^{2t}}\ (\text{t-env}_2)$$

$$\frac{\Gamma\ \mathsf{wf}^{2t}}{\Gamma \vdash^{2t} o : \top : \mathsf{Prop} : \mathsf{Type}}\ (\text{t-ax}) \qquad \frac{\Gamma, x : A, \Gamma'\ \mathsf{wf}^{2t}}{\Gamma, x : A, \Gamma' \vdash^{2t} x : A}\ (\text{t-var})$$

$$\frac{\Gamma, x : A \vdash^{2t} u : B : \mathsf{Prop}}{\Gamma \vdash^{2t} \lambda x^A.u : \forall x^A.B}\ (\text{t-abs}) \qquad \frac{\Gamma \vdash^{2t} u : \forall x^A.B \quad \Gamma \vdash^{2t} v : A}{\Gamma \vdash^{2t} u\ v : B[x \leftarrow v]}\ (\text{t-app})$$

$$\frac{\Gamma, x : A \vdash^{2t} B : \mathsf{Prop} \quad \sigma\ \mathsf{mot}_\Gamma\ \forall x^A.B}{\Gamma \vdash^{2t} \forall x^A.B : \mathsf{Prop}}\ (\text{t-prod})$$

where $\sigma\ \mathsf{mot}_\Gamma\ C$ abbreviates :

(a) σ exemplifies Γ, i.e. $\vdash^{2t} \sigma \cdot \Gamma$

(b) and there is term t such that $\vdash^{2t} t : \sigma(C)$

A formal definition and some examples

With implicit partial exemplifications – λ_p^2

$$\frac{}{\emptyset\ \mathsf{wf}^{2\mathsf{p}}}\ (\textsf{p-env}_\textbf{1}) \qquad \frac{\Gamma \vdash^{2\mathsf{p}} A : \kappa \quad x \notin \mathrm{dom}(\Gamma)}{\Gamma, x : A\ \mathsf{wf}^{2\mathsf{p}}}\ (\textsf{p-env}_\textbf{2})$$

$$\frac{\Gamma\ \mathsf{wf}^{2\mathsf{p}}}{\Gamma \vdash^{2\mathsf{p}} \mathsf{Prop} : \mathsf{Type}}\ (\textsf{p-ax}) \qquad \frac{\Gamma, x : A, \Gamma'\ \mathsf{wf}^{2\mathsf{p}}}{\Gamma, x : A, \Gamma' \vdash^{2\mathsf{p}} x : A}\ (\textsf{p-var})$$

$$\frac{\Gamma, x : A \vdash^{2\mathsf{p}} u : B : \mathsf{Prop}}{\Gamma \vdash^{2\mathsf{p}} \lambda x^A.u : \forall x^A.B}\ (\textsf{p-abs}) \qquad \frac{\Gamma \vdash^{2\mathsf{p}} u : \forall x^A.B \quad \Gamma \vdash^{2\mathsf{p}} v : A}{\Gamma \vdash^{2\mathsf{p}} u\ v : B[x \leftarrow v]}\ (\textsf{p-app})$$

$$\frac{\Gamma, x : A \vdash^{2\mathsf{p}} B : \mathsf{Prop} \quad \sigma\ \widetilde{\mathrm{mot}}_\Gamma\ \forall x^A.B}{\Gamma \vdash^{2\mathsf{p}} \forall x^A.B : \mathsf{Prop}}\ (\textsf{p-prod})$$

where $\sigma\ \widetilde{\mathrm{mot}}_\Gamma\ C$ abbreviates :

(a) σ partially exemplifies Γ, i.e. $\mathrm{dom}(\sigma) \subseteq \mathrm{dom}(\Gamma)$

(b) and there is a term t such that $\sigma(\Gamma) \vdash^{2\mathsf{p}} t : \sigma(C)$

A formal definition and some examples

With implicit partial exemplifications – λ_p^2

Theorems

- λ_p^2 equivalent to λ_t^2 : $\Gamma \vdash^{2p} t : A \quad \Leftrightarrow \quad \Gamma \vdash^{2t} t : A$

  ▷ exemplifications can be completed

- λ_p^2 **is a pedagogical sub-system of CC**

  ▷ definition exemplified !

General theorems

- λ_e^2, λ_t^2 and λ_p^2 are equivalents
- embeddings to and from pedagogical system F
- embedding from pedagogical λ^2

A formal definition and some examples

With implicit partial exemplifications – λ_p^2

Type checking ?

Undecidable for λ_e^2, λ_t^2, λ_p^2 and system Fp :

$$\begin{array}{lllll} \exists t \quad \Gamma \overset{\mathsf{f}}{\vdash} t : A & \Leftrightarrow & \exists t' & \Gamma^\gamma \overset{\mathsf{fp}}{\vdash} t' : A^\gamma \\ & \Leftrightarrow & \exists t'' & \overset{\mathsf{fp}}{\vdash} t'' : \forall \vec{\alpha}.\Gamma^\gamma \to A^\gamma \\ & \Leftrightarrow & & \overset{\mathsf{2t}}{\vdash} \forall \vec{\alpha}^{\mathsf{Prop}}.\Gamma^\gamma \to A^\gamma : \mathsf{Prop} \end{array}$$

where $\exists ? t \quad \Gamma \overset{\mathsf{f}}{\vdash} t : A$ undecidable [Urzyczyn (1997)]

Idea

Annotate types with terms to ensure exemplification :

$$\frac{\Gamma_\sigma \vdash A_a : \kappa \quad x \notin \mathrm{dom}(\Gamma)}{\Gamma_\sigma, x : A_a \,\mathrm{wf}}\ (\mathsf{env}_2) \qquad \frac{\Gamma_\sigma, x : A_a \vdash B_b : \mathsf{Prop} \quad \vdash t : \sigma(\forall x^{A_a}.B_b)}{\Gamma_\sigma \vdash (\forall x^{A_a}.B_b)_t : \mathsf{Prop}}\ (\mathsf{prod})$$

where $\Gamma_\sigma \equiv x_1 : A_{1\,a_1}, \ldots, x_n : A_{n\,a_n}$ and $\sigma \equiv [x_1 \mapsto a_1; \ldots; x_n \mapsto a_n]$.

Toward a Pedagogical Calculus of Constructions

Higher order

Goal

Obtain a Pedagogical λ^ω

New objects

- predicates/propositional functions
  $\triangleright \lambda A^{\mathsf{Prop}}.\lambda B^{\mathsf{Prop}\to\mathsf{Prop}}.B\ A$
- postulated into environments
  $\triangleright f : \mathsf{Prop} \to (\mathsf{Prop} \to \mathsf{Prop}) \to \mathsf{Prop}$

$\Rightarrow$ notion of predicate exemplification needed

Idea

Exemplifiable predicate $\Leftrightarrow$ useful propositional function

Toward a Pedagogical Calculus of Constructions

Higher order

Exemplifiable predicate (formally)

$P : \mathcal{O}_1 \to \ldots \to \mathcal{O}_n \to \text{Prop}$ exemplifiable if :

- can be completely applied ▷ there are $u_i : \mathcal{O}_i$
- reducible to an exemplifiable type ▷ $P\ \vec{u} \overset{*}{\rightsquigarrow} R$ and $\vdash \sigma \cdot R$

Abbreviated : $\sigma\,\text{mot}^{\mathcal{O}_1 \to \ldots \to \mathcal{O}_n \to \text{Prop}}(P)$

Examplifiable predicates

$P := \lambda A^{\text{Prop}}.A \to A$ ▷ $P\ \top \overset{*}{\rightsquigarrow} \top \to \top$

$Q := \lambda A^{\text{Prop}}.\lambda B^{\text{Prop}\to\text{Prop}}.B\ A$ ▷ $Q\ \top\ (\lambda C^{\text{Prop}}.\top) \overset{*}{\rightsquigarrow} \top$

Non exemplifiable predicate

$V := \lambda A^{\text{Prop}}.\forall B^{\text{Prop}}.A \to B$ ▷ hopefully no arguments

Toward a Pedagogical Calculus of Constructions

Pedagogical higher-order λ-calculus – λ_e^ω

Beware interaction of exemplifiable predicates

- $Q := \lambda R^{\mathsf{Prop}\to\mathsf{Prop}}.\forall F^{\mathsf{Prop}}.R\ F$ and $Id := \lambda A^{\mathsf{Prop}}.A$

  $\triangleright$ but $Q\ Id \overset{*}{\rightsquigarrow} \bot$

Necessary constraint

$$\frac{\Gamma \vdash_\sigma u : A \to B : \mathsf{Type} \quad \Gamma \vdash_\sigma v : A \quad \sigma\, \mathsf{mot}^B(u\ v)}{\Gamma \vdash_\sigma u\ v : B}\ (\omega e\text{-app}_\square)$$

Toward a Pedagogical Calculus of Constructions

Pedagogical higher-order λ-calculus – λ_e^ω

Beware interaction of exemplifiable predicates

- $Q := \lambda R^{\mathsf{Prop}\to\mathsf{Prop}}.\forall F^{\mathsf{Prop}}.R\ F$ and $Id := \lambda A^{\mathsf{Prop}}.A$
  $\triangleright$ but $Q\ Id \overset{*}{\rightsquigarrow} \bot$
- $S := \lambda A^{\mathsf{Prop}\to\mathsf{Prop}}.\lambda H^{\forall B^{\mathsf{Prop}}.A\ B}.H$
  $\triangleright$ but $S\ Id \overset{*}{\rightsquigarrow} \lambda H^{\bot}.H$

Necessary constraint

$$\frac{\Gamma \vdash_\sigma u : \forall x^A.B : \mathsf{Prop} \quad \Gamma \vdash_\sigma v : A \quad \sigma\,\mathsf{mot}^{\mathsf{Prop}}(B[x \leftarrow v])}{\Gamma \vdash_\sigma u\ v : B[x \leftarrow v]}\ (\omega e\text{-app}_\star)$$

Toward a Pedagogical Calculus of Constructions

Pedagogical higher-order λ-calculus – λ_e^ω

Beware interaction of exemplifiable predicates

- $Q := \lambda R^{\mathsf{Prop}\to\mathsf{Prop}}.\forall F^{\mathsf{Prop}}.R\ F$ and $Id := \lambda A^{\mathsf{Prop}}.A$
  ▷ but $Q\ Id \overset{*}{\rightsquigarrow} \bot$
- $S := \lambda A^{\mathsf{Prop}\to\mathsf{Prop}}.\lambda H^{\forall B^{\mathsf{Prop}}.A\ B}.H$
  ▷ but $S\ Id \overset{*}{\rightsquigarrow} \lambda H^{\bot}.H$

Necessary constraint

$$\frac{\Gamma \vdash_\sigma u : \forall x^A.B : \mathsf{Prop} \quad \Gamma \vdash_\sigma v : A \quad \sigma\,\mathsf{mot}^{\mathsf{Prop}}(B[x \leftarrow v])}{\Gamma \vdash_\sigma u\ v : B[x \leftarrow v]}\ (\omega e\text{-app}_\star)$$

Strong : only normal form examples ?

Toward a Pedagogical Calculus of Constructions

Pedagogical higher-order λ-calculus – λ_e^ω

Theorems

- λ_e^ω satisfies Poincaré criterion
- λ_e^ω satisfies the converse Poincaré criterion
- subject reduction still conjectured

  ▷ usual substitution lemma invalid :

  $$A : \star \to \star \vdash_{\lambda z^\star.\top} \lambda H^{\forall B^\star.A\ B}.H : (\forall B^\star.A\ B) \to (\forall B^\star.A\ B) : \star$$
  $$\vdash_{\emptyset} \lambda C^\star.C : \star \to \star$$

  $$\not\vdash_{\emptyset} \lambda H^{\forall B^\star.(\lambda C^\star.C)\ B}.H : (\forall B^\star.(\lambda C^\star.C)\ B) \to (\forall B^\star.(\lambda C^\star.C)\ B)$$

  where $\star := \mathrm{Prop}$

Toward a Pedagogical Calculus of Constructions

Summary of necessary constraints

$$\frac{\Gamma \vdash A : s_1 \quad \Gamma, x : A \vdash B : s_2}{\Gamma \vdash \forall x^A . B : s_2} \text{(prod)}$$

(s_1, s_2)	λ^2	λ^ω
(Prop, Prop)	✓	✓
(Type, Prop)	✗	✗
(Prop, Type)		
(Type, Type)		✓

- ✓ instance of the rule does not produce empty type
- ✗ instance of the rule can produce empty types

Toward a Pedagogical Calculus of Constructions

Summary of necessary constraints

$$\frac{\Gamma \vdash A : s_1 \quad \Gamma, x : A \vdash B : s_2}{\Gamma \vdash \forall x^A . B : s_2} \text{(prod)}$$

(s_1, s_2)	λ^2	λ^ω	λC
(Prop, Prop)	✓	✓	✗
(Type, Prop)	✗	✗	✗
(Prop, Type)			✓
(Type, Type)		✓	✓

- ✓ instance of the rule does not produce empty type
- ✗ instance of the rule can produce empty types

Toward a Pedagogical Calculus of Constructions

Summary of necessary constraints

$$\frac{\Gamma \vdash v : A : s_1 \quad \Gamma \vdash u : \forall x^A . B : s_2}{\Gamma \vdash u\ v : B[x \leftarrow v]}\ (\text{app})$$

(s_1, s_2)	λ^2	λ^ω
(Prop, Prop)	✓	✓
(Type, Prop)	✓	✗
(Prop, Type)		
(Type, Type)		✗

- ✓ instance of the rule does not produce empty type
- ✗ instance of the rule can produce empty types

Toward a Pedagogical Calculus of Constructions

Summary of necessary constraints

$$\frac{\Gamma \vdash v : A : s_1 \quad \Gamma \vdash u : \forall x^A.B : s_2}{\Gamma \vdash u\ v : B[x \leftarrow v]}\ (\text{app})$$

(s_1, s_2)	λ^2	λ^ω	λC
(Prop, Prop)	✓	✓	✗
(Type, Prop)	✓	✗	✗
(Prop, Type)			✗
(Type, Type)		✗	✗

- ✓ instance of the rule does not produce empty type
- ✗ instance of the rule can produce empty types

Toward a Pedagogical Calculus of Constructions

Pedagogical Calculus of Constructions ?

$$\frac{}{\emptyset \,\mathsf{wf}^{c_e}_{\sigma}}\,(\mathsf{env}_1)$$

$$\frac{\Gamma \vdash^{c_e}_{\sigma} A : \kappa \quad \vdash^{c_e}_{\emptyset} a : A' \quad \sigma(A) \overset{*}{\rightsquigarrow} A' \quad x \notin \mathsf{dom}(\Gamma)}{\Gamma, x : A \,\mathsf{wf}^{c_e}_{\sigma::(x \mapsto a)}}\,(\mathsf{env}_2)$$

$$\frac{\Gamma \,\mathsf{wf}^{c_e}_{\sigma}}{\Gamma \vdash^{c_e}_{\sigma} o : \top : \mathsf{Prop} : \mathsf{Type}}\,(\mathsf{ax})$$

$$\frac{\Gamma, x : A, \Gamma' \,\mathsf{wf}^{c_e}_{\sigma}}{\Gamma, x : A, \Gamma' \vdash^{c_e}_{\sigma} x : A}\,(\mathsf{var})$$

$$\frac{\Gamma, x : A \vdash^{c_e}_{\sigma::(x \mapsto a)} u : B : \kappa}{\Gamma \vdash^{c_e}_{\sigma} \lambda x^A.u : \forall x^A.B}\,(\mathsf{abs})$$

Toward a Pedagogical Calculus of Constructions

Pedagogical Calculus of Constructions ?

$$\frac{\Gamma \overset{c_e}{\underset{\sigma}{\vdash}} u : \forall x^A.B : \mathsf{Prop} \quad \Gamma \overset{c_e}{\underset{\sigma}{\vdash}} v : A \quad \sigma\, \mathsf{mot}^{\mathsf{Prop}}(B[x \leftarrow v])}{\Gamma \overset{c_e}{\underset{\sigma}{\vdash}} u\ v : B[x \leftarrow v]}\ (\mathsf{app}_\star)$$

$$\frac{\Gamma \overset{c_e}{\underset{\sigma}{\vdash}} u : \forall x^A.B : \mathsf{Type} \quad \Gamma \overset{c_e}{\underset{\sigma}{\vdash}} v : A \quad \sigma\, \mathsf{mot}^{B[x \leftarrow v]}(u\ v)}{\Gamma \overset{c_e}{\underset{\sigma}{\vdash}} u\ v : B[x \leftarrow v]}\ (\mathsf{app}_\Box)$$

$$\frac{\Gamma, x : A \overset{c_e}{\underset{\sigma::(x \mapsto a)}{\vdash}} B : \mathsf{Prop} \quad \sigma\, \mathsf{mot}^{\mathsf{Prop}}(\forall x^A.B)}{\Gamma \overset{c_e}{\underset{\sigma}{\vdash}} \forall x^A.B : \mathsf{Prop}}\ (\mathsf{prod}_\star)$$

$$\frac{\Gamma, x : A \overset{c_e}{\underset{\sigma::(x \mapsto a)}{\vdash}} B : \mathsf{Type}}{\Gamma \overset{c_e}{\underset{\sigma}{\vdash}} \forall x^A.B : \mathsf{Type}}\ (\mathsf{prod}_\Box)$$

$$\frac{\Gamma \overset{c_e}{\underset{\sigma}{\vdash}} u : A \quad A \simeq A' \quad \Gamma \overset{c_e}{\underset{\sigma}{\vdash}} A' : \kappa}{\Gamma \overset{c_e}{\underset{\sigma}{\vdash}} u : A'}\ (\mathsf{conv})$$

Conclusion and further work

Contributions

- formal definition of pedagogical sub-system of CC
- examples of pedagogical sub-system of CC (λ_e^2, λ_t^2, λ_p^2, λ_e^ω)
- formalisms with explicit examples
- study of type checking pedagogical calculi
- motivated conjectures : pedagogical higher-order and Calculus of Constructions

Further work

- show the conjectures
- study machine implementation
- extend to stronger systems
- formal verification of Griss' negationless mathematics
- study inconsistency and pedagogy

Certification of Spike proofs

Ideas on an example

Spike specification

function symbols	**axioms**	**symbol precedence**
$0 : nat$ $S : nat \to nat$ $+ : nat\ nat \to nat$	$0 + y = y$ $S(x) + y = S(x + y)$	$0 <_F S <_F +$

Spike proof

$$
\begin{array}{lrl}
 & (\{x + 0 = x\}, & \emptyset) \\
\vdash_{\text{case\_variable}} & (\{\underline{0 + 0} = 0, \underline{S(x') + 0} = S(x')\}, & \emptyset) \\
\vdash_{\text{rewrite}} & (\{0 = 0, \overline{S(x' + 0)} = S(x')\}, & \{x + 0 = x\}) \\
\vdash_{\text{delete}} & (\{S(x' + 0) = S(x')\}, & \{x + 0 = x\}) \\
\vdash_{\text{injection}} & (\{x' + 0 = x'\}, & \{x + 0 = x\}) \\
\vdash_{\text{subsumption}\ x \mapsto x'} & (\emptyset, & \{x + 0 = x\})
\end{array}
$$

Main ideas

- (E_i, H_i) : E_i conjectures to be refuted ; H_i formulas not containing minimal counter-example
- minimal counter-example preserved in succesives E_i
- at the end E_n empty : no counter-example, i.e. formulas of E_0 true

Certification of Spike proofs

Coq implementation

- $\mathcal{F}$, generated formulas with abstract representation :

$$\mathcal{F} = \left\{ \begin{array}{l} \text{fun } x : \text{nat} \Rightarrow (x + 0 = x, \langle [\![x]\!] + 0 = [\![x]\!] \rangle), \\ \text{fun } x : \text{nat} \Rightarrow (S(x) + 0 = S(x), \langle S([\![x]\!]) + 0 = S([\![x]\!]) \rangle), \\ \text{fun } x : \text{nat} \Rightarrow (S(x + 0) = S(x), \langle S([\![x]\!] + 0) = S([\![x]\!]) \rangle) \end{array} \right\}$$

  where $[\![\cdot]\!] : \text{nat} \rightarrow \text{term}$ and $\langle \cdot \rangle$ abstract representation (Coccinelle terms)

- main lemma :

$$\begin{array}{llllll} \forall F \in \mathcal{F} & \forall x & \neg (F\ x)_1 & \rightarrow & & \\ \exists F' \in \mathcal{F} & \exists y & \neg (F'\ y)_1 & \wedge & (F'\ y)_2 \ll (F\ x)_2 & \end{array}$$

  where $(\cdot)_1$ and $(\cdot)_2$ projections, $\ll$ multiset RPO (Coccinelle)

- main theorem :

$$\forall F \in \mathcal{F} \quad \forall x \quad (F\ x)_1$$

  since $\ll$ well-founded order

Certification of Spike proofs

Coq implementation (example)

Main lemma

$$\begin{array}{llllll} \forall F \in \mathcal{F} & \forall x & \neg(F\ x)_1 & \rightarrow & & \\ \exists F' \in \mathcal{F} & \exists y & \neg(F'\ y)_1 & \wedge & (F'\ y)_2 \ll (F\ x)_2 & \end{array}$$

Proof

Case $F \equiv \mathrm{fun}\, x : \mathrm{nat} \Rightarrow (x + 0 = x, \langle [\![x]\!] + 0 = [\![x]\!] \rangle)$.
Assume $x : nat$ and $\neg(F\ x)_1 \equiv \neg(x + 0 = x)$, then by cases on $x : \mathrm{nat}$:

- $x \mapsto 0$:
  $0 + 0 = 0 \overset{\rightsquigarrow}{\equiv} 0 = 0$ true
- $x \mapsto S(x')$:
  $S(x') + 0 = S(x') \overset{\rightsquigarrow}{\equiv} S(x' + 0) = S(x')$
  $F' := \mathrm{fun}\, x : \mathrm{nat} \Rightarrow (S(x) + 0 = S(x), \langle S([\![x]\!]) + 0 = S([\![x]\!]) \rangle)$ and
  $y := x'$ fits :
  $(F'\ y)_2 \equiv \langle S([\![x']\!] + 0) = S([\![x']\!]) \rangle \ll \langle S([\![x']\!]) + 0 = S([\![x']\!]) \rangle \equiv (F\ x)_2$

Certification of Spike proofs

Coq implementation (example)

State of the work

- constructivized : main lemma reformulated
- certification time improved : local reflection, tacticals, parallelisation, etc.
- application to conformance algorithm for ABR protocol : (33/ $\simeq$ 80) lemmas automatically processed
- Coq tactic : call Spike, generate proof script and import it