Investigations on a Pedagogical Calculus of Constructions

Loïc Colson, Vincent Demange

Investigations on a Pedagogical Calculus of Constructions

Loïc Colson
(LITA, University Paul-Verlaine – Metz, France
colson@univ-metz.fr)

Vincent Demange
(LITA, University Paul-Verlaine – Metz, France
demange@univ-metz.fr)

Abstract: In the last few years appeared *pedagogical propositional natural deduction systems*. In these systems, one must satisfy the *pedagogical constraint*: the user must give an *example* of any introduced notion. In formal terms, for instance in the propositional case, the main modification is that we replace the usual rule (hyp) by the rule (p-hyp)

$$\frac{\boldsymbol{F} \in \boldsymbol{\Gamma}}{\boldsymbol{\Gamma} \vdash \boldsymbol{F}}\,(\text{hyp}) \qquad \frac{\boldsymbol{F} \in \boldsymbol{\Gamma} \quad \vdash \boldsymbol{\sigma} \cdot \boldsymbol{\Gamma}}{\boldsymbol{\Gamma} \vdash \boldsymbol{F}}\,(\text{p-hyp})$$

where $\boldsymbol{\sigma}$ denotes a substitution which replaces variables of $\boldsymbol{\Gamma}$ with an example. This substitution $\boldsymbol{\sigma}$ is called the *motivation* of $\boldsymbol{\Gamma}$.

First we expose the reasons of such a constraint and properties of these "pedagogical" calculi: the absence of negation at logical side, and the "usefulness" feature of terms at computational side (through the Curry-Howard correspondence). Then we construct a simple pedagogical restriction of the calculus of constructions (CC) called $\mathrm{CC_r}$. We establish logical limitations of this system, and compare its computational expressiveness to Gödel system T.

Finally, guided by the logical limitations of $\mathrm{CC_r}$, we propose a formal and general definition of what a pedagogical calculus of constructions should be.

Key Words: mathematical logic, negationless mathematics, constructive mathematics, typed lambda-calculus, calculus of constructions, pedagogical system.

Category: F.1.1, F.4.1

1 Introduction and Motivations

1.1 The pedagogical constraint

Recently the articles [Colson and Michel(2007), Colson and Michel(2008), Colson and Michel(2009)] appeared in print, introducing *pedagogical natural deduction systems* and *pedagogical typed λ-calculi*. The main feature about these systems is that any proof (or any program) must satisfy the so named *pedagogical constraint*: in natural deduction systems (for instance) the rule (hyp) is replaced by (p-hyp)

$$\frac{F \in \Gamma}{\Gamma \vdash F}\,(\text{hyp}) \qquad \frac{F \in \Gamma \quad \vdash \sigma \cdot \Gamma}{\Gamma \vdash F}\,(\text{p-hyp})$$

where σ denotes a substitution which replaces propositional variables of Γ with an example, and $\vdash \sigma \cdot \Gamma$ stands for the derivations of those substituted formulas.

The idea of such a constraint is that, in order to assume a set Γ of hypotheses, one must first provide a "motivation" (the substitution σ under consideration) in which the set of hypotheses is fulfilled. In doing so, we can always exemplify introduced hypotheses. This is the formal counterpart of the usual informal teaching practice, consisting in giving examples of objects satisfying the assumed properties. This last point is a justification of the terminology *pedagogical systems*, and the necessity of such a constraint was already observed by [Poincaré(1913)] [see Section 3.1].

1.2 The pedagogical minimal propositional calculus

In [Colson and Michel(2007)], the minimal propositional calculus over $\rightarrow$, $\vee$ and $\wedge$ has been constrained as previously explained. It is shown in the article that the resulting calculus (P-MPC) is equivalent to the original one: a judgment $\Gamma \vdash F$ is derivable in the usual system (MPC) if and only if it is derivable in its pedagogical version (P-MPC).

1.3 The pedagogical second-order propositional calculi

The case of the second-order propositional calculus (Prop^2) is considered in [Colson and Michel(2008)]. Constraining only the rule of hypothesis as above, one is led to a *weakly pedagogical second-order calculus* (P$_s$-Prop^2), where rules dealing with quantification are the usual ones:

$$\frac{\Gamma \vdash F \quad \alpha \notin \mathcal{V}(F)}{\Gamma \vdash \forall \alpha.F}\,(\forall_i) \qquad \frac{\Gamma \vdash \forall \alpha.F}{\Gamma \vdash F[\alpha \leftarrow U]}\,(\forall_e)$$

The same remark as above holds for this calculus, but it is *not stable by normalization* of proofs. Indeed, it is shown that $\bot \rightarrow \bot$ is derivable in P$_s$-Prop^2 (where $\bot$ stands for $\forall \alpha.\alpha$):

$$\begin{array}{ll} 1.\ \beta \vdash \beta & (\beta \text{ is motivable}) \\ 2.\ \vdash \beta \rightarrow \beta & (\rightarrow_i\ 1) \\ 3.\ \vdash \forall \beta.\beta \rightarrow \beta & (\forall_i\ 2) \\ 4.\ \vdash \bot \rightarrow \bot & (\forall_e\ 3) \end{array}$$

But a normal form of this proof must end with a $(\rightarrow_i)$ rule of $\bot$, which is impossible since $\bot$ is not motivable. Hence the normal form of this proof is not a proof of P$_s$-Prop^2.

This motivates the more constrained system P-Prop^2 where the $(\forall_e)$ rule has been replaced by

$$\frac{\Gamma \vdash \forall \alpha.F \quad \vdash \sigma \cdot U}{\Gamma \vdash F[\alpha \leftarrow U]}\,(\text{P-}\forall_e)$$

It is shown about this system that the usual second-order encoding of connectives $\vee$ and $\wedge$ essentially works but it must be observed that the $\vee_i$ (at right for instance) becomes:

$$\frac{\Gamma \vdash A \quad \vdash \sigma \cdot B}{\Gamma \vdash A \vee B}\,(\vee_{ir})$$

The main result concerning P-Prop^2 is that there exists a translation $F \mapsto F^\gamma$ inspired by the A-translation of [Friedman(1978)] such that: $\Gamma \vdash F$ is derivable in Prop^2 if and only if $\Gamma^\gamma \vdash F^\gamma$ is derivable in P-Prop^2.

1.4 The pedagogical second-order λ-calculus

Through the Curry-Howard isomorphism, previous work about second-order propositional calculus is extended in [Colson and Michel(2009)] to the second-order λ-calculus. The system is shown to be stable by reduction (i.e. enjoys the so-called subject reduction property). An important feature for a λ-calculus is defined: the *usefulness* of functions. It means that every typable function in this pedagogical λ-calculus can be applied to a term: if $\vdash f : A \to B$, then there is a substitution σ such that $\sigma \cdot A$ is inhabited. Indeed, pedagogical λ-calculi do not allow one to write useless programs, which are not needed.

1.5 The calculus of constructions

The calculus of constructions (CC) has been first introduced in [Coquand and Huet(1984), Coquand(1985)]: it is a λ-calculus which encompasses higher-order λ-calculi and calculi with dependent types. It is then natural to extend previous works on "pedagogization" to CC in the aim of obtaining a uniform treatment of pedagogical λ-calculi.

1.6 Organization of the article

The paper is organized as follows: in section 2 we recall usual notations for the calculus of constructions (CC); in section 3 we introduce the main criterion for a subsystem of CC to be pedagogical, we discuss about the impossibility of a straightforward modification of CC, and we propose a better one; then in section 4 we show that this restriction meets this criterion; we present some limitations of it at logical and computational side in sections 5 and 6; finally we conclude by the first formal definition of a pedagogical subsystem of CC.

2 Background and Notations

In this section, we briefly recall usual definitions and notations about the calculus of constructions CC.

We try to use $x, y, ..$ as symbols for variables, $u, v, w, t, ..$ to denote terms, and $A, B, ..$ for types and formulas.

$\equiv$ is the syntactical equality of terms [1]. We note by $\rightsquigarrow_\beta$ the usual beta-reduction relation between terms; $\overset{*}{\rightsquigarrow}_\beta$ its reflexive and transitive closure; and $=_\beta$ its equivalence closure. $\mathcal{V}(t)$ is the set of free variables of t. t is said to be closed if $\mathcal{V}(t) = \emptyset$. $t[x \leftarrow u\,]$ is the usual substitution of u for x in t; and $t[x_1, .., x_n \leftarrow u_1, .., u_n\,]$ is the simultaneous substitution of u_1 for x_1, u_2 for x_2, etc. To shorten notations, we use a vector symbolism: $\vec{t}$ denotes the sequence of terms $t_1, .., t_n$; and $\forall \vec{x}^{\vec{A}}.B$ denotes $\forall x_1^{A_1}..\forall x_n^{A_n}.B$.

There are two kinds of judgments: Γ *wf* means that the environment Γ is syntactically well-formed, and $\Gamma \vdash t : A$ expresses that the term t is of type A in the environment Γ. Implicitly $\Gamma \vdash A : \kappa$ signifies that there exists $\kappa \in \{\text{Prop}, \text{Type}\}$ such that this previous statement holds. $\Gamma \vdash t : A : \kappa$ is the contraction of $\Gamma \vdash t : A$ and $\Gamma \vdash A : \kappa$. As usual, $A \to B$ is a shortcut notation for $\forall x^A.B$ when x does not appear in B.

Rules of CC are presented in [Fig. 1]: a close presentation can be found in [Bunder and Seldin(2004)] (without the well-formed judgment), or in [Coquand(1986), Barendregt(1992)].

Beta-reduction is known to be confluent and terms of this calculus to be strongly normalizing [Barendregt(1992)].
In the sequel we shall need the following elementary results (proofs in [Coquand(1985), Barendregt(1992)]):

Lemma 1. *If* Γ wf *holds, then* Type $\notin \Gamma$ *(the constant* Type *never appears in any well-formed environment). And if* $\Gamma \vdash t : A$ *holds, then* Type $\notin \Gamma \cup \{t\}$.

Lemma 2. *If* $\Gamma \vdash t : A$ *holds, then* $A \equiv$ Type *or* $\Gamma \vdash A : \kappa$.

Proposition 3. *(i) If* $\Gamma, x : A, \Gamma'$ wf *and* $\Gamma \vdash u : A$ *hold, then* $\Gamma, \Gamma'[x \leftarrow u\,]$ wf *also holds.*

(ii) If $\Gamma, x : A, \Gamma' \vdash t : B$ *and* $\Gamma \vdash u : A$ *hold, then* $\Gamma, \Gamma'[x \leftarrow u\,] \vdash t[x \leftarrow u\,] : B[x \leftarrow u\,]$ *holds.*

[1] As in [Coquand(1989)], we assume De Bruijn indexes for bound variables and identifiers for free variables. So there is no need for α-conversion notion.

$$\frac{}{[\,]\ wf}\,(\mathrm{env}_1) \qquad \frac{\Gamma \vdash A : \kappa \quad x \notin \mathcal{V}(\Gamma)}{\Gamma, x : A\ wf}\,(\mathrm{env}_2)$$

$$\frac{\Gamma\ wf}{\Gamma \vdash \mathrm{Prop} : \mathrm{Type}}\,(\mathrm{ax}) \qquad \frac{\Gamma, x : A, \Gamma'\ wf}{\Gamma, x : A, \Gamma' \vdash x : A}\,(\mathrm{var})$$

$$\frac{\Gamma, x : A \vdash u : B : \kappa}{\Gamma \vdash \lambda x^A.u : \forall x^A.B}\,(\mathrm{abs}) \qquad \frac{\Gamma, x : A \vdash B : \kappa}{\Gamma \vdash \forall x^A.B : \kappa}\,(\mathrm{prod})$$

$$\frac{\Gamma \vdash u : \forall x^A.B \quad \Gamma \vdash v : A}{\Gamma \vdash u\ v : B[x \leftarrow v\,]}\,(\mathrm{app}) \qquad \frac{\Gamma \vdash t : A \quad \Gamma \vdash A' : \kappa \quad A =_\beta A'}{\Gamma \vdash t : A'}\,(\mathrm{conv})$$

where κ stands for Prop or for Type.

Figure 1: Inference rules of CC

3 Pedagogizing CC

3.1 The Poincaré criterion

Let us recall the necessity of the pedagogical constraint —here in the case of definitions by postulate— by the following quotation:

> *A definition by postulate has value only when the existence of the object defined has been proved. In mathematical language, this means that the postulate does not imply a contradiction, we do not have the right to neglect this condition. Either it is necessary to admit the absence of contradiction as an intuitive truth, as an axiom, by a kind of act of faith —but then it is necessary to realize what we are doing and to remember that we have extended the list of indemonstrable axioms— or else it is necessary to construct a formal proof, either* by means of examples *or by the use of reasoning by recurrence. Not that this proof is less necessary when a direct definition is involved, but it is generally easier.*
>
> Henri Poincaré – Last thoughts [Poincaré(1913)]

In CC, a definition by postulate of an object x may be seen as an environment containing x followed by hypotheses about x. For instance,

Let x be a natural number verifying $P(x)$ and $Q(x)$.

is formally represented in CC by the following environment

$$x : \mathbb{N}, H_1 : P(x), H_2 : Q(x)$$

Poincaré pointed out that such a set of hypotheses is an admissible definition by postulate of x *only if* we are able to exhibit a natural satisfying both predicates P and Q. In other words, types $P(x)$ and $Q(x)$ must be inhabited for a given x (say n) in CC. Namely the following statements must hold:

$$\vdash n : \mathbb{N} \qquad \vdash t_1 : P(n) \qquad \vdash t_2 : Q(n)$$

If this is not possible (i.e. there is no such n, t_1 or t_2) then the definition is meaningless and should be avoided.

Let us generalize to any environment:

Definition 4 (Poincaré criterion). The environment $x_1 : A_1, .., x_n : A_n$ is respectful of the Poincaré criterion *only if* there exists terms $t_1, .., t_n$ such that the following judgments are derivable:

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

A formal system is said to meet the Poincaré criterion *only if* every well-formed environment are respectful of the Poincaré criterion.

3.2 On the naive extension of previous work

In the previous works on pedagogization [see section 1], each environment is motivated before being used. It is then immediate that each used environment can be motivated, hence such a system trivially satisfies the Poincaré criterion. Unfortunately such a simple adjustment can not be performed into CC.

The straightforward extension of the previous work to CC can be summed up by the following changes:

- remove (env_1) and (env_2) rules;
- replace (ax) and (var) rules by these ones:

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

where

– σ is the substitution $[x_1 \mapsto t_1; \ldots; x_n \mapsto t_n]$ when $\Gamma \equiv x_1 : A_1, \ldots, x_n : A_n$, and $\sigma \cdot \Gamma$ denotes the judgments:

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

– o and $\top$ are two added constants in order to be able to begin derivations (like in [Colson and Michel(2009)]).

In this subsection, we refer to this system as P, and index its judgments by p.

P is not a subsystem of CC:

Lemma 5. *The following derivations hold in P but not in CC:*

(a) $x_1 : \text{Type} \vdash_p \text{Prop} : \text{Type}$

(b) $x_1 : \text{Prop}, x_2 : (\lambda H^{\top \to x_1}.\top)\ (\lambda y^{\top}.y) \vdash_p \text{Prop} : \text{Type}$

(c) $x_1 : \mathbb{N}, x_2 : (\lambda H^{x_1 = 0}.\top)\ (\lambda P^{\mathbb{N} \to \text{Prop}}.\lambda H^{P\ 0}.H) \vdash_p \text{Prop} : \text{Type}$

Proof. Proofs that derivations hold in P are trivial as soon as we exhibit a motivation:

(a) $\sigma_1 := [x_1 \mapsto \text{Prop}]$

(b) $\sigma_2 := [x_1 \mapsto \top; x_2 \mapsto o]$

(c) $\sigma_3 := [x_1 \mapsto 0; x_2 \mapsto o]$

And it is easy to see that they are not derivable in CC:

(a) Type appears into an environment, which is forbidden in CC [see lemma 1];

(b) $(\lambda H^{\top \to x_1}.\top)\ (\lambda y^{\top}.y)$ is ill-typed since the function waits for a element of type $\top \to x_1$, but an element of type $\top \to \top$ is given instead;

(c) same reason as for (b): the function waits for a proof of $x_1 = 0$, whereas a proof of $0 = 0$ is passed.

□

Remark. Those examples involve dependent types. It seems that this naive extension can work for λ^{ω} [see [Michel(2008)]].

Remark. The first case can be avoided by enforcing the A_i to be of type Prop or Type in the definition of $\sigma \cdot \Gamma$.

CC has the advantage that well-formed types are built into the system. So we just need to find which rules need to be constrained and how in order to avoid not motivable types (i.e. empty types).

3.3 A simple attempt: $\mathbf{CC_r}$

In CC, we are able to introduce $\bot := \forall A^{\mathrm{Prop}}.A$ as an hypothesis if we have been able to derive $\bot$ as a type, which is allowed by the (prod) rule. Actually, the (prod) rule is the only one able to create vacuity, since other rules construct types and an inhabitant of it simultaneously. We then impose products to always be inhabited by replacing the usual (prod) rule of CC by the following more restrictive one:

$$\frac{\Gamma, x : A \vdash_r \mathbf{t} : B : \kappa}{\Gamma \vdash_r \forall x^A.B : \kappa}\ (\mathrm{prod_r})$$

This rule may be condensed together with (abs) to obtain a rule with two conclusions. So the resulting calculus can be viewed as CC without the (prod) rule.

From now on we will refer to the resulting calculus as $\mathrm{CC_r}$, whose judgments will be indexed by r.

Usual properties of CC from [Coquand(1985)] still hold for this calculus, especially substitution (prop.3 above), weakening and the well-known "subject reduction" (stability by reduction). These were formally checked in the Coq proof assistant by straightforward adaptation of the work in [Barras(1996)].

Example of derivation in $\mathbf{CC_r}$

Lemma 6. *The following rule is derivable:*

$$\frac{\Gamma\ \mathrm{wf_r}}{\Gamma \vdash_r o : \top : \mathrm{Prop}}$$

where $o := \lambda A^{\mathrm{Prop}}.\lambda x^A.x$ *and* $\top := \forall A^{\mathrm{Prop}}.A \to A$.

Proof.

1. Γ *wf*$_r$	(hyp)
2. $\Gamma \vdash_r \mathrm{Prop} : \mathrm{Type}$	(ax 1)
3. $\Gamma, A : \mathrm{Prop}$ *wf*$_r$	(env$_2$ 2)
4. $\Gamma, A : \mathrm{Prop} \vdash_r A : \mathrm{Prop}$	(var 3)
5. $\Gamma, A : \mathrm{Prop}, x : A$ *wf*$_r$	(env$_2$ 4)
6. $\Gamma, A : \mathrm{Prop}, x : A \vdash_r x : A : \mathrm{Prop}$	(var 5)
7. $\Gamma, A : \mathrm{Prop} \vdash_r \lambda x^A.x : A \to A : \mathrm{Prop}$	(abs+prod 6)
8. $\Gamma \vdash_r \lambda A^{\mathrm{Prop}}.\lambda x^A.x : \forall A^{\mathrm{Prop}}.A \to A : \mathrm{Prop}$	(abs+prod 7)

4 $\mathbf{CC_r}$ meets the Poincaré criterion

In this section we show that every type (term of sort Prop or Type) in a well-formed environment of $\mathrm{CC_r}$ is inhabited. A sketch of the proof is: we first notice

that in $\mathrm{CC_r}$ every product is inhabited, then, because each closed type reduces to a product, we can inhabit every type of a well-formed environment (beginning by its leftmost type, which is closed).

Lemma 7. *If $\Gamma \vdash_r \forall x^A.B : T$ holds, then there exists κ and a term t such that $\Gamma \vdash_r t : \forall x^A.B$ and $T =_\beta \kappa$.*

Proof. By induction on the derivation: if the last used rule is (prod) then we build t by (abs) rule, and if it is (conv) then we apply induction hypothesis to get t. □

Lemma 8. *If $\Gamma \vdash_r B : \mathrm{Type}$ holds, then there exists a term t such that $\Gamma \vdash_r t : B$ is derivable.*

Proof. By cases on the last applied rule; (ax) case is dealt with lemma 6; (var), (app) and (conv) cases are eliminated using lemmas 1 and 2; (prod) case is trivial using (abs) rule. □

Indeed, every element of type Type is syntactically of the form $\forall \vec{x}^{\vec{A}}.\,\mathrm{Prop}$, and then trivially inhabited by $\lambda \vec{x}^{\vec{A}}.\top$.

Lemma 9. *If $\Gamma \vdash_r B : \forall \vec{x}^{\vec{A}}.\,\mathrm{Prop}$ holds with B closed, then for all closed terms $w_1, \ldots, w_n$ verifying*

$$\begin{gathered}\Gamma \vdash_r w_1 : A_1 \\ \Gamma \vdash_r w_2 : A_2[x_1 \leftarrow w_1\,] \\ \vdots \\ \Gamma \vdash_r w_n : A_n[x_1, \ldots, x_{n-1} \leftarrow w_1, \ldots, w_{n-1}\,]\end{gathered}$$

there exists a term t such that

$$\Gamma \vdash_r t : B\ \vec{w}$$

Proof. Let us define by $\|t\|$ the length of the longest path of reduction from the term t to its normal form (which exists because terms of $\mathrm{CC_r}$ are strongly normalizing).

We proceed by induction on the lexicographical order of $\|B\ \vec{w}\|$ and the height of the derivation of $\Gamma \vdash_r B : \forall \vec{x}^{\vec{A}}.\,\mathrm{Prop}$.

Let us deal with non-trivial cases (others being mostly eliminated by lemmas 1 and 2):
(abs) If the last rule of the derivation is

$$\frac{\Gamma, x_1 : A_1 \vdash_r u : \forall x_2^{A_2} \ldots \forall x_n^{A_n}.\,\mathrm{Prop} : \mathrm{Type}}{\Gamma \vdash_r \lambda x_1^{A_1}.u : \forall \vec{x}^{\vec{A}}.\,\mathrm{Prop}}$$

Let $\vec{w}$ be the above closed terms.

Substituting v for x_1 in the premise, we obtain (property 3)

$$\Gamma \vdash_r u[x_1 \leftarrow w_1\,] : \forall x_2^{A_2[x_1 \leftarrow w_1\,]} \ldots \forall x_n^{A_n[x_1 \leftarrow w_1\,]}.\,\mathrm{Prop}$$

As $\|u[x_1 \leftarrow w_1\,]\ w_2\ ..\ w_n\| < \|(\lambda x_1^{A_1}.u)\ w_1\ w_2\ ..\ w_n\|$, and $u[x_1 \leftarrow w_1\,]$ is closed (since $\lambda x_1^{A_1}.u$ and w_1 are), we can apply induction hypothesis to built a term t such that $\Gamma \vdash_r t : u[x_1 \leftarrow w_1\,]\ w_2\ ..\ w_n$ from which by (conv) rule we finally get

$$\Gamma \vdash_r t : (\lambda x_1^{A_1}.u)\ \vec{w}$$

(app) If the last rule of the derivation looks like

$$\frac{\Gamma \vdash_r u : \forall y^C.\forall \vec{x}^{\vec{D}}.\,\mathrm{Prop} \quad \Gamma \vdash_r v : C}{\Gamma \vdash_r u\ v : \forall \vec{x}^{\vec{D}[y \leftarrow v\,]}.\,\mathrm{Prop}}$$

where $\vec{A} \equiv \vec{D}[y \leftarrow v\,]$ and $B \equiv u\ v$.

Let $\vec{w}$ be the above terms. Since for every i $x_i \notin \mathcal{V}(v)$, so

$$D_i[y \leftarrow v\,][x_1, .., x_{i-1} \leftarrow w_1, ..w_{i-1}\,] \equiv D_i[y, x_1, .., x_{i-1} \leftarrow v, w_1, ..w_{i-1}\,]$$

Noticing we have $\|u\ v\ \vec{w}\| = \|(u\ v)\ \vec{w}\|$, we can then apply induction hypothesis of the first premise on the terms $v, \vec{w}$ to obtain t such that

$$\Gamma \vdash_r t : (u\ v)\ \vec{w}$$

(conv)

$$\frac{\Gamma \vdash_r B : T \quad \Gamma \vdash_r \forall \vec{x}^{\vec{A}}.\,\mathrm{Prop} : \mathrm{Type} \quad T =_\beta \forall \vec{x}^{\vec{A}}.\,\mathrm{Prop}}{\Gamma \vdash_r B : \forall \vec{x}^{\vec{A}}.\,\mathrm{Prop}}$$

By lemma 2 on $\Gamma \vdash_r B : T$, we have three cases: $T \equiv \mathrm{Type}$, $\Gamma \vdash_r T : \mathrm{Prop}$ or $\Gamma \vdash_r T : \mathrm{Type}$. By confluency, the definition of beta-reduction, the properties of subject reduction and uniqueness of types, only $\Gamma \vdash_r T : \mathrm{Type}$ remains. Hence T must be of the form $\forall \vec{x}^{\vec{C}}.\,\mathrm{Prop}$ where $\vec{A} =_\beta \vec{C}$.

Let $\vec{w}$ be the above terms. In order to apply induction hypothesis on the first premise, it is necessary to show that

$$\begin{gathered}\Gamma \vdash_r w_1 : C_1 \\ \Gamma \vdash_r w_2 : C_2[x_1 \leftarrow w_1\,] \\ \vdots \\ \Gamma \vdash_r w_n : C_n[x_1, \ldots, x_{n-1} \leftarrow w_1, \ldots, w_{n-1}\,]\end{gathered}$$

First let us notice that since $\vec{A} =_\beta \vec{C}$, then for each i $A_i[x_1, .., x_{i-1} \leftarrow v_1, .., v_{i-1}\,]$ is convertible with $C_i[x_1, .., x_{i-1} \leftarrow v_1, .., v_{i-1}\,]$. Also, because $\Gamma \vdash_r \forall \vec{x}^{\vec{C}}.\,\mathrm{Prop} :$

Type, for each i there exists κ such that $\Gamma, x_1 : C_1, .., x_i : C_i \vdash_r C_{i+1} : \kappa$.
We can then proceed by induction on n:

$$
\begin{array}{ll}
1.\ \Gamma \vdash_r w_1 : A_1 & \text{(hyp)} \\
2.\ \Gamma \vdash_r C_1 : \kappa & \\
3.\ A_1 =_\beta C_1 & \\
4.\ \Gamma \vdash_{\mathbf{r}} \mathbf{w_1} : \mathbf{C_1} & \text{(conv 1 2 3)} \\
5.\ \Gamma \vdash_r w_2 : A_2[x_1 \leftarrow w_1\,] & \text{(hyp)} \\
6.\ \Gamma, x_1 : C_1 \vdash_r C_2 : \kappa & \\
7.\ \Gamma \vdash_r C_2[x_1 \leftarrow w_1\,] : \kappa & \text{(prop.3 4 6)} \\
8.\ A_2[x_1 \leftarrow w_1\,] =_\beta C_2[x_1 \leftarrow w_1\,] & \\
9.\ \Gamma \vdash_{\mathbf{r}} \mathbf{w_2} : \mathbf{C_2}[\mathbf{x_1} \leftarrow \mathbf{w_1}\,] & \text{(conv 5 7 8)} \\
\quad \vdots &
\end{array}
$$

Finally, we apply induction hypothesis of the first premise on those now well-typed $\vec{w}$ to get a term t satisfying

$$\Gamma \vdash_r t : B\ \vec{w}$$

□

The two previous lemmas can be summed up by the following statement:

Corollary 10. *If $\Gamma \vdash_r B : \kappa$ holds with B closed, then there exists a term t such that $\Gamma \vdash_r t : B$.*

So the pedagogical character of the calculus follows, every type of a well-formed environment is inhabited:

Theorem 11 (Poincaré criterion). *If $x_1 : A_1, \ldots, x_n : A_n$ $\mathrm{wf_r}$ holds, then there exists terms $t_1, \ldots, t_n$ such that*

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

Proof. By induction on the size of the environment n.

From the derivation $x_1 : A_1, \ldots, x_n : A_n$ wf_r, we have $\vdash_r A_1 : \kappa$ as a sub-derivation where A_1 is closed. So by corollary 10, we get t_1 such that

$$\vdash_r t_1 : A_1$$

Then by property 3 we have $x_2 : A_2[x_1 \leftarrow t_1\,], \ldots, x_n : A_n[x_1 \leftarrow t_1\,]$ wf_r. By the same way, we construct t_2 such that

$$\vdash_r t_2 : A_2[x_1 \leftarrow t_1\,]$$

and then $x_3 : A_3[x_1, x_2 \leftarrow t_1, t_2\,], \ldots, x_n : A_n[x_1, x_2 \leftarrow t_1, t_2\,]$ wf_r.

$$\vdots$$

□

This so named "motivation" may be transmitted to the conclusion of judgments:

Corollary 12. *If $x_1 : A_1, \ldots, x_n : A_n \vdash_r u : B$ holds, then there exists terms $t_1, \ldots, t_n$ such that*

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

and

$$\vdash_r u[\vec{x} \leftarrow \vec{t}\,] : B[\vec{x} \leftarrow \vec{t}\,]$$

Proof. Immediate by applying n times the property 3 using the terms obtained from the theorem. □

Theorem 13 (usefulness). *If $\vdash_r f : \forall x^A.B$ holds, then there exists a term u such that $\vdash_r u : A$.*

Proof. From $\vdash_r f : \forall x^A.B$, by lemma 2 we have $\vdash_r \forall x^A.B : \kappa$, then $x : A \vdash_r B : \kappa$ which implies that $x : A$ wf, and finally by theorem 11 we construct u. □

5 Limitations of the logical power of $\mathbf{CC_r}$

To introduce an hypothesis (which is not a variable) in an environment, it is necessary to first inhabit it. For instance, defining Leibniz equality over a type A by

$$x =_A y := \forall Q^{A \to \mathrm{Prop}}.Q\ x \to Q\ y$$

it is not possible to prove nor symmetry nor transitivity of this relation over A (whatever this type is). Indeed, because we are not permitted to derive $A : \mathrm{Prop}, x : A, y : A \vdash_r x =_A y : \mathrm{Prop}$, we can not introduce $x =_A y$ as an hypothesis and then we are not allowed to use it.

Theorem 14. *There is no term u such that $\vdash_r u : \forall A^{\mathrm{Prop}}.\forall x^A.\forall y^A.x =_A y \to y =_A x$ holds.*

Proof. Let us suppose such a term u exists. So we have a sort κ such that $A : \mathrm{Prop}, x : A, y : A \vdash_r x =_A y : \kappa$. And because $x =_A y$ is a product, by lemma 7, it is inhabited, say by t. But since $\mathrm{CC_r}$ is a restriction of CC, $A : \mathrm{Prop}, x : A, y : A \vdash t : x =_A y$ also holds in CC. Then, applying it to $\mathbb{N}$ and 0 and 1, we get a proof of $0 = 1$ in the empty environment in CC, which is known to be impossible (by a simple combinatoric discussion about the normal form of such a term). □

In fact, this calculus does not even natively contain simply typed λ-calculus:

Theorem 15. *There is no term u such that*

$$A\ B\ C : \mathrm{Prop} \vdash_r u : (A \to B) \to (B \to C) \to (A \to C)$$

holds.

Proof. Using same arguments as above, if such a u exists, then the following judgment holds:

$$A : \mathrm{Prop}, B : \mathrm{Prop}, C : \mathrm{Prop} \vdash_r A \to B : \mathrm{Prop}$$

so there is an inhabitant t of the product type $A \to B$ in $\mathrm{CC_r}$ and hence in CC, implying by (abs) rule that

$$\vdash \lambda ABC^{\mathrm{Prop}}.t : \forall ABC^{\mathrm{Prop}}.A \to B$$

which can be specialized to $\top$ and $\bot$ to obtain a proof of $\top \to \bot$ and finally a proof of $\bot$ in the empty environment, which is impossible since CC is consistent. □

Actually, every instances of the types in $\mathrm{CC_r}$ must be inhabited:

Theorem 16. *If $x_1 : A_1, .., x_n : A_n \vdash_r B : \kappa$ holds, then for all terms $w_1, \ldots, w_n$ such that*

$$\begin{gathered} \vdash_r w_1 : A_1 \\ \vdash_r w_2 : A_2[x_1 \leftarrow w_1\,] \\ \vdots \\ \vdash_r w_n : A_n[x_1, \ldots, x_{n-1} \leftarrow w_1, \ldots, w_{n-1}\,] \end{gathered}$$

there exists a term t such that

$$\vdash_r t : B[\vec{x} \leftarrow \vec{w}\,]$$

Proof. The proof is trivial by applying n times the substitution property 3, obtaining $\vdash_r B[\vec{x} \leftarrow \vec{w}\,] : \kappa$, inhabited by corollary 10. □

It is hard to precisely determine the logical expressiveness of $\mathrm{CC_r}$. We have at least simply typed λ-calculus on closed (and then inhabited) types of $\mathrm{CC_r}$ (e.g. $\top$, $\mathbb{N}$, etc.). The proof is the same as the one of lemma 21 below.

6 Computational expressivity of $\mathrm{CC_r}$

Although the logical strength of $\mathrm{CC_r}$ seems quite poor, its computational power is at least that of the Gödel system T. We use the usual well-known way to define terms, types (except cartesian product), and recursor (from iterator) of system T in lambda-calculus (see [Girard et al.(1990)]).

Definition 17.

$$\begin{aligned} \mathbb{N} &:= \forall A^{\mathrm{Prop}}.A \to (A \to A) \to A \\ 0 &:= \lambda A^{\mathrm{Prop}}.\lambda x^{A}.\lambda f^{A\to A}.x \\ S(n) &:= \lambda A^{\mathrm{Prop}}.\lambda x^{A}.\lambda f^{A\to A}.f\ (n\ A\ x\ f) \\ it_T(n,b,(y^T)step) &:= n\ T\ b\ (\lambda y^T.step) \end{aligned}$$

Lemma 18. *The following rules are derivable:*

$$\frac{\Gamma\ \mathrm{wf_r}}{\Gamma \vdash_r 0 : \mathbb{N} : \mathrm{Prop}} \qquad \frac{\Gamma \vdash_r n : \mathbb{N}}{\Gamma \vdash_r S(n) : \mathbb{N}}$$

$$\frac{\Gamma \vdash_r T : \mathrm{Prop} \quad \Gamma \vdash_r n : \mathbb{N} \quad \Gamma \vdash_r b : T \quad \Gamma, y : T \vdash_r step : T}{\Gamma \vdash_r it_T(n,b,(y^T)step) : T}$$

Lemma 19. *The following reductions hold:*

$$\begin{aligned} it_T(0,b,(y^T)step) &\overset{*}{\rightsquigarrow}_\beta b \\ it_T(S(n),b,(y^T)step) &\overset{*}{\rightsquigarrow}_\beta step[y \leftarrow it_T(n,b,(y^T)step)\,] \end{aligned}$$

Definition 20 (simple types on $\mathbb{N}$). Simple types on $\mathbb{N}$ are those obtained from $\mathbb{N}$ and $\to$.

Lemma 21. *If Γ $\mathrm{wf_r}$ holds and T is a simple type on $\mathbb{N}$, then there exists a term t such that $\Gamma \vdash_r t : T : \mathrm{Prop}$.*

Proof. By induction on T (as a simple type on $\mathbb{N}$):

- If T is $\mathbb{N}$, then 0 fits.
- If T is $A \to B$ where A and B are simple types on $\mathbb{N}$, then by induction hypothesis on A, we get $\Gamma \vdash_r A : \mathrm{Prop}$ and by (env_2) rule we obtain $\Gamma, x : A\ wf_r$. By induction hypothesis on B, we get $\Gamma \vdash_r b : B : \mathrm{Prop}$, and weakening it we have $\Gamma, x : A \vdash_r b : B : \mathrm{Prop}$, and finally, by (abs) and (prod) rules, $\Gamma \vdash_r \lambda x^A.b : A \to B : \mathrm{Prop}$.

□

$\mathrm{CC_r}$ does not allow us to derive the usual cartesian product defined by $A \times B := \forall C^{\mathrm{Prop}}.(A \to B \to C) \to C$. To simulate recursor from iterator, we define a restricted cartesian product $\mathbb{N} \times T$ for each T, simple type on $\mathbb{N}$, by encoding a natural into T.

Lemma 22. *If Γ $\mathrm{wf_r}$ holds and T is a simple type on $\mathbb{N}$ then there exists two terms enc_T and dec_T such that $\Gamma \vdash_r enc_T : \mathbb{N} \to T$ and $\Gamma \vdash_r dec_T : T \to \mathbb{N}$ and for every term n we have $dec_T(enc_T\ n) \overset{*}{\rightsquigarrow}_\beta n$.*

Proof. By induction on T (as a simple type on $\mathbb{N}$):

- If T is $\mathbb{N}$, then we take the identity on $\mathbb{N}$ for enc_T and dec_T.
- If T is $A \to B$, we take

$$\begin{aligned} enc_{A\to B} &:= \lambda x^{\mathbb{N}}.\lambda z^{A}.enc_B\ x \\ dec_{A\to B} &:= \lambda f^{A\to B}.dec_B\ (f\ a) \end{aligned}$$

  where a is a term of type A obtained from lemma 21.

□

Definition 23. We define the following abbreviations for couples

$$\begin{aligned} \mathbb{N} \times T &:= (T \to T \to T) \to T \\ \langle n, t\rangle^T &:= \lambda f^{T\to T\to T}.f\ (enc_T\ n)\ t \\ \pi_1(c) &:= dec_T\ (c\ (\lambda x^T.\lambda y^T.x)) \\ \pi_2(c) &:= c\ (\lambda x^T.\lambda y^T.y) \end{aligned}$$

Lemma 24. *The following rules are derivable:*

$$\frac{\Gamma\ \mathrm{wf_r}}{\Gamma \vdash_r \mathbb{N} \times T : \mathrm{Prop}} \qquad \frac{\Gamma \vdash_r n : \mathbb{N} \quad \Gamma \vdash_r t : T}{\Gamma \vdash_r \langle n, t\rangle^T : \mathbb{N} \times T}$$

$$\frac{\Gamma \vdash_r c : \mathbb{N} \times T}{\Gamma \vdash_r \pi_1(c) : \mathbb{N}} \qquad \frac{\Gamma \vdash_r c : \mathbb{N} \times T}{\Gamma \vdash_r \pi_2(c) : T}$$

Lemma 25. *The following reductions hold:*

$$\begin{aligned} \pi_1(\langle n, t\rangle^T) &\overset{*}{\rightsquigarrow}_\beta n \\ \pi_2(\langle n, t\rangle^T) &\overset{*}{\rightsquigarrow}_\beta t \end{aligned}$$

Definition 26. We define recursor from iterator by

$$rec_T(n, b, (x^{\mathbb{N}}, y^T)step) := \pi_2\left[it_{T\times T}(n, \langle 0, b\rangle^T, (z^{T\times T})step')\right]$$

where

$$step' := \langle S(\pi_1(z)), step[x, y \leftarrow \pi_1(z), \pi_2(z)\,]\rangle^{T\times T}$$

Lemma 27. *The following rule is derivable:*

$$\frac{\Gamma \vdash_r T : \mathrm{Prop} \quad \Gamma \vdash_r n : \mathbb{N} \quad \Gamma \vdash_r b : T \quad \Gamma, x : \mathbb{N}, y : T \vdash_r step : T}{\Gamma \vdash_r rec_T(n, b, (x^{\mathbb{N}}, y^T)step) : T}$$

Lemma 28. *The following reductions hold:*

$$\begin{aligned} rec_T(0, b, (x^{\mathbb{N}}, y^T)step) &\overset{*}{\rightsquigarrow}_\beta b \\ rec_T(S(n), b, (x^{\mathbb{N}}, y^T)step) &\overset{*}{\rightsquigarrow}_\beta step[x, y \leftarrow n, rec_T(n, b, (x^{\mathbb{N}}, y^T)step)\,] \end{aligned}$$

7 Conclusions and direction for further work

We have seen a simple attempt to pedagogize the calculus of constructions. It has a good computational power —at least Gödel system T— but lacks of logical expressivity —does not even natively contain simply typed λ-calculus. A pleasant aspect is the simplicity of the added constraint, which also emphasizes that the (prod) rule is responsible for vacuity in CC.

Logical limitations of our calculus $\mathrm{CC_r}$ suggest a more precise definition for a calculus of constructions to be pedagogical: in a pedagogical calculus, we should be able to prove the symmetry of the Leibniz equality, because the non-emptiness of $x =_A y$ can be justified by substituting $\mathbb{N}$ to A and 0 to x and y. It means that we not only need that a well-formed environment guarantees the non-emptiness of its types by exhibiting an example, but the converse should hold too.

But as it was already pointed out in section 3.2, the direct converse statement of the Poincaré criterion is not suitable. We then propose the following definition of a pedagogical subsystem of CC (whose judgments are indexed by p):

Definition 29 (pedagogical subsystem of CC).
P is a pedagogical subsystem of CC if:

1. $x_1 : A_1, \ldots, x_n : A_n$ wf_p holds **if and only if**
   (a) $x_1 : A_1, \ldots, x_n : A_n$ wf holds in CC,
   (b) and there exist terms $t_1, \ldots, t_n$ such that

$$\begin{array}{c} \vdash_p t_1 : A_1 : \kappa_1 \\ \vdash_p t_2 : A_2[x_1 \leftarrow t_1\,] : \kappa_2 \\ \vdots \\ \vdash_p t_n : A_n[x_1, \ldots, x_{n-1} \leftarrow t_1, \ldots, t_{n-1}\,] : \kappa_n \end{array}$$

2. the system is stable by reduction, namely if $\Gamma \vdash_p u : B$ and $u \rightsquigarrow_\beta u'$, then $\Gamma \vdash_p u' : B$.

Remark. 1. The left to right side of the equivalence is already known as "the Poincaré criterion", and enforces P to be a subsystem of CC. The right to left side should then be named "the converse of the Poincaré criterion".

2. The subject reduction must be explicitly stated here since [Colson and Michel(2008)] defined a "simple pedagogical second-order propositional calculus ($\mathrm{P_s}$-$\mathrm{Prop_2}$)" verifying 1 but not 2.

One can show, keeping only the rules of CC necessary to define second order λ-calculus and adding constraints of the pedagogical second order λ-calculus of [Colson and Michel(2009)], that we obtain a calculus which is pedagogical in the new sense just defined. For instance, P-MPC et P-Prop^2 [see section 1] satisfy: it exists F such that $\Gamma \vdash F$ *if and only if* it exists σ such that $\vdash \sigma \cdot \Gamma$.

By the same way, we can construct more expressive pedagogical restrictions of CC: a hint is given by [Michel(2008)] where he studies pedagogical propositional higher order systems. It thus raises the question of formally characterizing a maximally expressive pedagogical restriction of CC.

References

[Barendregt(1992)] Barendregt, H.: Lambda calculi with types; volume 2 of Handbook of Logic in Computer Science; 117–309; Oxford University Press, 1992.

[Barras(1996)] Barras, B.: "Coq en coq"; Rapport de Recherche 3026; INRIA (1996).

[Bunder and Seldin(2004)] Bunder, M., Seldin, J. P.: "Variants of the Basic Calculus of Constructions"; Journal of Applied Logic; 2 (2004), 2, 191–217.

[Colson and Michel(2007)] Colson, L., Michel, D.: "Pedagogical natural deduction systems: the propositional case"; J.UCS; 13 (2007), 10, 1396–1410.

[Colson and Michel(2008)] Colson, L., Michel, D.: "Pedagogical Second-order Propositional Calculi"; Journal of Logic and Computation; 18 (2008), 4, 669–695.

[Colson and Michel(2009)] Colson, L., Michel, D.: "Pedagogical second-order λ-calculus"; Theoretical Computer Science; 410 (2009), 4190–4203.

[Coquand(1985)] Coquand, T.: Une théorie des constructions; Ph.D. thesis; Université Paris VII (1985).

[Coquand(1986)] Coquand, T.: "An analysis of Girard's paradox"; Technical Report 531; INRIA (1986).

[Coquand(1989)] Coquand, T.: "Metamathematical investigations of a calculus of constructions"; Technical Report 1088; INRIA (1989).

[Coquand and Huet(1984)] Coquand, T., Huet, G.: "A Theory of Constructions"; International Symposium on Semantics of Data Types; Sophia-Antipolis, 1984.

[Friedman(1978)] Friedman, H.: "Classically and intuitionistically provably recursive functions"; Springer, ed., Higher Set Theory; volume 669; 21–27; 1978.

[Gilmore(1953)] Gilmore, P.: "The effect of Griss' criticism of the intuitionistic logic on deductive theories formalized within the intuitionistic logic"; Indagationes Mathematicæ; 15 (1953), 162–174, 175–186.

[Girard et al.(1990)] Girard, J.-Y., Taylor, P., Lafont, Y.: Proofs and types; Cambridge University Press, 1990.

[Griss(1946)] Griss, G.: "Negationless intuitionistic mathematics"; Indagationes Mathematicæ; 8 (1946), 675–681.

[Griss(1950)] Griss, G.: "Negationless intuitionistic mathematics II"; Indagationes Mathematicæ; 12 (1950), 108–115.

[Griss(1951a)] Griss, G.: "Negationless intuitionistic mathematics III"; Indagationes Mathematicæ; 13 (1951a), 193–199.

[Griss(1951b)] Griss, G.: "Negationless intuitionistic mathematics IVa, IVb"; Indagationes Mathematicæ; 13 (1951b), 452–462,463–471.

[Krivtsov(2000a)] Krivtsov, V. N.: "A Negationless Interpretation of Intuitionistic Theories. I"; Studia Logica; 64 (2000a), 3, 323–344.

[Krivtsov(2000b)] Krivtsov, V. N.: "A Negationless Interpretation of Intuitionistic Theories. II"; Studia Logica; 65 (2000b), 2, 155–179.

[Mezhlumbekova(1975)] Mezhlumbekova, V.: "Deductive capabilities of negationless intuitionistic arithmetic"; Moscow University Mathematical Bulletin; 30 (1975), 2.
[Michel(2008)] Michel, D.: Systèmes formels et systèmes fonctionnels pédagogiques; Ph.D. thesis; Université Paul-Verlaine – Metz (2008).
[Nelson(1966)] Nelson, D.: "Non-Null Implication"; The Journal of Symbolic Logic; 31 (1966), 4, 562–572.
[Nelson(1973)] Nelson, D.: "A complete negationless system"; Studia Logica; 32 (1973), 41–49.
[Poincaré(1913)] Poincaré, H.: Dernières pensées; Flammarion, 1913.
[Valpola(1955)] Valpola, V.: "Ein system der negationlosen Logik mit ausschliesslich realisierbaren Prädicaten"; Acta Philosophica Fennica; 9 (1955), 1–247.
[Vredenduin(1953)] Vredenduin, P.: "The logic of negationless mathematics"; Compositio Mathematica; 11 (1953), 204–277.