Proof Assistants for Free*

**Rates may apply*

Pierre-Marie Pédrot

Max Planck Institute for Software Systems

EUTypes 2018

24th January 2018

CIC: « Constructions dans un monde qui bouge »

CIC, the Calculus of Inductive Constructions.

CIC: « Constructions dans un monde qui bouge »

CIC, the Calculus of Inductive Constructions.

CIC, a very fancy **intuitionistic** **logical system**.

- Not just higher-order logic, not just first-order logic
- First class notion of computation and crazy inductive types

CIC, the Calculus of Inductive Constructions.

CIC, a very fancy **intuitionistic** **logical system**.

- Not just higher-order logic, not just first-order logic
- First class notion of computation and crazy inductive types

CIC, a very powerful **functional** **programming language**.

- Finest types to describe your programs
- No clear phase separation between runtime and compile time

CIC: « Constructions dans un monde qui bouge »

CIC, the Calculus of Inductive Constructions.

CIC, a very fancy **intuitionistic** **logical system**.

- Not just higher-order logic, not just first-order logic
- First class notion of computation and crazy inductive types

CIC, a very powerful **functional** **programming language**.

- Finest types to describe your programs
- No clear phase separation between runtime and compile time

The Pinnacle of the Curry-Howard correspondence

An Effective Object

One implementation to rule them all...

An Effective Object

One implementation to rule them all...

An Effective Object

One implementation to rule them all...

Many big developments using it for computer-checked proofs.

- Mathematics: Four colour theorem, Feit-Thompson, Unimath...
- Computer Science: CompCert, VST, RustBelt...

The CIC Tribe

Actually not quite one single theory.

Several flags tweaking the kernel:

- Impredicative Set
- Type-in-type
- Indices Matter
- Cumulative inductive types
- ...

The CIC Tribe

Actually not quite one single theory.

Several flags tweaking the kernel:

- Impredicative Set
- Type-in-type
- Indices Matter
- Cumulative inductive types
- ...

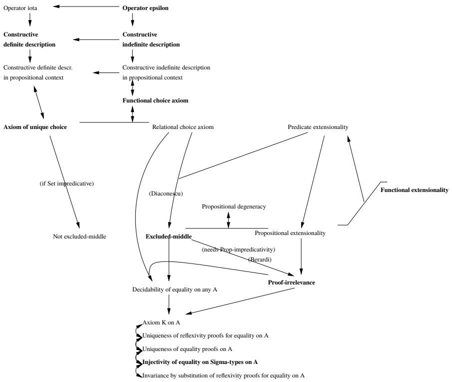
The Many Calculi of Inductive Constructions.

A crazy amount of axioms used in the wild!

A crazy amount of axioms used in the wild!

The *classical set-theory* pole:

- Excluded middle, UIP, choice



A crazy amount of axioms used in the wild!

The claſſical ſet-theory pole:

- Excluded middle, UIP, choice

The EXTENSIONAL pole:

- Funext, Propext, Bisim-is-eq

A crazy amount of axioms used in the wild!

The classical set-theory pole:

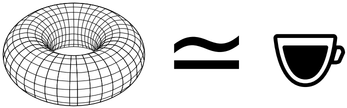
- Excluded middle, UIP, choice

The EXTENSIONAL pole:

- Funext, Propext, Bisim-is-eq

The univalent pole:

- Univalence, what else?



« A mathematician is a device for turning toruses into equalities (up to homotopy). »

A crazy amount of axioms used in the wild!

The claſſical ſet-theory pole:

- Excluded middle, UIP, choice

The EXTENSIONAL pole:

- Funext, Propext, Bisim-is-eq

The univalent pole:

- Univalence, what else?

The $\varepsilon\chi o\tau\iota c$ pole:

- Anti-classical axioms (???)

In the Axiom Jungle

A crazy amount of axioms used in the wild!

The claſſical ſet-theory pole:

- Excluded middle, UIP, choice

The Extensional pole:

- Funext, Propext, Bisim-is-eq

The univalent pole:

- Univalence, what else?

The $\varepsilon\chi o\tau\iota c$ pole:

- Anti-classical axioms (???)

Varying degrees of compatibility.

Reality Check

Theorem 0

Axioms Suck.

Reality Check

Theorem 0

Axioms Suck.

Proof.

- They break computation (and thus canonicity).
- They are hard to justify.
- They might be incompatible with one another.

□

Look ma, no Axioms

Alternative route to axioms: **implement** a new type theory.

Examples: Cubical, F*...

Look ma, no Axioms

Alternative route to axioms: **implement** a new type theory.

Examples: Cubical, F*...

Pro

- Computational by construction (hopefully)
- Tailored for a specific theory

Look ma, no Axioms

Alternative route to axioms: **implement** a new type theory.

Examples: Cubical, F*...

Pro

- Computational by construction (hopefully)
- Tailored for a specific theory

Con

- Requires a new proof of soundness (... *cough*... right, F*? *cough*...)
- Implementation task may be daunting (including bugs)
- Yet-another-language: say farewell to libraries, tools, community...

Summary of the Problem

Different users have different needs.

« From each according to his ability, to each according to his needs. »

(Excessive) Fragmentation of proof assistants is harmful.

« Divide et impera. »

Summary of the Problem

Different users have different needs.

« From each according to his ability, to each according to his needs. »

(Excessive) Fragmentation of proof assistants is harmful.

« Divide et impera. »

Are we thus doomed?

Teasing

In this talk, I'd like to advocate for a third way.

One implementation to rule them all...

In this talk, I'd like to advocate for a third way.

~~One imple[illegible]e them all...~~

Teasing

In this talk, I'd like to advocate for a third way.

~~One implementation to rule them all...~~

One **backend** implementation to rule them all!

Teasing

In this talk, I'd like to advocate for a third way.

~~One impleme[illegible] them all...~~

One **backend** implementation to rule them all!

via

Syntactic Models

Outrageously Gratuitous Ranting

Semantics of type theory have a fame of being horribly complex.

Outrageously Gratuitous Ranting

Semantics of type theory have a fame of being horribly complex.

I won't lie: **it is**. But part of this fame is due to its usual models.

Outrageously Gratuitous Ranting

Semantics of type theory have a fame of being horribly complex.

I won't lie: **it is**. But part of this fame is due to its usual models.

Set-theoretical models: because Sets are a (crappy) type theory.

- **Pro:** Sets!
- **Con:** Sets!

Outrageously Gratuitous Ranting

Semantics of type theory have a fame of being horribly complex.

I won't lie: **it is**. But part of this fame is due to its usual models.

Set-theoretical models: because Sets are a (crappy) type theory.

- **Pro:** Sets!
- **Con:** Sets!

Realizability models: construct programs that respect properties.

- **Pro:** Computational, computer-science friendly.
- **Con:** Not foundational (requires an alien meta-theory), not decidable.

Outrageously Gratuitous Ranting

Semantics of type theory have a fame of being horribly complex.

I won't lie: **it is**. But part of this fame is due to its usual models.

Set-theoretical models: because Sets are a (crappy) type theory.

- **Pro:** Sets!
- **Con:** Sets!

Realizability models: construct programs that respect properties.

- **Pro:** Computational, computer-science friendly.
- **Con:** Not foundational (requires an alien meta-theory), not decidable.

Categorical models: abstract description of type theory.

- **Pro:** Abstract, subsumes the two former ones.
- **Con:** Realizability + very low level, gazillion variants, intrisically typed, static.

Curry-Howard Orthodoxy

Instead, let's look at what Curry-Howard provides in simpler settings.

Program Translations $\Leftrightarrow$ Logical Interpretations

Curry-Howard Orthodoxy

Instead, let's look at what Curry-Howard provides in simpler settings.

Program Translations $\Leftrightarrow$ Logical Interpretations

On the **programming** side, enrich the language by program translation.

- Monadic style à la Haskell
- Compilation of higher-level constructs down to assembly

Curry-Howard Orthodoxy

Instead, let's look at what Curry-Howard provides in simpler settings.

Program Translations $\Leftrightarrow$ Logical Interpretations

On the **programming** side, enrich the language by program translation.

- Monadic style à la Haskell
- Compilation of higher-level constructs down to assembly

On the **logic** side, extend expressivity through proof interpretation.

- Double-negation $\Rightarrow$ classical logic (`callcc`)
- Friedman's trick $\Rightarrow$ Markov's rule (exceptions)
- Forcing $\Rightarrow$ $\neg\mathrm{CH}$ (global monotonous cell)

Syntactic Models

Let us do the same thing with CIC: build **syntactic models**.

Let us do the same thing with CIC: build **syntactic models**.

We take the following act of faith for granted.

CIC is.

Let us do the same thing with CIC: build **syntactic models**.

We take the following act of faith for granted.

CIC is.

Not caring for its soundness, implementation, whatever. It just is.

Do everything by interpreting the new theories relatively to this foundation!

Suppress technical and cognitive burden by lowering impedance mismatch.

Syntactic Models II

Step 0: Fix a theory $\mathcal{T}$ as close as possible* to CIC, ideally $\mathrm{CIC} \subseteq \mathcal{T}$.

Syntactic Models II

Step 0: Fix a theory $\mathcal{T}$ as close as possible* to CIC, ideally $\mathrm{CIC} \subseteq \mathcal{T}$.

Step 1: Define $[\cdot]$ on the syntax of $\mathcal{T}$ and derive $[\![\cdot]\!]$ from it s.t.

$$\vdash_{\mathcal{T}} M : A \qquad \text{implies} \qquad \vdash_{\mathrm{CIC}} [M] : [\![A]\!]$$

Step 0: Fix a theory $\mathcal{T}$ as close as possible* to CIC, ideally $\mathrm{CIC} \subseteq \mathcal{T}$.

Step 1: Define $[\cdot]$ on the syntax of $\mathcal{T}$ and derive $[\![\cdot]\!]$ from it s.t.

$$\vdash_{\mathcal{T}} M : A \qquad \text{implies} \qquad \vdash_{\mathrm{CIC}} [M] : [\![A]\!]$$

Step 2: Flip views and actually pose

$$\vdash_{\mathcal{T}} M : A \qquad \triangleq \qquad \vdash_{\mathrm{CIC}} [M] : [\![A]\!]$$

Syntactic Models II

Step 0: Fix a theory $\mathcal{T}$ as close as possible* to CIC, ideally $\mathrm{CIC} \subseteq \mathcal{T}$.

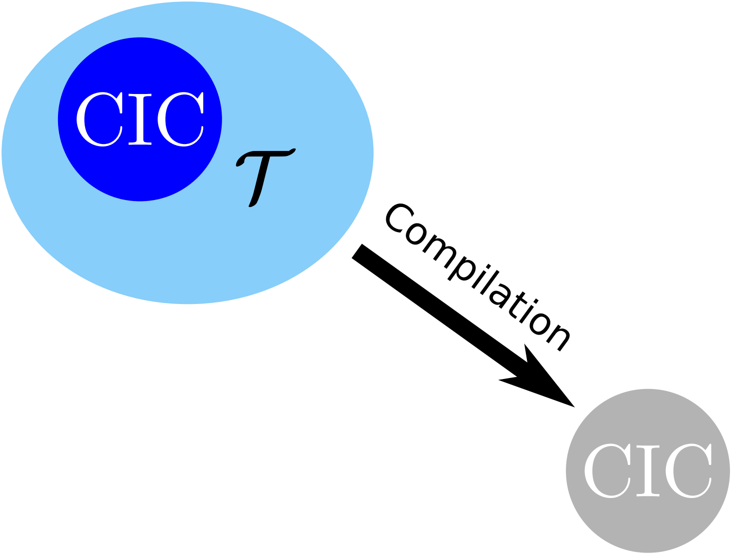
Step 1: Define $[\cdot]$ on the syntax of $\mathcal{T}$ and derive $[\![\cdot]\!]$ from it s.t.

$$\vdash_{\mathcal{T}} M : A \qquad \text{implies} \qquad \vdash_{\mathrm{CIC}} [M] : [\![A]\!]$$

Step 2: Flip views and actually pose

$$\vdash_{\mathcal{T}} M : A \qquad \triangleq \qquad \vdash_{\mathrm{CIC}} [M] : [\![A]\!]$$

Step 3: Expand $\mathcal{T}$ by going down to the *CIC assembly language*, implementing new terms given by the $[\cdot]$ translation.



« CIC, the LLVM of Type Theory »

Syntactic Models III

Obviously, that's subtle.

- The translation $[\cdot]$ must preserve typing (not easy)
- In particular, it must preserve conversion (even worse)

Syntactic Models III

Obviously, that's subtle.

- The translation $[\cdot]$ must preserve typing (not easy)
- In particular, it must preserve conversion (even worse)

Yet, a lot of nice consequences.

- Does not require non-type-theoretical foundations (*monism*)
- **Can be implemented in Coq** (*software monism*)
- Easy to show (relative) consistency, look at $[\![\texttt{False}]\!]$
- Inherit properties from CIC: computationality, decidability...

In Practice: Aknowledge the Existing

In Coq, first require the plugin implementing the desired model.

```
Require Import ExtendCoq.
```

In Practice: Aknowledge the Existing

In Coq, first require the plugin implementing the desired model.

```
Require Import ExtendCoq.
```

Soundness means that any Coq proof can be translated automatically.

```
ExtendCoq Translate cool_theorem.
```

In Practice: Aknowledge the Existing

In Coq, first require the plugin implementing the desired model.

```
Require Import ExtendCoq.
```

Soundness means that any Coq proof can be translated automatically.

```
ExtendCoq Translate cool_theorem.
```

Assuming `cool_theorem` : T, this command:

- defines `cool_theorem`$^{\bullet}$: $[\![T]\!]$
- register the fact that $[$`cool_theorem`$]$ $:=$ `cool_theorem`$^{\bullet}$

Thus any later use of `cool_theorem` in a translated term will be automatically turned into `cool_theorem`$^{\bullet}$.

In Practice: Enlarge Your Theory

The interest of this approach lies in the following command.

```
ExtendCoq Definition new : N.
```

In Practice: Enlarge Your Theory

The interest of this approach lies in the following command.

```
ExtendCoq Definition new : N.
```

This opens a goal $[\![\mathtt{N}]\!]$ you have to prove.

When the proof is finished:

1. an axiom `new` : `N` is added;
2. a term $\mathtt{new}^\bullet : [\![\mathtt{N}]\!]$ is defined with the proof;
3. the translation $[\![\mathtt{new}]\!] := \mathtt{new}^\bullet$ is registered.

In Practice: Dirty Tricks

In general, $[\![\mathtt{N}]\!]$ is some kind of mildly unreadable type that is crazy enough so that it has more inhabitants than $\mathtt{N}$.

```
forall
  (A : Type)
  (B : nat → Type),
  (A →
    { n : nat & B n }) →
  { n : nat &
    A → B n }
```

```
forall
  (A : El Type°)
  (B : nat° → El Type°),
  (El A →
    sigT° (TypeVal nat° nat#) (fun n : nat° => B n)) →
  sigT° (TypeVal nat° nat#)
    (fun n : nat° => Prod° (El A) (fun _ : El A => B n))
```

With a bit of practice, you can usually make sense of it though.

Back to Marketing

On-the-fly compilation of the extended theory to Coq!

No more axioms!

Your type-theoretic desires made true!

BEFORE

« Holy Celestial Teapot! »

AFTER

« Stock photos do not experience existential dread. »

**Text and pictures not contractually binding.*

Example: The reader translation, a.k.a. **Baby Forcing**

The Reader Translation

The reader translation extends type theory with

$$\begin{array}{rcl} \mathbb{R} & : & \square \\ \texttt{read} & : & \mathbb{R} \\ \texttt{into} & : & \square \to \mathbb{R} \to \square \\ \texttt{enter}_A & : & A \to \Pi r : \mathbb{R}.\, \texttt{into}\ A\ r \end{array}$$

satisfying a few expected definitional equations.

The Reader Translation

The reader translation extends type theory with

$$\begin{array}{ccl} \mathbb{R} & : & \square \\ \mathtt{read} & : & \mathbb{R} \\ \mathtt{into} & : & \square \to \mathbb{R} \to \square \\ \mathtt{enter}_A & : & A \to \Pi r : \mathbb{R}.\, \mathtt{into}\ A\ r \end{array}$$

satisfying a few expected definitional equations.

The $\mathtt{into}$ function has unfoldings on type formers:

$$\begin{array}{lcl} \mathtt{into}\ (\Pi x : A.\, B)\ r & \equiv & \Pi x : A.\, \mathtt{into}\ B\ r \\ \mathtt{into}\ \square\ r & \equiv & \square \\ \ldots & & \end{array}$$

and it is somewhat redundant:

$$\mathtt{enter}_{\square}\ A\ r \quad \equiv \quad \mathtt{into}\ A\ r$$

The Reader Implementation

Assuming $r : \mathbb{R}$, intuitively:

- Translate $A : \square$ into $[A]_r : \square$
- Translate $M : A$ into $[M]_r : [A]_r$

The Reader Implementation

Assuming $r : \mathbb{R}$, intuitively:

- Translate $A : \square$ into $[A]_r : \square$
- Translate $M : A$ into $[M]_r : [A]_r$

$$
\begin{array}{lcl}
[\square]_r & \equiv & \square \\
[\Pi x : A.\, B]_r & \equiv & \Pi x : (\Pi s : \mathbb{R}.\, [A]_s).\, [B]_r \\
[x]_r & \equiv & x\ r \\
[M\ N]_r & \equiv & [M]_r\ (\lambda s : \mathbb{R}.\, [N]_s) \\
[\lambda x : A.\, M]_r & \equiv & \lambda x : (\Pi s : \mathbb{R}.\, [A]_s).\, [M]_r
\end{array}
$$

All variables are thunked w.r.t. $\mathbb{R}$!

The Reader Implementation

Assuming $r : \mathbb{R}$, intuitively:

- Translate $A : \square$ into $[A]_r : \square$
- Translate $M : A$ into $[M]_r : [A]_r$

$$
\begin{array}{lcl}
[\square]_r & \equiv & \square \\
[\Pi x : A.\, B]_r & \equiv & \Pi x : (\Pi s : \mathbb{R}.\, [A]_s).\, [B]_r \\
[x]_r & \equiv & x\ r \\
[M\ N]_r & \equiv & [M]_r\ (\lambda s : \mathbb{R}.\, [N]_s) \\
[\lambda x : A.\, M]_r & \equiv & \lambda x : (\Pi s : \mathbb{R}.\, [A]_s).\, [M]_r
\end{array}
$$

All variables are thunked w.r.t. $\mathbb{R}$!

Soundness

If $\vec{x} : \Gamma \vdash M : A$ then $r : \mathbb{R}, \vec{x} : (\Pi s : \mathbb{R}.\, [\Gamma]_s) \vdash [M]_r : [A]_r$.

Extending the Reader

One can easily define the new operations through the translation.

$$
\begin{array}{lcl}
[\mathbb{R}]_r & : & [\square]_r \\
[\mathbb{R}]_r & : & \square \\
[\mathbb{R}]_r & \equiv & \mathbb{R} \\
\\
[\texttt{read}]_r & : & [\mathbb{R}]_r \\
[\texttt{read}]_r & : & \mathbb{R} \\
[\texttt{read}]_r & \equiv & r \\
\\
[\texttt{into}]_r & : & [\square \to \mathbb{R} \to \square]_r \\
[\texttt{into}]_r & : & (\mathbb{R} \to \square) \to (\mathbb{R} \to \mathbb{R}) \to \square \\
[\texttt{into}]_r & \equiv & \lambda(A : \mathbb{R} \to \square)(\varphi : \mathbb{R} \to \mathbb{R}).\, A\ (\varphi\ r) \\
\\
[\texttt{enter}_A]_r & : & [A \to \Pi s : \mathbb{R}.\, \texttt{into}\ A\ s]_r \\
[\texttt{enter}_A]_r & : & (\Pi s : \mathbb{R}.\, A\ s) \to \Pi(\varphi : \mathbb{R} \to \mathbb{R}).\, A\ (\varphi\ r) \\
[\texttt{enter}_A]_r & \equiv & \lambda(x : \Pi s : \mathbb{R}.\, A\ s)(\varphi : \mathbb{R} \to \mathbb{R}).\, x\ (\varphi\ r)
\end{array}
$$

More generally

Syntactic models were introduced by Hoffmann...

There have been quite a few around since.

Model	Source*	Implements
Parametricity	no `Prop`	Parametricity
Type-intensionality	no `Prop`	Dynamic typing
Reader	BTT	Proof-relevant Axiom
Forcing	BTT	step indexing, nominal reasoning, ...
Weaning	BTT	many effects
Exceptional	no sing. elim.	exceptions (inconsistent)
Exceptional (interm.)	no sing. elim.	Markov's rule
Param. Exceptional	no `Prop`	IP, ...
Extraction	CIC	???
Iso-Parametricity	???	Automatic transfer of properties
Intuitionistic CPS	only `Prop`	???
Dialectica	no `Prop`	Weak MP, ...

The Ugly

To be fair, syntactic models have a few limitations.

- Pretty hard to come up with such models
- Vanilla CIC doesn't seem ideal as a target
- Implementation issues (cf. Andrej's talk)
- For now still rather simple extensions
- Certain complex models seem out of reach (notably univalence)

Still, I argue that they are damn cool.

Thanks for your attention.