Russian Constructivism in a Prefascist Theory
Pierre-Marie Pédrot

To cite this version:


HAL Id: hal-02548315
https://inria.hal.science/hal-02548315
Submitted on 20 Apr 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Abstract
The results from this paper are twofold. First, we give a purely syntactic presheaf model of CIC. Contrarily to similar endeavours, this variant both preserves conversion and interprets full dependent elimination.

Using a particular instance of this model, we show how to extend CIC with Markov’s principle, while preserving all good meta-theoretical properties like canonicity and decidability of type-checking. The resulting construction can be seen as a synthetic presentation of Coquand-Hofmann’s syntactic model of PRA\(^{\omega} + \text{MP}\) as the composition of Pédrot-Tabareau’s exceptional model with our presheaf interpretation.

CCS Concepts:
- Theory of computation → Type theory; Control primitives; Constructive mathematics.

Keywords: syntactic model, presheaf, dependent types, strict propositions, Markov’s principle, exceptions

1 Introduction
The category of presheaves over some base category is a bread-and-butter model factory from topos theory. Well-known in the proof theory community as forcing or Kripke semantics, presheaves also provide models of dependent type theory. Yet, as functors into \(\text{Set}\), presheaves form a semantic model, which has various drawbacks. The first one is that they are not really computable, even though the target set theory is constructive. Indeed, the constructive existence of a natural number is always up to some extensional equality, which prevents set-theoretical proofs to be effectively run. The second one is that it is hard to control the precise metatheory used to prove the soundness of the model. What part of set theory is really needed for presheaves to model type theory? Third, a more philosophical issue arises. How can we claim that type theory can provide a sane alternative foundation to mathematics, like the HoTT clique does [45], when it lays on the muddy grounds of set theory?

In order to solve this conundrum, there have been several attempts at giving a syntax-conscious presentation of presheaves. One possible way is to describe an extension of usual type theory, justify its consistency into a set-theoretical presheaf model, but show at the same time good properties of the syntax, like strong normalization. This lukewarm compromise position was held for instance by cubical [13], guarded [11], parametric [9] and modal [24] type theories.

The vanguard approach consists instead in replacing set theory with type theory altogether in the presheaf translation, building what is called a syntactic model [27]. While there exist indeed reasonable instances of syntactic models [27, 40], presheaves have proven surprisingly subtle to be typified, despite a handful of unsatisfactory partial results [31, 32, 46]. The source of dissatisfaction itself is quite hard to pin down for non-experts in type theory, and will be described in detail in Section 2.

In this paper, we give a strict positive answer to the existence of type-theoretic presheaves given by a syntactic translation described at Section 4. By construction, this model ensures all the expected syntactic properties of the corresponding theory such as decidability of type-checking and canonicity. There are two critical ingredients to this recipe. First, a deep understanding of the constraints to respect, driven by an intuition from programming language theory, and the half-successes from the related work, which is also discussed in Section 2. Second, a relatively minor extension of type theory that introduces a tiny bit of extensionality without endangering the meta-theoretical properties of the resulting system, originally introduced in Gilbert et al. [23] and that will be recalled in Section 3.

Because presheaves per se are not that interesting, this paper culminates with an example of a mathematically useful extension of type theory. We show how to extend type theory with Markov’s principle (MP), a staple semi-classical principle from the Russian school of constructivism, discussed in Section 8. This theory,
once again, enjoys the usual meta-theoretical properties, and furthermore its soundness does not rely on the availability of MP in the meta-theory. It is given not by one, but two syntactic models. To be precise, it uses the combination of the exceptional model [40], which we will recall in Section 9 and use in Section 10, with an instance of the presheaf model introduced before, that we describe in Section 11. From an abstract standpoint, it is both a synthetic presentation and a dependently-typed generalization of the $\text{PRA}^\delta + \text{MP}$ model from Coquand-Hofmann [15]. As far as we know, this is a new result.

## 2 What is to be Done?

In this section, we review the previous attempts at a internal presentation of presheaves in type theory, and explain why they are subtly broken and how to fix them.

Jaber et al. gave a straightforward type-theoretic adaptation of presheaves [32], by merely translating all the set-theoretic constructs. Unfortunately, they realized that for this model to be sound, they needed what amounted to an extensional target theory. In particular, they interpreted conversion in the presheaf model by propositional equality in the target, relying on axioms such as function extensionality and UIP. In practice, it means that the computational content of the model is destroyed in the process, as well as decidability. Performing a $\beta$-reduction in a term becomes a non-local transformation that requires an explicit proof. To add insult to injury, this also makes canonicity pointless, as it is not possible to actually evaluate a term, as the axioms get in the way.

In an unpublished document, Xu follows the same path [46], and gives a precise analysis of the extensional principles needed for each feature of this model.

**Lemma 1.** In a type-theoretic presheaf model:

- $\Pi$-types require funext in the target.
- Universes require UIP in the target.

Thus, to preserve definitional equality, these principles better be computational in the target, otherwise the explicit rewriting nightmare described above appears again. Function extensionality holds in OTT [5] and CubicalTT [13], but only the former interprets UIP. Alas, those theories require deep changes w.r.t. CIC, which limit the applicability of any presheaf model that would target them, if ever this were possible.

A few years later, Jaber et al. [31] went on a radically different approach to the problem. By studying presheaves as an effect-inducing model, they showed that the usual presentation was squaring the circle. Namely, it was a naturally call-by-value interpretation, which required post-hoc equational properties to ensure full $\beta$-reduction, which in turn were the worm in the apple relying on extensionality. By taking the alternative call-by-name decomposition, all usual equations would become definitional. The key ingredient of this property was that all monotonocity properties were freely given. That is, all terms would start with a universal quantification over the set of smaller conditions.

Quite regrettably, the resulting model was broken, again. By excessively favouring the negative fragment, their translation was too naïve, resulting in a breakage of the positive side, i.e. dependent elimination.

As they realized later [41], this was an instance of a much more general phenomenon. The call-by-name forcing translation was introducing effects, which allowed non-standard inhabitants of inductive types contradicting their induction principle. Dually, the categorical presheaf model recovered a call-by-name equational theory thanks to the naturality property, corresponding exactly to Fürmann’s notion of purity called thunkability [21]. In call-by-name, this corresponds to eliminating troublemakers with parametricity, a technique better known as realizability.

Hence, it was deemed possible to build a parametric variant of the call-by-name presheaf construction, which would enjoy both definitional equations and dependent elimination, following Boulier’s generous variant [12] of Bernardy-Lasson parametricity [10]. Namely, every variable in the source should be mapped to two variables in the target, the first for the effectful term, and the second for the proof that it was pure, e.g. for booleans

\[(x : \mathbb{B}) \mapsto (x_0 : \Pi q \ (\alpha : q \leq p). \mathbb{B}), \ (x_\varepsilon : \mathbb{B}_\varepsilon \ p \ x_0)\]

with $\mathbb{B}_\varepsilon$ an inductive predicate ensuring that its argument is either constantly true or constantly false. This definitely enforces dependent elimination by construction, but we are now back to square one w.r.t. monotonicity. Indeed, one needs to lift the parametricity proof to any lower condition, and this needs to be done definitionally or else we have to reintroduce extensionality. Fair enough, we can apply the same free construction to the parametricity component, which results in

\[
\begin{align*}
(x_0 : \Pi q \ (\alpha : q \leq p). \mathbb{B}), \\
(x_\varepsilon : \Pi q \ (\alpha : q \leq p). \mathbb{B}_\varepsilon \ q \ (\alpha \circ x_0))
\end{align*}
\]

where $\alpha \circ (-)$ stands for precomposition by $\alpha$. We recover definitional equations, and by specializing $x_\varepsilon$ to $p$ and the identity, one can ensure that indeed $x_0$ is internally a boolean... except that *this does not suffice to prove dependent elimination!* All functions depend both on the effectful term and on the parametricity proof, which means that not only $x_0$ should be a boolean but also $x_\varepsilon$. Yet, there is no 2-parametricity proof at hand to enforce this on $x_\varepsilon$, which would require adding one more parametricity layer. But adding 2-parametricity
We now briefly recall what the extension looks like. Would just lift the problem one level higher, and so on, leading to the infamous coherence hell.

3 Strict Propositions

There are two opposite, canonical ways out of the coherence hell, the libertarian one and the authoritarian one. HoTT champions the libertarian approach, which consists in freely adding higher equalities, which are made available via the univalence principle and higher inductive types. The authoritarian tenet, contrastingly, is that there is only one way to be equal, a doctrine embodied by UIP, the principle of uniqueness of identity proofs. The resulting equality type, as found in OTT, is known as a strict equality.

While the HoTT stance seems a priori more attractive, we argue that this is currently not a tenable ideological position. There has been ongoing and very recent work [16, 28] to show that cubical type theory enjoyed the desirable syntactic properties of strong normalization and canonicity. For now, these results are still rudimentary, as they only consider a small subset of type theory. Worse, all their proofs rely on set-theoretic presheaves, and thus fundamentally take place in the contemplated anti-univalent set theory.

This is an aporia. Rather, we advocate for a two-stage cubical revolution. By first implementing presheaves in a minimalistically authoritarian type theory, we will be able to unroot the cubical model from set theory, eventually leading to a setless cubical theory.

We will implement parametric presheaves in sCIC, a HoTT-inspired extension of CIC with strict propositions and UIP, described in Section 4.4 of Gilbert et al. [23]. We now briefly recall what the extension looks like.

The basic sCIC theory extends CIC with a hierarchy of sorts\(^1\) \(s_i : \square_{s_i + 1}\) s.t. for any type \(A : s_i\); if \(M, N : A\) then \(M = N\). Such types are called definitionally proof-relevant. Furthermore, this sort is closed under irrelevant-codomain products, i.e. if \(A : \square_j\) and \(B : A \rightarrow s_j\) then \((\Pi x : A. B x) : s_{\text{max}(i,j)}\), and it also contains inductive types defined similarly to their relevant counterparts. The tricky problem to figure out is the legality of elimination of those \(s\)-dwellin inductive types into \(\square\). It turns out that the criterion is a restriction of the singleton elimination that applies to Coq’s Prop. Namely, while the latter only authorizes elimination from inductive types with at most one constructor with only Prop-living arguments, the former further mandates that the type is not recursive, and, depending on the legality of UIP, that it only has proof-irrelevant indices. Recursivity is forbidden because it entails non-decidability of type-checking, while allowing proof-relevant indices implies UIP.

We will embrace the single-equality doctrine, and thus allow elimination over proof-relevant indices of strict propositions. In this paper, we will write sCIC for this theory, implicitly assuming that it validates UIP.

The major change introduced by this extension is not about conversion, but reduction. Because any two proofs of \(eq A M N\) are convertible, this also means that any proof of \(eq A M M\) is convertible to \(\text{refl}_1 A M\), as their types coincide. Thus, to ensure canonicity, reduction must also be extended for the \(\square\)-valued operator \(J : \Pi (A : \square) (x : A) (P : \Pi y : A. eq A x y \rightarrow \square)\).

\(P x (\text{refl}_1 A x) \rightarrow \Pi (y : A) (e : eq A x y). P y e\)

with \(J A M P Q N E \rightarrow Q\) whenever \(M = N\). Notably, this makes reduction dependent on conversion.

We insist that sCIC is weaker that OTT, for it features neither function extensionality nor quotients. A representative subset of the UIP-free fragment has been formally showed to enjoy strong normalization and canonicity [22]. There is no such proof for the full sCIC extension, and worse, sCIC with an impredicative universe has been shown to break strong normaliztion while seemingly retaining canonicity [2]. We do not rely on impredicativity, thus we speculate that sCIC is indeed strongly normalizing.

4 Negative Forcing Translation

In this section, we will define the prefascist\(^2\) model for CC\(_\omega\), the negative fragment of type theory [31]. It follows the abstract scheme described in Section 2, i.e. it is intuitively the generously parametric restriction of the call-by-name presheaf model from Jaber et al. [31], where crucially, the parametricity predicate is a strict proposition. As such, we will use sCIC as the target theory of this syntactic interpretation. We will assume \(\eta\)-rules for functions and negative products, and we will write the strict equality in \(s_i\) as \(M = N\), omitting the type argument and the universe level. We highlight the differences with the effectful model when they appear.

Definition 1. A base category is given by

- objects \(P : \square_0\)
- morphisms \(\text{hom} : P \rightarrow P \rightarrow \square_0\)
- identity \(\text{id}_p : \text{hom} p p\)
- composition \(\times_{p,q,r} : \text{hom} p q \rightarrow \text{hom} q r \rightarrow \text{hom} p r\)

whose inferable arguments will be omitted and that will follow the usual infix notations for readability, furthermore subject to the following definitional equalities.

\(^1\)Sheaves were first introduced in French as faiseaux. Owing to this Romance etymology, and noting the lack of a corresponding formal Germanic counterpart, we are forced to conclude that the adjetivization of sheaf is fascist, fitting their authoritarian meta-theory.
\[
\begin{align*}
\{\Box_i\}^F_p & := \text{Psh}(\lambda(q\alpha:p), \Box_i^q) \\
\{\Pi x:A.B\}^F_p & := \text{Psh}(\chi(q\alpha:p), \Pi(q\alpha:p).((A\alpha\alpha).Tq\ id_q) = ((A\ p\ id_p).Tq\ alpha)) \\
\{\chi : A\ B\}^F_p & := \text{Psh}(\chi(q\alpha:p), \Pi(x:A\alpha\alpha\ T\chi\ A\alpha\alpha\ x)\ (A\alpha\alpha\ B\alpha\alpha\ x).\ (A\alpha\alpha\ B\alpha\alpha\ x).\ Tq\ id_q) \\
\{\Pi x:A.B\}^F_p & := \text{Psh}(\chi(q\alpha:p), \Pi(q\alpha:p).((A\alpha\alpha\ B\alpha\alpha\ x).\ (A\alpha\alpha\ B\alpha\alpha\ x).\ Tq\ id_q) \\
\{\Box\}^F_p & := \chi_0\ p\ id_p \\
\{\lambda x:A.M\}^F_p & := \chi(q\alpha:p), \chi(\alpha\alpha\ \ x)\ (\alpha\alpha\ \ x).\ \chi(M)^
\end{align*}
\]

The first field is exactly the universe interpretation from Jaber et al. \cite{31}. The main addition is the second field, which is a \textit{strict} parametricity predicate.

As in the parametricity interpretation \cite{10}, the translation will duplicate every context variable \(x\) into a base variable \(x_0\) and a parametricity variable \(x_r\), except that it does so both for base and parametricity terms as in Boulier’s generous variant \cite{12}. Critically, the sort of the type of a variable \(x_r\) will always be \(\ast\). This introduces a minor difference with usual parametricity, where the parametricity predicate of a type is literally the parametricity translation of that type. Since here the parametricity translation is always a proposition, we have to bundle the predicate with the type itself in the \(\Box\) record.

We will track the set of free variables in the translation to be able to maintain them at the right level. Given a set of variables \(\Gamma\), a morphism \(\alpha: \text{hom} q p\) and a term \(M\) we define \(\alpha \bullet\ M\) the lift of \(M\) along \(\Gamma\) as

\[
\alpha \bullet\ M := M\{x_0 := \alpha \ o\ x_0, x_r := \alpha \ o\ x_r \ |\ x \in \Gamma\}.
\]

\textbf{Lemma 2.} \textit{We have the immediate definitional equalities}

\[
\begin{align*}
id \ o\ M & \equiv M \\
(\alpha \ o\ \beta) \ o\ M & \equiv (\alpha \ o\ M) \\
(\alpha \ o\ \beta) \ o\ M & \equiv (\alpha \ o\ M) \\
\end{align*}
\]

We will call \(\text{rw} : \Pi(A\ B;\ \Box)\). \(A \rightarrow B \rightarrow A\) the transport function, and leave its type arguments implicit.

The prefascist translation of \(\text{CC}_{\alpha}\) is defined at Figure 1. It is quite a mouthful, so we first state the soundness theorem, whose proof is just a variant of Jaber et al. \cite{31}, and then we walk through the translation.

\section*{Figure 1. Prefascist Translation}

\[
\begin{align*}
\text{id} \ o\ \alpha & \equiv \alpha \\
\alpha \ o\ \text{id} & \equiv \alpha \\
(\alpha \ o\ \beta) \ o\ y & \equiv (\alpha \ o\ (\beta \ o\ y))
\end{align*}
\]

By convention, variables \(p, q, r\) range over objects, and \(\alpha, \beta, \gamma\) over morphisms. We use the binding notation \((q\alpha:p)\) for \((q: \text{P})\ (\alpha: \text{hom} q p)\). Given a term \(M : \Pi(q\alpha:p).\ A\ (q\alpha), \) and a morphism \(\alpha : \text{hom} q p, \) we write \(\alpha \ o\ M\) for the precomposition of \(M\) with \(\alpha,\ i.e.

\[
\alpha \ o\ M := \lambda(r\beta:q).\ M\ r\ (\alpha \ o\ \beta).
\]

\textbf{Remark 1.} As explained in Jaber et al. \cite{31}, the definitional equations on composition are not restrictive, even less so with a strict equality. Indeed, the Yoneda embedding

\[
\chi_{\text{hom} p q} := \Sigma\alpha : (\Pi r:\ P.\ \text{hom} q r \rightarrow \text{hom} p r) \ni \exists\alpha_0 : \text{hom} p q, (\alpha = \lambda r k.\ \alpha_0 \ o\ k)
\]

where \(\exists\) lives in \(\ast\), is internally isomorphic to \(\text{hom}\) in \(\text{sCIC}\), and can be equipped with a definitional composition by precomposition.

\textbf{Definition 2.} Let \(p : \text{P}\) and \(i\) a universe level, we define \(\square_p\) the type of \textit{pre}-presheaves at \(p\) as the negative record

\[
\square_p := \text{Psh}(\begin{align*}
\text{T} & := \Pi(q\alpha:p), \square_i \\
\text{R} & := (\Pi(q\alpha:p), T q\ alpha) \rightarrow \ast_i
\end{align*})
\]

The first field is exactly the universe interpretation from Jaber et al. \cite{31}. The main addition is the second field, which is a \textit{strict} parametricity predicate.
The prefascist translation is a model of CC_o.

**Theorem 1.** If \( \Gamma \vdash_{CC_o} M : A \) then

- \( \llbracket \Gamma \rrbracket P \vdash [M]_{P}^{\Gamma} : [A]_{P}^{\Gamma}, T \vdash_{P} 1d_{P} \)
- \( \llbracket \Gamma \rrbracket P \vdash \{M\}^{\Gamma}_{P} : \{A\}^{\Gamma}_{P}, R(\lambda(q \alpha : p). \text{rw} ((\{A\}^{\Gamma}_{P} q \alpha) (\alpha \bullet_{\Gamma} [M]^{\Gamma}_{q}))) \)

Likewise, if \( M \equiv_{CC_o} N \) then \([M]^{\Gamma}_{P} \equiv_{\text{CIC}} [N]^{\Gamma}_{P} \) and \([M]^{\Gamma}_{P} \equiv_{\text{CIC}} [N]^{\Gamma}_{P} \).

**Remark 2.** In particular, if \( \Gamma \vdash_{CC_o} A : \square_{\Gamma} \),

- \( \llbracket \Gamma \rrbracket P \vdash [A]^{\Gamma}_{P} : \square^{\Gamma}_{P} \)
- \( \llbracket \Gamma \rrbracket P \vdash \{A\}^{\Gamma}_{P} : \Pi(q \alpha : p), (\alpha \bullet_{\Gamma} [A]^{\Gamma}_{q})). T \vdash_{P} q 1d_{q} = [A]^{\Gamma}_{P}, T q \alpha \)

First, observe that all variables have a thunked type, i.e., are quantified over some \( (q \alpha : p) \). Therefore, we get definitional monotonocity for free.

**Lemma 3 (Free Monotonicity).** Assume that we have \( \llbracket \Gamma \rrbracket P \vdash M_{0} : \llbracket A \rrbracket^{\Gamma}_{P} \) and \( \llbracket \Gamma \rrbracket P \vdash M_{0} : \llbracket A \rrbracket^{\Gamma}_{P} M_{0} \). Then we also have for any \( \alpha : \text{hom} p \):

- \( \llbracket \Gamma \rrbracket P \vdash \alpha \circ M_{0} : \alpha \bullet_{\Gamma} [A]^{\Gamma}_{P} \)
- \( \llbracket \Gamma \rrbracket P \vdash \alpha \circ M_{0} : (\alpha \bullet_{\Gamma} [A]^{\Gamma}_{P}) (\alpha \circ M_{0}) \).

The \(-\Gamma\) part corresponds to the model from Jaber et al. [31] except that types are enriched with a correctness predicate, and that all arguments come with an additional correctness proof. We also use an explicit lift \( \alpha_{\Gamma} \) every time we thunk w.r.t. \( \alpha \) in the style of Miquel [39] instead of accumulating constraints as in Jaber et al. [31], but this is merely cosmetic.

The new part is the \(-\Gamma\) translation, which corresponds to the parametricity proof. There are several points to highlight. First, as already explained, this translation always lives in a proof-relevant sort. Second, applying the parametricity predicate of a type \( A \) on some thunk \( x_{0} \) requires a type cast, as exemplified in the type soundness for \( \llbracket M \rrbracket^{\Gamma}_{P} \). There, \( \alpha \bullet_{\Gamma} [M]^{\Gamma}_{q} \) has type \( \alpha \bullet_{\Gamma} [A]^{\Gamma}_{q} \), \( T \vdash_{P} q 1d_{q} \), but \([A]^{\Gamma}_{P}, R \) expects a thunk of type \( \Pi(q \alpha : p). [A]^{\Gamma}_{P}, T q \alpha \). Luckily, the parametricity proof \([A]^{\Gamma}_{P} \) precisely allows to cast from one type to the other. The bit of magic that makes this work is that this equality is convertible to the universe predicate as in Remark 2.

We do not detail the proof of Theorem 1, it is a simple mutual induction over derivations. A direct consequence though is the following theorem.

**Theorem 2.** The prefascist translation is a model of CC_o.

The soundness theorem for the negative fragment does not rely on proof-relevance. In particular, replacing \( *_{\Gamma} \) with \( \square_{\Gamma} \) in the definition of \( \square_{\Gamma} \) would not have any effect yet.

---

5 Positive Types

So far, the additional parametricity layer has been but a burden, we did not use it actively. Its only interest is to recover dependent elimination that was lost in the naive presheaf model. We therefore show how by translating inductive types in this section.

Once again the translation is very similar to Jaber et al. [31], up to the fact that we now translate a type \( \Gamma \) into a base type \( I_{0} \) and a strict predicate \( I_{0} \) over that type. As in the negative case, the universe parametricity equation will hold definitionally. The translation is straightforward.

**Definition 3.** Given an inductive type \( I \) with parameters \( \Gamma_{I} \), indices \( \Delta_{I} \) and constructors \( c_{i} \), we define \( I_{0} \) with non-uniform parameters \( \llbracket \Gamma_{I} \rrbracket_{P} \), indices \( \llbracket \Delta_{I} \rrbracket_{P} \) without the leading \( p_{I} \), and constructors \( c_{i_{I}} \) whose types are the pointwise \( \llbracket \Gamma_{I} \rrbracket_{P} \), \( \llbracket \Delta_{I} \rrbracket_{P} \) translation, with \( \llbracket \Gamma_{I} \rrbracket_{P}, T \vdash_{P} \beta \) replaced by \( I_{0} r \) and quantifications over \( \llbracket I \rrbracket_{P}, R \) erased, for any \( \Xi, q_{I}, r, \beta \). We define the \( I_{0} \) the same, except that is has one more index \( x_{0} : I_{0} \Gamma_{I} \Delta_{I} \), that it lands in \( * \) and that its constructors \( c_{i_{0}} \) have type \( \llbracket * \rrbracket_{P} \) applied to the corresponding thunked \( I_{0} \) constructor, with replacement for both translations of the underlying inductive.

The usual strict positivity condition ensures that the replacements of the self inductive is sound\(^3\). We give somewhat clearer representative examples of the translation in Figure 2, for booleans, lists and equality. Note e.g. how \( \text{cons}_{0} \) does not mention the parametricity predicate on its recursive call, but \( \text{cons}_{0} \) does. We extend the translation in Figure 3 using a bit of syntactic sugar for context handling.

It is possible to write recursors for any inductive type, satisfying the expected definitional equations. Nonetheless, the resulting terms are quite hideous and unreadable. Hence, we explain instead at a high level how strict parametricity saves the day on the particular example of booleans. Barring conversion, it suffices to prove that

\[
\begin{align*}
P & : \Pi(x_{0} : \llbracket B \rrbracket_{P}) (x_{r} : \llbracket B \rrbracket_{P} x_{0}). \boxdot \\
p_{t} & : P (\lambda(q \alpha : p). \text{true}_{0} q) (\lambda(q \alpha : p). \text{true}_{0} q) \\
p_{f} & : P (\lambda(q \alpha : p). \text{false}_{0} q) (\lambda(q \alpha : p). \text{false}_{0} q) \\
x_{0} & : \Pi(q \alpha : p). B_{0} q \\
x_{r} & : \Pi(q \alpha : p). B_{0} q (\alpha \circ x_{0})
\end{align*}
\]

implies \( P x_{0} x_{r} \). The trick is the following: \( x_{r} p 1d_{p} \) will provide an irrelevant proof that \( x_{0} \) is indeed a boolean. From this, we get a propositional equality between \( x_{0} \) and its \( \eta \)-expansion:

\[
\text{if } x_{0} p 1d_{p} \text{ then } (\lambda q \alpha. \text{true}_{0} q) \text{ else } (\lambda q \alpha. \text{false}_{0} q)
\]

which we use to rewrite in \( P x_{0} x_{r} \). This step is a critical use of UIP. By dependent elimination over \( x_{0} p 1d_{p} \), we are almost done. Thanks to the irrelevance of \( B_{0} \), any

---

\(^3\)Nested inductive types would require induction-induction though.
Theorem 4. The prefascist translation is a model of CIC.

6 Canonicity

Let us call $\Psi_{\beta}\beta$ the type theory generated by the prefascist translation over the category $\mathbb{P}$. By virtue of the soundness theorem, $\Psi_{\beta}\beta$ contains CIC. We have a syntactic model, so it is trivial to peek at the whereabouts of canonicity.

Theorem 3. The prefascist translation is a model of CIC.

Figure 3. Translation Extension

By canonicity of sCIC, $M_e(p := 1)$ ensures that either $(\lambda(q\alpha : 1). M_0(p := q))$ or $(\lambda(q\alpha : 1). M_0(p := q))$. Either way, by applying both sides to the weak terminal morphism $\lambda_q : \text{hom} q 1$, we get canonicity of $M_0$.

While there is no proof in sight that $M_e$ is a constant constructor, it does not matter because by canonicity of $M_0$, it is necessarily convertible to such a constructor.

We insist that canonicity is relative to the target theory, and that there is currently no proof that sCIC enjoys canonicity, although it is believed so [2].

7 A Categorical Equivalence

It so happens that Set models strict propositions [23], where they are interpreted by subsingletons. Observe that, by taking Set as our target type theory, a base category as in Definition 1 is a (small) category. We can thus apply the prefascist translation and compare the result to usual set-theoretic presheaves. We will ignore size issues.
We will describe a standard presheaf without relying on any extensionality axiom. \( \mathcal{A} \) the same as the traditional one. But ours shines by the metatheory, our new notion of presheaves is virtually definitionally featuring function extensionality. This shows an equivalence of categories.

Similarly, let \( A \) be a prefascist type. We define the presheaf \( \mathcal{L}(A) \) as

\[
\begin{align*}
(\mathcal{L}(A))_p & := \text{El}_p A \\
\theta_p^\mathcal{L}(A) q \alpha x & := \alpha \circ x.
\end{align*}
\]

The proof can be carried out in any model of sCIC additionally featuring function extensionality. This shows that as long as one is willing to accept funest in the meta-theory, our notion of presheaves is virtually the same as the traditional one. But ours shines by the fact that it makes all conversions purely definitionally without relying on any extensionality axiom.

8 **Russian Constructivism**

Russian constructivism is a splinter group from orthodox intuitionism. Its defining feature [8], that puts it apart both from Bishop’s minimal intuitionism and Brouwer’s radical constructivism\(^3\), is that they decree Markov’s principle (MP), usually stated as

\[
\Pi(f : \mathbb{N} \to \mathbb{B}), \quad \neg\neg(\Sigma n : \mathbb{N} . f n = \text{true}) \to \Sigma n : \mathbb{N} . f n = \text{true}.
\]

It is equivalent to saying that a Turing machine that does not loop necessarily terminates. While not provable in intuitionistic logic [44], Markov’s principle has been long known to be somewhat compatible with it, insofar as it does not break the witness property. Moreover, MP turns out to be necessary for many completeness results [25, 36].

There are various justifications of MP in the literature, with varying degrees of convincing strength. We review the most representative ones in the remainder of this section.

The oldest one is probably Kleene realizability [34], where MP is realized via an unbounded loop. The realizer does not use at all the doubly-negated premise, and its validity critically relies in MP being provable in the meta-theory. As such, it is arguably cheating. The requirement of arbitrary fixpoints in the language of realizers is also an issue, as in general it entails undecidability of the realizability relation.

Dialectica [6] also interprets MP, in a more intricate way. Contrarily to Kleene realizability, the Dialectica realizer of a negation contains exploitable data [35]. MP is realized by extracting the integer witness from its double-negated premise, allowing to be at the same time more efficient than a clueless loop, and less demanding logically as this does not require meta-MP.

Coquand and Hofmann [15] gave a syntactic model of PRA\(^*\) and MP into PRA\(^*\) itself, which was allegedly a variant of Kripke semantics enriched with an additional layer looking like Friedman’s A-translation [20].

More recently, Herbelin [25] and Ilić [29] described how to implement MP using a weak form of delimited continuations. Their realizer creates a fresh, statically-bound exception and uses it to feed the doubly-negated premise with a failing term. The exception carries an integer as an argument, which is the witness of the existential being proved. The realizor thus catches the exception ensuring it does not escape, and returns its carried value. This is valid because the double negation

\(^3\)Members of the Markovian school also insist that all proofs should correspond to a realizor. In first-order logic this often leads to the acceptance of some form of Church’s thesis [38]. We argue that according to a lax interpretation of this requirement, dependent types fulfill it by construction, since in CIC proofs are literally programs.
is applied to a hereditarily positive type, which guarantees that the fresh exception cannot be involuntarily caught in a closure and escape its handler.

So far, all known models of a dependent type theory extended with MP relied on classical logic at the meta-level, and in particular broke decidability of type-checking and computational canonicity. As a matter of fact, there were two distinct countermodels to the derivability of MP in CIC [17, 40].

In the remainder of this paper, we give a generalization of the Coquand-Hofmann model to CIC, and make the proof more synthetic. The resulting model is the composition of two simpler model transformations, namely an instance of the prefascist interpretation described above, followed by an exceptional interpretation [40]. We will call the resulting system CCCP, the Calculus of Constructions with Completeness Principles, which will be an extension of CIC validating MP and enjoying by construction canonicity and the like. The whole process can be pictorially summarized as

\[
\begin{align*}
\text{CCCP} & \xrightarrow{\text{Exn}} \text{CIC} + E \xrightarrow{\text{Push}} \text{sCIC}
\end{align*}
\]

where \(E\) is an exotic type introduced by the presheaf interpretation together with a few combinators, and the exceptional translation is performed with \(E\) as the type of exceptions.

9 Exception is the Rule

We briefly summarize the exceptional model [40] in this section. We will not dwell too much on the details for lack of space, instead we invite the reader to refer to the cited paper for a more in-depth exposition.

Intuitively, given a type theory \(\mathcal{T}\) containing CIC, together with a type \(\vdash \mathcal{T} E : \Box\) that will stand for the type of exceptions, the exceptional translation builds a new type theory \(\mathcal{T}_E\) where failure is allowed, under the form of terms

\[
\begin{align*}
\vdash \mathcal{T}_E E & : \Box \\
\vdash \mathcal{T}_E \text{raise} : \Pi A : \Box. E \rightarrow A
\end{align*}
\]

where \(E\) reflects \(\mathcal{B}\), and subject to equations such as

\[
\begin{align*}
\text{raise } (\Pi x : A.B) e & \equiv \lambda x : A. \text{raise } B e \\
\text{match } (\text{raise } I e) \text{ return } P & \text{ with } \bar{P} \equiv \text{ raise } \bar{P} e.
\end{align*}
\]

Said otherwise, we have a primitive that allows to escape from the surrounding context, i.e. exceptions. They obey a call-by-name equational theory, so they are quite distinct from their realworld counterparts. In particular, it is not possible to catch exceptions at an arbitrary type. They can only be caught over inductive types, in which case the \(\text{catch}\) primitive is a generalization of the usual dependent eliminator. For instance, exception-catching on booleans is given by the primitive

\[
\begin{align*}
\vdash \mathcal{T}_E \text{catch}_B : \Pi P : B \rightarrow \Box. \\
P \text{ true } \rightarrow P \text{ false } \rightarrow (\Pi e : E.P (\text{raise } B e)) \rightarrow \\
P b : B, P b
\end{align*}
\]

which enjoys the obvious reduction rules. Alternatively, this can be presented as a pattern-matching rules where branches may optionally handle an exception.

In what follows we fix a theory \(\mathcal{T}\) containing CIC, a type \(\vdash \mathcal{T} B : \Box_0\) and an arbitrary family of terms of type \(\vdash \mathcal{T} \Omega_i : B \rightarrow \Box_i\), where \(\Box_i := \Sigma A : \Box_i. (B \rightarrow A)^5\). This family of terms is used to fix the meaning of judgments of the shape \(\vdash \mathcal{T}_E M : \text{raise } \Box N\). Note that the type of \(\Omega_i\) is always inhabited, hence such a term can always be constructed regardless of the actual value of \(B\). Once again, \(\mathcal{T}_E\) is given by a syntactic translation into \(\mathcal{T}\). The basic idea is that we enrich types through the interpretation with their own \(\text{raise}\) function. In particular,

\[
\begin{align*}
\vdash \mathcal{T}_E A & : \Box \quad \rightarrow \quad \vdash \mathcal{T} [A] : \Box \\
\vdash \mathcal{T}_E M : A & \rightarrow \quad \vdash \mathcal{T} [M : [A].\pi_1.
\end{align*}
\]

Translation of the negative fragment is formally given at Figure 4.

Inductive types can be added straightforwardly, we sketch their translation here. Given an inductive type \(I\), we set \([I] := (\mathcal{I}_B, \mathcal{I}_E)\) where \(\mathcal{I}_B\) is an inductive type in \(\mathcal{T}\) whose constructors have as type the pointwise translation of those of \(I\), plus one additional constructor \(\mathcal{I}_E : B \rightarrow \mathcal{I}_B\). Constructors in the source theory are then interpreted by their counterpart from the extended inductive in the target theory. This interpretation is readily adapted to parameters and indices. As an example, we show the translation on lists below.

\[
\begin{align*}
\text{Inductive list}_B (A : \Box) : \Box := \\
| \text{nil}_B : \text{list}_B A \\
| \text{cons}_B : A.\pi_1 \rightarrow \text{list}_B A \rightarrow \text{list}_B A \\
| \text{list}_E : B \rightarrow \text{list}_B A
\end{align*}
\]

This fully defines the introduction rules for inductive types. As usual, the subtle part lies in the interpretation of dependent elimination. Essentially, we interpret pattern-matching pointwise. This almost works thanks to the preservation of typing, except for the additional constructor which is not accounted for. For this one constructor, we use instead the raising primitive given by the return type of the pattern-matching, which corresponds computationally with reraising the exception in the error case.

**Theorem 6.** \(\mathcal{T}_E\) is a model of CIC.

---

5We will reuse in this section the same kind of notations as for the forcing translation, because all these syntactic models follow the same pattern. They should not be confused though.
We do not further detail the implementation of the aforementioned exceptional combinators, although it is quite direct. Instead, we turn to the metatheoretical properties of the translation. To clarify the vocabulary, we say that a type $A$ is inhabited in a theory $T$ when there is a closed term $\Gamma \vdash \emptyset A : A$.

It is immediate to make the following observation.

**Lemma 6.** $T_E$ is consistent iff $E$ is not inhabited in $T$.

**Proof.** We have $\mathtt{⊥} \equiv E$ in $T$. \hfill $\square$

It is more generally possible to show a weak form of canonicity for $T_E$, which is obtained directly from the constructor-adding interpretation of inductive types.

**Lemma 7.** Assuming $T$ enjoys canonicity, if $I$ is an inductive type in $T_E$ with constructors $\tilde{c}$ and $\tilde{r}_E M : I$, then either $M \equiv c_i \tilde{N}$ for some $i$ or $M \equiv \mathtt{raise} \ I \ e$ for some $\tilde{r}_E e : E$.

Note that a direct consequence of this property is that if $E$ is not inhabited in $T$, then $T_E$ does enjoy usual canonicity.

Interestingly, this model can already be used to show a very weak form of MP. Rather than the full fledged internal principle, it is possible to show the admissibility of Markov’s rule in CIC. This derivation rule is defined as

$$
\frac{\vdash_{\text{CIC}} M : \neg \neg P}{\vdash_{\text{CIC}} \langle M \rangle : P}
$$

where $P$ is some hereditarily positive type, e.g. $P := \Sigma n : \mathbb{N}. \ f \ n = \mathtt{true}$. Note that this rule crucially requires the proof environment to be empty, thus forbidding to derive MP.

**Lemma 8** (Friedman’s trick). Markov’s rule is admissible in CIC.

**Proof.** The proof goes as follows. Let $\vdash_{\text{CIC}} M : \neg \neg P$. By soundness of the exceptional model, for any parameter $E$ we get a proof $\vdash_{\text{CIC}} [M] : [\neg \neg P]$. Unfolding the definitions, we get in CIC an isomorphism $[\neg \neg P] \equiv ([P] \to E) \to E$. Now, the crux of the proof lies in the observation that if $P$ is hereditarily positive, then there is actually a closed CIC term $\theta_P : [P] \to P + E$. Such a term is called a storage operator [37], and is defined by recursively matching over its argument and reconstructing a purified proof, and propagating the exception in case of error. The ability to do so is fundamentally tied to the positivity of $P$, which allows to locally force exceptions on its inhabitants, and intuitively corresponds to enforcing a delimited form of call-by-value.

We now have all the required ingredients. Let us set $E := P$, in which case $[M]$ provides us with a term $([P] \to P) \to P$, and the storage operator has type $\theta_P : [P] \to P + P$. By plugging both together with get a closed proof of $P$ in CIC, hence concluding the proof. \hfill $\square$

## 10 From the Rule to the Principle

We argue that implementing Markov’s rule is almost sufficient to get the full Markov’s principle. Obviously, it is not enough per se. We can actually show that $T_E$ disproves MP when $E$ is inhabited [40], which is the case for the instance used in the extraction of Markov’s rule. Yet, the key point is that this rule already features the necessary basic computational extension to implement MP with a little bit of tweaking. The rationale is the following. Any finite number of closed uses of Markov’s rule can be eliminated via the above trick. What prevents us from generalizing to MP is the requirement to pick $E$ beforehand, as it will be fixed once and for all inside the exceptional translation.

What if we were able to dynamically change the value of $E$ to track the set of Markov’s rules being applied?

**Definition 6** (Dynamic prompt). We now assume that the target theory of the exceptional translation is an extension of CIC dubbed CIC $+ E$ which contains the data described at Figure 5. We furthermore assume that $E$ is not inhabited.

This extension is intuitively defined in a theory where there is an ambient global cell $p$ of type $\mathbb{N} \to E$, which
can be locally mutated. Only types are allowed to really observe this cell, otherwise this would break the behaviour of the pure CIC fragment. A typical example is given by the local modality, which allows evaluating its type argument inside a cell set to the pointwise boolean or between the current cell value and the function argument. Likewise, \( E \) is inhabited if there is some \( n : N \) s.t. \( \phi \) if \( n = true \). Its commutation principles with \( \exists \) reflect this semantics. Finally, \( return \) is the unit of the modality, and captures the monotonocity of the pure fragment.

Let CCCP be the theory obtained by unrolling the model construction of the previous section by setting \( T := \text{CIC} + E \) and \( B := E \). We immediately get the following results.

**Lemma 9.** We have the following.

- CCCP contains CIC.
- If \( \text{CIC} + E \) is consistent then so is CCCP.
- If \( \text{CIC} + E \) enjoys canonicity then so does CCCP.

**Proof.** The first property follows from soundness, and the two last ones from the uninhabitedness of \( E \).

Note that we are walking a tight rope here. Consistency of CCCP only requires the absence of a term \( M \) s.t. \( \vdash_{\text{CIC}+E} M : E \), which is a much weaker property than internally having a term \( N \) such that \( \vdash_{\text{CIC}+E} N : \neg E \). The latter would have been enough to show the degeneracy of the construction, i.e. every type would be isomorphic to its exceptional translation.

Thanks to our fancily uninhabited type of exceptions, we actually get a non-trivial extension of CIC.

**Theorem 7.** CCCP validates Russian constructivism.

**Proof.** The proof is actually quite easy. MP is translated by the exceptional translation in \( \text{CIC} + E \) as

\[
\Pi(\varphi : N_E \rightarrow B_E) \rightarrow ((\Sigma_E(n : N_E). \varphi n = E \text{ true} E) \rightarrow \bot_E) \rightarrow \Sigma_E(n : N_E). \varphi n = E \text{ true} E.
\]

Recall that in CIC + \( E \),

\[
\bot_E \equiv E, \quad M = E N \equiv (M = N) + E, \quad \Sigma_E(x : A). B \equiv (\Sigma x : A. B) + E
\]

By intuitionistic symbol pushing, it is thus logically equivalent to prove the simpler statement

\[
\Pi(\varphi : N_E \rightarrow B_E) \rightarrow ((\Sigma n : N_E. \varphi n = \text{ true} E) \rightarrow E) \rightarrow (\Sigma n : N_E. \varphi n = \text{ true} E) + E.
\]

The first part of the proof is to get rid of the exceptional encoding on \( \varphi \). Let us assume for now some \( \varphi : N_E \rightarrow B_E \). Let \( \llbracket n \rrbracket : N \rightarrow N_E \) be the injective function that recursively maps every pure constructor to its exceptional counterpart. Remark now we can easily build a function \( \hat{\varphi} : N \rightarrow B \) by pattern-matching as

\[
\begin{align*}
\hat{\varphi} n & := \text{ true} & \text{ if } \varphi (\llbracket n \rrbracket) \equiv \text{ true} E \\
\hat{\varphi} n & := \text{ false} & \text{ if } \varphi (\llbracket n \rrbracket) \equiv \text{ false} E \\
\hat{\varphi} n & := \text{ false} & \text{ if } \varphi (\llbracket n \rrbracket) \equiv \bot_E \varepsilon.
\end{align*}
\]

Moreover, we have both

\[
(\Sigma n : N_E. \varphi n = \text{ true} E) \rightarrow (\Sigma n : N. \hat{\varphi} n = \text{ true}) + E
\]
\[
(\Sigma n : N. \hat{\varphi} n = \text{ true}) \rightarrow (\Sigma n : N_E. \varphi n = \text{ true} E)
\]

the first one being proved by recursively forcing the integer witness, and the second by trivial injection. By combining these results together, \( MP \) is reducible to

\[
\Pi(\varphi : N \rightarrow B) \rightarrow ((\Sigma n : N. \varphi n = \text{ true}) \rightarrow E) \rightarrow (\Sigma n : N. \varphi n = \text{ true}) + E.
\]

So far we have not used the additional structure on \( E \) and have only reasoned intuitionistically. The second part of the proof is precisely about the use of dynamic prompt to show the above statement.
Let us assume now some \( \varphi : \mathbb{N} \to \mathbb{B} \) and a proof \( e : ((\Sigma n : \mathbb{N}, \varphi n = \text{true}) \to \mathcal{E}) \to \mathcal{E} \), we need to show \((\Sigma n : \mathbb{N}, \varphi n = \text{true}) + \mathcal{E}\). By applying \text{return} to \(e\) we get a proof of
\[
\text{local } \varphi \quad ((\Sigma n : \mathbb{N}, \varphi n = \text{true}) \to \mathcal{E}) \to \mathcal{E}.
\]
Now, by applying the various distribution lemmas from Figure 5, we get a proof of
\[
((\Sigma n : \mathbb{N}, \varphi n = \text{true}) \to \text{local } \varphi \mathcal{E}) \to \text{local } \varphi \mathcal{E}.
\]
But remember that
\[
\text{local } \varphi \mathcal{E} \leftrightarrow (\Sigma n : \mathbb{N}, \varphi n = \text{true}) + \mathcal{E}
\]
so by writing
\[
\mathcal{E}' := \text{local } \varphi \mathcal{E}
\]
\[
P := \Sigma n : \mathbb{N}, \varphi n = \text{true}
\]
we only have to prove
\[
(\mathcal{E}' \leftrightarrow P + \mathcal{E}) \to ((P \to \mathcal{E}') \to \mathcal{E}') \to P + \mathcal{E}'
\]
which is an intuitionistic tautology, regardless of \(\mathcal{E}, \mathcal{E}'\) and \(P\).

\(\square\)

## 11 The Prompt Dialectics

In this section, we justify CIC + \(\mathcal{E}\) via a specific instance of the prefascist construction. In contrast with the previous section, CIC + \(\mathcal{E}\) will now be the source theory, while the target will be sCIC. Similarly, any syntactic translation will refer to the prefascist model, not the exceptional one.

As a minimal departure on the definition from Section 4, we will use a strict preorder rather than a category. That is, hom will live in \(\ast_0\) rather than \(\Box_0\), and we will evocatively write \(p \leq q\) rather than \(\text{hom } p q\). We stress out that this does not affect neither the translation nor the soundness theorems in any way.

Without much surprise, the preorder we will consider is the one from Coquand-Hofmann [15].

**Definition 7.** We define in sCIC the preorder \(\mathbb{F}\) as
- \(\mathbb{F} := \mathbb{N} \to \mathbb{B}\).
- \(p \leq q := \Pi n : \mathbb{N}, q n = \text{true} \rightarrow p n = \text{true}\).

Going down in the preorder means becoming truer. This preorder has a meet semi-lattice structure, which we will put at good use, with
- \(\top := \lambda n : \mathbb{N}. \text{false}\).
- \(p \land q := \lambda n : \mathbb{N}. (p n) \land (q n)\).

We will write \(\text{CIC + } \mathcal{E} := \Psi \mathcal{S}\mathcal{B}_\mathbb{F}\). By Theorem 3, it is clear that CIC + \(\mathcal{E}\) contains CIC. Remark that by Theorem 4 the existence of the maximal element \(\top\) ensures that \(\Psi \mathcal{S}\mathcal{B}_\mathbb{F}\) enjoys canonicity, and thus the premises of Lemma 9 hold.

Let us now implement in the extensions from Figure 5 inside \(\Psi \mathcal{S}\mathcal{B}_\mathbb{F}\) in Figure 6. We focus on the computational parts in the paper, the commutation lemmas are proved by mere symbol pushing. We need a bit of boilerplate, made explicit below.

Because we work in a strict preorder, for simplicity we will not explicitly write the corresponding proofs, and write \(p < q\) for some proof of type \(p \leq q\) derivable from the current context. We write \(\text{True}\) for the one-constructor iuctive type.

By induction it is easy to define a pair of lift functions \(\Pi_{\mathbb{F}_0} : \mathbb{N} \rightarrow \mathbb{N}\mathbb{F}_p\) and \(\Pi_{\mathbb{F}_1} : \Pi n : \mathbb{N}, \mathbb{N}\mathbb{F}_p (\mathbb{N}\mathbb{F}_0, n)\) that map source constructors to their prefascist counterparts. From it, we can derive a function \(\chi : (\Pi n : \mathbb{N}\mathbb{F}_p) (n, \mathbb{N}\mathbb{F}_p n_0). \mathbb{B}_0 p \rightarrow \mathbb{N} \rightarrow \mathbb{B}\) that we use to cast prefascist functions \(\mathbb{N} \rightarrow \mathbb{B}\mathbb{F}_p\) to sCIC functions \(\mathbb{N} \rightarrow \mathbb{B}\).

There is a bit of noise, but the implementation corresponds literally to the intuitive description from the previous section. We have to freeify the presentation of local by adding a spurious quantification, although this is just a technical detail.

**Lemma 10.** The \(\mathcal{E}\) type is not inhabited.

**Proof.** This would require that for any \(p : \mathbb{F}\),
\[
[\mathcal{E}]_p.T \triangleright p \triangleright \Pi n : \mathbb{N}, p n = \text{true}
\]
is inhabited in sCIC. But it is obvious that this type is provably empty for \(p := \top\), and thus uninhabited by consistency of sCIC.

\(\square\)

Note that such an exotic type is typical of presheaf models, as its contents depends on the modal value of the global state.

**Theorem 8.** The prompt API is realized in \(\Psi \mathcal{S}\mathcal{B}_\mathbb{F}\).

By gathering the results from the previous sections, we readily get the following.

**Theorem 9.** There is a syntactic model of CIC + MP enjoying normalization, canonicity and decidability of type-checking, as long as sCIC also enjoys those properties.

## 12 Related Work

The usefulness of strict propositions in the construction of syntactic models was first observed by Altenkirch [4] more than twenty years ago, although this particular instance did not rely on UIP. We find it hard to believe that it took so long for this feature to make it into mainstream proof assistants. It is undeniable that the HoTT
trend triggered a revival of the activity around equality that had gone into dormancy at the beginning of the twenty-first century.

When unfolding the composition of the exceptional and prefascist models proving MP, the resulting syntactic translation is, up to implementation details, a dependently-typed variant of the one given by Coquand-Hofmann [15] for PRAω. This is not surprising, as they describe their model as a mix between the Friedman’s A-translation [20] and Kripke semantics [19]. The former is an ad-hoc first-order variant of the exceptional model, while the latter is a non-dependent variant of the presheaf model. The main contribution of our paper is thus the extension of Coquand-Hofmann’s model to CIC, together with its two-stage decomposition that makes it easier to grasp.

We will argue that Herbelin’s implementation of MP using a weak form of delimited continuations [25] is, from the computational point of view, essentially the same as the Coquand-Hofmann model. Herbelin’s system features statically bound exceptions, that can be introduced through a try – with clause and used as a static jump. In Ilík’s presentation [29], this system can be typed with an ordered stack of prompts, where failure is allowed to return at any point in this stack. Thus, the intended meaning of a term of type $\Sigma$ in a stack $\Sigma$ is a sum $A + \Sigma$ where the right case corresponds to an exception. Furthermore, given a stack $\Sigma$ extending $\Sigma$, it is always possible to lower a value $A$ in $\Sigma$ to a value $A$ in $\Sigma$, mimicking the presheaf monotonocity. The ability to create a new prompt to prove MP is thus tantamount to the action of moving along the order in the Kripke construction. Said otherwise, the prompt stack indexing follows a presheaf discipline.

This is even more obvious in Herbelin-Ghelizan presentation of call-by-name delimited continuations [26], where types that would correspond to a call-by-push-value thunk are indexed by the prompt stack. The CPS they give makes it explicit that a type $A_{\Xi}$ can be lowered to $A_{\Xi}$ by weakening, provided $\Xi$ extends $\Sigma$. This suggests a strong relationship between typed delimited continuations and presheaves.

An extremely similar phenomenon occurs in normalization-by-evaluation (NbE) proofs for $\lambda$-calculi featuring positive types [1, 3, 14, 18, 30, 33, 43]. While proving NbE of the negative fragment can be performed in the syntactic model of presheaves over contexts, there is a fundamental problem as soon as one considers positive types, which require an involved modification of the model, typically in two different ways. The first one [18, 30] is to add MP to the meta-language, either in direct style or by precomposition with a CPS. The second one consists in extending the interpretation of positive types to include neutral terms in the ambient context [1, 14]. With enough squinting, it becomes apparent that those neutral terms behave like statically bound exceptions, an observation already made by Barral [7]. They are made available each time the context is extended with a bound variable, and raised when a term has not enough information to reduce to a normal form. In particular, at toplevel there are no neutral terms because the context is empty, which implies that the model is consistent. This bears a clear kinship with our model of MP.

Let us also mention that our prompt mechanism is reminiscent a of technique recently used by Rahli and Bickford [42] to implement Brouwer’s continuity principle based on the generation of fresh exceptions. Their work suggests new uses for our exceptional presheaf model.

\section*{References}


Russian Constructivism in a Prefascist Theory


