Gluing together Proof Environments: Canonical extensions of LF Type Theories featuring Locks
Furio Honsell, Luigi Liquori, Petar Maksimovic, Ivan Scagnetto

To cite this version:
Furio Honsell, Luigi Liquori, Petar Maksimovic, Ivan Scagnetto. Gluing together Proof Environments: Canonical extensions of LF Type Theories featuring Locks. LFMTP’15. 9th International Workshop on Logical Frameworks and Meta-languages, Berlin, Germany, Aug 2015, Berlin, Germany. Electronic Proceedings in Theoretical Computer Science (EPTCS), 2015, <10.4204/EPTCS.185.1>. <hal-01170029>

HAL Id: hal-01170029
https://hal.archives-ouvertes.fr/hal-01170029
Submitted on 30 Jun 2015

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.
Gluing together Proof Environments: 
Canonical extensions of 
LF Type Theories featuring Locks*

Furio Honsell  
Department of Mathematics and Computer Science  
University of Udine, Italy  
furio.honsell@uniud.it

Luigi Liquori  
Inria Sophia Antipolis Méditerranée, France  
luigi.liquori@inria.fr

Petar Maksimović  
Inria Rennes Bretagne Atlantique, France  
Mathematical Institute of the Serbian Academy  
of Sciences and Arts, Serbia  
petar.maksimovic@inria.fr

Ivan Scagnetto  
Department of Mathematics and Computer Science  
University of Udine, Italy  
ivan.scagnetto@uniud.it

We present two extensions of the LF Constructive Type Theory featuring monadic locks. A lock is a monadic type construct that captures the effect of an external call to an oracle. Such calls are the basic tool for gluing together diverse Type Theories and proof development environments. The oracle can either be invoked in order to check that a constraint holds or to provide a suitable witness. The systems are presented in the canonical style developed by the CMU School. The first system, CLLF_{\varphi}, is the canonical version of the system LLF_{\varphi}, presented earlier by the authors. The second system, CLLF_{\varphi?}, features the possibility of invoking the oracle to obtain a witness satisfying a given constraint. We discuss encodings of Fitch-Prawitz Set theory, call-by-value \( \lambda \)-calculi, and systems of Light Linear Logic. Finally, we show how to use Fitch-Prawitz Set Theory to define a type system that types precisely the strongly normalizing terms.

1 Introduction

In recent years, the authors have introduced in a series of papers [17, 15, 20, 19] various extensions of the Constructive Type Theory LF, with the goal of defining a simple Universal Meta-language that can support the effect of gluing together, i.e. interconnecting, different type systems and proof development environments.

The basic idea underpinning these logical frameworks is to allow for the user to express explicitly, in an LF type-theoretic framework the invocation, and uniform recording of the effect, of external tools by means of a new monadic type-constructor \( L_{\varphi}^M[\cdot] \), called a lock. More specifically, locks permit to express the fact that, in order to obtain a term of a given type, it is necessary to verify, first, a constraint \( \varphi(\Gamma \vdash \Sigma M : \sigma) \), i.e. to produce suitable evidence. No restrictions are enforced on producing such evidence. It can be supplied by calling an external proof search tool or an external oracle, or exploiting some other epistemic source, such as diagrams, physical analogies, or explicit computations according to the Poincaré Principle [3]. Thus, by using lock constructors, one can factor-out the goal, produce pieces of evidence using different proof environments and glue them back together, using the unlock operator, which releases the locked term in the calling framework.

*The work presented in this paper was partially supported by the Serbian Ministry of Education, Science, and Technological Development, projects ON174026 and III44006.
One of the original contributions of this paper is that we show how locks can delegate to external tools not only the task of producing suitable evidence but also that of exhibiting suitable witnesses, to be further used in the calling environment.

Locks subsume different proof attitudes, such as proof-irrelevant approaches, where one is only interested in knowing that a proof witness exists, or approaches relying on powerful terminating metalanguages. Indeed, they allow for a straightforward accommodation of many different proof cultures within a single Logical Framework; which otherwise can be embedded only very deeply \[5\] or axiomatically \[21\].

Differently from our earlier work, we focus in this paper only on systems presented in the canonical format introduced by the CMU school \[12\] \[13\]. This format is syntax-directed and produces a unique derivation for each derivable judgement. Terms are all in normal form and equality rules are replaced by hereditary substitution. Canonical systems are very handy in establishing adequacy of encodings.

First, we present the very expressive system CLLF \(\mathcal{S}\) and discuss the relationship to its non-canonical counterpart LLF \(\mathcal{S}\) in \[19\], where we introduced lock-types following the paradigm of Constructive Type Theory (à la Martin-Löf), via introduction, elimination, and equality rules. This paradigm needs to be rephrased for the canonical format used here. Introduction rules correspond to type checking rules of canonical objects, whereas elimination rules correspond to type synthesis rules of atomic objects. Equality rules are rendered via the rules of hereditary substitution. In particular, we introduce a lock constructor for building canonical objects \(\mathcal{L}_{N,\sigma}^{\mathcal{S}}[M]\) of type \(\mathcal{L}_{N,\sigma}^{\mathcal{S}}[\rho]\), via the type checking rule (O-Lock). Correspondingly, we introduce an unlock destructor, \(\mathcal{U}_{N,\sigma}^{\mathcal{S}}[M]\), and an atomic rule (O-Unlock), allowing elimination, in the hereditary substitution rules, of the lock-type constructor, under the condition that a specific predicate \(\mathcal{P}\) is verified, possibly externally, on a judgement:

\[
\begin{align*}
\Gamma \vdash M &\Rightarrow \rho \quad \Gamma \vdash N \Leftarrow \sigma \quad (O-Lock) \\
\Gamma \vdash \mathcal{L}_{N,\sigma}^{\mathcal{S}}[M] &\Leftarrow \mathcal{L}_{N,\sigma}^{\mathcal{S}}[\rho] \\
\Gamma \vdash \mathcal{L}_{N,\sigma}^{\mathcal{S}}[A] &\Rightarrow \rho \quad \Gamma \vdash N \Leftarrow \sigma \\
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash A &\Rightarrow \mathcal{L}_{N,\sigma}^{\mathcal{S}}[\rho] \\
\Gamma \vdash N &\Leftarrow \sigma \\
\Gamma \vdash \mathcal{U}_{N,\sigma}^{\mathcal{S}}[A] &\Rightarrow \rho \\
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash \mathcal{L}_{N,\sigma}^{\mathcal{S}}[M] &\Leftarrow \mathcal{L}_{N,\sigma}^{\mathcal{S}}[\rho] \\
\end{align*}
\]

Capitalizing on the monadic nature of the lock constructor, as we did for the systems in \[20\] \[19\], one can replace locked terms without necessarily establishing the predicate. This increases the expressivity of the system, and allows for reasoning under the assumption that the verification is successful, as well as for postponing verifications. The crucial rules are:

\[
\begin{align*}
\Gamma, x : \tau \vdash \mathcal{L}_{S,\sigma}^{\mathcal{S}}[\rho] &\text{ type} \\
\Gamma \vdash A &\Rightarrow \mathcal{L}_{S,\sigma}^{\mathcal{S}}[\tau] \\
\rho[\mathcal{U}_{S,\sigma}^{\mathcal{S}}[A]/x]_{\tau}^{\mathcal{F}} &\Rightarrow \rho' \\
\end{align*}
\]

\[
\begin{align*}
\Gamma, x : \tau \vdash \mathcal{L}_{S,\sigma}^{\mathcal{S}}[\rho] &\text{ type} \\
\Gamma \vdash A &\Rightarrow \mathcal{L}_{S,\sigma}^{\mathcal{S}}[\tau] \\
\rho[\mathcal{U}_{S,\sigma}^{\mathcal{S}}[A]/x]_{\tau}^{\mathcal{F}} &\Rightarrow \rho' \\
M[\mathcal{U}_{S,\sigma}^{\mathcal{S}}[A]/x]_{\tau}^{\mathcal{O}} &\Rightarrow M' \\
\end{align*}
\]

\[
\begin{align*}
\Gamma \vdash \mathcal{L}_{S,\sigma}^{\mathcal{S}}[M] &\Leftarrow \mathcal{L}_{S,\sigma}^{\mathcal{S}}[\rho'] \\
\end{align*}
\]

The (O-Nested-Unlock)-rule is the counterpart of the elimination rule for monads, once we realize that \(let_{\mathcal{L}_{\mathcal{S}}}[\mathcal{L}_{\mathcal{S}}]\cdot x = A\) in \(N\) can be replaced by \(N[\mathcal{U}_{\mathcal{S}}^{\mathcal{S}}[A]/x]\). And this holds since the \(\mathcal{L}_{\mathcal{S}}^{\mathcal{S}}[\cdot]\)-monad satisfies the property \(let_{\mathcal{L}_{\mathcal{S}}}[x = M] in N \Rightarrow N\) if \(x \notin Fv(N)\), provided \(x\) occurs guarded in \(N\), i.e. within subterms of the appropriate lock-type. The rule (F-Nested-Unlock) takes care of elimination at the level of types.

We proceed then to introduce CLLF \(\mathcal{S}\). Syntactically, it might appear as a minor variation of CLLF \(\mathcal{S}\), but the lock constructor is used here to express the request for a witness satisfying a given property, which is then replaced by the unlock operation. In CLLF \(\mathcal{S}\), the lock acts as a binding operator and the unlock as an application.
To illustrate the expressive power of CLLF and CLLF, we discuss various challenging encodings of subtle logical systems, as well as some novel applications. First, we encode in LLF Fitch-Prawitz consistent Set-Theory (FPST), as presented in [29], and to illustrate its expressive power, we show, by way of example, how it can type all strongly normalizing terms. Next, we give signatures in LLF of a strongly normalizing λ-calculus and a system of Light Linear Logic [2]. Finally, in Section 4.5, we show how to encode functions in CLLF.

The paper is organized as follows: in Section 2 we present the syntax, the type system and the metatheory of CLLF, whereas CLLF is introduced in Section 3. Section 4 is devoted to the presentation and discussion of case studies. Finally, connections with related work in the literature appear in Section 5.

2 The Canonical System CLLF

In this section, we discuss the canonical counterpart of LLF, i.e. CLLF, in the style of [12, 13]. This approach amounts to restricting the language only to terms in long βη-normal form. These are the normal forms of the original system which are normal also w.r.t. typed η-like expansion rules, namely $M \rightarrow \lambda x: \sigma. M x$ and $M \rightarrow \mathcal{P} \mathcal{L}_N^\sigma [\mathcal{P} \mathcal{L}_N^\sigma [M]]$. The syntax of CLLF defines the normal forms of LLF, and the typing system captures all the judgements in long βη-normal form which are derivable in LLF. The added value of canonical systems such as CLLF is that one can streamline results of adequacy for encoded systems. Indeed, reductions in the meta-language of non-canonical terms reflect only the history of how the proof was developed using lemmata.

2.1 Syntax and Type System for CLLF

The syntax of CLLF is presented in Figure 1. The type system for CLLF is shown in Figure 2. The judgements of CLLF are the following:

- $\Sigma \rightarrow \Sigma$ sig
- $\Gamma \vdash \Sigma$ is a valid signature
- $\Gamma \vdash \Sigma$ is a valid context in $\Sigma$
- $\Gamma \vdash \Sigma K$ is a kind in $\Gamma$ and $\Sigma$
- $\Gamma \vdash \Sigma \sigma$ type $\sigma$ is a canonical family in $\Gamma$ and $\Sigma$
- $\Gamma \vdash \Sigma \alpha \Rightarrow K$ is the kind of the atomic family $\alpha$ in $\Gamma$ and $\Sigma$
- $\Gamma \vdash \Sigma M \leftarrow \sigma$ $M$ is a canonical term of type $\sigma$ in $\Gamma$ and $\Sigma$
- $\Gamma \vdash \Sigma A \Rightarrow \sigma$ $\sigma$ is the type of the atomic term $A$ in $\Gamma$ and $\Sigma$

The judgements $\Sigma$ sig, $\Gamma \vdash \Sigma$, and $\Gamma \vdash \Sigma K$ are as in Section 2.1 of [18], whereas the remaining ones are peculiar to the canonical style. Informally, the judgment $\Gamma \vdash \Sigma M \leftarrow \sigma$ uses $\sigma$ to check the type of the canonical term $M$, while the judgment $\Gamma \vdash \Sigma A \Rightarrow \sigma$ uses the type information contained in the atomic term $A$ and $\Gamma$ to synthesize $\sigma$. Predicates $\mathcal{P}$ in CLLF are defined on judgements of the shape...
Gluing together Proof Environments: CLLF_¬ & CLLF_¬?

Valid signatures
\[ \theta \vdash \text{sig} \quad \frac{C \vdash \text{sig}}{\Sigma \vdash \text{sig}} \] (\text{S-Empty})
\[ \Sigma \vdash \text{K} \quad \frac{\Sigma \vdash \text{a} \not\in \text{Dom} (\Sigma)}{\Sigma, \text{a:K} \vdash \text{sig}} \] (\text{S-Kind})
\[ \Sigma \vdash \text{c:σ} \quad \frac{\Sigma, \text{c:σ} \vdash \text{sig}}{} \] (\text{S-Type})

Kind rules
\[ \frac{\Sigma \vdash \text{Γ}}{\Sigma \vdash \text{Γ} \text{ type}} \] (K-Type)
\[ \frac{\Gamma, \text{x:σ} \vdash \Sigma \text{K}}{\Gamma \vdash \Pi \text{x:σ.K}} \] (K-Pi)

Atomic Family rules
\[ \frac{\Sigma \vdash \text{Γ} \quad \alpha \in \Sigma}{\Gamma \vdash \alpha : M \Rightarrow K} \] (A-App)

Canonical Family rules
\[ \frac{\Sigma \vdash \text{Γ} \quad \alpha \Rightarrow \text{type}}{\Gamma \vdash \alpha \Rightarrow \text{type}} \] (F-Atom)
\[ \frac{\Sigma \vdash \text{Γ} \quad \Pi \text{x:σ.K}}{\Gamma \vdash \Pi \text{x:σ.K}} \] (F-App)
\[ \frac{\Sigma \vdash \text{Γ} \quad \text{ρ type}}{\Gamma \vdash \text{L}_N^{\text{ρ}}[\rho]} \] (F-Lock)
\[ \frac{\Sigma \vdash \text{Γ} \quad \Pi \text{x:σ.K}}{\Gamma \vdash \Pi \text{x:σ.K}} \] (F-Nested-Lock)

Context rules
\[ \frac{\Sigma \vdash \text{Γ} \quad \text{σ type}}{\Sigma, \text{c:σ} \vdash \text{sig}} \] (C-Type)
\[ \frac{\Sigma \vdash \text{Γ} \quad \text{σ type} \quad \text{x:σ}}{\Gamma \vdash \text{x:σ}} \] (C-Var)

Atomic Object rules
\[ \frac{\Sigma \vdash \text{Γ} \quad \text{ρ type} \quad \text{σ:σ type}}{\Gamma \vdash \text{ρ} \Rightarrow \text{σ}} \] (O-App)
\[ \frac{\Sigma \vdash \text{Γ} \quad \text{σ type} \quad \text{x:σ} \quad \Pi \text{x:σ.K}}{\Gamma \vdash \Pi \text{x:σ.K}} \] (O-NLock)

Canonical Object rules
\[ \frac{\Sigma \vdash \text{Γ} \quad \text{σ type} \quad \text{ρ type}}{\Gamma \vdash \text{ρ} \Rightarrow \text{σ}} \] (O-Lock)

Figure 2: The CLLF_¬ Type System

\[ \Gamma \vdash \text{M} \Leftarrow \sigma. \] The type system makes use, in the rules (A-App) and (F-App), of the notion of Hereditary Substitution, which computes the normal form resulting from the substitution of one normal form into another. The general form of the hereditary substitution judgement is \( \text{T} = \text{T}' \), where \( \text{T} \) is the term being substituted, \( x \) is the variable being substituted for, \( T \) is the term being substituted into, \( T' \) is the result of the substitution, \( \rho \) is the simple-type of \( M \), and \( t \) denotes the syntactic class (e.g. atomic families/object, canonical families/object, etc.) under consideration.

The simple-type \( \rho \) of \( M \) is obtained via the erasure function of [13] (Figure 3), mapping dependent into simple-types. The rules for Hereditary Substitution are presented in Figures 4 and 5 using Barendregt's hygiene condition.

Notice that, in the rule (O-Atom) of the type system (Figure 2), the syntactic restriction of the classifier to \( \alpha \) atomic ensures that canonical forms are long \( \beta\eta \)-normal forms for the suitable notion of long

\[ \Gamma \vdash \text{M} \Leftarrow \sigma. \]
\[ (a)^- = a \quad \frac{(\alpha)^- = \rho}{(\alpha M)^- = \rho} \quad \frac{(\sigma)^- = \rho_1}{\frac{(\Pi: \sigma. \tau)^- = \rho_1 \rightarrow \rho_2}{(\tau)^- = \rho}} \]

\[ (L_{\sigma, \tau}^p \downarrow)^- = L_{\sigma, \tau}^p[\rho] \]

Figure 3: Erasure to simple-types

Substitution in Kinds
\[ \text{type}[M_0/x_0]^p_{\rho_0} = \text{type} \quad (\mathcal{F}K\text{-Type}) \]
\[ \frac{\sigma[M_0/x_0]^p_{\rho_0} = \sigma' \quad K[M_0/x_0]^p_{\rho_0} = K'}{(\Pi: \sigma.K)[M_0/x_0]^p_{\rho_0} = \Pi: \sigma'.K'} \]

(\mathcal{F}K\Pi)

Substitution in Atomic Families
\[ a[M_0/x_0]^p_{\rho_0} = a \quad (\mathcal{F}\text{-Const}) \]
\[ \frac{\alpha[M_0/x_0]^p_{\rho_0} = \alpha' \quad M[M_0/x_0]^p_{\rho_0} = M'}{(\alpha M)[M_0/x_0]^p_{\rho_0} = \alpha'M'} \]

(\mathcal{F}\text{-App})

Substitution in Canonical Families
\[ \frac{\alpha[M_0/x_0]^p_{\rho_0} = \alpha'}{(\mathcal{F}\text{-Atom})} \]
\[ \frac{\sigma_1[M_0/x_0]^p_{\rho_0} = \sigma_1' \quad \sigma_2[M_0/x_0]^p_{\rho_0} = \sigma_2'}{(\Pi: \sigma_1.\sigma_2)[M_0/x_0]^p_{\rho_0} = \Pi: \sigma_1'.\sigma_2'} \]

(\mathcal{F}\text{-Pi})

\[ \frac{\sigma_1[M_0/x_0]^p_{\rho_0} = \sigma_1' \quad M_1[M_0/x_0]^p_{\rho_0} = M_1'}{(\Pi: \sigma_1.\sigma_2)[M_0/x_0]^p_{\rho_0} = \Pi: \sigma_1'.\sigma_2'} \]

(\mathcal{F}\text{-Lock})

Figure 4: Hereditary substitution, kinds and families of CLLF_\forall

\[ \beta \eta \text{-normal form, which extends the standard one for lock-types. For one, the judgement } x: \Pi: \sigma.a.a \vdash x \equiv \Pi: \sigma.a.a \text{ is not derivable, as } \Pi: \sigma.a.a \text{ is not atomic, hence } \vdash \lambda x: (\Pi: \sigma.a.a).x \equiv \Pi: (\Pi: \sigma.a.a).x \text{ is not derivable. On the other hand, } \vdash \lambda x: (\Pi: \sigma.a.a).\lambda y:a.xy \equiv \Pi: (\Pi: \sigma.a.a).\Pi: \sigma.a.a, \text{ where } a \text{ is a family constant of kind Type, is derivable. Analogously, for lock-types, the judgement } x: L_{\sigma, \tau}^p[\rho] \vdash x \equiv L_{\sigma, \tau}^p[\rho] \text{ is not derivable, since } L_{\sigma, \tau}^p[\rho] \text{ is not atomic. As a consequence, we have that } \vdash \lambda x: L_{\sigma, \tau}^p[\rho] . x \equiv \Pi: L_{\sigma, \tau}^p[\rho] . L_{\sigma, \tau}^p[\rho] \text{ is not derivable. However, } \vdash x: L_{\sigma, \tau}^p[\rho] \vdash \Pi: L_{\sigma, \tau}^p[x] = L_{\sigma, \tau}^p[\rho] \text{ is derivable, if } \rho \text{ is atomic. Hence, the judgment } \vdash \lambda x: L_{\sigma, \tau}^p[\rho] . L_{\sigma, \tau}^p[\Pi: L_{\sigma, \tau}^p[x]] \equiv \Pi: L_{\sigma, \tau}^p[\rho] . L_{\sigma, \tau}^p[\rho] \text{ is derivable. Note that the unlock constructor takes an atomic term as its main argument, thus avoiding the creation of possible } L^\rho \text{-redexes under substitution. Moreover, since unlocks can only receive locked terms in their body, no abstractions can ever arise. In Definition 2.3 we formalize the notion of } \eta \text{-expansion of a judgement, together with correspondence theorems between } \text{LLF}_\forall \text{ and } \text{CLLF}_\forall \text{.}

We present CLLF_\forall in a fully-typed style, i.e. à la Church, but we could also follow [13] and present a version à la Curry, where the canonical forms } \lambda x.M \text{ and } L_M^p[N] \text{ do not carry type information. The type rules would then be, e.g.:

\[ \frac{\Gamma, x: \sigma \vdash M \equiv \tau}{\Gamma \vdash \lambda x.M \equiv \Pi: \sigma.\tau} \quad (O\text{-Abs}) \quad \frac{\Gamma \vdash M \equiv \sigma \quad \Gamma \vdash N \equiv \tau}{\Gamma \vdash \lambda x.M \equiv \Pi: \sigma.\tau} \quad (O\text{-Lock}) \]

This latter syntax is more suitable in implementations because it optimises the notation. Following [17], we stick to the typeful syntax because it allows for a more direct comparison with non-canonical systems. This, however, is technically immaterial. Since judgements in canonical systems have unique derivations, one can show by induction on derivations that any provable judgement in the system where object terms are à la Curry has a unique type decoration of its object subterms, which turns it into a provable judgement in the version à la Church. Vice versa, any provable judgement in the version à la Church can forget the types in its object subterms, yielding a provable judgement in the version à la Curry.
Substitution in Atomic Objects

\[
\frac{c[M_0/x_0]_{\rho_0} = c}{(\mathcal{F} \cdot \text{O-Const})} \quad \frac{x_0[M_0/x_0]_{\rho_0} = M_0 : \rho_0}{(\mathcal{F} \cdot \text{O-Var})} \quad \frac{x \neq x_0}{(\mathcal{F} \cdot \text{O-Var})}
\]

\[
\frac{A_1[M_0/x_0]_{\rho_0} = \lambda x : \rho_2. M'_1 : \rho_2 \rightarrow \rho}{M_2[M_0/x_0]_{\rho_0} = M'_2 \quad M'_1[M'_2/x]_{\rho_2} = M'} \quad (\mathcal{F} \cdot \text{O-App-H})
\]

\[
\frac{A_1[M_0/x_0]_{\rho_0} = A'_1 \quad M_2[M_0/x_0]_{\rho_0} = M'_2}{(A_1M_2)[M_0/x_0]_{\rho_0} = M'_2} \quad (\mathcal{F} \cdot \text{O-App})
\]

\[
\frac{\sigma[M_0/x_0]_{\rho_0} = \sigma' \quad M[M_0/x_0]_{\rho_0} = M'}{A[M_0/x_0]_{\rho_0} = \mathcal{L}_{M, \sigma} \cdot [M_1] : \mathcal{L}_{M', \sigma'} \cdot [\rho]} \quad (\mathcal{F} \cdot \text{O-Unlock-H})
\]

\[
\frac{M_0/x_0_{\rho_0} = \sigma' \quad M[M_0/x_0]_{\rho_0} = M'}{A[M_0/x_0]_{\rho_0} = A' \quad \mathcal{U}_{M, \sigma} \cdot [A_0]_{\rho_0} = \mathcal{U}_{M', \sigma'} \cdot [A'] \quad (\mathcal{F} \cdot \text{O-Unlock})
\]

Substitution in Canonical Objects

\[
\frac{A[M_0/x_0]_{\rho_0} = A'}{(\mathcal{F} \cdot \text{O-R})} \quad \frac{A[M_0/x_0]_{\rho_0} = M' : \rho}{(\mathcal{F} \cdot \text{O-R-H})} \quad \frac{M[M_0/x_0]_{\rho_0} = M'}{\lambda x : \sigma. M[M_0/x_0]_{\rho_0} = \lambda x : \sigma. M' \quad (\mathcal{F} \cdot \text{O-Abs})}
\]

\[
\frac{\sigma[M_0/x_0]_{\rho_0} = \sigma' \quad M_1[M_0/x_0]_{\rho_0} = M'_1 \quad M_2[M_0/x_0]_{\rho_0} = M'_2}{\mathcal{L}_{M, \sigma} \cdot [M_1][M_0/x_0]_{\rho_0} = \mathcal{L}_{M', \sigma'} \cdot [M'_2] \quad (\mathcal{F} \cdot \text{O-Lock})}
\]

Substitution in Contexts

\[
\frac{[M_0/x_0]_{\rho_0} = \sigma}{(\mathcal{F} \cdot \text{Cxt-Empty})} \quad \frac{x_0 \neq x \quad x \notin \text{Fv}(M_0)}{[\Gamma, x \sigma][M_0/x_0]_{\rho_0} = [\Gamma \vdash x \sigma]} \quad \frac{\sigma[M_0/x_0]_{\rho_0} = \sigma'}{(\mathcal{F} \cdot \text{Cxt-Term})}
\]

Figure 5: Hereditary substitution, objects and contexts of CLLF

2.2 The Metatheory of CLLF

We start by studying the basic properties of hereditary substitution and the type system. First of all, we need to assume that the predicates are well-behaved in the sense of \[\text{(18)}\]. In the context of canonical systems, this notion needs to be rephrased as follows:

**Definition 2.1** (Well-behaved predicates for canonical systems). A finite set of predicates \(\{\mathcal{P}_i\}_{i \in I}\) is well-behaved if each \(\mathcal{P}\) in the set satisfies the following conditions:

1. **Closure under signature and context weakening and permutation:**
   a. If \(\Sigma\) and \(\Omega\) are valid signatures such that \(\Sigma \subseteq \Omega\) and \(\mathcal{P}(\Gamma \vdash \Sigma N \Leftarrow \sigma)\), then \(\mathcal{P}(\Gamma \vdash \Omega N \Leftarrow \sigma)\).
   b. If \(\Gamma\) and \(\Delta\) are valid contexts such that \(\Gamma \subseteq \Delta\) and \(\mathcal{P}(\Gamma \vdash \Sigma N \Leftarrow \sigma)\), then \(\mathcal{P}(\Delta \vdash \Sigma N \Leftarrow \sigma)\).
2. **Closure under hereditary substitution:** If \(\mathcal{P}(\Gamma, x : \sigma', \Gamma' \vdash \Sigma N \Leftarrow \sigma)\) and \(\Gamma \vdash \Sigma N' : \sigma'\), then \(\mathcal{P}(\Gamma, \Gamma'[N'/x]_{\sigma'} \vdash \Sigma N'[N'/x]_{\sigma'} \Leftarrow \sigma)\).

As canonical systems do not feature reduction, the “classical” third constraint for well-behaved predicates (closure under reduction) is not needed here. Moreover, the second condition (closure under substitution) becomes “closure under hereditary substitution”.

**Lemma 2.1** (Decidability of hereditary substitution).

1. For any \(T\) in \(\{\mathcal{K}, \mathcal{F}, \mathcal{F}, \mathcal{F}, \mathcal{F}\}\), and any \(M, x, \rho\), it is decidable whether there exists a \(T'\) such that \(T[M/x]_{\rho} = T'\) or there is no such \(T'\).
2. For any \(M, x, \rho,\) and \(A\), it is decidable whether there exists an \(A'\), such that \(A[M/x]_{\rho} = A'\), or there exist \(M'\) and \(\rho'\), such that \(A[M/x]_{\rho} = M' : \rho'\), or there are no such \(A'\) and \(M'\).
Lemma 2.2 (Head substitution size). If \( A[M_0/x_0]^{\sigma_0} = M : \rho \), then \( \rho \) is a subexpression of \( \rho_0 \).

Proof. By induction on the derivation of \( A[M_0/x_0]^{\sigma_0} = M : \rho \). \( \square \)

Lemma 2.3 (Uniqueness of substitution and synthesis).

1. It is not possible that \( A[M_0/x_0]^{\sigma_0} = A' \) and \( A[M_0/x_0]^{\sigma_0} = M : \rho \).
2. For any \( T \), if \( T[M_0/x_0]^{\mu_0} = T' \), and \( T[M_0/x_0]^{\mu_0} = T'' \), then \( T' = T'' \).
3. If \( \Gamma \vdash \Sigma \alpha \Rightarrow K \), and \( \Gamma \vdash \Sigma \alpha \Rightarrow K' \), then \( K = K' \).
4. If \( \Gamma \vdash \Sigma \alpha \Rightarrow \sigma \), and \( \Gamma \vdash \Sigma \alpha \Rightarrow \sigma' \), then \( \sigma = \sigma' \).

Proof. From the definition of hereditary substitution and the CLLF system. \( \square \)

Lemma 2.4 (Composition of hereditary substitution). Let \( x \neq x_0 \) and \( x \notin \text{Fv}(M_0) \). Then:

1. For all \( T' \) in \( \{ \text{x}, \text{F}, \text{G}, \text{O}, \text{E} \} \), if \( M_2[M_0/x_0]^{\sigma_0} = M_2', T_1[M_2/x]^{\mu_0} = T_1', \) and \( T_1[M_0/x_0]^{\mu_0} = T_1'' \), then there exists a \( T' : T' \Gamma \vdash \Sigma \rho_0 = M \vdash \rho_0 = T \), and \( T_1''[M_2'/x]^{\mu_0} = \rho_0 \).
2. If \( M_2[M_0/x_0]^{\sigma_0} = M_2' \), \( A_1[M_2/x]^{\rho_0} = M : \rho \), and \( A_1[M_0/x_0]^{\sigma_0} = A \), then there exists an \( M' : M[M_0/x_0]^{\sigma_0} = M' \), and \( A[M_2/x]^{\rho_0} = M' : \rho \).
3. If \( M_2[M_0/x_0]^{\sigma_0} = M_2' \), \( A_1[M_2/x]^{\rho_0} = A \), and \( A_1[M_0/x_0]^{\sigma_0} = M : \rho \), then there exists an \( M' : A[M_0/x_0]^{\sigma_0} = M' \), and \( A[M_2'/x]^{\rho_0} = M' \).

By induction on derivations, similar to one in [13] p.14–15, we can prove:

Theorem 2.5 (Transitivity). Let \( \Sigma \vdash \Sigma \Gamma, x_0 ; \rho_0, \Gamma' \) and \( \Gamma \vdash \Sigma M_0 \iff \rho_0 \), and assume that all predicates are well-behaved. Then,

1. There exists a \( \Gamma'' : [M_0/x_0]^{\sigma_0} = \Gamma'' \) and \( \vdash \Sigma \Gamma, \Gamma'' \).
2. If \( \Gamma, x_0 ; \rho_0, \Gamma' \vdash \Sigma K \) then there exists a \( K' : [M_0/x_0]^{\sigma_0} K = K' \) and \( \vdash \Sigma \Gamma', \Gamma'' \vdash \Sigma K' \).
3. If \( \Gamma, x_0 ; \rho_0, \Gamma' \vdash \Sigma \sigma \) type, then there exists a \( \sigma' : [M_0/x_0]^{\sigma_0} \sigma = \sigma' \) and \( \vdash \Sigma \Gamma', \Gamma'' \vdash \Sigma \sigma' \) type.
4. If \( \Gamma, x_0 ; \rho_0, \Gamma' \vdash \Sigma M \iff \sigma \), then there exists \( \sigma' M' : [M_0/x_0]^{\sigma_0} \sigma = \sigma' \) and \( [M_0/x_0]^{\sigma_0} M = M' \) and \( \vdash \Sigma \Gamma', \Gamma'' \vdash \Sigma M' \iff \sigma' \).

Theorem 2.6 (Decidability of typing). If predicates in CLLF \( \varphi \) are decidable, then all of the judgements of the system are decidable.

Proof. By induction on the complexity of judgements. \( \square \)

We can now precisely state the relationship between CLLF \( \varphi \) and the LLF \( \varphi \) system of [19]:

Theorem 2.7 (Soundness). For any predicate \( \varphi \) of CLLF \( \varphi \), we define a corresponding predicate in LLF \( \varphi \) as follows: \( \varphi(\Gamma \vdash \Sigma M : \sigma) \) holds if and only if \( \Gamma \vdash \Sigma M : \sigma \) is derivable in LLF \( \varphi \) and \( \varphi(\Gamma \vdash \Sigma M \iff \sigma) \) holds in CLLF \( \varphi \). Then, we have:

1. If \( \Sigma \vdash \Sigma X \) is derivable in CLLF \( \varphi \), then \( \Sigma \vdash \Sigma X \) is derivable in LLF \( \varphi \).
2. If \( \vdash \Sigma \Gamma \) is derivable in CLLF \( \varphi \), then \( \vdash \Sigma \Gamma \) is derivable in LLF \( \varphi \).
3. If \( \vdash \Sigma \Gamma \) is derivable in CLLF \( \varphi \), then \( \vdash \Sigma \Gamma \) is derivable in LLF \( \varphi \).
4. If \( \vdash \Sigma \alpha \Rightarrow K \) is derivable in CLLF \( \varphi \), then \( \vdash \Sigma \alpha : K \) is derivable in LLF \( \varphi \).
5. If \( \vdash \Sigma \sigma \) type is derivable in CLLF \( \varphi \), then \( \vdash \Sigma \sigma : \) type is derivable in LLF \( \varphi \).
6. If \( \vdash \Sigma A \Rightarrow \sigma \) is derivable in CLLF \( \varphi \), then \( \vdash \Sigma A : \sigma \) is derivable in LLF \( \varphi \).
7. If \( \vdash \Sigma M \iff \sigma \) is derivable in CLLF \( \varphi \), then \( \vdash \Sigma M : \sigma \) is derivable in LLF \( \varphi \).
Vice versa, all LLF \( \mathcal{P} \) judgements in long \( \beta \eta \)-normal form (\( \beta \eta \)-lnf) are derivable in CLLF \( \mathcal{P} \). The definition of a judgement in \( \beta \eta \)-lnf is based on the following extension of the standard \( \eta \)-rule to the lock constructor \( \lambda x: \sigma. Mx \to_M M \) and \( \mathcal{L}_{\xi, \sigma}^\mathcal{P}[\mathcal{U}_{N, \sigma}[M]] \to_M M \).

**Definition 2.2.** An occurrence \( \xi \) of a constant or a variable in a term of an LLF \( \mathcal{P} \) judgement is fully applied and unlocked w.r.t. its type or kind if \( \xi \) appears only in contexts that are of the form \( \mathcal{V}_n[(\ldots (\mathcal{V}_1[\xi \mathcal{M}_1]) \ldots) \mathcal{M}_n] \), where \( \mathcal{M}_1, \ldots, \mathcal{M}_n, \mathcal{V}_1, \ldots, \mathcal{V}_n \) have the same arities of the corresponding vectors of \( \Gamma \)’s and locks.

**Definition 2.3 (Judgements in long \( \beta \eta \)-normal form).**

1. A term \( T \) in a judgement is in \( \beta \eta \)-lnf if \( T \) is in normal form and every constant and variable occurrence in \( T \) is fully applied and unlocked w.r.t. its classifier in the judgement.
2. A judgement is in \( \beta \eta \)-lnf if all terms appearing in it are in \( \beta \eta \)-lnf.

**Theorem 2.8 (Correspondence).** Assume that all predicates in LLF \( \mathcal{P} \) are well-behaved, according to Definition 2.1 \([18]\). For any predicate \( \mathcal{P} \) in LLF \( \mathcal{P} \), we define a corresponding predicate in CLLF \( \mathcal{P} \) with: \( \mathcal{P}(\Gamma \vdash \Sigma M \leftarrow \sigma) \) holds if \( \Gamma \vdash \Sigma M \leftarrow \sigma \) is derivable in LLF \( \mathcal{P} \) and \( \mathcal{P}(\Gamma \vdash \Sigma M : \sigma) \) holds in LLF \( \mathcal{P} \). Then, we have:

1. If \( \Sigma \) sig is in \( \beta \eta \)-lnf and is LLF \( \mathcal{P} \)-derivable, then \( \Sigma \) sig is CLLF \( \mathcal{P} \)-derivable.
2. If \( \Gamma \vdash \Sigma \) is in \( \beta \eta \)-lnf and is LLF \( \mathcal{P} \)-derivable, then \( \Gamma \vdash \Sigma \) is CLLF \( \mathcal{P} \)-derivable.
3. If \( \Gamma \vdash \Sigma K \) is in \( \beta \eta \)-lnf, and is LLF \( \mathcal{P} \)-derivable, then \( \Gamma \vdash \Sigma K \) is CLLF \( \mathcal{P} \)-derivable.
4. If \( \Gamma \vdash \Sigma \alpha : K \) is in \( \beta \eta \)-lnf and is LLF \( \mathcal{P} \)-derivable, then \( \Gamma \vdash \Sigma \alpha \Rightarrow K \) is CLLF \( \mathcal{P} \)-derivable.
5. If \( \Gamma \vdash \Sigma \sigma : \text{type} \) is in \( \beta \eta \)-lnf and is LLF \( \mathcal{P} \)-derivable, then \( \Gamma \vdash \Sigma \sigma \text{ type} \) is CLLF \( \mathcal{P} \)-derivable.
6. If \( \Gamma \vdash \Sigma \lambda : \alpha \) is in \( \beta \eta \)-lnf and is LLF \( \mathcal{P} \)-derivable, then \( \Gamma \vdash \Sigma \lambda \Rightarrow \alpha \) is CLLF \( \mathcal{P} \)-derivable.
7. If \( \Gamma \vdash \Sigma M : \sigma \) is in \( \beta \eta \)-lnf and is LLF \( \mathcal{P} \)-derivable, then \( \Gamma \vdash \Sigma M \leftarrow \sigma \) is CLLF \( \mathcal{P} \)-derivable.

**Proof.** Follows closely the proof of the corresponding Correspondence Theorem 7 \([17]\). \( \square \)

Notice that, by the Correspondence Theorem above, any well-behaved predicate \( \mathcal{P} \) in LLF \( \mathcal{P} \) in the sense of Definition 2.1 \([18]\) induces a well-behaved predicate in CLLF \( \mathcal{P} \). Finally, notice that not all LLF \( \mathcal{P} \) judgements have a corresponding \( \beta \eta \)-lnf. Namely, the judgement \( x : \mathcal{L}_{\mathcal{N}, \sigma}^\mathcal{P}[\rho] \vdash \Sigma x : \mathcal{L}_{\mathcal{N}, \sigma}^\mathcal{P}[\rho] \) does not admit an \( \eta \)-expanded normal form when the predicate \( \mathcal{P} \) does not hold on \( \mathcal{N} \), as the rule \((O\text{-Unlock})\) can be applied only when the predicate holds.

### 3 The Type System CLLF \( \mathcal{P} \)

The main idea behind CLLF \( \mathcal{P} \) (see Figures 6, 7, and 8) is to “empower” the framework of CLLF \( \mathcal{P} \) by adding to the lock/unlock mechanism the possibility to receive from the external oracle a witness satisfying suitable constraints. Thus, we can pave way for the gluing together of different proof development environments beyond proof irrelevance scenarios. In this context, the lock constructor behaves as a binder. The new \((O\text{-Lock})\) rule is the following:

\[
\begin{align*}
\Gamma, x : \sigma & \vdash \Sigma M \leftarrow \rho \\
\Gamma \vdash \Sigma \mathcal{L}_{\mathcal{N}, \sigma}^\mathcal{P}[M] \leftarrow \mathcal{L}_{\mathcal{N}, \sigma}^\mathcal{P}[\rho]
\end{align*}
\]

\( ^1 \)For lack of space, we present in these figures only the categories and rules of CLLF \( \mathcal{P} \) that differ from their CLLF \( \mathcal{P} \) counterparts.
\[ \sigma, \tau, \rho \in \mathcal{F} \quad \sigma \equiv \alpha \mid \Pi x: \sigma. \tau \mid \mathcal{L}^{\rho}_{x, \sigma}[\rho] \quad \text{Canonical Families} \]
\[ M, N \in \mathcal{O} \quad M \equiv A \mid \lambda x: \sigma.M \mid \mathcal{L}^{\rho}_{x, \sigma}[M] \quad \text{Canonical Objects} \]

Figure 6: CLLF_{\mathcal{O}} Syntax — changes w.r.t. CLLF_{\mathcal{O}}

Canonical Family rules
\[
\begin{align*}
\Gamma, x: \sigma \vdash_{\Sigma} & \rho \text{ type} & (F\text{-Lock}) \\
\Gamma \vdash_{\Sigma} & \mathcal{L}^{\rho}_{x, \sigma}[\rho] \text{ type} & (F\text{-Nested-Unlock}) \\
\end{align*}
\]

Atomic Object rules
\[
\begin{align*}
\Gamma \vdash_{\Sigma} & A \Rightarrow \mathcal{L}^{\rho}_{x, \sigma}[\rho] & \Gamma \vdash_{\Sigma} N \leftarrow \sigma & \mathcal{P}(\Gamma \vdash_{\Sigma} N \leftarrow \sigma) & \rho[N/x]_{(\sigma)} = \rho' \quad (O\text{-Unlock}) \\
\Gamma \vdash_{\Sigma} & \mathcal{U}_{N, \sigma}[A] \Rightarrow \rho' & \Gamma \vdash_{\Sigma} M \leftarrow \rho & \mathcal{O}(\Gamma \vdash_{\Sigma} M \leftarrow \rho) & (O\text{-Lock}) \\
\Gamma, y: \tau \vdash_{\Sigma} & \mathcal{L}^{\rho}_{x, \sigma}[M] \leftarrow \mathcal{L}^{\rho}_{x, \sigma}[\rho] & \Gamma \vdash_{\Sigma} A \Rightarrow \mathcal{L}^{\rho}_{x, \sigma}[\tau] & \rho[\mathcal{U}_{x, \sigma}^{\rho}[A]/y]_{(\tau)} = \rho' & M[\mathcal{U}_{x, \sigma}^{\rho}[A]/y]_{(\tau)} = M' & (O\text{-Nested-Unlock}) \\
\end{align*}
\]

Figure 7: The CLLF_{\mathcal{O}} Type System — changes w.r.t. CLLF_{\mathcal{O}}

where the variable \( x \) is a placeholder bound in \( M \) and \( \rho \), which will be replaced by the concrete term that will be returned by the external oracle call. The intuitive meaning behind the \((O\text{-Unlock})\) rule is, therefore, that of recording the need to delegate to the external oracle the inference of a suitable witness of a given type. Indeed, \( M \) can be thought of as an “incomplete” term which needs to be completed by an inhabitant of a given type \( \sigma \) satisfying the constraint \( \mathcal{P} \). The actual term, possibly synthesized by the external tool, will be “released” in CLLF_{\mathcal{O}}, by the unlock constructor in the \((O\text{-Unlock})\) rule as follows:

\[
\begin{align*}
\Gamma \vdash_{\Sigma} A \Rightarrow \mathcal{L}^{\rho}_{x, \sigma}[\rho] & \quad \rho[N/x]^{\Sigma}_{(\sigma)} = \rho' & \Gamma \vdash_{\Sigma} N \leftarrow \sigma & \mathcal{P}(\Gamma \vdash_{\Sigma} N \leftarrow \sigma) \\
\Gamma \vdash_{\Sigma} & \mathcal{U}_{N, \sigma}[A] \Rightarrow \rho' \\
\end{align*}
\]

The term \( \mathcal{U}_{N, \sigma}[M] \) intuitively means that \( N \) is precisely the synthesized term satisfying the constraint \( \mathcal{P}(\Gamma \vdash_{\Sigma} N \leftarrow \sigma) \) that will replace in CLLF_{\mathcal{O}} all the free occurrences of \( x \) in \( \rho \). This replacement is executed in the \((S\text{-O-Unlock}\cdot \text{H})\) hereditary substitution rule (Figure 8).

Similarly to CLLF_{\mathcal{O}}, in CLLF_{\mathcal{O}} it is also possible to “postpone” or delay the verification of an external predicate. Whence, the synthesis of the actual inhabitant \( N \) can be delayed, thanks to the \((O\text{-Nested-Unlock})\) rule:

\[
\begin{align*}
\Gamma, y: \tau \vdash_{\Sigma} & \mathcal{L}^{\rho}_{x, \sigma}[M] \leftarrow \mathcal{L}^{\rho}_{x, \sigma}[\rho] & \Gamma \vdash_{\Sigma} A \Rightarrow \mathcal{L}^{\rho}_{x, \sigma}[\tau] & \rho[\mathcal{U}_{x, \sigma}^{\rho}[A]/y]_{(\tau)} = \rho' & M[\mathcal{U}_{x, \sigma}^{\rho}[A]/y]_{(\tau)} = M' \\
\Gamma \vdash_{\Sigma} & \mathcal{L}^{\rho}_{x, \sigma}[M'] \leftarrow \mathcal{L}^{\rho}_{x, \sigma}[\rho'] \\
\end{align*}
\]

The Metatheory of CLLF_{\mathcal{O}} follows closely that of CLLF_{\mathcal{O}} as far as decidability. We have no correspondence theorem since we did not introduce a non-canonical variant CLLF_{\mathcal{O}}. This could have been done similarly to LLF_{\mathcal{O}}.

4 Case studies

In this section, we discuss the encodings of a collection of logical systems which illustrate the expressive power and the flexibility of CLLF_{\mathcal{O}} and CLLF_{\mathcal{O}}. We discuss Fitch-Prawitz Consistent Set theory, FPST
Gluing together Proof Environments: CLLF $\mathcal{F}$ & CLLF $\mathcal{F}?$

Substitution in Canonical Families

$$\sigma_1[M_0/x_0]^F_{\rho_0} = \sigma'_1 \quad \sigma_2[M_0/x_0]^F_{\rho_0} = \sigma'_2$$

\[
\frac{\mathcal{L}_{x,\sigma_1}[\sigma_2][M_0/x_0]^F_{\rho_0} = \mathcal{L}_{x,\sigma'_1}[\sigma'_2]}{\mathcal{L}_{x,\sigma}[\sigma_2][M_0/x_0]^F_{\rho_0}} \quad (\mathcal{F}\cdot F\text{-Lock})
\]

Substitution in Atomic Objects

$$\sigma[M_0/x_0]^F_{\rho_0} = \sigma' \quad M[M_0/x_0]^F_{\rho_0} = M' \quad M_1[M'/x]^o_{\sigma}\cdot = M_2 \quad A[M_0/x_0]^o_{\rho_0} = \mathcal{L}_{x,\sigma}[M_1] : \mathcal{L}_{x,\sigma}^o[\rho]$$

\[
\frac{\mathcal{L}_{x,\sigma}[\sigma][M_0/x_0]^o_{\rho_0}}{\mathcal{L}_{x,\sigma}[\sigma_2][M_0/x_0]^o_{\rho_0}} = M_2 : \rho \quad (\mathcal{F}\cdot O\text{-Unlock-H})
\]

Substitution in Canonical Objects

$$\sigma_1[M_0/x_0]^F_{\rho_0} = \sigma'_1 \quad M_1[M_0/x_0]^o_{\rho_0} = M'_1$$

\[
\frac{\mathcal{L}_{x,\sigma_1}[M_1][M_0/x_0]^o_{\rho_0} = \mathcal{L}_{x,\sigma_1}[M'_1]}{\mathcal{L}_{x,\sigma}[\sigma][M_0/x_0]^o_{\rho_0}} \quad (\mathcal{F}\cdot O\text{-Lock})
\]

Figure 8: CLLF $\mathcal{F}?$, Hereditary Substitution — changes w.r.t. CLLF $\mathcal{F}$

[29], some applications of FPST to normalizing $\lambda$-calculus, a system of Light Linear Logic in CLLF $\mathcal{F}$, and an encoding of a partial function in CLLF $\mathcal{F}?$.

The crucial step in encoding a logical system in CLLF $\mathcal{F}$ or CLLF $\mathcal{F}?$ is to define the predicates involved in locks. Predicates defined on closed terms are usually unproblematic. Difficulties arise in enforcing the properties of closure under hereditary substitution and closure under signature and context extension, when predicates are defined on open terms. To be able to streamline the definition of well-behaved predicates we introduce the following:

Definition 4.1. Given a signature $\Sigma$ let $\Lambda_\Sigma$ (respectively $\Lambda^c_\Sigma$) be the set of LLF $\mathcal{F}$ terms (respectively closed LLF $\mathcal{F}$ terms) definable using constants from $\Sigma$. A term $M$ has a skeleton in $\Lambda_\Sigma$ if there exists a term $N[x_1, \ldots, x_n] \in \Lambda_\Sigma$, whose free variables (called holes of the skeleton) are in $\{x_1, \ldots, x_n\}$, and there exist terms $M_1, \ldots, M_n$ such that $M \equiv N[M_1/x_1, \ldots, M_n/x_n]$.

4.1 Fitch Set Theory à la Prawitz - FPST

In this section, we present the encoding of a formal system of remarkable logical as well as historical significance, namely the system of consistent Naïve Set Theory, FPST, introduced by Fitch [10]. This system was first presented in Natural Deduction style by Prawitz [29]. As Naïve Set Theory is inconsistent, to prevent the derivation of inconsistencies from the unrestricted abstraction rule, only normalizable deductions are allowed in FPST. Of course, this side-condition is extremely difficult to capture using traditional tools.

In the present context, instead, we can put to use the machinery of CLLF $\mathcal{F}$ to provide an appropriate encoding of FPST where the global normalization constraint is enforced locally by checking the proof-object. This system is a beautiful illustrative example of the bag of tricks that CLLF $\mathcal{F}$ supports. Checking that a proof term is normalizable would be the obvious predicate to use in the corresponding lock-type, but this would not be a well-behaved predicate if free variables, i.e. assumptions, are not sterilized. To this end, we introduce a distinction between generic judgements, which cannot be directly utilized in arguments, but which can be assumed, and apodictic judgements, which are directly involved in proof rules. In order to make use of generic judgements, one has to downgrade them to an apodictic one. This is achieved by a suitable coercion function.

Definition 4.2 (Fitch Prawitz Set Theory, FPST). The full system of Fitch (see [29]), as presented by Prawitz is defined into Appendix A here only we give the crucial rules for implication and for set-
abstraction and the corresponding elimination rules:

\[
\begin{align*}
\frac{\Gamma, A \vdash_{FPST} B}{\Gamma \vdash_{FPST} A \bowtie B} (\Box I) & \quad \frac{\Gamma \vdash_{FPST} A \bowtie B}{\Gamma \vdash_{FPST} A} (\Diamond I) \\
\frac{\Gamma \vdash_{FPST} A[T/x]}{\Gamma \vdash_{FPST} T \in \lambda x.A} (\lambda I) & \quad \frac{\Gamma \vdash_{FPST} T \in \lambda x.A}{\Gamma \vdash_{FPST} A[T/x]} (\lambda E)
\end{align*}
\]

In Fitch’s system, FPST, conjunction and universal quantification are defined as usual, while negation is defined constructively, but it still allows for the usual definitions of disjunction and existential quantification. What makes FPST consistent is that not all standard deductions in FPST are legal. Standard deductions are called quasi-deductions in FPST. A legal deduction in FPST is defined instead, as a quasi-deduction which is normalizable in the standard sense of Natural Deduction, namely it can be transformed in a derivation where all elimination rules occur before introductions.

**Definition 4.3** (LLF signature $\Sigma_{FPST}$ for Fitch Prawitz Set Theory). The following constants are introduced:

- $0 : \text{Type}$
- $1 : \text{Type}$
- $T : o \to \text{Type}$
- $\delta : \Pi A:o. \ (V(A) \to T(A))$
- $V : o \to \text{Type}$
- $\lambda \text{intro} : \Pi A:i \to o. \Pi x:i. T(A x) \to T(\epsilon x (\lambda \text{A}))$
- $\lambda : (i \to o) \to i$
- $\lambda \text{elim} : \Pi A:i \to o. \Pi x:i. T(\epsilon x (\lambda \text{A})) \to T(A x)$
- $\epsilon : i \to i \to o$
- $\gamma \text{intro} : \Pi A,B:o. (V(A) \to T(B)) \to (T(A \bowtie B))$
- $\gamma : o \to o \to o$
- $\gamma \text{elim} : \Pi A,B:o. \Pi x:A. \Pi y:B. T(A \bowtie B) \to \mathcal{L}_{\text{Fitch}}^{\gamma}(\Pi x:A, \Pi y:B. T(A \bowtie B))$

where $o$ is the type of propositions, $\gamma$ and the “membership” predicate $\epsilon$ are the syntactic constructors for propositions, $\lambda$ is the “abstraction” operator for building “sets”, $T$ is the apodictic judgement, $V$ is the generic judgement, $\delta$ is the coercion function, and $\langle x, y \rangle$ denotes the encoding of pairs, whose type is denoted by $\sigma \times \tau$, e.g. $\lambda u: \sigma \to \tau \to \rho$. $u \times y : (\sigma \to \tau \to \rho) \to \rho$. The predicate in the lock is defined as follows:

\[
\text{Fitch}(\Gamma \vdash_{\Sigma_{FPST}} (x, y) \iff T(A) \times T(A \bowtie B))
\]

it holds iff $x$ and $y$ have skeletons in $\Lambda_{\Sigma_{FPST}}$, all the holes of which have either type $o$ or are guarded by a $\delta$, and hence have type $V(A)$, and, moreover, the proof derived by combining the skeletons of $x$ and $y$ is normalizable in the natural sense.

For lack of space, we do not spell out the rules concerning the other logical operators, because they are all straightforward provided we use only the apodictic judgement $T(\cdot)$, but a few remarks are mandatory. The notion of normalizable proof is the standard notion used in natural deduction. The predicate Fitch is well-behaved because it considers terms only up-to holes in the skeleton, which can have type $o$ or are generic judgements. Adequacy for this signature can be achieved in the format of [18]:

**Theorem 4.1** (Adequacy for Fitch-Prawitz Naive Set Theory). *If $A_1, \ldots, A_n$ are the atomic formulas occurring in $B_1, \ldots, B_m, A$, then $B_1 \ldots B_m \vdash_{FPST} A$ iff there exists a normalizable $M$ such that $A_1:o, \ldots, A_n:o, x_1:V(B_1), \ldots, x_m:V(B_m) \vdash_{\Sigma_{FPST}} M \Rightarrow T(A)$ (where $A$, and $B_1$ represent the encodings of, respectively, $A$ and $B_i$ in CLLF, for $1 \leq i \leq m$).*

### 4.2 A Type System for strongly normalizing $\lambda$-terms

Fitch-Prawitz Set Theory, FPST, is a rather intriguing, albeit unexplored, set theoretic system. The normalizability criterion for accepting a quasi-deduction prevents the derivation of contradictions, and
hence makes the system consistent. Of course, some intuitive rules are not derivable. For instance modus ponens does not hold and if \( t \in \lambda x.A \) then we do not have necessarily that \( A[t/x] \) holds. Similarly, the transitivity property does not hold. However, it is interesting to point out that FPST is also a very expressive type system which encompasses all kinds of quantification.

In this subsection, we sketch how to use FPST to define a type system which can type precisely all the strongly normalizing \( \lambda \)-terms. First we need to adapt to FPST, Proposition 4, Appendix A.1 of [12], originally given by J-Y. Girard for Light Linear Logic, as follows:

**Theorem 4.2 (Fixpoint).** Let \( A[P,x_1,\ldots,x_n] \) be a formula of FPST with an \( n \)-ary predicate variable \( P \). Then, there exists a formula \( B \) of FPST, such that there exists a normalizable deduction in FPST between \( A[\lambda x_1,\ldots,x_n.B[x_1,\ldots,x_n],x_1,\ldots,x_n] \) and \( B \), and vice versa.

**Proof.** Let equality be defined as Leibniz equality, then, assuming \( n = 1 \), define \( \Lambda \equiv \lambda z.\exists x.\exists y.z = \langle x,y \rangle \& A[\langle \lambda w.\langle w,y \rangle \in y \rangle,x] \). Then \( \langle x,\Lambda \rangle \in \Lambda \) is equivalent, in the sense of FPST, to \( A[\langle \lambda w.\langle w,\Lambda \rangle \in \Lambda \rangle,x] \).

The above Fixpoint Theorem can be used to define recursive functions and inductive definitions. Hence, let us consider a concrete representation, possibly over natural numbers, of the terms of \( \Lambda \)-calculus in FPST, and call it \( \Lambda_0 \). It exists, because even if the theory is non-standard, it allows the definition of some putative notion of a natural number. Using again the Fixed Point Theorem, we can define a fixpoint \( \Lambda \) such that \( x \in \Lambda \) is equivalent, in the sense of Fitch, to \( x \in \Lambda_0 \& \forall y.y \in \Lambda_0 \subset app(x,y) \in \Lambda \). Here, \( app(x,y) \) denotes the concrete representation of “applying” \( x \) to \( y \). It is now straightforward to check that only normalizing terms can “be typed in FPST by \( \Lambda \)”, \( i.e. \) belong to \( \Lambda \). Since one can derive in FPST that a representation of a \( \lambda \)-term, say \( M \), belongs to \( \Lambda \), only if there is a normalizable derivation of \( M \in \Lambda \), then there is a natural reflection of the normalizability of the FPST derivation of the typing judgement \( M \in \Lambda \), and the fact that the term represented by \( M \) is indeed normalizable.

### 4.3 A Normalizing call-by-value \( \lambda \)-calculus

In this section we sketch how to express in CLLF \( \varphi \) a call-by-value \( \lambda \)-calculus where \( \beta \)-reductions fire only if the result is normalizing.

**Definition 4.4 (Normalizing call-by-value \( \lambda \)-calculus, \( \Sigma_{\Lambda,N} \)).**

\[
\begin{align*}
  o & : \text{Type} & \text{Eq} & : o \to o \to \text{Type} & \text{app} & : o \to o \to o \\
  v & : \text{Type} & \text{var} & : v \to o & \text{lam} & : (v \to o) \to o \\
  c_{\beta} & : \Pi M : o \to o, N : o . \varphi[o,o,o].\varphi[N,N],(o\to o) \times o . \text{Eq}(\text{app}(\text{lam} \lambda x : v . \text{M}(\text{var} x)), N) (MN) \\
\end{align*}
\]

where the predicate \( \varphi \) holds on \( \Gamma \vdash_{\Sigma_{\Lambda,N}} (M,N) \leftarrow (o\to o) \times o \) if both \( M \) and \( N \) have skeletons in \( \Lambda_{\Sigma_{\Lambda,N}} \) whose holes are guarded by a \text{var} and, moreover, \( MN \) “normalizes”, in the intuitive sense, outside terms guarded by a \text{var}.

### 4.4 Elementary Affine Logic

In this section we give a shallow encoding of Elementary Affine Logic as presented in [2]. This example will exemplify how locks can be used to deal with global syntactic constraints as in the promotion rule of Elementary Affine Logic.

**Definition 4.5 (Elementary Affine Logic [2]).** Elementary Affine Logic can be specified by the following rules:
\[
\begin{array}{lllllllllllllllllll}
\text{Var} & \frac{A \vdash_{\text{EAL}} A}{\text{App}l} & \frac{\Gamma \vdash_{\text{EAL}} \Delta \vdash_{\text{EAL}} A \rightarrow B}{\Delta \vdash_{\text{EAL}} \Gamma \vdash_{\text{EAL}} A \rightarrow B} & \frac{\Gamma \vdash_{\text{EAL}} A}{\text{Abst}} & \frac{\Gamma \vdash_{\text{EAL}} B}{\Gamma \vdash_{\text{EAL}} A \rightarrow B} & \frac{\Gamma \vdash_{\text{EAL}} A \rightarrow B}{\text{Contr}} & \frac{\Gamma \vdash_{\text{EAL}} A \rightarrow B}{\text{Weak}} \end{array}
\]

**Definition 4.6** (LLF, signature \(\Sigma_{\text{EAL}}\) for Elementary Affine Logic).

- \(o : \text{Type}\)  
- \(T : o \rightarrow \text{Type}\)  
- \(V : o \rightarrow \text{Type}\)  
- \(\text{–} : o \rightarrow o \rightarrow o\)  
- \(! : o \rightarrow o\)  
- \(c_{\text{appl}} : \Pi A, B : o. \ T(A) \rightarrow T(A \rightarrow B) \rightarrow T(B)\)  
- \(c_{\text{val}} : \Pi A : o. \ V(A) \rightarrow T(!A)\)  
- \(c_{\text{abstr}} : \Pi A, B : o. \ \Pi x : (T(A) \rightarrow T(B)) \rightarrow \bigotimes^L x, T(A) \rightarrow T(B)[T(A \rightarrow B)]\)  
- \(c_{\text{promV}_1} : \Pi A, B : o. \ \Pi x : (T(A \rightarrow B)) \rightarrow \bigotimes^C x, T(A \rightarrow B)[T(!A) \rightarrow V(B)]\)  
- \(c_{\text{promV}_2} : \Pi A, B : o. \ \Pi x : (\vdash) \rightarrow \bigotimes^C x, V(A \rightarrow B)[T(!A) \rightarrow V(B)]\)

where \(o\) is the type of propositions, \(\rightarrow\) and \(!\) are the obvious syntactic constructors, \(T\) is the basic judgement, and \(V(\cdot)\) is an auxiliary judgement. The predicates involved in the locks are defined as follows:

- **Light** \((\Gamma \vdash_{\Sigma_{\text{EAL}}} x \Leftarrow T(A) \rightarrow T(B))\) holds if \(A\) is not of the shape \(!A\) then the bound variable of \(x\) occurs at most once in the normal form of \(x\).
- **Closed** \((\Gamma \vdash_{\Sigma_{\text{EAL}}} x \Leftarrow T(A))\) holds if the skeleton of \(x\) contains only free variables of type \(o\), i.e. no variables of type \(T(B)\), for any \(B : o\).

A few remarks are mandatory. The promotion rule in [2] is in effect a family of natural deduction rules with a growing number of assumptions. Our encoding achieves this via the auxiliary judgement \(V(\cdot)\), the effect of which is self-explanatory. Adequacy for this signature can be achieved only in the format of [13], namely:

**Theorem 4.3** (Adequacy for Elementary Affine Logic). if \(A_1, \ldots, A_n\) are the atomic formulas occurring in \(B_1, \ldots, B_m, A\), then \(B_1 \ldots B_m \vdash_{\text{EAL}} A\) iff there exists \(M\) and \(A_1 : o, \ldots, A_n : o, x_1 : T(B_1), \ldots, x_m : T(B_m) \vdash_{\Sigma_{\text{EAL}}} M \Leftarrow T(A)\) (where \(A\) and \(B_i\) represent the encodings of, respectively, \(A\) and \(B_i\) in LLF, for \(1 \leq i \leq m\)) and all variables \(x_1 \ldots x_m\) occurring more than once in \(M\) have type of the shape \(T(B_i) \equiv T(!C_i)\) for some suitable formula \(C_i\).

The check on the context of the Adequacy Theorem is external to the system LLF, but this is in the nature of results which relate internal and external concepts. For example, the very concept of LLF context, which appears in any adequacy result, is external to LLF. Of course, this check is internalized if the term is closed.

### 4.5 Square roots of natural numbers in CLLF

It is well-known that logical frameworks based on Constructive Type Theory do not permit definitions of non-terminating functions (i.e., all the functions one can encode in such frameworks are total). One interesting example of CLLF system is the possibility of reasoning about partial functions by delegating their computation to external oracles, and getting back their possible outputs, via the lock-unlock mechanism of CLLF.

For instance, we can encode natural numbers and compute their square roots by means of the following signature \((x, y)\) denotes the encoding of pairs, whose type is denoted by \(\sigma \times \tau\), and \(\text{fst}\) and \(\text{snd}\) are the first and second projections, respectively):

- \(\text{nat}: \text{type}\)  
- \(0: \text{nat}\)  
- \(\text{S}: \text{nat} \rightarrow \text{nat}\)  
- \(\text{plus}: \text{nat} \rightarrow \text{nat} \rightarrow \text{nat}\)  
- \(\text{minus}: \text{nat} \rightarrow \text{nat} \rightarrow \text{nat}\)  
- \(\text{mult}: \text{nat} \rightarrow \text{nat} \rightarrow \text{nat}\)  
- \(\text{sqroot}: \text{nat} \rightarrow \text{nat}\)  
- \(\text{sqrt}: \Pi x: \text{nat} \Rightarrow \text{nat} \times \sigma[(\text{eval} (\text{sqroot} x) (\text{fst} y))]\)
Gluing together Proof Environments: CLLF $\&$ CLLF $\forall$

where \text{eval} represents the usual evaluation predicate, the variable \( y \) is a pair and

\[
\sigma \equiv (\text{eval} (\text{plus} (\text{minus} x (\text{mult} z z)) (\text{minus} (\text{mult} z z) x) 0))
\]

and \( SQRT(\Gamma \vdash y \Leftarrow \text{nat} \times \sigma) \) holds if and only if the first projection of \( y \) is the minimum number \( N \) such that \( (x - N \times N) + (N \times N - x) = 0 \), where \( + \) and \( * \) are represented by \text{plus} and \text{mult}, while \( - \) (represented by \text{minus} in our signature) is defined as follows:

\[
x - y = \begin{cases} x - y & \text{if } x \geq y \\ 0 & \text{otherwise} \end{cases}
\]

Thus, the specification of \text{sqrt} is not explicit in CLLF $\forall$, since it is implicit in the definition of \( SQRT \).

5 Related work

Building a universal framework with the aim of “gluing” different tools and formalisms together is a longstanding goal that has been extensively explored in the inspiring work on Logical Frameworks by \[4, 26, 32, 6, 25, 27, 28, 16\]. Moreover, the appealing monadic structure and properties of the lock/unlock mechanism go back to Moggi’s notion of computational monads \[24\]. Indeed, our system can be seen as a generalization to a family of dependent lax operators of Moggi’s \textit{partial} $\lambda$-calculus \[23\] and of the work carried out in \[7, 22\] (which is also the original source of the term “lax”). A correspondence between lax modalities and monads in functional programming was pointed out in \[11\]. On the other hand, although the connection between constraints and monads in logic programming was considered in the past, e.g., in \[25, 9, 8\], to our knowledge, our systems are the first attempt to establish a clear correspondence between side conditions and monads in a \textit{higher-order dependent-type theory} and in logical frameworks. Of course, there are a lot of interesting points of contact with other systems in the literature which should be explored. For instance, in \[25\], the authors introduce a contextual modal logic, where the notion of context is rendered by means of monadic constructs. We only point out that, as we did in our system, they could have also simplified their system by doing away with the \texttt{let} construct in favor of a deeper substitution. Schröder-Heister has discussed in a number of papers, see e.g. \[31, 30\], various restrictions and side conditions on rules and on the nature of assumptions that one can add to logical systems to prevent the arising of paradoxes. There are some potential connections between his work and ours. It would be interesting to compare his requirements on side conditions being “closed under substitution” to our notion of \textit{well-behaved} predicate. Similarly, there are commonalities between his distinction between \textit{specific} and \textit{unspecific} variables, and our treatment of free variables in well-behaved predicates.

References


A  Fitch Set Theory

Definition A.1 (Fitch Prawitz Set Theory). The full system of Fitch (see [29]), as presented by Prawitz is defined as follows:

\[
\frac{\Gamma, A \vdash_{\text{FPST}} B}{\Gamma \vdash_{\text{FPST}} A \supset B} \quad (\supset I) \quad \frac{\Gamma \vdash_{\text{FPST}} A \quad \Gamma, A \vdash_{\text{FPST}} B}{\Gamma \vdash_{\text{FPST}} A \supset B} \quad (\supset E)
\]

\[
\frac{\Gamma \vdash_{\text{FPST}} A}{\Gamma \vdash_{\text{FPST}} A \land B} \quad (\land I) \quad \frac{\Gamma \vdash_{\text{FPST}} A \quad \Gamma \vdash_{\text{FPST}} A \land B}{\Gamma \vdash_{\text{FPST}} A} \quad (\land E)
\]

\[
\frac{\Gamma \vdash_{\text{FPST}} A}{\Gamma \vdash_{\text{FPST}} A \lor B} \quad (\lor I) \quad \frac{\Gamma \vdash_{\text{FPST}} B}{\Gamma \vdash_{\text{FPST}} A \lor B} \quad \frac{\Gamma \vdash_{\text{FPST}} A \quad \Gamma \vdash_{\text{FPST}} B}{\Gamma \vdash_{\text{FPST}} A \lor B} \quad (\lor E)
\]

\[
\frac{\Gamma \vdash_{\text{FPST}} A}{\Gamma \vdash_{\text{FPST}} \exists x A} \quad (\exists I) \quad \frac{\Gamma \vdash_{\text{FPST}} A}{\Gamma \vdash_{\text{FPST}} \exists x A} \quad \frac{\Gamma, A[a/x] \vdash_{\text{FPST}} B}{\Gamma \vdash_{\text{FPST}} B} \quad (\exists E)
\]

\[
\frac{\Gamma \vdash_{\text{FPST}} \lambda x A}{\Gamma \vdash_{\text{FPST}} A} \quad (\lambda I) \quad \frac{\Gamma, \neg A \vdash_{\text{FPST}} \lambda x A}{\Gamma \vdash_{\text{FPST}} A} \quad (\lambda C)
\]

As noticed in [29], negation in Fitch’s system is usually defined in a constructive way as follows:

\[
\frac{\Gamma \vdash_{\text{FPST}} \neg A}{\Gamma \vdash_{\text{FPST}} \neg (A \& B)} \quad (\neg \& I) \quad \frac{\Gamma \vdash_{\text{FPST}} B}{\Gamma \vdash_{\text{FPST}} \neg (A \& B)} \quad (\neg \& 2)
\]

\[
\frac{\Gamma \vdash_{\text{FPST}} A \quad \Gamma \vdash_{\text{FPST}} \neg B}{\Gamma \vdash_{\text{FPST}} A \supset B} \quad (\supset I) \quad \frac{\Gamma \vdash_{\text{FPST}} A \quad \Gamma \vdash_{\text{FPST}} B}{\Gamma \vdash_{\text{FPST}} A \supset B} \quad (\supset E)
\]

\[
\frac{\Gamma \vdash_{\text{FPST}} \neg A}{\Gamma \vdash_{\text{FPST}} \neg \forall x A} \quad (\neg \forall I) \quad \frac{\Gamma \vdash_{\text{FPST}} \neg \exists x A}{\Gamma \vdash_{\text{FPST}} \forall x A} \quad \frac{\Gamma, \neg A[a/x] \vdash_{\text{FPST}} B}{\Gamma \vdash_{\text{FPST}} B} \quad (\neg \forall E)
\]