Higher-order Representation of Substructural Logics

Karl Crary
Carnegie Mellon University

Follow this and additional works at: http://repository.cmu.edu/compsci
Higher-order Representation of Substructural Logics

Karl Crary
Carnegie Mellon University

Abstract

We present a technique for higher-order representation of substructural logics such as linear or modal logic. We show that such logics can be encoded in the (ordinary) Logical Framework, without any linear or modal extensions. Using this encoding, metatheoretic proofs about such logics can easily be developed in the Twelf proof assistant.

1 Introduction

The Logical Framework (or LF) [6] provides a powerful and flexible framework for encoding deductive systems such as programming languages and logics. LF employs an elegant account of binding structure by identifying object-language variables with LF variables, object-language contexts with (fragments of) the LF context, and object-language binding occurrences with LF lambda abstraction. This account of binding, often called higher-order abstract syntax [12], automatically handles most operations that pertain to binding, including alpha-equivalence, substitution, and variable-freshness conventions [3].

Since the object-language context is maintained implicitly, as part of the built-in LF context, the structural properties of LF contexts (such as weakening and contraction) automatically apply to the object language as well. Ordinarily this is desirable, but it poses a problem for encoding substructural logics that do not possess those properties. For example, linear logics (by design) satisfy neither weakening nor contraction, so it would seem that they cannot be encoded in LF.

One solution to this problem is to extend LF with linear features. Linear LF [4] extends LF with linear assumptions and connectives. This provides the ability to encode linear logics. However, linearity has yet to be implemented in Twelf [13], the proof assistant that implements LF, in part due to unresolved complications that linearity creates in its metalogical apparatus. Consequently, Linear LF is not currently an option for those engaged in formalizing metatheory. Moreover, Linear LF does not give us any assistance with other substructural logics, such as affine, strict, or modal logic.

Another option is to break with standard LF practice and model object-language contexts explicitly [5]. Explicit contexts can be reconciled with higher-order abstract syntax, thereby retaining many of the benefits of LF. Once contexts are explicit, it is easy to state inference rules that handle the context in an appropriate way for a substructural logic. However, the explicit context method is clumsy to work with and sacrifices some of the advantages of LF. For example, although substitution is still free (since the syntax of terms is unchanged), the substitution lemma is not. The explicit context method is typically used internally within a proof, rather than in the “official” formalization of a logic.

In this paper we advocate a more general and workable approach in which we look at substructural logic from a slightly different perspective. Rather than viewing a substructural logic from the perspective of its contexts (that is, collections of assumptions), we suggest it is profitable to look at it from the perspective of its individual assumptions.

The essence of linear logic is not that type-checking splits the context when it checks a (multiplicative) term with multiple subterms. The essence of linear logic is that an assumption is used exactly once. The latter property can be stated on an assumption-by-assumption basis, without reference to contexts. Thus, wherever an assumption is introduced, as part of the typing rule that introduced it, we can check that that assumption is used linearly.

At first glance, it might appear that linearity must be a meta-judgement, tracing the use of assumptions throughout a typing derivation. That would make it very awkward to use in practice. Fortunately, however, to check the linear use of assumptions, we need look only at proof terms; there is no need to examine typing derivations.

The idea of linearity as a judgement over proof terms dates to the early days of LF. Avron et al. [2, 1] suggested that linearity can be expressed by imposing a lattice structure on proof terms and defining linear proof terms as those that are strict and distributive, when viewed as a function of their linear variables.

In this paper, we suggest a simpler formulation of linearity, based on tracking variables through the proof terms of linear logic. This allows for a clean, practical definition of linearity.

We express linear logic using two judgements, the usual typing judgement:

\[ \text{of} : \text{term} \rightarrow \text{tp} \rightarrow \text{type}. \]

and a linearity judgement:

\[ \text{linear} : (\text{term} \rightarrow \text{term}) \rightarrow \text{type}. \]
The judgement \( \text{linear}(\lambda x.Mx) \) should be read as “the variable \( x \) is used linearly (i.e., is used exactly once) in \( Mx \).”

In this paper, we illustrate the use of a substructural judgement (such as \( \text{linear} \)) in three settings: linear logic, dependently typed linear logic, and judgemental modal logic [11]. Many other substructural logics including affine logic and strict logic can be handled analogously. Some others, such as ordered logic [15, 14], cannot, because the rules of the logic make it impossible to handle assumptions independently. We briefly discuss the latter in Section 5.

The full Twelf development can be found on-line at:


In our discussion, we assume familiarity with the Logical Framework, and with linear and modal logic. Some familiarity with Twelf may also be helpful. The sections on adequacy are technical, but the remainder of the paper should be accessible to the casual practitioner.

2 Linear Logic

We begin by representing the syntax of linear logic in the usual fashion. The LF encoding, with the standard on-paper notation written alongside it for reference, is shown in Figure 1. The type \( \text{atom} \) ranges over a fixed set of atomic propositions.

On paper, we represent linear logic with the typing judgment \( \Gamma; \Delta \vdash M : A \). In this, the first context, \( \Gamma \), represents the unrestricted context (i.e., truth), and the second context, \( \Delta \), represents the linear context (i.e., resources). To simplify the notation, we adopt the convention that the linear context is unordered. Thus \( (\Delta, \Delta') \) refers to a context that can be split into two pieces \( \Delta \) and \( \Delta' \) that may possibly be interleaved. We also adopt the convention that all the variables appearing in either context must be distinct.

The encoding of the static semantics, as discussed previously, is given by two judgements:

\[
\begin{align*}
\text{of} & : \text{term} \rightarrow \text{tp} \\
\text{linear} & : (\text{term} \rightarrow \text{term}) \rightarrow \text{tp}
\end{align*}
\]

We read “of \( M A \)” as “\( M \) is of type \( A \),” and we read “\( \text{linear} \) (\( x:\text{term} \) \( M x \))” as “\( x \) is used linearly in \( (M x) \).” Note that [\( x:\text{term} \)] is Twelf’s concrete syntax for LF lambda abstraction\(^2\) \( \lambda x.\text{term} \). Twelf can usually infer the domain type, leaving just \( [x] \).

We proceed rule-by-rule to show the encoding of the static semantics.

Variables The rule for linear variables states that a linear variable may be used provided there are no other linear variables in scope:

\[
\Gamma; x:A \vdash x : A
\]

There is no typing rule for variables in the encoding: that is handled automatically by higher-order representations. However, there is a linearity rule that states that \( x \) is linear in \( x \):

\[\text{linear/var} : \text{linear} ([x] x).\]

The rule for unrestricted variables states that an unrestricted variable may be used provided there any no linear variables in scope:

\[
\begin{align*}
\Gamma(x) & = A \\
\Gamma; e \vdash x : A
\end{align*}
\]

As with linear variables, there is no typing rule for unrestricted variables in the encoding. There is also no linearity rule for unrestricted variables.

Linear implication The introduction rule for linear implication is:

\[
\begin{align*}
\Gamma; (\Delta, x:A) \vdash M : B \\
\Gamma; \Delta \vdash \lambda x. M : A \multimap B
\end{align*}
\]

This is encoded using two rules:
of/llam
: of (llam ([x] M x)) (lolli A B)
<- (({x:term} of x A -> of (M x) B)
<- linear ([x] M x).

linear/llam
: linear ([y] llam ([x] M y x))
<- ({x:term} linear ([y] M y x)).

Note that \{x:term\} is Twelf’s concrete syntax for the dependent function space (\Pi_{x:term}. This again, Twelf can usually infer the domain type, leaving just \{x\}.

The typing rule has the usual typing premise, plus a second premise that requires that the argument be used linearly in the body. The linearity rule says that a variable y is linear in a function (llam ([x] M y x)) if it is linear in its body (M y x) for any choice of x.

The elimination rule splits the linear context between the function and argument:

\[
\Gamma; \Delta \vdash M : A \rightarrow B \quad \Gamma; \Delta' \vdash N : A \\
\Gamma; (\Delta, \Delta') \vdash MN : B
\]

This is encoded using three rules:

of/lapp
: of (lapp M N) B
<- of M (lolli A B)
<- of N A.

linear/lapp1
: linear ([x] lapp (M x) N)
<- linear ([x] M x).

linear/lapp2
: linear ([x] lapp M (N x))
<- linear ([x] N x).

The typing rule is standard. There are two linearity rules, one for each way a linear variable might be used. The first linearity rule says that x is linear in (lapp (M x) N) if it is linear in (M x) and does not appear in N. (Since implicitly bound meta-variables such as M and N are quantified on the outside, stating N without a dependency on x means that N is closed with respect to x.) The second linearity rule provides the symmetric case.

Multiplicative conjunction
The introduction rule for tensor is:

\[
\Gamma; \Delta \vdash M : A \quad \Gamma; \Delta' \vdash N : B \\
\Gamma; (\Delta, \Delta') \vdash MN : A \otimes B
\]

This is encoded using three rules, in a similar fashion to function application:

of/tpair
: of (tpair M N) (tensor A B)
<- of M A
<- of N B.

linear/tpair1
: linear ([x] tpair (M x) N)
<- linear ([x] M x).

linear/tpair2
: linear ([x] tpair M (N x))
<- linear ([x] N x).

The elimination rule is:

\[
\Gamma; \Delta \vdash M : A \otimes B \\
\Gamma; (\Delta', x:A, y:B) \vdash N : C \\
\Gamma; (\Delta, \Delta') \vdash letx@y = M in N : C
\]

In the encoding, the typing rule requires that x and y are linear in N. As in previous cases where the linear context is split, there are two linearity rules depending on whether a linear variable is used in the let-bound term or the body:

of/lett
: of (lett M ([x] [y] N x y)) C
<- of M (tensor A B)
<- (({x} of x A
-> {y} of y B -> of (N x y) C)
<- (({x} linear ([x] N x y))
<- (({x} linear ([y] N x y)).

linear/lett1
: linear ([z] lett (M z) ([x] [y] N x y))

linear/lett2
: linear ([z] lett M ([x] [y] N z x y))
<- (({x} {y} linear ([z] N z x y)).

Additive conjunction
The introduction rule for “with” does not split the context:

\[
\Gamma; \Delta \vdash M : A \\
\Gamma; \Delta \vdash N : B \\
\Gamma; (\Delta, \Delta') \vdash \langle M, N \rangle : A \& B
\]

In the encoding, there is one linearity rule, requiring that linear variables be linear in both constituents of the pair:

of/pair
: of (pair M N) (with A B)
<- of M A
<- of N B.

linear/pair
: linear ([x] pair (M x) (N x))
<- linear ([x] M x)
<- linear ([x] N x).

The elimination rules are straightforward:

\[
\Gamma; \Delta \vdash M : A \\
\Gamma; \Delta \vdash \pi_1 M : A \\
\Gamma; \Delta \vdash \pi_2 M : B
\]

of/pi1
: of (pi1 M) A
<- of M (with A B).

of/pi2
: of (pi2 M) B
<- of M (with A B).

linear/pi1
: linear ([x] pi1 (M x))
<- linear ([x] M x).

linear/pi2
: linear ([x] pi2 (M x))
<- linear ([x] M x).
Disjunction

The introduction rules for plus are straightforward:

\[
\begin{align*}
\Gamma; \Delta \vdash M : A & \quad \Gamma; \Delta \vdash M : B \\
\Gamma; \Delta \vdash \text{in1}_M : A + B & \quad \Gamma; \Delta \vdash \text{in2}_M : A + B
\end{align*}
\]

\[
\begin{align*}
of/\text{in1} & : \text{of} (\text{in1}_M) (\text{plus} A B) \\
of/\text{in2} & : \text{of} (\text{in2}_M) (\text{plus} A B) \\
\text{linear/in1} & : \text{linear} ([x] \text{in1}_M (M x)) \\
\text{linear/in2} & : \text{linear} ([x] \text{in2}_M (M x)).
\end{align*}
\]

The elimination rule splits the context into two pieces, one for the discriminant and one used by both arms:

\[
\begin{align*}
\Gamma; \Delta \vdash M : A + B & \\
\Gamma; (\Delta', x:A) \vdash N_1 : C & \\
\Gamma; (\Delta', x:B) \vdash N_2 : C \\
\Gamma; (\Delta, \Delta') \vdash \text{case}(M, x. N_1, x. N_2) : C
\end{align*}
\]

Exponentiation

The introduction rule for exponentiation requires that the linear context be empty:

\[
\begin{align*}
\Gamma; \epsilon \vdash M : A & \\
\Gamma; \epsilon \vdash !M : !A
\end{align*}
\]

In the encoding, this means there is no linearity rule, since variables cannot be linear in exponents:

\[
\begin{align*}
of/\text{bang} & : \text{of} (\text{bang} M) (! A) \\
of/\text{letb} & : \text{of} (\text{letb} M ([x] N x)) B \\
\text{linear/letb1} & : \text{linear} ([y] \text{letb} (M y) N) \\
\text{linear/letb2} & : \text{linear} ([y] \text{letb} M ([x] N y x)) \\
\end{align*}
\]

Units

The unit for tensor is 1:

\[
\begin{align*}
\Gamma; \Delta \vdash \ast : 1 & \\
\Gamma; (\Delta, \Delta') \vdash \text{let} \ast = M \text{ in } N : C
\end{align*}
\]

The encoding is straightforward, with no linearity rule for introduction since variables cannot be linear in *:

\[
\begin{align*}
of/\text{star} & : \text{of} \text{star} \text{ one}. \\
of/\text{leto} & : \text{of} (\text{leto} M N) C \\
\text{linear/leto1} & : \text{linear} ([x] \text{leto} (M x) N) \\
\text{linear/leto2} & : \text{linear} ([x] \text{leto} M ([x] N x)) \\
\end{align*}
\]

The unit for “with”, ⊤, is more interesting. It stands for an unknown collection of resources, and consequently has an introduction form but no elimination form:

\[
\begin{align*}
of/unit & : \text{of} \text{unit} \text{ top}. \\
\text{linear/unit} & : \text{linear} ([x] \text{unit}).
\end{align*}
\]

The unit for plus, 0, represents falsehood. Accordingly, it has an elimination form but no introduction form. The elimination form behaves a little bit like \(\ast\); any resources not used to prove 0 may be discarded:

\[
\begin{align*}
of/\text{any} & : \text{of} (\text{any} M) T \\
\text{linear/any1} & : \text{linear} ([x] \text{any} (M x)) \\
\text{linear/any2} & : \text{linear} ([x] \text{any} M).
\end{align*}
\]
Note that it is tempting but incorrect to simplify this to the single rule:

\[
\text{linear/any-wrong} : \text{linear (}[x]\text{ any (M x))}. 
\]

That rule would allow x to be used multiple times in (M x), which is not permitted. It would be tantamount to moving the entire linear context into the unrestricted context, rather than merely discarding any unused resources.

### 2.1 Adequacy

It seems intuitively clear that the preceding is a faithful representation of linear logic. We wish to go further and make the correspondence rigorous, following the adequacy argument of Harper et al. [6]. Adequacy establishes an isomorphism between the object language (linear logic in this case) and its encoding in LF. As usual, an isomorphism is a bijection that respects the relevant operations.

For syntax, the only primitively meaningful operation is substitution. (Other operations are given by defined semantics.) Thus, an isomorphism for syntax is a bijective translation that respects substitution. Our translation for syntax (written \(-\) ) is standard, so we will omit the obvious details of its definition and simply state its adequacy theorem for reference:

**Definition 2.1** Translation of variable sets is defined:

\[
\{x_1, \ldots, x_n\} = x_1: \text{term}, \ldots, x_n: \text{term} 
\]

**Theorem 2.2 (Syntactic adequacy)**

1. Let Type be the set of linear logic types. Then there exists a bijection \(-\) between Type and LF canonical forms \(P\) such that \(\vdash_{LF} P : \text{tp}\). (Variables cannot appear within types, so there is no substitution to respect.)

2. Let \(S\) be a set of variables and let \(\text{Term}_S\) be the set of linear logic terms whose free variables are contained in \(S\). Then there exists a bijection \(-\) between \(\text{Term}_S\) and LF canonical forms \(P\) such that \(\vdash_{LF} P : \text{term}\). Moreover, \(-\) respects substitution: \(\{M/x\}N = \{M\}N/\{x\}\).

For semantic adequacy, we wish to establish a bijective translation between typing derivations and LF canonical forms. The usual statement of adequacy for typing is something to the effect of:

**Definition 2.3** Translation of contexts is defined:

\[
\{x_1: A_1, \ldots, x_n: A_n\} = x_1: \text{term}, dx_1: \text{of } x_1: A_1, \ldots, x_n: \text{term}, dx_n: \text{of } x_n: A_n 
\]

**Non-Theorem 2.4** There exists a bijection between derivations of the judgement \(\Gamma \vdash M : A\) and LF canonical forms \(P\) such that \(\vdash_{LF} P : \text{of } \Gamma M\).

Unfortunately, this simple statement of adequacy does not work in the presence of linearity. Consider the judgement \(\epsilon; x: A \vdash \langle \rangle \otimes \langle \rangle : T \otimes T\). It has two derivations, depending on which conjunct is chosen to consume the assumption:

\[
\begin{align*}
\epsilon; x: A &\vdash \langle \rangle : T \\
\epsilon; \epsilon &\vdash \langle \rangle : \top \otimes T \\
\epsilon; \epsilon &\vdash \langle \rangle : T \otimes \top \otimes T \\
\epsilon; x: A &\vdash \langle \rangle : \top \otimes \top \\
\end{align*}
\]

However, the LF type corresponding to that judgement,

\[
\{x: \text{term}\} \text{ of } x \text{ (atomic a)} \\
\rightarrow \text{ of } (\text{tpair unit unit}) \text{ (tensor top top)}
\]

contains only one canonical form, namely:

\[
\{x: \text{term}\} \text{ [dx of } x \text{ (atomic a)]} \\
\text{of/tpair of/unit of/unit}
\]

So linear-logic typing derivations are not in bijection with the LF encoding of typing in general. Our isomorphism must take linearity into account, and not only where linearity is a premise of a typing rule.

Consequently, we establish a correspondence between each linear-logic typing derivation on the one hand, and an LF proof of typing paired with a collection of LF proofs of linearity on the other. Alas, this is notionally awkward when compared with the usual adequacy theorem.

**Definition 2.5** An encoding structure for \(\Gamma; \Delta \vdash A\) is a pair \((P, H)\) of an LF canonical form \(P\) and a finite mapping \(H\) from variables to LF canonical forms, such that:

- \(\Gamma, \Delta \vdash \text{of } M : A\), and
- \(\text{Domain}(H) = \text{Domain}(\Delta)\), and
- For each variable \(y\) in \(\text{Domain}(\Delta)\), \(\exists S_y \vdash_{LF} H(y) : \text{linear } (\text{of } y : \text{term}) \Gamma M\), where \(S_y = \text{Domain}(\Gamma, \Delta) \setminus \{y\}\).

**Theorem 2.6 (Semantic adequacy)** There exists a bijection \(-\) between derivations of the judgement \(\Gamma; \Delta \vdash M : A\) and encoding structures for \(\Gamma; \Delta \vdash M : A\).

Proving adequacy is typically straightforward but tedious once it is stated correctly. The same is true here, but the tedium is a bit more pronounced because of the need to manipulate encoding structures, rather than just canonical forms. We give a few cases by way of example:

**Proof Sketch**

First, by induction on derivations, we construct the translation and show it is type correct.

- Suppose \(\nabla\) is the derivation:

\[
\Gamma; x: A \vdash x : A 
\]

Then \(\nabla \equiv (dx, \{x \mapsto \text{linear/var}\})\).

- Suppose \(\nabla\) is the derivation:

\[
\Gamma (x) \equiv A \\
\Gamma; \epsilon \vdash x : A 
\]

Then \(\nabla \equiv (dx, \emptyset)\).
• Suppose \( \nabla \) is the derivation:

\[
\begin{align*}
\nabla_1 \\
\vdots \\
\Gamma; (\Delta, x:A) \vdash M : B \\
\Gamma; \Delta \vdash \lambda x. M : A \rightarrow B
\end{align*}
\]

Let \( \nabla_1 = (p_1, H_1) \). By induction, \((p_1, H_1)\) is an encoding structure for \( \Gamma; (\Delta, x:A) \vdash M : B \), so:

\[
\Gamma; \Delta \vdash x : \text{term}, dx: (\forall \lambda \in \text{Type} . x \in A \rightarrow B)
\]

and

\[
\text{Domain}(\Gamma, \Delta) \vdash \text{linear}(\lfloor x \rfloor \mapsto M^\gamma)
\]

Therefore:

\[
(\forall \lambda \in \text{Type} . x \in A \rightarrow B) \quad \quad \Gamma; \Delta \vdash \text{linear}(\lfloor x \rfloor \mapsto M^\gamma)
\]

where for each \( y \in \text{Domain}(\Delta) \), \( H(y) \overset{\text{def}}{=} \text{linear}(\lfloor x \rfloor \mapsto H_1(x)) \).

• Suppose \( \nabla \) is the derivation:

\[
\begin{align*}
\nabla_1 \\
\vdots \\
\Gamma; \Delta_1 \vdash M : A \rightarrow B \\
\Gamma; \Delta_2 \vdash N : A \\
\Gamma; (\Delta_1, \Delta_2) \vdash MN : B
\end{align*}
\]

Let \( \nabla_1 = (p_1, H_1) \) and let \( \nabla_2 = (p_2, H_2) \). By induction, \((p_1, H_1)\) is an encoding structure for \( \Gamma; \Delta_1 \vdash M : A \rightarrow B \) and \((p_2, H_2)\) is an encoding structure for \( \Gamma; \Delta_2 \vdash N : A \). Let \( y \in \text{Domain}(\Delta_1, \Delta_2) \) be arbitrary. Let \( S = \text{Domain}(\Gamma) \) and \( S_i = \text{Domain}(\Delta_i) \). Then either \( y \in S_1 \) and \( y \not\in S_2 \) or vice versa. Suppose the former. Then:

\[
\begin{align*}
\nabla_1 \\
\vdots \\
\Gamma; \Delta_1 \vdash M : A \rightarrow B \\
\Gamma; \Delta_2 \vdash N : A \\
\Gamma; (\Delta_1, \Delta_2) \vdash MN : B
\end{align*}
\]

\[
\nabla_2
\]

It remains to show that \( \nabla \) is a bijection. To do so, we exhibit an inverse \( \iota \). The interesting cases are those that split the context. We give the application case as an example.

Suppose \((\text{of/lapp} \ P_1, H_1')\) is an encoding structure for \( \Gamma; \Delta \vdash O : B' \). Then \( O \) has the form \( M'N' \), and \( \Gamma; \Delta \vdash M' \rightarrow A' \rightarrow B' \), and \( \Gamma; \Delta \vdash LF P_2 : \text{of} \ M' \rightarrow A' \rightarrow B' \).

We must sort \( \Delta \) into two pieces. Define:

\[
\begin{align*}
\Delta_1 &= \{ (y:C) \in \Delta \mid \exists R. H'(y) = \text{linear/lapp} 1 \} \\
\Delta_2 &= \{ (y:C) \in \Delta \mid \exists R. H'(y) = \text{linear/lapp} 2 \} \\
H_1' &= \{ y \mapsto R | H'(y) = \text{linear/lapp} 1 \} \\
H_2' &= \{ y \mapsto R | H'(y) = \text{linear/lapp} 2 \}
\end{align*}
\]

Note that \( \Delta = \Delta_1, \Delta_2 \). Also note that no variable in \( \Delta_1 \) appears free in \( N' \) or vice versa. Therefore it is easy to show that no assumption in \( \nabla_1 \) appears free in \( P_2 \) and vice versa. Hence \( \Gamma; \Delta_1 \vdash LF P_1 : \text{of} \ M' \rightarrow A' \rightarrow B' \) and \( \Gamma; \Delta_2 \vdash LF P_2 : \text{of} \ N' \rightarrow A' \). Also, \( \text{Domain}(H_1') = \text{Domain}(\Delta_1) \).

Therefore \((p_2, H_1')\) is an encoding structure for \( \Gamma; \Delta_1 \vdash M' : A' \rightarrow B' \) and \((p_2, H_2')\) is an encoding structure for \( \Gamma; \Delta_2 \vdash N' : A' \). Let \( \nabla_2 = \iota(p_2, H_1') \). Then either \( \nabla_2 \) is a derivation of \( \Gamma; \Delta_1 \vdash \text{linear}(\lfloor x \rfloor \mapsto B') \) and \( \nabla_2 \), or \( \nabla_2 \) is a derivation of \( \Gamma; \Delta_2 \vdash \text{linear}(\lfloor x \rfloor \mapsto A') \). So \( \iota(P_2, P_1, H') \) be the derivation:

\[
\begin{align*}
\nabla_1 \\
\vdots \\
\Gamma; \Delta_1 \vdash M : A \rightarrow B \\
\Gamma; \Delta_2 \vdash N : A \\
\Gamma; (\Delta_1, \Delta_2) \vdash MN : B
\end{align*}
\]

We can show, by induction over LF canonical forms, that \( \iota \) is fully defined over encoding structures. It is easy to verify that \( \nabla \) and \( \iota \) are inverses. Therefore \( \nabla \) is a bijection. \( \square \)

When the linear context is empty, the \( H \) portion of an encoding structure is empty, and we recover the usual notion of adequacy:

**Corollary 2.7** There exists a bijection between derivations of the judgement \( \Gamma; e \vdash \text{of} \ M \rightarrow \text{type} \) and LF canonical forms \( P \) such that \( \nabla \) is a bijection.

### 2.2 Metatheory

To demonstrate the practicality of our encoding, we proved the subject reduction theorem in Twelf. We give the definition of reduction in Figure 2. Reduction is encoded with the judgement:

\[
\text{reduce} : \text{term} \rightarrow \text{term} \rightarrow \text{type}.
\]

We will not discuss the encoding of reduction and its adequacy, as they are standard.

We prove subject reduction by a series of four metatheorems. To make the development more accessible to readers not familiar with Twelf’s logic programming notation for proofs, we give those metatheorems in English.

---

4This fact, that non-appearing variables may be omitted from the context, requires a strengthening lemma for LF that is proved by Harper and Pfenning [7, Theorem 6.6].
Lemma 2.8 (Composition of linearity) Suppose the ambient context is made up of bindings of the form \( x: \text{term} \) (and other bindings not subordinate\(^5\) to linear). If linear \((\{x\} M_1 x)\) and linear \((\{x\} M_2 x)\) are derivable, then linear \((\{x\} M_1 M_2 x)\) is derivable.

The next lemma is usually glossed over in proofs on paper:

Lemma 2.9 (Reduction of closed terms) Suppose the ambient context is made up of bindings of the form \( x: \text{term} \) (and other bindings not subordinate to reduce). If \((\{x: \text{term}\} \text{reduce } M_1 (M_2 x))\) is derivable, then there exists \( M_2': \text{term} \) such that \( M_2' = ([_] M_2) \).

Lemma 2.10 (Subject reduction for linear) Suppose the ambient context is made up of bindings of the form \( x: \text{term}, \text{dx:of} \ x A \) (and other bindings not subordinate to reduce or of). If \((\{x: \text{term}\} \text{reduce } M_1 (M_2 x))\) and \((\{x: \text{of} \ x A \to \text{of} \ (M x) B\)\) and linear \((\{x\} M x)\) are derivable, then linear \((\{x\} M' x)\) is derivable.

Proof Sketch
By induction on the first derivation. Cases involving substitution (most of the beta-reduction cases) use Lemma 2.8. Multiple-subterm compatibility cases use Lemma 2.9 to show that reduction of subterms not mentioning a linear variable will not create such a reference.

Theorem 2.11 (Subject reduction for of) Suppose the ambient context is made up of bindings of the form \( x: \text{term}, \text{dx:of} \ x A \) (and other bindings not subordinate to reduce or of). If \( \text{reduce } M M' \) and of \( M T \) are derivable, then of \( M' T \) is derivable.

Proof Sketch
By induction on the first derivation. Cases with linearity premises (reduce/1lam, reduce/relett, and reduce/case) use Lemma 2.10 to show that the linearity premises are preserved by reduction.

Corollary 2.12 If \( \Gamma; \Delta \vdash M : A \) and \( M \rightarrow M' \) then \( \Gamma; \Delta \vdash M' : A \).

Proof
Immediate from Subject Reduction and Adequacy.

3 Dependently Typed Linear Logic

Adding dependent types to linear logic is straightforward syntactically. The revised syntax is shown in Figure 3. We delete atomic propositions, and replace them with constants that take a single term parameter. (That parameter may be a unit or tuple, which provides implicit support for zero or multiple parameters.)

In the static semantics, a new wrinkle arises. Now that terms can appear within types, the typing rules must ensure that linear variables are not used within types. However, a variable can appear within a term's type without appearing in the term itself. This is obvious because our lambda abstractions are unlabelled, but it would still be the case even if all bindings were labeled with types. This is because of the equivalence rule:

\[
\frac{\Gamma; \Delta \vdash M : A \quad \Gamma \vdash A' \text{ type } A \equiv_{\beta} A'}{\Gamma; \Delta \vdash M : A'}
\]

Using the equivalence rule, a term's type can mention any variable in scope.

\[\begin{array}{ll}
\text{tp} & : \text{type}. \\
\text{A} & ::= \\
\text{...} & \\
\text{atomic} : \text{atom} \rightarrow \text{tp}. & a \\
\text{const} : \text{constant} \rightarrow \text{term} \rightarrow \text{tp}. & c(M) \\
\text{pi} & : \text{tp} \rightarrow (\text{term} \rightarrow \text{tp}) \rightarrow \text{tp}. & \Pi x : A. B \\
\text{term} : \text{type}. & M ::= \\
\text{...} & \\
\text{ulam} & : (\text{term} \rightarrow \text{term}) \rightarrow \text{term}. & \lambda x . M \\
\text{uapp} & : \text{term} \rightarrow \text{term} \rightarrow \text{term}. & M \bullet M \\
\end{array}\]
One solution to this problem is to make linearity a judgement over typing derivations, rather than over proof terms. However, that would make linearity a dependently typed meta-judgement, which would be too cumbersome to work with in practice. It is better to maintain linear as a judgement over proof terms.

Instead, we change our view of unrestricted variables. In non-dependently typed linear logic, we viewed unrestrictedness as merely the absence of a linearity restriction. Now we will view unrestrictedness as conferring an affirmative capability; specifically, the capability to appear within types.

We add a new judgement $\textit{unrest}$ that applies to unrestricted variables. We extend that judgement to terms by saying that a term is unrestricted if all its free variables are unrestricted:

$$\text{unrest} : \text{term} \to \text{type}.$$  

- $\text{unrest/lam} : \text{unrest} \ (\lambda \ x \ M) \ \to \ \text{unrest} \ (M\ x).$
- $\text{unrest/lapp} : \text{unrest} \ (\text{lapp} \ M \ N) \ \to \ \text{unrest} \ (M) \ \to \ \text{unrest} \ (N).$

Note that, within the $\text{unrest}$ judgement, all bound variables are taken to be unrestricted, even linear ones.

Only unrestricted terms are permitted to serve as the parameter to a constant. On paper, this is written:

$$c : A \to \text{type} \quad \Gamma; \epsilon \vdash M : A \quad \Gamma \vdash c(M) : \text{type}$$

where we assume some pre-specified collection of axioms of the form $c : A \to \text{type}$. In our encoding, the well-formedness judgement for types is $\text{wf} : \text{tp} \to \text{type}$. The constant rule is written:

$$\text{wf/const} : \text{wf} \ (\text{const} \ C \ M) \ \to \ \text{cparam} \ C \ A \ \to \ \text{of} \ M \ A \ \to \ \text{unrest} \ M.$$

We assume there exists a unique $\text{cparam}$ rule for each axiom $c : A \to \text{type}$. The remaining $\text{wf}$ rules are uninteresting (but note that the rule for $\text{pi}$ introduces an unrestricted variable).

Our existing typing rules must be altered in two ways. First, now that types can be ill-formed, several rules must add a $\text{wf}$ premise. This is straightforward. Second, the rules for the exponential must be rewritten to use the $\text{unrest}$ judgement:

$$\text{of/bang} : \text{of} \ (\text{bang} \ M) \ (1 \ A) \ \to \ \text{of} \ M \ A \ \to \ \text{unrest} \ M.$$

$$\text{of/letb} : \text{of} \ (\text{letb} \ M \ ([x] \ N \ x)) \ B \ \to \ \text{of} \ M \ (1 \ A) \ \to \ ([x] \ \text{of} \ x \ A) \ \to \ \text{unrest} \ x \ \to \ \text{of} \ (N \ x) \ B \ \to \ \text{wf} \ B.$$

We also have the new rules for unrestricted functions and application:

$$\Gamma \vdash A \ \text{type} \quad (\Gamma, x : A) ; \Delta \vdash M : B \quad \Gamma; \Delta \vdash (\lambda x. M) : \Pi x : A . B$$

$$\Gamma; \Delta \vdash M : \Pi x : A . B \quad \Gamma; \epsilon \vdash N : A \quad \Gamma; \Delta \vdash M \ \alpha \ N : [(N/x) B]$$

$$\text{of/ulam} : \text{of} \ (\text{ulam} \ ([x] \ M \ x)) \ (\pi A \ ([x] B \ x)) \ \to \ \text{of} \ A \ \to \ ([x] \ \text{of} \ x \ A) \ \to \ \text{unrest} \ x \ \to \ \text{of} \ (M \ x) \ (B \ x).$$

$$\text{of/uapp} : \text{of} \ (\text{uapp} \ M \ N) \ (B \ N) \ \to \ \text{of} \ M \ (\pi A \ ([x] B \ x)) \ \to \ \text{of} \ N \ A \ \to \ \text{unrest} \ N.$$

$$\text{linear/ulam} : \text{linear} \ ([y] \ \text{ulam} \ ([x] \ M \ y \ x)) \ \to \ ([y] \ \text{linear} \ ([x] \ M \ y \ x)).$$

$$\text{linear/uapp} : \text{linear} \ ([x] \ \text{uapp} \ (M \ x) \ N) \ \to \ \text{linear} \ ([x] \ M \ x).$$

And finally equivalence:

$$\text{of/equiv} : \text{of} \ M \ A' \ \to \ \text{of} \ M \ A \ \to \ \text{wf} \ A' \ \to \ \text{equiv} \ A \ A'.$$

The addition of dependent types complicates the proof of subject reduction in a number of ways, but nearly all are orthogonal to linearity. One issue that does relate to linearity is we require one additional lemma to show that unrestrictedness is preserved by reduction:

**Lemma 3.1 (Subject reduction for unrest)** Suppose the ambient context is made up of bindings of the form $x : \text{term}, \text{ex:unrest} \ x$ and bindings of the form $x : \text{term}$ (and other bindings not subordinate to reduce or unrest). If reduce $M \ M'$ and unrest $M$ are derivable, then unrest $M'$ is derivable.

### 3.1 Adequacy

Adequacy for dependently typed linear logic proceeds in much the same fashion as before. We must make four changes. First, we revise syntactic adequacy of types, now that types are not closed:

**Theorem 3.2 (Syntactic adequacy)**

1. Let $S$ be a set of variables and let $\text{Type}_S$ be the set of linear logic types whose free variables are contained in $S$. Then there exists a bijection $\sim$ between $\text{Type}_S$ and LF canonical forms $P$ such that $\sim S \vdash_{LF} P : \text{tp}$. Moreover, $\sim$ respects substitution: $\sim [M/x] A = \sim [M' /x] A'$.  
2. Let $S$ be a set of variables and let $\text{Term}_S$ be the set of linear logic terms whose free variables are contained in $S$. Then there exists a bijection $\sim$ between $\text{Term}_S$ and LF canonical forms $P$ such that $\sim S \vdash_{LF} P : \text{term}$. Moreover, $\sim$ respects substitution: $\sim [M/x] N \sim [M' /x] N'$. 


Second, we define a translation for unrestricted contexts:

\[
\begin{align*}
\pi x_1 & : A_1, \ldots, x_n : A_n \\
= & \pi x_1 : \text{term}, dx_1 : \text{of} x_1 \cdot A_1 \cdot \text{ex}, \ldots, x_n : \text{term}, dx_n : \text{of} x_n \cdot A_n \cdot \text{ex, unrest} \cdot x_n
\end{align*}
\]

and we alter the first clause of the definition of encoding structures to read:

\[
\pi \Gamma, \pi \Delta \vdash_{LF} P : \text{of} \pi \Gamma \Rightarrow \pi \Delta A
\]

Third, we state adequacy for typing and for well-formedness of types simultaneously:

**Theorem 3.3 (Semantic adequacy)**

1. There exists a bijection \( \pi \rightarrow - \) between derivations of the judgement \( \Gamma; \Delta \vdash M : A \) and encoding structures for \( \Gamma; \Delta \vdash M : A \).

2. There exists a bijection \( \pi \rightarrow - \) between derivations of the judgement \( \Gamma \vdash A \) type and LF canonical forms \( P \) such that \( \pi \Gamma \vdash_{LF} P : \text{unrest} \pi \Gamma A \).

Fourth, we state a new lemma to deal with unrest derivations:

**Lemma 3.4**

1. Suppose \( \Gamma; \Delta \vdash M : A \). Then there exists a unique LF canonical form \( P \) such that \( \pi \Gamma, \pi \Delta \vdash_{LF} P : \text{unrest} \pi \Gamma M \).

2. Suppose there exists an LF canonical form \( P \) such that \( \pi \Gamma, \pi \Delta \vdash_{LF} P : \text{unrest} \pi \Gamma M \). Then no variable in \( \text{Domain}(\Delta) \) appears free in \( M \).

3. Suppose there exists an LF canonical form \( P \) such that \( \pi \Gamma, \pi \Delta \vdash_{LF} P : \text{unrest} \pi \Gamma M \). Then no variable in \( \text{Domain}(\Delta) \) appears free in \( M \).

We give the adequacy case for unrestricted application to illustrate how Lemma 3.4 is used.

**Proof Sketch of Theorem 3.3**

Suppose \( \nabla \) is the derivation:

\[
\begin{array}{c}
\nabla_1 \\
\vdots \\
\nabla_2 \\
\end{array}
\]

\[
\begin{array}{l}
\Gamma; \Delta \vdash M : \Pi x. A B \\
\Gamma; \epsilon \vdash N : A
\end{array}
\]

\[
\begin{array}{l}
\Gamma; \Delta \vdash M \circ N : [N/x]B
\end{array}
\]

Let \( \nabla_1 = (P_1, H_1) \) and let \( \nabla_2 = (P_2, H_2) \). By induction \( (P_1, H_1) \) is an encoding structure for \( \Gamma; \Delta \vdash M : \Pi x. A B \) and \( (P_2, H_2) \) is an encoding structure for \( \Gamma; \epsilon \vdash N : A \).

By Lemma 3.4, there exists a unique \( Q \) such that \( \pi \Gamma, \pi \Delta \vdash_{LF} \text{unrest} \pi \Gamma N \). So let \( \nabla \) def. \( (\text{of/uapp} Q P_2 P_1 H) \), where for each \( y \) in \( \text{Domain}(\Delta) \), \( H(y) = \text{linear}/uapp (H_1(y)) \).

As an example of the definition of the inverse, suppose \( (\text{of/uapp} Q P_2 P_1 H) \) is an encoding structure for \( \Gamma; \Delta \vdash O : C \). Then \( O \) has the form \( M \circ N \) and \( C \) has the form \( [N/x]B \). Also, \( \pi \Gamma, \pi \Delta \vdash_{LF} P_2 : \pi \Gamma M \Rightarrow \Pi x. A B \) and \( \pi \Gamma, \pi \Delta \vdash_{LF} P_2 : \pi \Gamma M \Rightarrow \Pi x. A B \), and \( \pi \Gamma, \pi \Delta \vdash_{LF} P_1 : \pi \Gamma M \Rightarrow \Pi x. A B \), and \( \pi \Gamma, \pi \Delta \vdash_{LF} P_1 : \pi \Gamma M \Rightarrow \Pi x. A B \).

\[
\begin{align*}
\Delta(x) = A & \\
\Gamma(x) = A
\end{align*}
\]

As usual, there is no typing rule for variables in the encoding, but there are two locality rules. First, \( x \) is local in \( x \):

**4 Modal Logic**

There are (at least) two ways to specify modal logic. One is using an explicit notion of Kripke worlds and accessibility [16]. Such a formulation does not behave as a substructural logic (in that all assumptions are available throughout their scope) and can be encoded in LF without difficulty [8]. A second, which we consider here, is judgemental modal logic [11].

Judgemental modal logic distinguishes between two sorts of assumption, truth and validity. Although judgemental modal logic has no explicit notion of Kripke worlds, one can think of truth as applying to only the current world, and validity as applying to all worlds. Consequently, the introduction rule for \( \Box A \), which internalizes validity, must require that no truth assumptions are used.

This is accomplished with the rule:

\[
\begin{array}{l}
\Gamma; \Delta \vdash M : A \\
\Gamma; \Delta \vdash \Box M : \Box A
\end{array}
\]

Here, \( \Gamma \) is the validity context and \( \Delta \) is the truth context. Whatever truth assumptions exist are discarded while type checking \( M \). Since assumptions in \( \Delta \), are unavailable in \( M \) despite being in scope, judgemental modal logic behaves as a substructural logic.

We express this restriction using a judgement reminiscent of \text{linear}, indicating that an assumption is used locally to the current world:

\[
\text{local} : \text{term} \rightarrow \text{term} \rightarrow \text{type}
\]

The judgement \( \text{local}(x) M x \) should be read as “the variable \( x \) is used locally \( i.e., \text{not within boxes} \) in \( M x \).”

The syntax of modal logic is given in Figure 4. In the interest of brevity, we omit discussion of the possibility modality here. A treatment of possibility appears in the full Twelf development.

**Variables**

The rules for variables allow the use of any variable in the context:

\[
\begin{align*}
\Delta(x) = A & \\
\Gamma(x) = A
\end{align*}
\]

As usual, there is no typing rule for variables in the encoding, but there are two locality rules. First, \( x \) is local in \( x \):
recall the introduction rule for necessity:

\[ \text{Necessity} \]

Second, we wish to say that

\[ \text{The introduction rule for implication is:} \]

\[ \text{Implication} \]

or validity) other than \( x \) is encoded with the single rule:

\[ \text{This is encoded using two rules, reminiscent of the ones for } \]

\[ \text{linear implication:} \]

\[ \text{This is encoded using two rules, reminiscent of the ones for } \]

\[ \text{linear logic:} \]

\[ \text{The important thing here is the absence of any locality rule for } \]

\[ \text{bx. The only way to show that a variable is local in } (bx \]

\[ \text{M is using the } \text{local} / \text{closed} \text{ rule, which requires that the } \]

\[ \text{variable not appear in } M, \text{ as desired.} \]

\[ \text{The elimination rule for necessity is:} \]

\[ \Gamma; \Delta \vdash M : \square A \quad (\Gamma, x : A) ; \Delta \vdash N : C \]

\[ \Gamma; \Delta \vdash \text{let } bx = M \text{ in } N : C \]

This is encoded using two rules:

\[ \text{of/letbx} \]

\[ \text{of/letbx} \]

\[ \text{local/letbx} \]

\[ \text{Since the variable introduced by letbx is a validity assumption, we do not check that it is local in the body.} \]

\[ \text{Metatheory} \]

Subject reduction for modal logic follows the same development as for linear logic in Section 2.2, with \text{local} standing in for \text{linear}. One lemma must be generalized: since local variables can appear multiple times in modal logic, composition of locality must allow the local variable to appear (locally) in the scope of substitution \( (M1 \]

\[ \text{below), as well as in the substitutend (} \]

\[ \text{M2} \]

\[ \text{below):} \]

\[ \text{Lemma 4.1 (Composition of locality)} \]

\[ \text{Suppose the} \]

\[ \text{translation, we do not check that it is local in the body.} \]

\[ \text{The function’s argument is a truth assumption, so it must} \]

\[ \text{be used locally in the body.} \]

\[ \text{The elimination rule for implication is straightforward:} \]

\[ \Gamma; \Delta \vdash M : A \rightarrow B \quad \Gamma; \Delta \vdash N : A \rightarrow B \]

\[ \Gamma; \Delta \vdash \text{let } bx = M \text{ in } N : B \]

\[ \text{of/app} \]

\[ \text{of/app} \]

\[ \text{local/app} \]

\[ \text{local/app} \]

\[ \text{The important thing here is the absence of any locality rule for } \]

\[ \text{bx. The only way to show that a variable is local in } (bx \]

\[ \text{M is using the } \text{local} / \text{closed} \text{ rule, which requires that the } \]

\[ \text{variable not appear in } M, \text{ as desired.} \]

\[ \text{The elimination rule for necessity is:} \]

\[ \Gamma; \Delta \vdash M : \square A \quad (\Gamma, x : A) ; \Delta \vdash N : C \]

\[ \Gamma; \Delta \vdash \text{let } bx = M \text{ in } N : C \]

This is encoded using two rules:

\[ \text{of/letbx} \]

\[ \text{of/letbx} \]

\[ \text{local/letbx} \]

\[ \text{Since the variable introduced by letbx is a validity assumption, we do not check that it is local in the body.} \]

\[ \text{Metatheory} \]

Subject reduction for modal logic follows the same development as for linear logic in Section 2.2, with \text{local} standing in for \text{linear}. One lemma must be generalized: since local variables can appear multiple times in modal logic, composition of locality must allow the local variable to appear (locally) in the scope of substitution \( (M1 \]

\[ \text{below), as well as in the substitutend (} \]

\[ \text{M2} \]

\[ \text{below):} \]

\[ \text{Lemma 4.1 (Composition of locality)} \]

\[ \text{Suppose the} \]

\[ \text{translation, we do not check that it is local in the body.} \]

\[ \text{The function’s argument is a truth assumption, so it must} \]

\[ \text{be used locally in the body.} \]

\[ \text{The elimination rule for implication is straightforward:} \]

\[ \Gamma; \Delta \vdash M : A \rightarrow B \quad \Gamma; \Delta \vdash N : A \rightarrow B \]

\[ \Gamma; \Delta \vdash \text{let } bx = M \text{ in } N : B \]

\[ \text{of/app} \]

\[ \text{of/app} \]

\[ \text{local/app} \]

\[ \text{local/app} \]

\[ \text{The important thing here is the absence of any locality rule for } \]

\[ \text{bx. The only way to show that a variable is local in } (bx \]

\[ \text{M is using the } \text{local} / \text{closed} \text{ rule, which requires that the } \]

\[ \text{variable not appear in } M, \text{ as desired.} \]

\[ \text{The elimination rule for necessity is:} \]

\[ \Gamma; \Delta \vdash M : \square A \quad (\Gamma, x : A) ; \Delta \vdash N : C \]

\[ \Gamma; \Delta \vdash \text{let } bx = M \text{ in } N : C \]

This is encoded using two rules:

\[ \text{of/letbx} \]

\[ \text{of/letbx} \]

\[ \text{local/letbx} \]

\[ \text{Since the variable introduced by letbx is a validity assumption, we do not check that it is local in the body.} \]

\[ \text{Metatheory} \]

Subject reduction for modal logic follows the same development as for linear logic in Section 2.2, with \text{local} standing in for \text{linear}. One lemma must be generalized: since local variables can appear multiple times in modal logic, composition of locality must allow the local variable to appear (locally) in the scope of substitution \( (M1 \]

\[ \text{below), as well as in the substitutend (} \]

\[ \text{M2} \]

\[ \text{below):} \]

\[ \text{Lemma 4.1 (Composition of locality)} \]

\[ \text{Suppose the} \]

\[ \text{translation, we do not check that it is local in the body.} \]

\[ \text{The function’s argument is a truth assumption, so it must} \]

\[ \text{be used locally in the body.} \]

\[ \text{The elimination rule for implication is straightforward:} \]

\[ \Gamma; \Delta \vdash M : A \rightarrow B \quad \Gamma; \Delta \vdash N : A \rightarrow B \]

\[ \Gamma; \Delta \vdash \text{let } bx = M \text{ in } N : B \]

\[ \text{of/app} \]

\[ \text{of/app} \]

\[ \text{local/app} \]

\[ \text{local/app} \]

\[ \text{The important thing here is the absence of any locality rule for } \]

\[ \text{bx. The only way to show that a variable is local in } (bx \]

\[ \text{M is using the } \text{local} / \text{closed} \text{ rule, which requires that the } \]

\[ \text{variable not appear in } M, \text{ as desired.} \]

\[ \text{The elimination rule for necessity is:} \]

\[ \Gamma; \Delta \vdash M : \square A \quad (\Gamma, x : A) ; \Delta \vdash N : C \]

\[ \Gamma; \Delta \vdash \text{let } bx = M \text{ in } N : C \]

This is encoded using two rules:

\[ \text{of/letbx} \]

\[ \text{of/letbx} \]

\[ \text{local/letbx} \]
ways, \( \text{local} \) expresses a fact that essentially can be satisfied in only one way, by the variable not appearing in any boxes. In this regard, \( \text{local} \) is more like \text{unrest} than \text{linear}. However, unlike \text{unrest}, derivations of \( \text{local} \) are not unique.

The problem stems from the fact that the \( \text{local/closed} \) rule can apply to terms that also have another rule. For example, suppose \( \text{H} \) and \( \text{N} \) are closed terms. Then \( \text{local} \) (\( [x] \ app \text{N M} \)) has at least two derivations: \( \text{local/closed} \) and \( \text{local/app local/closed local/closed} \).

One solution to the problem would be to restrict \( \text{local/closed} \) to variables (and add another rule for closed boxes). This would ensure that \( \text{local} \) derivations are unique (like \text{unrest} derivations). We could impose the restriction by creating a judgement (say, \( \text{var} \)) to identify variables, and then rewrite the \( \text{local/closed} \) rule as:

\[
\text{local/closed-varonly} : \text{local} ([y] \ X) \leftarrow \text{var} \ X.
\]

However, this solution has a significant shortcoming: the substitution lemma would no longer be a free consequence of higher-order representation. Under such a regime, variable assumptions would take the form \( (\text{of x A} \leftarrow \text{var x} \leftarrow \ldots \text{whatever} \ldots) \). Consequently, we would only obtain substitution for free when the substitutend possesses a \( \text{var} \) derivation; that is, when the substitutend is another variable. The general substitution lemma would have to be proved and used explicitly.

A better solution is to rephrase adequacy to quotient out the excess derivations:

**Definition 4.4** *Translation of contexts is defined:*

\[
\Gamma; A_1, \ldots, A_n \vdash x : \text{term}, \text{dx} : \text{of x} \Gamma; A_1, \ldots, A_n -\ldots-x_n : \text{term}, \text{dx} : \text{of x} \Gamma; A_1, \ldots, A_n
\]

**Definition 4.5** Let \( \equiv \) be the least congruence over LF canonical forms such that \( P \equiv P' \) for any \( P, P' : \text{local} F \) (where \( F : \text{term} \leftarrow \text{term} \)).

An encoding structure for \( \Gamma; \Delta \vdash M : A \) is a nonempty equivalence class \( (\equiv) \) of LF canonical forms \( P \) such that:

- \( \Gamma, \Delta \vdash \text{lfl P : of } P^\equiv A^\equiv \), and
- For every \( y \) in \( \text{Domain(\Delta)} \), there exists an LF canonical form \( Q_y \) such that \( \Gamma, \Delta \vdash \text{local (y:term) M^\equiv} \), where \( S_y = \text{Domain(\Gamma, \Delta)} \setminus \{y\} \).

**Theorem 4.6** (Semantic adequacy) *There exists a bijection between derivations of the judgement \( \Gamma; \Delta \vdash M : A \) and encoding structures for \( \Gamma; \Delta \vdash M : A \).*

**Proof Sketch**

We give one case in each direction, by way of example. Suppose \( \nabla \) is the derivation:

\[
\nabla_1 = \ldots
\]

\[\Gamma; (\Delta, x : A) \vdash M : B\]

\[\Gamma; \Delta \vdash \lambda x. M : A \rightarrow B\]

Let \( \nabla_m = (P_1, H_1) \). By induction, \( (P_1, H_1) \) is an encoding structure for \( \Gamma; (\Delta, x : A) \vdash M : B \); so:

\[
\Gamma, \Delta; x : \text{term}, \text{dx} : \text{of x} \Gamma^\equiv \vdash \text{lfl P_1 : of } M^\equiv B^\equiv
\]

and, for every \( y \in \text{Domain(\Delta, x : A)} \), there exists a \( Q_y \) such that:

\[
\Gamma, \Delta; (x : A) \setminus \{y\} \vdash \text{lfl Q_y : local (y:term) M^\equiv}
\]

In particular, \( x \in \text{Domain(\Delta, x : A)} \), so:

\[
\Gamma, \Delta \vdash \text{lfl Q_y : local (y:term) M^\equiv}
\]

Therefore:

\[
\Gamma, \Delta \vdash \text{lfl of/lam Q_y : of } \lambda x. M^\equiv \rightarrow A \rightarrow B
\]

Also, for every \( y \in \text{Domain(\Delta)} \),

\[
\Gamma, \Delta \vdash \text{lfl of/lam Q_y : local (y:term) \lambda x. M^\equiv}
\]

So let \( \nabla^\equiv \) be the equivalence class containing \( \text{lfl Q_y P_1} \), which is an encoding structure for \( \Gamma, \Delta \vdash \lambda x. M : A \rightarrow B \).

As an example of the definition of the inverse, suppose \( \text{lfl of/lam Q} \) belongs to an encoding structure for \( \Gamma, \Delta \vdash O : C \). Then \( O \) has the form \( \text{box M^\equiv} \), and \( C \) has the form \( A^\equiv \).

Further, for every \( y \) in \( \text{Domain(\Delta)} \), there exists \( Q_y \) such that \( \Gamma, \Delta \vdash \text{lfl Q_y : local (y:term) bx M^\equiv} \), where \( S_y = \text{Domain(\Gamma, \Delta)} \setminus \{y\} \). Each \( Q_y \) must be \text{linear/closed}, so no \( y \) in \( \text{Domain(\Delta)} \) appears in \( M^\equiv \). Therefore \( \Gamma, \Delta \vdash \text{lfl P^\equiv : of } M^\equiv \rightarrow A^\equiv \).

The second criterion of encoding structures is vacuously satisfied for an empty truth context, so \( P^\equiv \) belongs to an encoding structure for \( \Gamma, \Delta \vdash M^\equiv : A' \). Let \( \nabla'^\equiv = \langle P'^\equiv \rangle \).

Then let \( \text{lfl of/lam P^\equiv} \) be the derivation:

\[
\nabla' = \ldots\]

\[
\Gamma, \Delta \vdash \text{lfl box M^\equiv : of A^\equiv}
\]

It is easy to verify that, for the appropriate \( \nabla \) and \( P \), \( (\text{local } \nabla) \equiv \nabla \) and \( (\text{local } P) \equiv P \). Therefore \( \text{local } \equiv \) and \( \equiv \) are inverses. □

**5 Conclusion**

The Logical Framework is not only (nor even primarily) a type theory. More importantly, it is a methodology for representing deductive systems using higher-order representation of syntax and semantics, and a rigorous account of adequacy. Where applicable, the LF methodology provides a powerful and elegant tool for formalizing programming languages and logics.

There are two reasons it might not apply. First, limitations of existing tools for LF, such as Twelf, might prevent one from carrying out the desired proofs once a system were encoded in LF. Second, there might be an inherent problem representing the desired deductive system adequately using a higher-order representation. When a language cannot be cleanly represented in a higher-order fashion, it often indicates that something about the language is suspect, such as an incorrect (or at least nonstandard) notion of binding and/or scope.
In some cases, however, languages with unconventional notions of binding or scope are nevertheless sensible. Substructural logics are probably the most important example. In this paper, we show that many substructural logics can be given a clean higher-order representation by isolating its “substructuralness” (e.g., linearity or locality) and expressing that as a judgement over proof terms.

Our strategy applies to other substructural logics as well. For example, affine logic and strict logic can each be encoded along very similar lines as linear logic. We conjecture that contextual modal logic [9] is encodable along similar lines as judgemental modal logic. This is a good avenue for future work. The logic of bunched implications [10] is another.

On the other hand, since our method relies on enforcing “substructuralness” on an assumption-by-assumption basis, there are some substructural logics it does not support, such as ordered logic [15, 14]. In ordered logic, the context is taken to be ordered and assumptions must be processed in order. We cannot enforce this restriction on assumptions independently, as the very nature of the restriction is that assumptions are not independent. The usability of one assumption can depend on the disposition of every other assumption in scope.

References


