

## A DEPENDENT NOMINAL TYPE THEORY \*

JAMES CHENEY

Laboratory for Foundations of Computer Science, University of Edinburgh  
*e-mail address*: jcheney@inf.ed.ac.uk

ABSTRACT. Nominal abstract syntax is an approach to representing names and binding pioneered by Gabbay and Pitts. So far nominal techniques have mostly been studied using classical logic or model theory, not type theory. Nominal extensions to simple, dependent and ML-like polymorphic languages have been studied, but decidability and normalization results have only been established for simple nominal type theories. We present a LF-style dependent type theory extended with name-abstraction types, prove soundness and decidability of  $\beta\eta$ -equivalence checking, discuss adequacy and canonical forms via an example, and discuss extensions such as dependently-typed recursion and induction principles.

### 1. INTRODUCTION

Nominal abstract syntax, introduced by Gabbay and Pitts [10, 28, 29], provides a relatively concrete approach to abstract syntax with binding. Nominal techniques support built-in alpha-equivalence with the ability to compare names as data, but (unlike higher-order abstract syntax [14, 26, 23]) do not provide built-in support for substitution or contexts. On the other hand, definitions that involve comparing names as values are sometimes easier to define using nominal abstract syntax, and both single and simultaneous substitution can be defined easily as primitive recursive functions over nominal abstract syntax (see e.g. [4, 5, 30]). Thus, nominal abstract syntax is an alternative approach to representing languages with bound names that has different strengths and weaknesses compared to higher-order abstract syntax.

Historically, one weakness has been the absence of a clean type-theoretic framework for nominal abstract syntax, paralleling elegant frameworks such as LF [14],  $\lambda$ Prolog [23], and more recently Delphin [32] and Beluga [27]. Some previous steps have been taken towards nominal type theories sufficient for reasoning about nominal abstract syntax [37, 5, 30, 42], but as yet a full dependent type theory equipped with metatheoretic results such as decidability of typechecking has not been developed.

In this article, we take a step towards such a nominal type theory, by extending a previously-developed simply typed calculus [5] with dependent types, roughly analogous to the LF system (though with some different modes of use in mind). We call our system  $\lambda^{\text{PI}}$ ,

---

1998 ACM Subject Classification: F.4.1.

Key words and phrases: dependent types, nominal abstract syntax.

\* This article extends “A simple nominal type theory”, published in LFMTTP 2008 [5].

$$\begin{aligned}
v & : \text{ name. } e : \text{ type.} \\
\text{var} & : v \rightarrow e. \quad \text{app} : e \rightarrow e \rightarrow e. \quad \text{lam} : \langle\langle v \rangle\rangle e \rightarrow e.
\end{aligned}$$
Figure 1: Lambda-calculus syntax in  $\lambda^{\Pi\Pi}$ 

$$\begin{aligned}
\text{neq} & : e \rightarrow e \rightarrow \text{type.} \\
\text{neq\_v\_v} & : \mathbf{Ia.Ib}.\text{neq} (\text{var } \mathbf{a}) (\text{var } \mathbf{b}). \\
\text{neq\_a\_a}_i & : \text{neq } M_i N_i \rightarrow \text{neq} (\text{app } M_1 M_2) (\text{app } N_1 N_2). \\
\text{neq\_l\_l} & : (\mathbf{Ia}.\text{neq} (M@{\mathbf{a}}) (N@{\mathbf{a}})) \rightarrow \text{neq} (\text{lam } M) (\text{lam } N). \\
\text{neq\_v\_a} & : \text{neq} (\text{var } V) (\text{app } M N). \\
\text{neq\_v\_l} & : \text{neq} (\text{var } V) (\text{lam } M). \\
\text{neq\_a\_l} & : \text{neq} (\text{app } M N) (\text{lam } P).
\end{aligned}$$
Figure 2: Alpha-inequality in  $\lambda^{\Pi\Pi}$ 

or *dependent nominal type theory*.  $\lambda^{\Pi\Pi}$  provides simple techniques for encoding judgments that depend on name-distinctness and can be soundly extended with recursion combinators useful for defining functions and proofs involving nominal abstract syntax. Because  $\lambda^{\Pi\Pi}$  lacks built-in support for substitution over nominal abstract syntax, it should so far be viewed as a step towards dependently-typed programming and reasoning with nominal features and not as a self-contained logical framework like LF. For example, our approach could serve as a starting point (or domain-specific embedded language) for dependently-typed programming with names and binding within systems such as Agda or Coq based on constructive type theories, as advocated by Licata et al. [19], Westbrook et al. [42], or Poulliard and Pottier [34].

We add *names*  $\mathbf{a}, \mathbf{b}, \dots$ , *name types*  $\alpha$ , and a *dependent name-abstraction* type constructor  $\mathbf{Ia}:\alpha.B$  to LF, which is introduced by *abstraction*  $\langle\langle \mathbf{a} \rangle\rangle M$  and eliminated by *concretion*  $(M@{\mathbf{a}})$ . The abstraction term can be viewed as constructing an  $\alpha$ -equivalence class that binds a name; the concretion term instantiates the name bound by an abstraction to a *fresh* name  $\mathbf{a}$ . This freshness requirement ensures that no two (syntactically) distinct names can ever be identified via renaming, so it is possible to reason about inequalities among names in  $\lambda^{\Pi\Pi}$ . Moreover, this restriction justifies a semantic interpretation of name and name-abstraction types in  $\lambda^{\Pi\Pi}$  as names and name-abstraction constructions in nominal logic, which in turn justifies adding recursion combinators that can be used to define functions on and reason about inductively-defined types with name-binding within  $\lambda^{\Pi\Pi}$ .

Example. As a simple example of a relation that is easily definable in  $\lambda^{\Pi\Pi}$ , but cannot as easily be defined in LF, consider the signature in Figure 1 and alpha-inequivalence relation defined in Figure 2. (The notation  $\langle\langle v \rangle\rangle e$  stands for the non-dependent name-abstraction type  $\mathbf{Ia}:v.e$ .) The key rules are  $\text{neq\_v\_v}$  and  $\text{neq\_l\_l}$ ; several other symmetric rules are omitted. Both rules use the  $\mathbf{I}$ -quantifier to generate fresh names. The type of  $\text{neq\_v\_v}$  states that two variables are alpha-inequivalent if their names are distinct. The type of  $\text{neq\_l\_l}$  states that two lambda-abstractions are alpha-inequivalent if their bodies are inequivalent when instantiated to the same fresh name  $\mathbf{a}$ . We discuss this example further in Section 5 and Section 7.

Contributions. The main contribution of this article is the formulation of  $\lambda^{\text{PIII}}$  and the proof of key metatheoretic properties such as decidability of typechecking, canonicalization, and conservativity over LF. At a technical level, our contribution draws upon Harper and Pfenning’s proof of these properties for LF [15], and we focus on the aspects in which  $\lambda^{\text{PIII}}$  differs from LF, primarily having to do with the treatment of name-abstraction types and concretion via the restriction judgment.

Outline. The structure of the rest of this article is as follows. Section 2 discusses additional related work. Section 3 presents the  $\lambda^{\text{PIII}}$  type theory, along with basic syntactic properties. Section 4 develops the metatheory of  $\lambda^{\text{PIII}}$ . Section 5 considers canonical forms and adequacy of representations of nominal abstract syntax in  $\lambda^{\text{PIII}}$  via a standard example. Section 6 discusses several examples and extensions such as recursion combinators. Section 7 contrasts  $\lambda^{\text{PIII}}$  with closely related systems. Section 8 discusses future work and concludes.

## 2. RELATED WORK

Typed programming languages and type theories incorporating nominal features have already been studied [39, 37, 35, 33, 5, 41]. As in some previous work [37, 35, 5, 41], we employ bunched contexts [25] to enforce the freshness side-conditions on concretions. Specifically, following [5], we employ an explicit context restriction judgment in order to prevent references to the name  $a$  within  $M$  in a concretion  $M@a$ . Previously [5], we proved strong normalization for a simple nominal type theory by translation to ordinary lambda-calculus. Here, we prove completeness of a  $\beta\eta$ -equivalence algorithm more directly by adapting Harper and Pfenning’s logical-relations proof for LF [15]. The restriction judgment is used essentially in the modified logical relation.

Schöpp and Stark [37, 35] and Westbrook et al. [41, 42] have considered richer nominal type theories than  $\lambda^{\text{PIII}}$ . However, Schöpp and Stark did not investigate normalization or decidability, whereas Westbrook proves  $\beta$ -normalization for a “Calculus of Nominal Inductive Constructions” (CNIC) by a (somewhat complex) translation to ordinary CIC [41]; our logical-relations proof handles  $\beta\eta$ -equivalence and seems more direct but does not deal with inductive types or polymorphism. Westbrook et al. are developing an implementation of CNIC called Cinic [42].

Pitts [30, 31] has recently investigated a “Nominal System T” that extends simple nominal type theory [5] with locally-scoped names ( $\nu$ -expressions) and recursion over lambda-terms encoded using nominal abstract syntax. Strong normalization modulo a structural congruence is proved via normalization-by-evaluation. An extended version of this work [31] is different in some ways, and gives an alternative proof of  $\beta$ -normalization. Both techniques draw on Odersky’s  $\lambda\nu$ -calculus [24].

In Pitts’ approach, contexts are standard and do not incorporate freshness assertions, but as a result there are “exotic” terms such as  $\nu a. \text{var } a : e$ , which do not correspond to any object language term and complicate the argument for adequacy. Nevertheless, Pitts’ approach is an interesting development that may lead to a more expressive and flexible facilities for dependently-typed programming with nominal abstract syntax. However, as discussed in Section 7, there are potential complications in pushing this approach beyond simple  $\Pi$ -types.

Our approach also bears some similarity to work on weak higher-order abstract syntax, primarily employed in constructive type theories such as Coq [9, 8, 38]. Here, in contrast to

ordinary higher-order abstract syntax the idea is to use a different, atomic type for binders via a function space  $v \rightarrow e$ . The type  $v$  can be an abstract type with decidable equality; this makes it possible to define the type of expressions inductively, but primitive recursion over weak HOAS is not straightforward to incorporate into Coq. This approach has been formalized as a consistent extension called the Theory of Contexts [17, 3], and this theory has been related to nominal abstract syntax by Miculan et al. [21].

There has also been recent work on techniques for recursion over higher-order abstract syntax. Pientka [27], Poswolsky and Schürmann [32], and Licata et al. [19] have developed novel (and superficially different) techniques. Schürmann and Poswolsky’s approach seems particularly similar to ours; they distinguish between variables and parameters (names), and use ordered contexts with a restriction operation similar to ours. Each of them is considerably more complicated than  $\lambda^{\text{III}}$ , while sharing the advantages of higher-order abstract syntax. Poulliard and Pottier [34] recently proposed an interface in Agda which can be implemented either using nominal terms or de Bruijn terms. This approach may provide a starting point for encoding a  $\lambda^{\text{III}}$ -like language in Agda or Coq, analogous to Harper and Licata’s embedding of higher-order abstract syntax. It is a compelling open question how to relate these techniques to nominal techniques (and to each other). Developing such encodings for nominal and various higher-order approaches in a common metalanguage could be a way to compare their expressiveness.

### 3. DEPENDENT NOMINAL TYPE THEORY

The syntax of  $\lambda^{\text{III}}$  is a straightforward extension of that of LF. We fix countable, disjoint sets of variables  $x, y$ , names  $\mathbf{a}, \mathbf{b}$ , object constants  $c, d$ , type constants  $a, b$ , and name-type constants  $\alpha, \beta$ . The syntactic classes comprise *objects*, *type families* (or just *types*) which classify objects, and *kinds* which classify types. The syntax of  $\lambda^{\text{III}}$  kinds, types, and objects is as follows:

$$\begin{aligned} K & ::= \text{type} \mid \Pi x:A.K \\ A, B & ::= a \mid A M \mid \Pi x:A.B \quad \parallel \alpha \mid \mathbf{Ia}:\alpha.B \\ M, N & ::= c \mid x \mid \lambda x:A.M \mid M N \quad \parallel \mathbf{a} \mid \langle \mathbf{a}:\alpha \rangle M \mid M @ \mathbf{a} \end{aligned}$$

We omit type-level lambda-abstraction, as it complicates the metatheory yet does not add any expressive power to LF [11]. The new syntactic cases of  $\lambda^{\text{III}}$  are distinguished using two parallel bars ( $\parallel$ ). As in LF, kinds include type, the kind of all types, and dependent kinds  $\Pi x:A.K$  that classify type families. Types include constants  $a$ , applications  $A M$  of type constructors to term arguments, and dependent types  $\Pi x:A.B$ . Name-types  $\alpha$  are constants and thus cannot depend on objects. We include a dependent name-abstraction type constructor,  $\mathbf{Ia}:\alpha.B$ , where  $\alpha$  must be a name type. Terms include term constants  $c$ , variables  $x$ , applications  $M N$ , and  $\lambda$ -abstractions  $\lambda x:A.M$  as in LF. In addition, terms include names  $\mathbf{a}$ , name-abstractions  $\langle \mathbf{a}:\alpha \rangle M$ , and name-applications  $M @ \mathbf{a}$  (also known as concretions). Note that the name argument of a concretion must be a literal name, not an arbitrary term. We adopt the same precedence conventions for abstractions and concretions as for  $\lambda$ -abstraction and application. For example,  $\langle \mathbf{a}:\alpha \rangle M @ \mathbf{a} = \langle \mathbf{a}:\alpha \rangle (M @ \mathbf{a})$ , not  $(\langle \mathbf{a}:\alpha \rangle M) @ \mathbf{a}$ .

The  $\Pi$  type constructor and  $\lambda$  term constructor bind variables in the usual way. The  $\mathbf{Ia}:\alpha.B$  type constructor and  $\langle \mathbf{a}:\alpha \rangle M$  term constructor bind the name  $\mathbf{a}$  in  $B$  or  $M$  respectively, so are subject to  $\alpha$ -renaming. The functions  $FV(-)$  and  $FN(-)$  compute the set of

$$\begin{array}{lcl}
\text{type}[\theta] & = & \text{type} \\
(\Pi x:A.K)[\theta] & = & \Pi x:A[\theta].K[\theta] \quad (x \notin FV(\theta)) \\
a[\theta] & = & a \\
\alpha[\theta] & = & \alpha \\
(A M)[\theta] & = & A[\theta] M[\theta] \\
(\Pi x:A.B)[\theta] & = & \Pi x:A[\theta].B[\theta] \quad (x \notin FV(\theta)) \\
(\mathbf{I}a:\alpha.B)[\theta] & = & \mathbf{I}a:\alpha.B[\theta] \quad (a \notin FN(\theta)) \\
c[\theta] & = & c \\
x[\theta] & = & \theta(x) \\
(\lambda x:A.M)[\theta] & = & \lambda x:A[\theta].M[\theta] \quad (x \notin FV(\theta)) \\
(M N)[\theta] & = & M[\theta] N[\theta] \\
\mathbf{a}[\theta] & = & \theta(\mathbf{a}) \\
(\langle \mathbf{a}:\alpha \rangle M)[\theta] & = & \langle \mathbf{a}:\alpha \rangle M[\theta] \quad (\mathbf{a} \notin FN(\theta)) \\
(M @ \mathbf{a})[\theta] & = & M[\theta] @ \mathbf{a}[\theta] \\
\cdot[\theta] & = & \cdot \\
(\sigma, M/x)[\theta] & = & \sigma[\theta], M[\theta]/x
\end{array}$$

Figure 3: Substitution application and composition

free variables or free names of a kind, type, or object; we write  $FVN(-)$  for  $FV(-) \cup FN(-)$ . As in LF, when  $x \notin FV(B)$ , we write  $\Pi x:A.B$  as the function type  $A \rightarrow B$ ; similarly, if  $\mathbf{a} \notin FN(B)$ , we write  $\mathbf{I}a:\alpha.B$  as the name-abstraction type  $\langle\langle\alpha\rangle\rangle B$ . We employ simultaneous substitutions  $\theta$  of the form

$$\theta ::= \cdot \mid \theta, M/x \mid \theta, \mathbf{a}/\mathbf{b}$$

By convention, a substitution assigns at most one expression/name to each variable/name. We write  $\theta(x)$  or  $\theta(\mathbf{a})$  for the expression which  $\theta$  assigns to  $x$  or  $\mathbf{a}$  respectively. Simultaneous substitution application  $M[\theta]$  is defined in Figure 3.

As in LF, the language of constants used in a specification is described by a *signature* assigning (closed) kinds to type constants and (closed) types to object constants. The contexts  $\Gamma$  used in  $\lambda^{\text{PIII}}$  are also similar to those of LF, except that bindings of names introduced by  $\mathbf{I}$  are written  $\Gamma \# \mathbf{a}:\alpha$ , to indicate that such names must be “fresh” for the rest of the context:

$$\begin{array}{lcl}
\Sigma & ::= & \cdot \mid \Sigma, c:A \mid \Sigma, a:K \quad \parallel \Sigma, \alpha:\text{name} \\
\Gamma & ::= & \cdot \mid \Gamma, x:A \quad \parallel \Gamma \# \mathbf{a}:\alpha
\end{array}$$

By convention, the constants and variables on the left-hand side of ‘ $\cdot$ ’ in a signature or context are always distinct. This implicitly constrains the inference rules.

We extend Harper and Pfenning’s presentation of the LF typing and equality rules [15]. All judgments except signature formation are implicitly parametrized by a signature  $\Sigma$ . We omit explicit freshness and signature or context well-formedness constraints.

The well-formedness rules of  $\lambda^{\text{PIII}}$  are shown in Figures 4–7. The additional definitional equivalence rules of  $\lambda^{\text{PIII}}$  are shown in Figure 9. We omit the standard definitional equivalence rules of LF; we add a type-level extensionality rule that was omitted from Harper and Pfenning’s presentation but is admissible [40]. The new rules define the behavior of names and name-abstraction or  $\mathbf{I}$ -types. The  $\mathbf{I}$ -type formation rule is similar to the  $\Pi$ -type formation rule, except using the  $\Gamma \# \mathbf{a}:\alpha$  context former. The rule for name-abstraction is

$$\begin{array}{c}
\frac{}{\vdash \cdot \text{sig}} \quad \frac{\cdot \vdash K : \text{kind} \quad \vdash \Sigma \text{ sig}}{\vdash \Sigma, a : K \text{ sig}} \quad \frac{\cdot \vdash A : \text{type} \quad \vdash \Sigma \text{ sig}}{\vdash \Sigma, c : A \text{ sig}} \quad \frac{}{\vdash \Sigma \text{ sig}} \\
\frac{}{\vdash \cdot \text{ctx}} \quad \frac{\Gamma \vdash A : \text{type} \quad \vdash \Gamma \text{ ctx}}{\vdash \Gamma, x : A \text{ ctx}} \quad \frac{\alpha : \text{name} \in \Sigma \quad \vdash \Gamma \text{ ctx}}{\vdash \Gamma \# a : \alpha \text{ ctx}}
\end{array}$$

Figure 4:  $\lambda^{\text{PIII}}$  well-formedness rules: signatures, contexts

$$\frac{}{\Gamma \vdash \text{type} : \text{kind}} \text{type\_k} \quad \frac{\Gamma \vdash A : \text{type} \quad \Gamma, x : A \vdash K : \text{kind}}{\Gamma \vdash \Pi x : A. K : \text{kind}} \text{pi\_k}$$

Figure 5:  $\lambda^{\text{PIII}}$  well-formedness rules: kinds

$$\begin{array}{c}
\frac{a : K \in \Sigma}{\Gamma \vdash a : K} \text{con\_t} \quad \frac{\Gamma \vdash A : \Pi x : B. K \quad \Gamma \vdash M : B}{\Gamma \vdash A M : K[M/x]} \text{app\_t} \\
\frac{\Gamma \vdash A : \text{type} \quad \Gamma, x : A \vdash B : \text{type}}{\Gamma \vdash \Pi x : A. B : \text{type}} \text{pi\_t} \quad \frac{\Gamma \vdash A : K' \quad \Gamma \vdash K = K' : \text{kind}}{\Gamma \vdash A : K} \text{conv\_t} \\
\frac{\alpha : \text{name} \in \Sigma}{\Gamma \vdash \alpha : \text{type}} \text{nm\_t} \quad \frac{\alpha : \text{name} \in \Sigma \quad \Gamma \# a : \alpha \vdash B : \text{type}}{\Gamma \vdash \mathbf{I}a : \alpha. B : \text{type}} \text{new\_t}
\end{array}$$

Figure 6:  $\lambda^{\text{PIII}}$  well-formedness rules: type families

$$\begin{array}{c}
\frac{c : A \in \Sigma}{\Gamma \vdash c : A} \text{con\_o} \quad \frac{x : A \in \Gamma}{\Gamma \vdash x : A} \text{var\_o} \quad \frac{a : \alpha \in \Gamma}{\Gamma \vdash a : \alpha} \text{nm\_o} \\
\frac{\Gamma \vdash A : \text{type} \quad \Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x : A. M : \Pi x : A. B} \text{lam\_o} \quad \frac{\Gamma \vdash M : \Pi x : A. B \quad \Gamma \vdash N : A}{\Gamma \vdash M N : B[N/x]} \text{app\_o} \\
\frac{\alpha : \text{name} \in \Sigma \quad \Gamma \# a : \alpha \vdash M : B}{\Gamma \vdash \langle a : \alpha \rangle M : \mathbf{I}a : \alpha. B} \text{abs\_o} \quad \frac{\Gamma \vdash a : \alpha \setminus \Gamma' \quad \Gamma' \vdash M : \mathbf{I}a : \alpha. B}{\Gamma \vdash M @ a : B} \text{conc\_o}
\end{array}$$

Figure 7:  $\lambda^{\text{PIII}}$  well-formedness rules: objects

$$\begin{array}{c}
\frac{}{\Gamma \# a : \alpha \vdash a : \alpha \setminus \Gamma} \text{res\_id} \quad \frac{\Gamma \vdash a : \alpha \setminus \Gamma'}{\Gamma \# b : \beta \vdash a : \alpha \setminus \Gamma' \# b : \beta} \text{res\_nm} \quad \frac{\Gamma \vdash a : \alpha \setminus \Gamma'}{\Gamma, x : A \vdash a : \alpha \setminus \Gamma'} \text{res\_var} \\
\cdot - a = \cdot \quad (\theta, M/x) - a = \theta - a \quad (\theta, a'/a) - a = \theta \quad (\theta, b'/b) - a = (\theta - a), b'/b
\end{array}$$

Figure 8: Context and substitution restriction

similar. In the rule for concretion, the name at which the abstraction term is instantiated is *removed* from the context using a *context restriction* judgment  $\Gamma \vdash a : \alpha \setminus \Gamma'$ , shown in Figure 8. This judgment states that  $a : \alpha$  is bound in  $\Gamma$  and  $\Gamma'$  is the result of removing the name  $a$  from  $\Gamma$ , along with any variables that were introduced more recently than  $a$ . For technical reasons, we also need a *substitution restriction* operation  $\theta - a$ , also shown in Figure 8.

The use of an explicit context restriction judgment is a key difference between  $\lambda^{\text{PIII}}$  and other systems that use bunched contexts, such as Schöpp and Stark's system [35, 37]

$$\begin{array}{c}
\frac{\Gamma, x : B \vdash A_1 \quad x = A_2 \quad x : K}{\Gamma \vdash A_1 = A_2 : \Pi x : B. K} \text{eq\_ext\_t} \quad \frac{\Gamma \# a : \alpha \vdash A = B : \text{type}}{\Gamma \vdash \mathbb{I}a : \alpha. A = \mathbb{I}a : \alpha. B : \text{type}} \text{eq\_new\_t} \\
\frac{a : \alpha \in \Gamma}{\Gamma \vdash a = a : \alpha} \text{eq\_nm} \\
\frac{\Gamma \# a : \alpha \vdash M = N : A}{\Gamma \vdash \langle a : \alpha \rangle M = \langle a : \alpha \rangle N : \mathbb{I}a : \alpha. A} \text{eq\_abs} \quad \frac{\Gamma \vdash b : \alpha \setminus \Gamma' \quad \Gamma' \vdash M = N : \mathbb{I}a : \alpha. A}{\Gamma \vdash M @ b = N @ b : A[b/a]} \text{eq\_conc} \\
\frac{\Gamma \vdash b : \alpha \setminus \Gamma' \quad \Gamma' \# a : \alpha \vdash M = N : A}{\Gamma \vdash (\langle a : \alpha \rangle M) @ b = N[b/a] : A[b/a]} \text{eq\_nm\_beta} \quad \frac{\Gamma \# a : \alpha \vdash M @ a = N @ a : A}{\Gamma \vdash M = N : \mathbb{I}a : \alpha. A} \text{eq\_nm\_eta}
\end{array}$$

Figure 9: New definitional equivalence rules of  $\lambda^{\text{PIII}}$ 

or O’Hearn and Pym’s Logic of Bunched Implications [25]. In those theories, context conversion steps can be performed nondeterministically at any point. This complicates equivalence-checking in the presence of dependent types, because we have to be careful to ensure that context conversion steps do not make the context ill-formed. In  $\lambda^{\text{PIII}}$ , we constrain the use of bunched contexts so that standard typechecking and equivalence algorithms for LF can be re-used with minimal changes.

We consider a substitution to be well-formed (written  $\Gamma \vdash \theta : \Gamma'$ ) when it maps the variables and names of some context  $\Gamma'$  to terms and names well-formed with respect to another context  $\Gamma$ , while respecting the freshness requirements of  $\Gamma'$ . This is formalized as follows:

$$\frac{}{\Gamma \vdash \dots} \quad \frac{\Gamma \vdash \theta : \Gamma' \quad \Gamma \vdash M : A[\theta]}{\Gamma \vdash \theta, M/x : \Gamma', x:A} \quad \frac{\Gamma \vdash a : \alpha \setminus \Gamma'' \quad \Gamma'' \vdash \theta : \Gamma'}{\Gamma \vdash \theta, a/b : \Gamma' \# b : \alpha}$$

In addition, we consider a context  $\Gamma'$  to be a *subcontext* of  $\Gamma$  (written  $\Gamma' \preceq \Gamma$ ) if  $\Gamma \vdash \text{id}_{\Gamma'} : \Gamma'$  holds, where  $\text{id}_{\Gamma'}$  denotes the identity substitution on context  $\Gamma'$ . Note that, for example,  $\cdot, x:A \# a : \alpha \preceq \cdot \# a : \alpha, x:A$  holds but not the converse, because the former context guarantees that  $a$  is fresh for  $x$  and the latter does not.

We employ a number of standard metatheoretic results about LF, which extend to  $\lambda^{\text{PIII}}$  without difficulty. We next summarize some basic metatheoretic properties of  $\lambda^{\text{PIII}}$ . Let  $\mathcal{J}$  range over well-formedness assertions  $K : \text{kind}$ ,  $A : K$ ,  $M : A$  or equality assertions  $K = K' : \text{kind}$ ,  $A = A' : K$ ,  $M = M' : A$ .

**Lemma 3.1** (Determinacy of restriction). *If  $\Gamma \vdash a : \alpha \setminus \Gamma_1$  and  $\Gamma \vdash a : \alpha \setminus \Gamma_2$  then  $\Gamma_1 = \Gamma_2$ .*

*Proof.* Straightforward induction on the first derivation using inversion on the second.  $\square$

**Lemma 3.2** (Restriction implies weakening). *If  $\Gamma \vdash a : \alpha \setminus \Gamma'$  then  $\Gamma' \# a : \alpha \preceq \Gamma$ .*

*Proof.* Straightforward, by induction on the structure of derivations.  $\square$

**Lemma 3.3** (Weakening). *Suppose  $\Gamma' \succeq \Gamma$ . Then (1) If  $\Gamma \vdash a : \alpha \setminus \Gamma_0$  then  $\Gamma' \vdash a : \alpha \setminus \Gamma'_0$  for some  $\Gamma'_0 \succeq \Gamma_0$ . (2) If  $\Gamma \vdash \mathcal{J}$  then  $\Gamma' \vdash \mathcal{J}$ .*

**Lemma 3.4** (Substitution restriction). *If  $\Gamma' \vdash \theta : \Gamma$  and  $\Gamma \vdash a : \alpha \setminus \Gamma_0$  then  $\Gamma' \vdash \theta(a) : \alpha \setminus \Gamma'_0$  and  $\Gamma'_0 \vdash \theta - a : \Gamma_0$  for some  $\Gamma'_0$ .*

**Lemma 3.5** (General Substitution). *Assume  $\Gamma \vdash \mathcal{J}$  and  $\Gamma' \vdash \theta : \Gamma$ . Then  $\Gamma' \vdash \mathcal{J}[\theta]$ .*

*Proof.* The cases for existing LF rules are straightforward. Of the new cases, only the rule for concretion is interesting. Suppose we have

$$\frac{\mathcal{D}_1 \quad \mathcal{D}_2}{\Gamma \vdash \mathbf{b}:\alpha \setminus \Gamma_0 \quad \Gamma_0 \vdash M : \mathbf{I}\mathbf{a}:\alpha.B} \Gamma \vdash M@\mathbf{b} : B[\mathbf{b}/\mathbf{a}]$$

Then by assumption, we have  $\Gamma' \vdash \theta : \Gamma$ . Using Lemma 3.4 on  $\mathcal{D}_1$ , we have  $\Gamma' \vdash \mathbf{b}[\theta]:\alpha \setminus \Gamma'_0$  and  $\Gamma'_0 \vdash \theta - \mathbf{b} : \Gamma_0$  for some  $\Gamma'_0$ . Thus, by induction,  $\Gamma'_0 \vdash M[\theta - \mathbf{b}] : (\mathbf{I}\mathbf{a}:\alpha.B)[\theta - \mathbf{b}]$  and by definition,  $\Gamma'_0 \vdash M[\theta - \mathbf{b}] : \mathbf{I}\mathbf{a}:\alpha.B[\theta - \mathbf{b}]$ . Moreover, we may derive

$$\frac{\Gamma' \vdash \mathbf{b}[\theta]:\alpha \setminus \Gamma'_0 \quad \Gamma'_0 \vdash M[\theta - \mathbf{b}] : \mathbf{I}\mathbf{a}:\alpha.B[\theta - \mathbf{b}]}{\Gamma' \vdash M[\theta - \mathbf{b}]@\mathbf{b}[\theta] : B[\theta - \mathbf{b}][\mathbf{b}[\theta]/\mathbf{a}]}$$

To conclude, we observe that  $M[\theta - \mathbf{b}] = M[\theta]$  and  $B[\theta - \mathbf{b}][\mathbf{b}[\theta]/\mathbf{a}] = B[\mathbf{b}/\mathbf{a}][\theta]$  since the extra variables and names mentioned in  $\theta$  cannot be mentioned in  $M$  or  $B$ . So  $\Gamma' \vdash (M@\mathbf{b})[\theta] : B[\mathbf{b}/\mathbf{a}][\theta]$ .  $\square$

**Corollary 3.6** (Substitution). *If  $\Gamma \vdash M : A$  and  $\Gamma, x:A \vdash \mathcal{J}$ , then  $\Gamma \vdash \mathcal{J}[M/x]$ .*

*Proof.* Follows from Lemma 3.5, using  $\theta = \text{id}_\Gamma, M/x$ , which is easily seen to satisfy  $\Gamma \vdash \text{id}_\Gamma, M/x : \Gamma, x:A$ .  $\square$

**Corollary 3.7** (Renaming). *If  $\Gamma \vdash \mathbf{a}:\alpha \setminus \Gamma'$  and  $\Gamma' \#\mathbf{b}:\alpha \vdash \mathcal{J}$ , then  $\Gamma \vdash \mathcal{J}[\mathbf{a}/\mathbf{b}]$ .*

*Proof.* Follows from Lemma 3.5, using  $\theta = \text{id}_{\Gamma'}, \mathbf{a}/\mathbf{b}$ , which satisfies  $\Gamma \vdash \text{id}_{\Gamma'}, \mathbf{a}/\mathbf{b} : \Gamma' \#\mathbf{b}:\alpha$ .  $\square$

As an initial check that these rules are sensible, we verify the *local soundness* and *completeness* properties expressing that typability is preserved by  $\beta$ -reduction and  $\eta$ -expansion steps. For  $\beta$ -reductions of name-abstractions, given

$$\frac{\Gamma \#\mathbf{a}:\alpha \vdash M : B(\mathbf{a})}{\Gamma \vdash \mathbf{b}:\alpha \setminus \Gamma' \quad \Gamma' \vdash \langle \mathbf{a}:\alpha \rangle M : \mathbf{I}\mathbf{a}:\alpha.B(\mathbf{a})} \Gamma \vdash (\langle \mathbf{a}:\alpha \rangle M)@\mathbf{b} : B(\mathbf{b})$$

we conclude that  $\Gamma \vdash M[\mathbf{b}/\mathbf{a}] : B(\mathbf{b})$  by Corollary 3.7. For  $\eta$ -expansion of name-abstractions, given a derivation of  $\Gamma \vdash M : \mathbf{I}\mathbf{a}:\alpha.B$ , and  $\mathbf{a} \notin \Gamma$ , we can expand to:

$$\frac{\Gamma \#\mathbf{a}:\alpha \vdash \mathbf{a}:\alpha \setminus \Gamma \quad \Gamma \vdash M : \mathbf{I}\mathbf{a}:\alpha.B}{\Gamma \#\mathbf{a}:\alpha \vdash M@\mathbf{a} : B} \Gamma \vdash \langle \mathbf{a}:\alpha \rangle M@\mathbf{a} : \mathbf{I}\mathbf{a}:\alpha.B$$

As further examples of the properties of  $\lambda^{\text{PI}}$ , observe that for any  $A, B$  with  $\mathbf{a} \notin FN(B)$  we have “weakening” and “exchange” properties for  $\mathbf{I}$ :

$$\begin{aligned} &\vdash \lambda x:B.\langle \mathbf{a}:\alpha \rangle x : B \rightarrow \mathbf{I}\mathbf{a}:\alpha.B, \\ &\vdash \lambda x:(\mathbf{I}\mathbf{a}:\alpha.\mathbf{I}\mathbf{b}:\beta.A).\langle \mathbf{b}:\beta \rangle \langle \mathbf{a}:\alpha \rangle x@\mathbf{a}@\mathbf{b} : \mathbf{I}\mathbf{a}:\alpha.\mathbf{I}\mathbf{b}:\beta.A \rightarrow \mathbf{I}\mathbf{b}:\beta.\mathbf{I}\mathbf{a}:\alpha.A. \end{aligned}$$

We might expect an inverse “strengthening” property, that is,  $\mathbf{I}\mathbf{a}:\alpha.B \rightarrow B$ , but this does not hold in general. The following derivation gets stuck because there is no name  $\mathbf{a}$  to which to apply  $x$ :

$$\frac{x:\mathbf{I}\mathbf{a}:\alpha.B \vdash ?? : B}{\vdash \lambda x:(\mathbf{I}\mathbf{a}:\alpha.B).?? : \mathbf{I}\mathbf{a}:\alpha.B \rightarrow B}$$

This makes sense, semantically speaking, because for example there is no equivariant function from the nominal set  $\langle \mathbb{A} \rangle \mathbb{A}$  to  $\mathbb{A}$  (where  $\mathbb{A}$  is a set of names). We will not develop a



nominal set semantics of  $\lambda^{\text{III}}$  here, but such a semantics was developed for a simply-typed calculus in [5].

There are natural functions that are definable in the nominal set semantics that are not definable in  $\lambda^{\text{III}}$ . Suppose we have a function  $h : \mathbb{A} \times X \rightarrow Y$  such that for any name  $\mathbf{a}$ , if  $\mathbf{a}$  is fresh for  $x$  then  $\mathbf{a}$  is fresh for  $h(\mathbf{a}, x)$ . Then, as discussed by Pitts [29], we can define a function  $h' : \langle \mathbb{A} \rangle X \rightarrow Y$  satisfying  $h(\mathbf{a}, x) = h'(\langle \mathbf{a} \rangle x)$ . (This function is obtained by lifting  $h$  to equivalence classes of name-abstractions; the freshness condition for  $h$  is sufficient to ensure that  $h$  respects  $\alpha$ -equivalence classes.)

As a simple example, suppose for the moment we include a standard option type and consider the function  $g' : \langle \mathbb{A} \rangle \mathbb{A} \rightarrow \mathbb{A}$  *option* defined by

$$g(\mathbf{a}, x) = \begin{cases} \text{NONE} & \mathbf{a} = x \\ \text{SOME}(x) & \mathbf{a} \neq x \end{cases}$$

This function lets us test whether an abstraction is of the form  $\langle \mathbf{a} \rangle \mathbf{a}$ , and if it is not, extracts the body. We have  $\mathbf{a} \# x$  implies  $\mathbf{a} \# g(\mathbf{a}, x)$ , but  $g'$  cannot be defined as a  $\lambda^{\text{III}}$  term  $N : \langle \alpha \rangle \alpha \rightarrow \alpha$  *option*. As another example, consider the function  $k' : \langle \mathbb{A} \rangle \mathbb{N} \rightarrow \mathbb{N}$  obtained from  $k(\mathbf{a}, n) = n$ . We can obviously define a natural number type *nat* in  $\lambda^{\text{III}}$ , but we cannot define a  $\lambda^{\text{III}}$  function  $M : \langle \langle \alpha \rangle \rangle \text{nat} \rightarrow \text{nat}$  satisfying  $M(\langle \mathbf{a} \rangle n) = n$ .

In  $\lambda^{\text{III}}$ , we currently have no general way to define such functions, and it is not immediately obvious how to accommodate them. One possibility might be to add a term constructor  $\nu \mathbf{a} : \alpha. M$  with well-formedness rule:

$$\frac{\Gamma \# \mathbf{a} : \alpha \vdash M : A \quad \text{“}\mathbf{a} \text{ fresh for } M\text{”}}{\Gamma \vdash \nu \mathbf{a} : \alpha. M : A}$$

Roughly this approach (without the freshness side-condition) is taken in a simply-typed calculus called Nominal System T [30, 31]. However, there are significant complications with incorporating this approach to name-restriction into a dependent type theory, explored further in Section 7.

In addition to the basic results presented so far, we need to establish a number of straightforward properties for  $\lambda^{\text{III}}$ , including validity, inversion, and injectivity for  $\Pi$  and  $\mathbb{I}$ . These properties (and their proofs) are essentially the same as for LF as given in [15, 40] and are omitted.

#### 4. EQUIVALENCE AND CANONICAL FORMS

In this section we show that the definitional equivalence and well-formedness judgments of  $\lambda^{\text{III}}$  are decidable. In previous work [5], we showed strong normalization for a simply-typed lambda calculus with names and name-abstraction types by translating name-types to function types and re-using standard results for the simply-typed lambda calculus. Here, we prove the desired results directly, based on Harper and Pfenning’s decidability proof [15].

Harper and Pfenning’s approach is based on an algorithmic equivalence judgment that weak head-normalizes LF terms. The judgment only tracks simple types  $\tau$  for variables and terms may not necessarily be well-formed. The algorithm is shown sound and complete for well-formed LF terms with respect to the definitional equivalence rules. Soundness is proved syntactically, whereas completeness involves a logical relation argument. The logical relation is defined by induction on the structure of simple types.

$$\frac{M \xrightarrow{\text{whr}} N}{M N \xrightarrow{\text{whr}} M' N} \quad \frac{}{(\lambda x : A.M) N \xrightarrow{\text{whr}} M[N/x]} \quad \frac{M \xrightarrow{\text{whr}} N}{M@a \xrightarrow{\text{whr}} N@a} \quad \frac{}{\langle a:\alpha \rangle M @b \xrightarrow{\text{whr}} M[b/a]}$$

Figure 10: Weak head reduction

$$\frac{\frac{M \xrightarrow{\text{whr}} M' \quad \Delta \vdash M' \Leftrightarrow N : a^-}{\Delta \vdash M \Leftrightarrow N : a^-} \quad \frac{N \xrightarrow{\text{whr}} N' \quad \Delta \vdash M \Leftrightarrow N' : a^-}{\Delta \vdash M \Leftrightarrow N : a^-}}{\Delta \vdash M \Leftrightarrow N : a^-} \quad \frac{\Delta \vdash M \Leftrightarrow N : a^- \quad \Delta, x : \tau_1 \vdash M x \Leftrightarrow N x : \tau_2}{\Delta \vdash M \Leftrightarrow N : \tau_1 \rightarrow \tau_2} \quad \frac{\Delta \# a:\alpha \vdash M@a \Leftrightarrow N@a : \tau}{\Delta \vdash M \Leftrightarrow N : \langle \alpha \rangle \tau}}{\frac{\frac{x:\tau \in \Delta}{\Delta \vdash x \Leftrightarrow x : \tau} \quad \frac{c:A \in \Sigma}{\Delta \vdash c \Leftrightarrow c : A^-} \quad \frac{a:\alpha \in \Delta}{\Delta \vdash a \Leftrightarrow a : \alpha}}{\Delta \vdash M_1 \Leftrightarrow N_1 : \tau_1 \rightarrow \tau_2} \quad \Delta \vdash M_2 \Leftrightarrow N_2 : \tau_1} \quad \frac{\Delta \vdash a:\alpha \setminus \Delta' \quad \Delta' \vdash M \Leftrightarrow N : \langle \alpha \rangle \tau}{\Delta \vdash M@a \Leftrightarrow N@a : \tau}}$$

Figure 11: Algorithmic and structural equivalence rules for objects

$$\frac{\frac{\Delta \vdash A \Leftrightarrow B : \text{type}^-}{\Delta \vdash A \Leftrightarrow B : \text{type}^-} \quad \frac{\Delta, x:\tau \vdash A x \Leftrightarrow B x : \kappa}{\Delta \vdash A \Leftrightarrow B : \tau \rightarrow \kappa}}{\Delta \vdash A_1 \Leftrightarrow B_1 : \text{type}^- \quad \Delta, x : A_1^- \vdash A_2 \Leftrightarrow B_2 : \text{type}^-} \quad \frac{\Delta \# a:\alpha \vdash B \Leftrightarrow B' : \text{type}^-}{\Delta \vdash \mathbf{I}a:\alpha.B \Leftrightarrow \mathbf{I}a:\alpha.B' : \text{type}^-}}{\frac{\frac{a:K \in \Sigma}{\Delta \vdash a \Leftrightarrow a : K^-} \quad \frac{\alpha : \text{name} \in \Sigma}{\Delta \vdash \alpha \Leftrightarrow \alpha : \text{type}^-} \quad \frac{\Delta \vdash A \Leftrightarrow B : \tau \rightarrow \kappa \quad \Delta \vdash M \Leftrightarrow N : \tau}{\Delta \vdash A M \Leftrightarrow B N : \kappa}}$$

Figure 12: Algorithmic and structural equivalence rules for types

$$\frac{}{\Delta \vdash \text{type} \Leftrightarrow \text{type} : \text{kind}^-} \quad \frac{\Delta \vdash A \Leftrightarrow B : \text{type}^- \quad \Delta, x : A^- \vdash K \Leftrightarrow L : \text{kind}^-}{\Delta \vdash \Pi x:A.K \Leftrightarrow \Pi x:B.L : \text{kind}^-}$$

Figure 13: Algorithmic equivalence rules for kinds

We extend their simple types and kinds with name-abstraction types as follows:

$$\tau ::= a^- \mid \tau \rightarrow \tau' \mid \langle \alpha \rangle \tau \mid \alpha \quad \kappa ::= \text{type}^- \mid \tau \rightarrow \kappa$$

and extend the erasure function by defining  $(\alpha)^- = \alpha$  and  $(\mathbf{I}a:\alpha.A)^- = \langle \alpha \rangle A^-$ . We consider simple contexts  $\Delta$  mapping variables to simple types. We extend the weak head reduction and algorithmic equivalence judgments with rules for names and name-abstractions (Figure 11). Also, we define a restriction judgment  $\Delta \vdash a:\alpha \setminus \Delta'$  for simple contexts; its definition is identical to that for dependently-typed contexts and so is omitted.

There are a number of additional properties of erasure and algorithmic equivalence that are needed for the following soundness and completeness results, but again these are essentially the same as in [15, 40] so are omitted.

4.1. **Soundness.** The proof of soundness is syntactic. Note however that we include a rule for type-level extensionality, avoiding a subtle problem in Harper and Pfenning's presentation (see [40, sec. 3.4]).

**Theorem 4.1** (Subject reduction). *If  $\Gamma \vdash M : A$  and  $M \xrightarrow{\text{whr}} M'$  then  $\Gamma \vdash M = M' : A$  (and hence  $\Gamma \vdash M' : A$  also).*

*Proof.* By induction on the derivation of  $M \xrightarrow{\text{whr}} M'$ , with most cases standard.

- If the derivation is of the form:

$$\frac{M \xrightarrow{\text{whr}} M'}{M@a \xrightarrow{\text{whr}} M'@a}$$

then by inversion we must have  $\Gamma \vdash a:\alpha \setminus \Gamma'$  and  $\Gamma' \vdash M : \mathbf{I}b:\alpha.A'$  where  $\Gamma' \vdash A = A'[a/b] : \text{type}$ . Hence, by induction we know that  $\Gamma' \vdash M = M' : \mathbf{I}b:\alpha.A'$ , and we may derive

$$\frac{\frac{\Gamma \vdash a:\alpha \setminus \Gamma' \quad \Gamma' \vdash M = M' : \mathbf{I}b:\alpha.A'}{\Gamma \vdash M@a = M'@a : A'[a/b]} \quad \Gamma' \vdash A = A'[a/b] : \text{type}}{\Gamma \vdash M@a = M'@a : A}$$

- If the derivation is of the form:

$$\frac{}{\langle a:\alpha \rangle M @ b \xrightarrow{\text{whr}} M[b/a]}$$

then by inversion we must have  $\Gamma \vdash b:\alpha \setminus \Gamma'$  and  $\Gamma' \vdash \langle a:\alpha \rangle M : \mathbf{I}a:\alpha.A'$ , where  $\Gamma \vdash A = A'[b/a] : \text{type}$ . Moreover, again by inversion we must have  $\Gamma' \# a:\alpha \vdash M : A''$  where  $\Gamma' \# a:\alpha \vdash A' = A'' : \text{type}$ . Thus, we may derive:

$$\frac{\frac{\Gamma' \# a:\alpha \vdash M : A'' \quad \Gamma' \# a:\alpha \vdash A' = A'' : \text{type}}{\Gamma' \# a:\alpha \vdash M : A'}}{\frac{\Gamma \vdash b:\alpha \setminus \Gamma' \quad \Gamma' \# a:\alpha \vdash M = M : A'}{\Gamma \vdash \langle a:\alpha \rangle M @ b = M[b/a] : A'[b/a]}}$$

Since  $\Gamma \vdash A = A'[b/a] : \text{type}$ , we can conclude  $\Gamma \vdash \langle a:\alpha \rangle M @ b = M[b/a] : A$ , as desired.  $\square$

**Lemma 4.2** (Soundness of restriction). *If  $\Gamma, \Gamma_0$  are well-formed and  $\Gamma^- \vdash a:\alpha \setminus \Gamma_0^-$  then  $\Gamma \vdash a:\alpha \setminus \Gamma_0$ .*

*Proof.* Straightforward induction on derivations.  $\square$

**Theorem 4.3** (Soundness).

- (1) *If  $\Gamma^- \vdash M \Leftrightarrow N : A^-$  and  $\Gamma \vdash M, N : A$  then  $\Gamma \vdash M = N : A$ .*
- (2) *If  $\Gamma^- \vdash M \Leftrightarrow N : \tau$  and  $\Gamma \vdash M : A$  and  $\Gamma \vdash N : B$  then  $\Gamma \vdash A = B : \text{type}$  and  $\Gamma \vdash M = N : A$  and  $A^- = \tau = B^-$ .*

*Proof.* By simultaneous induction on the derivations of  $\Gamma^- \vdash M \Leftrightarrow N : A^-$  and  $\Gamma^- \vdash M \Leftrightarrow N : \tau$ . Again most cases are standard; we show the new cases only.

- If the derivation is of the form:

$$\frac{\mathbf{a}:\alpha \in \Gamma^-}{\Gamma^- \vdash \mathbf{a} \leftrightarrow \mathbf{a} : \alpha}$$

then we must have  $\mathbf{a}:\alpha \in \Gamma$  so we can conclude that  $\Gamma \vdash \alpha = \alpha : \text{type}$  and  $\Gamma \vdash \mathbf{a} = \mathbf{a} : \alpha$  and  $A^- = \alpha^- = \alpha = \alpha^- = B^-$ .

- If the derivation is of the form:

$$\frac{\Gamma^- \# \mathbf{a}:\alpha \vdash M@_{\mathbf{a}} \leftrightarrow N@_{\mathbf{a}} : \tau}{\Gamma^- \vdash M \leftrightarrow N : \langle \alpha \rangle \tau}$$

where  $A^- = \langle \alpha \rangle \tau$ , then without loss of generality we assume  $\mathbf{a}$  is fresh for  $\Gamma, A, M, N$ . Then by inversion of erasure we must have  $A = \mathbf{I}b:\alpha.A_0$  for some  $A_0$  with  $A_0^- = \tau$ . Without loss of generality, assume that  $\mathbf{b}$  is fresh for  $\mathbf{a}, \Gamma, A, M, N$ . Moreover, we can easily show that  $\Gamma \# \mathbf{a}:\alpha \vdash M@_{\mathbf{a}} : A_0[\mathbf{a}/\mathbf{b}]$  and similarly for  $N$ . Then by induction, we know that  $\Gamma \# \mathbf{a}:\alpha \vdash M@_{\mathbf{a}} = N@_{\mathbf{a}} : A_0[\mathbf{a}/\mathbf{b}]$ , hence we can derive

$$\frac{\Gamma \# \mathbf{a}:\alpha \vdash M@_{\mathbf{a}} = N@_{\mathbf{a}} : A_0[\mathbf{a}/\mathbf{b}]}{\Gamma \vdash M = N : \mathbf{I}a:\alpha.A_0[\mathbf{a}/\mathbf{b}]}$$

Since  $A = \mathbf{I}b:\alpha.A_0$  and  $\mathbf{a}$  is sufficiently fresh,  $A$  is  $\alpha$ -equivalent to  $\mathbf{I}a:\alpha.A_0[\mathbf{a}/\mathbf{b}]$ , so  $\Gamma \vdash M = N : A$ , as desired.

- If the derivation is of the form:

$$\frac{\Gamma^- \vdash \mathbf{a}:\alpha \setminus \Gamma_0^- \quad \Gamma_0^- \vdash M \leftrightarrow N : \langle \alpha \rangle \tau}{\Gamma^- \vdash M@_{\mathbf{a}} \leftrightarrow N@_{\mathbf{a}} : \tau}$$

then we know that  $\Gamma \vdash \mathbf{a}:\alpha \setminus \Gamma_0$  by the soundness of restriction. Moreover, by inversion we know that  $\Gamma \vdash \mathbf{a}:\alpha \setminus \Gamma_1$  and  $\Gamma_1 \vdash M : \mathbf{I}a:\alpha.A_0$  and  $\Gamma \vdash A_0 = A : \text{type}$  for some  $\Gamma_1, A_0$ , and similarly for  $N$  for some  $\Gamma_2, B_0$ . By determinacy of restriction (Lemma 3.1) we know that  $\Gamma_0 = \Gamma_1 = \Gamma_2$ . Hence, by induction we have that  $\Gamma_0 \vdash \mathbf{I}a:\alpha.A_0 = \mathbf{I}a:\alpha.B_0 : \text{type}$  and  $\Gamma_0 \vdash M = N : \mathbf{I}a:\alpha.A_0$  and  $(\mathbf{I}a:\alpha.A_0)^- = \langle \alpha^- \rangle \tau = (\mathbf{I}a:\alpha.B_0)^-$ . It follows immediately that  $A_0^- = \tau = B_0^-$ . In addition, we have that  $\Gamma_0 \# \mathbf{a}:\alpha \vdash A_0 = B_0 : \text{type}$  by injectivity of  $\mathbf{I}$ -type equality.

To conclude, we can derive:

$$\frac{\frac{\Gamma_0 \# \mathbf{a}:\alpha \vdash A_0 = B_0 : \text{type}}{\Gamma \vdash A_0 = B_0 : \text{type}} \quad W \quad \Gamma \vdash B_0 = B : \text{type}}{\Gamma \vdash A_0 = B : \text{type}}$$

where the inference labeled  $W$  is by weakening since we must have  $\Gamma_0 \# \mathbf{a}:\alpha \preceq \Gamma$  by Lemma 3.2. Next, observe that by transitivity we have  $\Gamma \vdash A = B : \text{type}$  since  $\Gamma \vdash A = A_0 : \text{type}$  holds. Finally, we can also derive:

$$\frac{\Gamma \vdash \mathbf{a}:\alpha \setminus \Gamma_0 \quad \Gamma_0 \vdash M = N : \mathbf{I}a:\alpha.A_0}{\Gamma \vdash M@_{\mathbf{a}} = N@_{\mathbf{a}} : A_0}$$

This completes the proof. □

$$\begin{array}{l}
\Delta \vdash M = N \in [\delta] \iff \Delta \vdash M \Leftrightarrow N : \delta \quad (\delta \in \{\alpha, a^-\}) \\
\Delta \vdash M = N \in [\tau_1 \rightarrow \tau_2] \iff \forall \Delta' \succeq \Delta. \Delta' \vdash M' = N' \in [\tau_1] \implies \Delta' \vdash M \ M' = N \ N' \in [\tau_2] \\
\Delta \vdash M = N \in [\langle \alpha \rangle \tau] \iff \forall \Delta'', \mathbf{a}, \Delta' \succeq \Delta. \Delta'' \vdash \mathbf{a} : \alpha \setminus \Delta' \implies \Delta'' \vdash M @ \mathbf{a} = N @ \mathbf{a} \in [\tau] \\
\\
\frac{}{\Delta \vdash \cdot = \cdot \in [\cdot]} \quad \frac{\Delta \vdash M = N \in [\tau] \quad \Delta \vdash \theta = \sigma \in [\Theta]}{\Delta \vdash \theta, M/x = \sigma, N/x \in [\Theta, x:\tau]} \quad \frac{\Delta \vdash \mathbf{b} : \alpha \setminus \Delta' \quad \Delta' \vdash \theta = \sigma \in [\Theta]}{\Delta \vdash \theta, \mathbf{b}/\mathbf{a} = \sigma, \mathbf{b}/\mathbf{a} \in [\Theta \# \mathbf{a} : \alpha]}
\end{array}$$

Figure 14: Logical relation for objects and substitutions

**4.2. Completeness.** The proof of completeness is by a Kripke logical relation argument. The logical relation is extended with a case for name-abstraction types in Figure 14. We first state the key properties of the logical relations:

**Lemma 4.4** (Logical substitution restriction). *Suppose that  $\Delta \vdash \theta = \sigma \in [\Gamma^-]$  and  $\Gamma \vdash \mathbf{a} : \alpha \setminus \Gamma_0$ . Then  $\theta(\mathbf{a}) = \sigma(\mathbf{a})$  and there exists  $\Delta_0$  such that  $\Delta \vdash \theta(\mathbf{a}) : \alpha \setminus \Delta_0$  and  $\Delta_0 \vdash \theta - \mathbf{a} = \sigma - \mathbf{a} \in [\Gamma_0^-]$ .*

*Proof.* It is straightforward to show that  $\theta(\mathbf{a}) = \sigma(\mathbf{a})$  by induction on the first derivation. For the second part, the proof is by induction on the second derivation, using inversion and the definition of substitution restriction.  $\square$

**Lemma 4.5** (Weakening). *If  $\Delta \vdash M = N \in [\tau]$  and  $\Delta' \succeq \Delta$  then  $\Delta' \vdash M = N \in [\tau]$ .*

*Proof.* By induction on  $\tau$ . The only new case is for name-abstraction types  $\langle \alpha \rangle \tau$ . Suppose  $\Delta \vdash M = N \in [\langle \alpha \rangle \tau]$  and  $\Delta' \succeq \Delta$ . Let  $\Delta'', \Delta''', \mathbf{a}$  be given with  $\Delta''' \vdash \mathbf{a} : \alpha \setminus \Delta''$  and  $\Delta'' \succeq \Delta'$ . Then by transitivity we have  $\Delta''' \succeq \Delta$  so by definition of the logical relation,  $\Delta''' \vdash M @ \mathbf{a} = N @ \mathbf{a} \in [\tau]$ . Thus, we conclude that  $\Delta' \vdash M = N \in [\langle \alpha \rangle \tau]$  by the definition of the logical relation.  $\square$

**Lemma 4.6** (Symmetry). *If  $\Delta \vdash M = N \in [\tau]$  then  $\Delta \vdash N = M \in [\tau]$ .*

*Proof.* The proof is by induction on types; we show the case for  $\langle \alpha \rangle \tau$ . Assume  $\Delta \vdash M = N \in [\langle \alpha \rangle \tau]$ , and let  $\Delta'', \mathbf{a}, \Delta'$  be given with  $\Delta'' \vdash \mathbf{a} : \alpha \setminus \Delta'$  and  $\Delta' \succeq \Delta$ . Then by definition we have  $\Delta'' \vdash M @ \mathbf{a} = N @ \mathbf{a} \in [\tau]$  and by induction we have  $\Delta'' \vdash N @ \mathbf{a} = M @ \mathbf{a} \in [\tau]$  so we may conclude that  $\Delta \vdash N = M \in [\tau]$ .  $\square$

**Lemma 4.7** (Transitivity). *If  $\Delta \vdash M = N \in [\tau]$  and  $\Delta \vdash N = O \in [\tau]$  then  $\Delta \vdash M = O \in [\tau]$ .*

*Proof.* The proof is by induction on types; we show the case for  $\langle \alpha \rangle \tau$ . Suppose  $\Delta \vdash M = N \in [\langle \alpha \rangle \tau]$  and  $\Delta \vdash N = O \in [\langle \alpha \rangle \tau]$ , and let  $\Delta'', \mathbf{a}, \Delta'$  be given with  $\Delta'' \vdash \mathbf{a} : \alpha \setminus \Delta'$  and  $\Delta' \succeq \Delta$ . Then by definition we have both  $\Delta'' \vdash M @ \mathbf{a} = N @ \mathbf{a} \in [\tau]$  and  $\Delta'' \vdash N @ \mathbf{a} = O @ \mathbf{a} \in [\tau]$  and by induction we have  $\Delta'' \vdash M @ \mathbf{a} = O @ \mathbf{a} \in [\tau]$ , so we may conclude that  $\Delta \vdash M = O \in [\tau]$ .  $\square$

**Lemma 4.8** (Closure under head expansion). *If  $M \xrightarrow{\text{whr}} M'$  and  $\Delta \vdash M' = N \in [\tau]$  then  $\Delta \vdash M = N \in [\tau]$ .*

*Proof.* The proof is by induction on types; we show the case for  $\langle \alpha \rangle \tau$ . Suppose  $M \xrightarrow{\text{whr}} M'$  and  $\Delta \vdash M' = N \in [\langle \alpha \rangle \tau]$ . Let  $\Delta'', \mathbf{a}, \Delta'$  be given with  $\Delta'' \vdash \mathbf{a} : \alpha \setminus \Delta'$  and  $\Delta' \succeq \Delta$ . Then

$\Delta'' \vdash M'@a = N@a \in \llbracket \tau \rrbracket$  by definition of the logical relation. Moreover, we have that  $M \xrightarrow{\text{whr}} M'$  implies  $M@a \xrightarrow{\text{whr}} M'@a$ . So, by induction we know that  $\Delta'' \vdash M@a = N@a \in \llbracket \tau \rrbracket$ , and we may conclude  $\Delta \vdash M = N \in \llbracket \langle \alpha \rangle \tau \rrbracket$ .  $\square$

**Lemma 4.9** (Identity substitution). *For any  $\Gamma$  we have  $\Gamma^- \vdash \text{id}_\Gamma = \text{id}_\Gamma \in \llbracket \Gamma^- \rrbracket$ .*

*Proof.* Induction on the structure of  $\Gamma$ . The base case and variable case are standard. Suppose  $\Gamma = \Gamma_0 \# a : \alpha$ . Then by induction,  $\Gamma_0^- \vdash \text{id}_{\Gamma_0} = \text{id}_{\Gamma_0} \in \llbracket \Gamma_0^- \rrbracket$ . By weakening, we know that  $\Gamma_0^- \# a : \alpha \vdash \text{id}_{\Gamma_0} = \text{id}_{\Gamma_0} \in \llbracket \Gamma_0^- \rrbracket$  holds. Moreover,  $\Gamma_0^- \# a : \alpha \vdash a : \alpha \setminus \Gamma_0^-$  is derivable. Hence, we may conclude:

$$\frac{\Gamma_0^- \# a : \alpha \vdash a : \alpha \setminus \Gamma_0^- \quad \Gamma_0^- \# a : \alpha \vdash \text{id}_{\Gamma_0} = \text{id}_{\Gamma_0} \in \llbracket \Gamma_0^- \rrbracket}{\Gamma_0^- \# a : \alpha \vdash \text{id}_{\Gamma_0, a/a} = \text{id}_{\Gamma_0, a/a} \in \llbracket \Gamma_0^- \# a : \alpha \rrbracket}$$

This concludes the proof.  $\square$

We now state the main properties relating definitional and algorithmic equality and the logical relation.

**Theorem 4.10** (Logical implies algorithmic).

- (1) *If  $\Delta \vdash M = N \in \llbracket \tau \rrbracket$  then  $\Delta \vdash M \Leftrightarrow N : \tau$ .*
- (2) *If  $\Delta \vdash M \Leftrightarrow N : \tau$  then  $\Delta \vdash M = N \in \llbracket \tau \rrbracket$ .*

*Proof.* By simultaneous induction on  $\tau$ . The new cases are those for  $\tau = \langle \alpha \rangle \tau_0$ .

- (1) Suppose  $\Delta \vdash M = N \in \llbracket \langle \alpha \rangle \tau \rrbracket$ . Then we wish to show that  $\Delta \vdash M \Leftrightarrow N : \langle \alpha \rangle \tau$ . Choose a fresh name  $a$  not present in  $\Delta$ . Then we can immediately derive  $\Delta \# a : \alpha \vdash a : \alpha \setminus \Delta$ , and obviously  $\Delta \succeq \Delta$ , so by definition of the logical relation,  $\Delta \# a : \alpha \vdash M@a = N@a \in \llbracket \tau \rrbracket$ . By induction, we have  $\Delta \# a : \alpha \vdash M@a \Leftrightarrow N@a : \tau$ , so we may conclude:

$$\frac{\Delta \# a : \alpha \vdash a : \alpha \setminus \Delta \quad \Delta \# a : \alpha \vdash M@a \Leftrightarrow N@a : \tau}{\Delta \vdash M \Leftrightarrow N : \langle \alpha \rangle \tau}$$

- (2) Suppose  $\Delta \vdash M \Leftrightarrow N : \langle \alpha \rangle \tau$ . Let  $\Delta', a, \Delta''$  be given with  $\Delta'' \vdash a : \alpha \setminus \Delta'$  and  $\Delta' \succeq \Delta$ . Then we may derive:

$$\frac{\Delta \vdash M \Leftrightarrow N : \langle \alpha \rangle \tau \quad \Delta' \vdash M \Leftrightarrow N : \langle \alpha \rangle \tau}{\Delta'' \vdash M@a \Leftrightarrow N@a : \tau} W$$

where the step labeled  $W$  is by weakening using  $\Delta \preceq \Delta'$ . Hence, the induction hypothesis applies and we have  $\Delta'' \vdash M@a = N@a \in \llbracket \tau \rrbracket$ , so we may conclude by definition that  $\Delta \vdash M = N \in \llbracket \langle \alpha \rangle \tau \rrbracket$ .

This completes the proof.  $\square$

**Theorem 4.11** (Definitional implies logical). *If  $\Gamma \vdash M = N : A$  and  $\Delta \vdash \theta = \sigma \in \llbracket \Gamma^- \rrbracket$  then  $\Delta \vdash M[\theta] = N[\sigma] \in \llbracket A^- \rrbracket$ .*

*Proof.* By induction on the definitional equality derivation. We show new cases involving new definitional equality rules.

- If the derivation is of the form:

$$\frac{a : \alpha \in \Gamma}{\Gamma \vdash a = a : \alpha} \text{eq\_nm}$$

then it is immediate that  $\Gamma^- \vdash a \Leftrightarrow a : \alpha$  and hence  $\Gamma^- \vdash a = a \in \llbracket \alpha \rrbracket$ .

- If the derivation is of the form:

$$\frac{\Gamma \# \mathbf{a} : \alpha \vdash M = N : A}{\Gamma \vdash \langle \mathbf{a} : \alpha \rangle M = \langle \mathbf{a} : \alpha \rangle N : \forall \mathbf{a} : \alpha. A} \text{ eq\_abs}$$

then we wish to show that  $\Delta'' \vdash (\langle \mathbf{a} : \alpha \rangle M)[\theta] = (\langle \mathbf{a} : \alpha \rangle N)[\sigma] \in \llbracket \langle \alpha \rangle A^- \rrbracket$ . To prove this, suppose  $\Delta', \Delta'', \mathbf{b}$  are given with  $\Delta'' \vdash \mathbf{b} : \alpha \setminus \Delta'$  and  $\Delta' \succeq \Delta$ . Using logical relation weakening, we have that  $\Delta' \vdash \theta = \sigma \in \llbracket \Gamma^- \rrbracket$ . So we may derive

$$\frac{\Delta'' \vdash \mathbf{b} : \alpha \setminus \Delta' \quad \Delta' \vdash \theta = \sigma \in \llbracket \Gamma^- \rrbracket}{\Delta'' \vdash \theta, \mathbf{b}/\mathbf{a} = \sigma, \mathbf{b}/\mathbf{a} \in \llbracket \Gamma^- \# \mathbf{a} : \alpha \rrbracket}$$

So by induction, we have  $\Delta'' \vdash M[\theta, \mathbf{b}/\mathbf{a}] = N[\sigma, \mathbf{b}/\mathbf{a}] \in \llbracket A^- \rrbracket$ . Moreover,

$$\langle \mathbf{a} : \alpha \rangle M[\theta] @ \mathbf{b} = \langle \mathbf{a} : \alpha \rangle M[\theta] @ \mathbf{b} \xrightarrow{\text{whr}} M[\theta][\mathbf{b}/\mathbf{a}] = M[\theta, \mathbf{b}/\mathbf{a}].$$

Similarly,

$$\langle \mathbf{a} : \alpha \rangle N[\sigma] @ \mathbf{b} = \langle \mathbf{a} : \alpha \rangle N[\sigma] @ \mathbf{b} \xrightarrow{\text{whr}} N[\sigma][\mathbf{b}/\mathbf{a}] = N[\sigma, \mathbf{b}/\mathbf{a}].$$

Hence, using Lemma 4.8, we can conclude that  $\Delta'' \vdash \langle \mathbf{a} : \alpha \rangle M[\theta] @ \mathbf{b} = \langle \mathbf{a} : \alpha \rangle N[\sigma] @ \mathbf{b} \in \llbracket A^- \rrbracket$ . Moreover, since  $\Delta'', \Delta', \mathbf{b}$  were arbitrary, we have that  $\Delta'' \vdash \langle \mathbf{a} : \alpha \rangle M[\theta] = \langle \mathbf{a} : \alpha \rangle N[\sigma] \in \llbracket \langle \alpha \rangle A^- \rrbracket$ , as desired.

- If the derivation is of the form:

$$\frac{\Gamma \vdash \mathbf{b} : \alpha \setminus \Gamma_0 \quad \Gamma_0 \vdash M = N : \forall \mathbf{a} : \alpha. A}{\Gamma \vdash M @ \mathbf{b} = N @ \mathbf{b} : A[\mathbf{b}/\mathbf{a}]} \text{ eq\_conc}$$

then we wish to show that  $\Delta \vdash (M @ \mathbf{b})[\theta] = (N @ \mathbf{b})[\sigma] \in \llbracket A^- \rrbracket$  (noting that  $A[\mathbf{b}/\mathbf{a}]^- = A^-$ ). By Lemma 4.4, we know that  $\theta(\mathbf{b}) = \sigma(\mathbf{b})$  and there must exist  $\Delta_0$  such that  $\Delta \vdash \theta(\mathbf{b}) : \alpha \setminus \Delta_0$  and  $\Delta_0 \vdash \theta - \mathbf{b} = \sigma - \mathbf{b} \in \llbracket \Gamma_0^- \rrbracket$ . Moreover, by induction we have that  $\Delta_0 \vdash M[\theta - \mathbf{b}] = N[\sigma - \mathbf{b}] \in \llbracket \langle \alpha \rangle A^- \rrbracket$ . Observe that  $\Delta_0 \# \theta(\mathbf{b}) : \alpha \vdash \theta(\mathbf{b}) : \alpha \setminus \Delta_0$  is immediately derivable, and that  $\Delta_0 \succeq \Delta_0$  trivially holds. Thus, by definition we have  $\Delta_0 \# \theta(\mathbf{b}) : \alpha \vdash M[\theta - \mathbf{b}] @ \theta(\mathbf{b}) = N[\sigma - \mathbf{b}] @ \theta(\mathbf{b}) \in \llbracket A^- \rrbracket$ . To conclude, we observe that  $M[\theta - \mathbf{b}] @ \theta(\mathbf{b}) = (M @ \mathbf{b})[\theta]$  and  $N[\sigma - \mathbf{b}] @ \theta(\mathbf{b}) = (N @ \mathbf{b})[\sigma]$  since  $\theta(\mathbf{b}) = \sigma(\mathbf{b})$ , and in addition  $\Delta_0 \# \theta(\mathbf{b}) : \alpha \preceq \Delta$  so by weakening we have  $\Delta \vdash (M @ \mathbf{b})[\theta] = (N @ \mathbf{b})[\sigma] \in \llbracket A^- \rrbracket$ , as desired.

- If the derivation is of the form:

$$\frac{\Gamma \vdash \mathbf{b} : \alpha \setminus \Gamma_0 \quad \Gamma_0 \# \mathbf{a} : \alpha \vdash M = N : A}{\Gamma \vdash \langle \mathbf{a} : \alpha \rangle M @ \mathbf{b} = N[\mathbf{b}/\mathbf{a}] : A[\mathbf{b}/\mathbf{a}]} \text{ eq\_nm\_beta}$$

then we must show that  $\Delta \vdash (\langle \mathbf{a} : \alpha \rangle M @ \mathbf{b})[\theta] = (N[\mathbf{b}/\mathbf{a}])[\sigma] \in \llbracket A^- \rrbracket$ , again noting  $A^- = A[\mathbf{b}/\mathbf{a}]^-$ . Again using Lemma 4.4, we know that  $\theta(\mathbf{b}) = \sigma(\mathbf{b})$  and there must exist  $\Delta_0$  such that  $\Delta \vdash \theta(\mathbf{b}) : \alpha \setminus \Delta_0$  and  $\Delta_0 \vdash \theta - \mathbf{b} = \sigma - \mathbf{b} \in \llbracket \Gamma_0^- \rrbracket$ . Moreover, we can derive

$$\frac{\overline{\Delta_0 \# \theta(\mathbf{b}) : \alpha \vdash \theta(\mathbf{b}) : \alpha \setminus \Delta_0 \quad \Delta_0 \vdash \theta - \mathbf{b} = \sigma - \mathbf{b} \in \llbracket \Gamma_0^- \rrbracket}}{\Delta_0 \# \theta(\mathbf{b}) : \alpha \vdash (\theta - \mathbf{b}), \theta(\mathbf{b})/\mathbf{a} = (\sigma - \mathbf{b}), \theta(\mathbf{b})/\mathbf{a} \in \llbracket \Gamma_0^- \# \mathbf{a} : \alpha \rrbracket}}$$

and so, by induction, we have  $\Delta_0 \# \theta(\mathbf{b}) : \alpha \vdash M[\theta - \mathbf{b}, \theta(\mathbf{b})/\mathbf{a}] = N[\sigma - \mathbf{b}, \theta(\mathbf{b})/\mathbf{a}] \in \llbracket A^- \rrbracket$ . Now we observe that:

$$\begin{aligned} ((\langle \mathbf{a} : \alpha \rangle M) @ \mathbf{b})[\theta] &= (\langle \mathbf{a} : \alpha \rangle M)[\theta] @ \mathbf{b}[\theta] \\ &= (\langle \mathbf{a} : \alpha \rangle M[\theta]) @ \theta(\mathbf{b}) \\ &\xrightarrow{\text{whr}} M[\theta][\theta(\mathbf{b})/\mathbf{a}] \\ &= M[\theta - \mathbf{b}][\theta(\mathbf{b})/\mathbf{a}] = M[\theta - \mathbf{b}, \theta(\mathbf{b})/\mathbf{a}] \end{aligned}$$

and

$$\begin{aligned} N[\sigma - \mathbf{b}, \theta(\mathbf{b})/\mathbf{a}] &= N[\sigma - \mathbf{b}][\theta(\mathbf{b})/\mathbf{a}] \\ &= N[\sigma][\sigma(\mathbf{b})/\mathbf{a}] \\ &= N[\mathbf{b}/\mathbf{a}][\sigma]. \end{aligned}$$

Hence, by Lemma 4.8 and weakening  $\Delta_0 \# \theta(\mathbf{b}) : \alpha \preceq \Delta$  we can conclude  $\Delta \vdash ((\langle \mathbf{a} : \alpha \rangle M) @ \mathbf{b})[\theta] = N[\mathbf{b}/\mathbf{a}][\sigma] \in \llbracket A^- \rrbracket$  as desired.

- If the derivation is of the form:

$$\frac{\Gamma \# \mathbf{a} : \alpha \vdash M @ \mathbf{a} = N @ \mathbf{a} : A}{\Gamma \vdash M = N : \mathbb{I} \mathbf{a} : \alpha . A} \text{ eq\_nm\_eta}$$

then we wish to show that  $\Delta \vdash M[\theta] = N[\sigma] \in \llbracket \langle \alpha \rangle A^- \rrbracket$ . To prove this, let  $\Delta', \Delta'', \mathbf{b}$  be given such that  $\Delta'' \vdash \mathbf{b} : \alpha \setminus \Delta'$  and  $\Delta' \succeq \Delta$ . We may then derive:

$$\frac{\Delta'' \vdash \mathbf{b} : \alpha \setminus \Delta' \quad \frac{\Delta \vdash \theta = \sigma \in \llbracket \Gamma^- \rrbracket}{\Delta' \vdash \theta = \sigma \in \llbracket \Gamma^- \rrbracket} W}{\Delta'' \vdash \theta, \mathbf{b}/\mathbf{a} = \sigma, \mathbf{b}/\mathbf{a} \in \llbracket \Gamma^- \# \mathbf{a} : \alpha \rrbracket}$$

where the step labeled  $W$  is by logical relation weakening. So, by induction, we obtain  $\Delta'' \vdash (M @ \mathbf{a})[\theta, \mathbf{b}/\mathbf{a}] = (N @ \mathbf{a})[\sigma, \mathbf{b}/\mathbf{a}] \in \llbracket A^- \rrbracket$ . Moreover, we calculate  $(M @ \mathbf{a})[\theta, \mathbf{b}/\mathbf{a}] = M[\theta, \mathbf{b}/\mathbf{a}] @ \mathbf{b} = M[\theta] @ \mathbf{b}$  since  $\mathbf{a}$  must not appear in  $M$ . Similarly,  $(N @ \mathbf{a})[\sigma, \mathbf{b}/\mathbf{a}] = N[\sigma] @ \mathbf{b}$ . We thus have  $\Delta'' \vdash M[\theta] @ \mathbf{b} = N[\sigma] @ \mathbf{b} \in \llbracket A^- \rrbracket$ , as desired to show  $\Delta \vdash M[\theta] = N[\sigma] \in \llbracket \langle \alpha \rangle A^- \rrbracket$ .

This completes the proof. □

**Theorem 4.12** (Completeness). *If  $\Gamma \vdash M = N : A$  then  $\Gamma^- \vdash M \Leftrightarrow N : A^-$ .*

*Proof.* Immediate, combining Lemma 4.9, Theorem 4.11, and Theorem 4.10. □

**4.3. Decidability, canonical forms and conservativity.** Once we have established that algorithmic equivalence is sound and complete for well-formed terms, we can also extend the algorithmic typechecking rules in Harper and Pfenning's system to handle name-abstractions and verify that all judgments are decidable:

**Theorem 4.13** (Decidability). *All judgments of  $\lambda^{\text{PIII}}$  are decidable.*

We say that a  $\lambda^{\text{PIII}}$  expression is in *canonical form* if it is  $\beta$ -normal and cannot be  $\eta$ -expanded without introducing a  $\beta$ -redex. Canonical forms of  $\lambda^{\text{PIII}}$  are similar to those for



$$\begin{array}{c}
\frac{}{atomic(a)} \quad \frac{atomic(A)}{atomic(A M)} \\
\\
\frac{c : A \in \Sigma}{\Gamma \vdash c \downarrow c : A} \quad \frac{x : A \in \Gamma}{\Gamma \vdash x \downarrow x : A} \quad \frac{\Gamma \vdash M \downarrow M' : \Pi x:A.B \quad \Gamma \vdash N \uparrow N' : A}{\Gamma \vdash M N \downarrow M' N' : B[N'/x]} \\
\frac{a : \alpha \in \Gamma}{\Gamma \vdash a \downarrow a : \alpha} \quad \frac{\Gamma \vdash a:\alpha \setminus \Gamma' \quad \Gamma' \vdash M \downarrow N : \mathbf{!}a:\alpha.B}{\Gamma \vdash M@a \downarrow N@a : B} \\
\frac{\Gamma, x : A \vdash M x \uparrow N : B}{\Gamma \vdash M \uparrow \lambda x:A.N : \Pi x:A.B} \quad \frac{\Gamma \# a:\alpha \vdash M@a \uparrow N : B}{\Gamma \vdash M \uparrow \langle a:\alpha \rangle N : \mathbf{!}a:\alpha.A} \\
\frac{\Gamma \vdash M \downarrow N : A \quad atomic(A)}{\Gamma \vdash M \uparrow N : A} \quad \frac{M \xrightarrow{whr} M' \quad \Gamma \vdash M' \uparrow N : A \quad atomic(A)}{\Gamma \vdash M \uparrow N : A} \\
\\
\frac{a : K \in \Sigma}{\Gamma \vdash a \downarrow a : K} \quad \frac{\alpha : name \in \Sigma}{\Gamma \vdash \alpha \downarrow \alpha : K} \quad \frac{\Gamma \vdash A \downarrow A' : \Pi x:A.K \quad \Gamma \vdash M \uparrow M' : A}{\Gamma \vdash A M \downarrow A' M' : K[M'/x]} \\
\frac{\Gamma \vdash A \downarrow A' : type}{\Gamma \vdash A \uparrow A' : type} \quad \frac{\Gamma \vdash A \uparrow A' : type \quad \Gamma, x:A' \vdash B \uparrow B' : type}{\Gamma \vdash \Pi x:A.B \uparrow \Pi x:A'.B' : type} \quad \frac{\Gamma \# a:\alpha \vdash B \uparrow B' : type}{\Gamma \vdash \mathbf{!}a:\alpha.B \uparrow \mathbf{!}a:\alpha.B' : type} \\
\\
\frac{}{\Gamma \vdash type \uparrow type : kind} \quad \frac{\Gamma \vdash A \uparrow A' : type \quad \Gamma, x:A' \vdash K \uparrow K' : kind}{\Gamma \vdash \Pi x:A.K \uparrow \Pi x:A'.K' : kind}
\end{array}$$

Figure 15: Canonicalization

LF, but can include name-abstractions and concretions. The following grammar describes the syntax of canonical and atomic forms:

$$\begin{aligned}
M_c & ::= \lambda x:A_c.M_c \mid \langle a:\alpha \rangle M_c \mid M_a \\
M_a & ::= c \mid a \mid M_a M_c \mid M_a@a \\
A_c & ::= a \mid \alpha \mid A_c M_c \mid \Pi x:A_c.B_c \mid \mathbf{!}a:\alpha.A_c \\
K_c & ::= type \mid \Pi x:A_c.K_c
\end{aligned}$$

Note, however, that not all terms matching the above grammar are in canonical or atomic form; further typing constraints are needed to ensure full  $\eta$ -expansion. We give an inference rule system for canonicalizing object terms, which also implicitly gives the typing constraints that canonical forms must satisfy, in Figure 15. In particular, the  $atomic(-)$  predicate is used to restrict weak head normalization and ensure only atomic forms whose type is an atomic type  $A M_1 \cdots M_n$  can be considered canonical.

We will show:

**Theorem 4.14** (Canonical forms). *Assume that all the types and kinds in  $\Gamma$ ,  $\Sigma$  and  $A$  are in canonical form. Then:*

- (1) *If  $\Gamma \vdash M : A$  then there exists a canonical  $P$  such that  $\Gamma \vdash M \uparrow P : A$  and  $\Gamma \vdash M = P : A$ .*
- (2) *If  $P'$  also satisfies  $\Gamma \vdash M \uparrow P' : A$ , then  $P = P'$ .*
- (3) *If  $\Gamma \vdash M = N : A$  holds, then their canonical forms are equal.*

To show the canonicalization theorem, we first show the stronger property:

**Lemma 4.15** (Algorithmically equivalent terms have common canonical forms). *Assume that all types and kinds in  $\Sigma, \Gamma, A$  and  $B$  are in canonical form. Then:*

- (1) *If  $\Gamma \vdash M : A$  and  $\Gamma \vdash N : B$  and  $\Gamma^- \vdash M \leftrightarrow N : \tau$  then  $\Gamma \vdash A = B : \text{type}$  and  $A^- = B^- = \tau$  and there exists  $P$  such that  $\Gamma \vdash M \downarrow P : A$  and  $\Gamma \vdash N \downarrow P : A$ .*
- (2) *If  $\Gamma \vdash M : A$  and  $\Gamma \vdash N : A$  and  $\Gamma^- \vdash M \leftrightarrow N : A^-$  then there exists  $P$  such that  $\Gamma \vdash M \uparrow P : A$  and  $\Gamma \vdash N \uparrow P : A$ .*

*Proof.* By structural induction on the algorithmic derivations, using inversion and injectivity of products as appropriate. For the ordinary cases, we need the assumption that  $\Sigma, \Gamma, A, B$  are already canonical in order to ensure that type tags in  $M, N$  are compatible. We show the cases specific to  $\lambda^{\text{PI}}$ :

- If the derivation is of the form

$$\frac{\mathbf{a}:\alpha \in \Gamma^-}{\Gamma^- \vdash \mathbf{a} \leftrightarrow \mathbf{a} : \alpha}$$

then we must have that  $M = \mathbf{a} = N$  and  $A = \alpha = B$  and  $\mathbf{a}:\alpha \in \Gamma$ , so we can conclude that  $\Gamma \vdash \alpha = \alpha : \text{type}$  and derive

$$\frac{\mathbf{a}:\alpha \in \Gamma}{\Gamma \vdash \mathbf{a} \downarrow \mathbf{a} : \alpha} \quad \frac{\mathbf{a}:\alpha \in \Gamma}{\Gamma \vdash \mathbf{a} \downarrow \mathbf{a} : \alpha}$$

- If the derivation is of the form

$$\frac{\Gamma^- \vdash \mathbf{a}:\alpha \setminus \Delta' \quad \Delta' \vdash M \leftrightarrow N : \langle \alpha \rangle \tau}{\Gamma^- \vdash M @ \mathbf{a} \leftrightarrow N @ \mathbf{a} : \tau}$$

By inversion we have  $\Gamma \vdash \mathbf{a}:\alpha_1 \setminus \Gamma_1$  and  $\Gamma_1 \vdash M : \mathbf{Ia}:\alpha_1.A_1$ . Similarly, we have  $\Gamma \vdash \mathbf{a}:\alpha_2 \setminus \Gamma_2$  and  $\Gamma_2 \vdash N : \mathbf{Ia}:\alpha_2.A_2$ . Moreover we must have  $\alpha_1 = \alpha_2$  and  $\Gamma_1 = \Gamma_2$ ; also, we must have  $\Gamma_0^- = \Delta'$ . So, the induction hypothesis applies and we know that  $\Gamma_1 \vdash \mathbf{Ia}:\alpha_1.A_1 = \mathbf{Ia}:\alpha_2.A_2 : \text{type}$  and  $(\mathbf{Ia}:\alpha_1.A_1)^- = \langle \alpha \rangle \tau = (\mathbf{Ia}:\alpha_2.A_2)^-$ , which implies that  $\alpha_1 = \alpha = \alpha_2$  and  $A_1^- = \tau = A_2^-$ . In fact, since  $A_1$  and  $A_2$  are in canonical form already, we must have  $A_1 = A_2$ . Furthermore, by induction we also have  $\Gamma \vdash M \downarrow P : \mathbf{Ia}:\alpha.A_1$  and  $\Gamma \vdash N \downarrow P : \mathbf{Ia}:\alpha.A_1$ . To conclude, we may derive:

$$\frac{\frac{\Gamma \vdash \mathbf{a}:\alpha \setminus \Gamma_1 \quad \Gamma_1 \vdash M \downarrow P : \mathbf{Ia}:\alpha.A_1}{\Gamma \vdash M @ \mathbf{a} \downarrow P @ \mathbf{a} : A_1}}{\Gamma \vdash \mathbf{a}:\alpha \setminus \Gamma_1 \quad \Gamma_1 \vdash N \downarrow P : \mathbf{Ia}:\alpha.A_1}}{\Gamma \vdash N @ \mathbf{a} \downarrow P @ \mathbf{a} : A_1}$$

- If the derivation is of the form

$$\frac{\Gamma^- \# \mathbf{a}:\alpha \vdash M @ \mathbf{a} \leftrightarrow N @ \mathbf{a} : \tau}{\Gamma^- \vdash M \leftrightarrow N : A^-}$$

then we must have that  $A^- = \langle \alpha \rangle \tau$  for some  $\alpha$  and  $\tau$  and so  $A$  must be of the form  $\mathbf{Ia}:\alpha.B$  where  $B^- = \tau$ . Thus, we have derivation  $\Gamma^- \# \mathbf{a}:\alpha \vdash M @ \mathbf{a} \leftrightarrow N @ \mathbf{a} : B^-$ . Moreover, we can derive  $\Gamma \# \mathbf{a}:\alpha \vdash M @ \mathbf{a} : B$  and  $\Gamma \# \mathbf{a}:\alpha \vdash N @ \mathbf{a} : B$ . So by induction we have derivations  $\Gamma \# \mathbf{a}:\alpha \vdash M @ \mathbf{a} \uparrow P : B$  and  $\Gamma \# \mathbf{a}:\alpha \vdash N @ \mathbf{a} \uparrow P : B$ , so we can conclude by deriving:

$$\frac{\Gamma \# \mathbf{a}:\alpha \vdash M @ \mathbf{a} \uparrow P : B}{\Gamma \vdash M \uparrow \langle \mathbf{a}:\alpha \rangle P : \mathbf{Ia}:\alpha.B} \quad \frac{\Gamma \# \mathbf{a}:\alpha \vdash N @ \mathbf{a} \uparrow P : B}{\Gamma \vdash N \uparrow \langle \mathbf{a}:\alpha \rangle P : \mathbf{Ia}:\alpha.B}$$

□

We also can easily show that canonicalization is sound with respect to definitional equivalence:

**Lemma 4.16** (Soundness of canonicalization).

- (1) If  $\Gamma \vdash M \downarrow P : A$  then  $\Gamma \vdash M = P : A$ .
- (2) If  $\Gamma \vdash M \uparrow P : A$  then  $\Gamma \vdash M = P : A$ .

We also need to show that the canonicalization judgment is deterministic:

**Lemma 4.17** (Determinism of canonicalization).

- (1) If  $\Gamma \vdash M \downarrow P : A$  and  $\Gamma \vdash M \downarrow P' : A'$  then  $P = P'$  and  $A = A'$ .
- (2) If  $\Gamma \vdash M \uparrow P : A$  and  $\Gamma \vdash M \uparrow P' : A'$  then  $P = P'$ .

*Proof.* By induction on derivations and inversion. □

The above lemmas imply the first and second parts of the Canonicalization Theorem. The third part follows by inspection of the rules for canonicalization, since if  $A$  and  $\Gamma$  are already in canonical form then any types that are copied into the result of canonicalization will also be canonical.

Moreover, we can use the canonicalization rules for types and kinds shown in Figure 15 to canonicalize  $\Sigma$ ,  $\Gamma$  and  $A$ , so we have the following stronger result:

**Theorem 4.18.** *If  $\Sigma$  and  $\Gamma$  are in canonical form and  $\Gamma \vdash M : A$  then there exist unique canonical  $A'$  and  $M'$  such that  $\Gamma \vdash A = A' : \text{type}$  and  $\Gamma \vdash M = M' : A'$ .*

Finally, the canonical forms theorem implies  $\lambda^{\text{PIII}}$  is a conservative extension of LF in the sense that it introduces no new derivable LF judgments.

**Corollary 4.19** (Conservativity). *If  $\Gamma \vdash \mathcal{J}$  is an LF judgment over a valid LF signature  $\Sigma$  and is derivable in  $\lambda^{\text{PIII}}$ , then  $\Gamma \vdash \mathcal{J}$  is derivable in LF.*

## 5. ADEQUACY

It is a significant concern whether a given signature correctly represents an object language we have in mind. This property is often referred to as *adequacy* in an LF settings [15, 6]. As in LF, adequacy in  $\lambda^{\text{PIII}}$  relies upon the existence of (unique) canonical forms.

In this section, we sketch an adequacy argument for a typical object language, the untyped lambda-calculus equipped with an inequality predicate (as shown in the introduction).

Recall the signature given in Figure 1. The canonical forms of expressions of type  $e$  in  $\lambda^{\text{PIII}}$  are generated by the grammar:

$$M_0, N_0 ::= \text{var } x \mid \text{app } M_0 N_0 \mid \text{lam } \langle x : e \rangle M_0$$

The encoding is defined on object-language terms as follows:

$$\ulcorner x \urcorner = \text{var } x \quad \ulcorner t \ u \urcorner = \text{app } \ulcorner t \urcorner \ulcorner u \urcorner \quad \ulcorner \lambda x. t \urcorner = \text{lam } \langle x \rangle \ulcorner t \urcorner$$

The main result concerning the correctness of the encoding is:

**Theorem 5.1** (Adequacy of encoding). *The encoding function  $\ulcorner - \urcorner$  is injective and maps object language terms  $t$  (having free variables  $x_1, \dots, x_n$ ) onto the set of canonical forms of type  $e$  (in context  $x_1 : v \# \dots \# x_n : v$ ). Moreover, the encoding function commutes with renaming, that is,  $\ulcorner t[x/y] \urcorner = \ulcorner t \urcorner[x/y]$ .*

Furthermore, we can reason by inversion on canonical forms to establish that the alpha-inequality judgment holds precisely for terms whose encodings are different modulo alpha-equivalence:

**Theorem 5.2** (Adequacy of *neq*). *Suppose we have object terms  $t, u$  with free variables  $x_1, \dots, x_n$ . Then  $t \not\equiv_\alpha u$  if and only if  $x_1:v \# \dots \# x_n:v \vdash \mathcal{D} : neq \ulcorner t \urcorner \ulcorner u \urcorner$  is derivable for some (canonical)  $\mathcal{D}$ .*

*Proof.* The forward direction is straightforward. The reverse direction is proved by induction on the canonical form of the proof term  $\mathcal{D}$ . One key case is when  $\mathcal{D}$  is of the form  $neq\_v\_v @_{x_i} @_{x_j}$ . In this case, we must have  $\ulcorner t \urcorner = var\ x_i$  and  $\ulcorner u \urcorner = var\ x_j$  for some  $i \neq j$ , since otherwise  $\mathcal{D}$  would be ill-formed. Clearly, then  $t$  must be  $x_i$  and  $u$  must be  $x_j$  which are not  $\alpha$ -equivalent.

Another key case is that for  $\mathcal{D} = neq\_l\_l M_1 M_2 \mathcal{D}' : neq (\ulcorner t_1 \urcorner) (\ulcorner t_2 \urcorner)$ . In this case, we know that  $\ulcorner t_1 \urcorner = lam\ M_1$  and  $\ulcorner t_2 \urcorner = lam\ M_2$ , so  $t_1 = \lambda x.t'_1$  and  $t_2 = \lambda x.t'_2$  for some  $x, t'_1, t'_2$  (without loss of generality we can assume the same name  $x$  is used for both and  $x$  is fresh for all other terms). Hence  $M_1 = \langle x \rangle \ulcorner t'_1 \urcorner$  and  $M_2 = \langle x \rangle \ulcorner t'_2 \urcorner$  which means that the subderivation  $\mathcal{D}'$  must have type  $\mathbf{I}x.neq ((\langle x \rangle \ulcorner t'_1 \urcorner) @ x) ((\langle x \rangle \ulcorner t'_2 \urcorner) @ x)$ . By weakening the context to include name  $x : v$  and  $\beta$ -converting, we can see that  $\mathcal{D}' @ x$  must also have type  $neq (\ulcorner t'_1 \urcorner) (\ulcorner t'_2 \urcorner)$ . Moreover,  $\mathcal{D}' @ x$  must have a canonical form of this type, and so by induction we know that  $t'_1 \not\equiv_\alpha t'_2$ . This implies  $t_1 = \lambda x.t'_1 \not\equiv_\alpha \lambda x.t'_2 = t_2$ .  $\square$

## 6. EXTENSIONS AND EXAMPLES

In previous work on a simple nominal type theory [5] we discussed extensions such as name-comparison operations, lists, datatypes involving name-binding, and recursion combinators for defining functions over such datatypes. These extensions were motivated by a denotational interpretation of SNTT using nominal sets (following [28]). We will not develop a denotational semantics of  $\lambda^{\text{PIII}}$  here; however, the topos of nominal sets provides all of the necessary structure to interpret dependent types, and it seems clear that the extensions we consider can be justified using Schöpp and Stark's semantics for a more general nominal type theory [37, 35] or using Pitts' approach to recursion in a slightly different nominal type theory [30, 31].

In this section we recapitulate and generalize extensions for name-comparison, recursive function definitions and inductive reasoning in  $\lambda^{\text{PIII}}$ . The computational extensions can easily be proved type-sound but do not necessarily preserve the canonicalization or decidability properties established earlier; we expect that these extensions would be more relevant to intensional type theories where only  $\beta$ -normalization results are needed. We also discuss applications of  $\lambda^{\text{PIII}}$  as a framework for defining logics and for encoding proof terms about languages with names and binding.

**Name-comparison.** First, we consider a name comparison operation:

$$\begin{aligned} cond_\alpha &: \langle \langle \alpha \rangle \rangle \alpha \rightarrow A \rightarrow (\alpha \rightarrow A) \rightarrow A \\ cond_\alpha &(\langle x \rangle x) M N \rightarrow_\beta M \quad cond_\alpha(\langle x \rangle y) M N \rightarrow_\beta N y \end{aligned}$$

This takes a name-abstraction and two additional arguments  $M : A, N : \alpha \rightarrow A$ . If the abstraction is of the form  $\langle x \rangle x$ , we return  $M$ , otherwise, if it is of the form  $\langle y \rangle x$  where  $x \neq y$ ,

we return  $N x$ . Note that it would make little sense to allow the type  $A$  to depend on  $x$  since  $x$  may not “escape” in the first case.

Recursion. Now consider the standard nominal datatype encoding of the lambda-calculus introduced in the introduction (Figure 1). This datatype admits an obvious dependently-typed recursion principle:

$$\begin{aligned} \text{rec}_e^T & : (\Pi X : v.T (\text{var } X)) \rightarrow \\ & (\Pi M, N : e.T M \rightarrow T N \rightarrow T (\text{app } M N)) \rightarrow \\ & (\Pi M : \langle\langle v \rangle\rangle e. (\Pi \mathbf{a} : v.T (M @ \mathbf{a})) \rightarrow T (\text{lam } M)) \rightarrow \\ & \Pi M : e.T M \end{aligned}$$

for any  $T : \Pi x : e.\text{type}$ . We also equip  $\text{rec}_e^T$  with the obvious rewriting rules for *var* and *app*, along with

$$\text{rec}_e^T V A L (\text{lam } F) \rightarrow_{\beta} L(\langle \mathbf{a} : v \rangle \text{rec}_e^T V A L (F @ \mathbf{a}))$$

(provided  $\mathbf{a} \notin FV(V, A, L, F)$ ) for lambda-abstractions.

**6.1. Closure conversion.** *Closure conversion* (see for example [1]) is an important transformation in functional language compilation. A function is closed if it refers only to its argument and locally defined variables, not to variables whose scope began outside the function. Closure conversion translates an arbitrary expression to one containing only closed functions. There are many ways of doing this, embodying different approaches to managing the environment. We consider a simplistic approach in which each function is translated to a pair consisting of a closed function and an environment containing all non-local variable values. We define the translation of a term  $e$  that is well-formed in context  $\Gamma$  and environment  $env$  as  $C[\Gamma \vdash e]env$ , where

$$\begin{aligned} C[\Gamma, x \vdash x]env & = \pi_1(env) \\ C[\Gamma, x \vdash y]env & = C[\Gamma \vdash y]\pi_2(env) \\ C[\Gamma \vdash e_1 e_2]env & = \mathbf{let } z = C[\Gamma \vdash e_1]env \\ & \quad \mathbf{in } (\pi_1(z)) \langle C[\Gamma \vdash e_2]env, \pi_2(z) \rangle \\ C[\Gamma \vdash \lambda x.e]env & = \langle \lambda y.C[\Gamma, x \vdash e]y, env \rangle \end{aligned}$$

where  $x \neq y$  in the second equation,  $z \notin FV(\Gamma, e_1, e_2)$  in the third, and  $y \notin FV(\Gamma, x, e, e_0)$  in the fourth. Note that we include let-bindings here for convenience.

**Example 6.1.** As a simple example, consider the closure-conversion of the  $K$ -combinator:

$$\begin{aligned} C[\Gamma \vdash \lambda x.\lambda y.x]env & = \langle \lambda x'.C[\Gamma, x \vdash \lambda y.x]x', env \rangle \\ & = \langle \lambda x'.\langle \lambda y'.C[\Gamma, x, y \vdash x]y', x' \rangle, env \rangle \\ & = \langle \lambda x'.\langle \lambda y'.C[\Gamma, x \vdash x](\pi_2(y')), x' \rangle, env \rangle \\ & = \langle \lambda x'.\langle \lambda y'.\pi_1(\pi_2(y')), x' \rangle, env \rangle \end{aligned}$$

Closure conversion seems like a natural candidate for encoding in a logical framework, because it seems to involve only syntactic manipulation of ordinary  $\lambda$ -terms. For example, Hannan [12] studied closure conversion algorithms encoded in LF. However, there are some subtle issues which seem to complicate formalizing closure conversion in LF. First, if we take  $\text{lam} : (exp \rightarrow exp) \rightarrow exp$ , there is no explicit case for variables. This can be fixed by making sure to add a local hypothesis  $is\_var(x)$  for each  $\lambda$ -term variable  $x$  as  $x$  is added to the context. This approach is commonly taken in LF developments [7], and is believed correct as long as there is no way to construct a term of type  $is\_var(M)$  where  $M$  is not a variable.

<i>unit</i>	: <i>exp</i> .
<i>pair</i>	: <i>exp</i> → <i>exp</i> → <i>exp</i> .
<i>pi</i> <sub>1</sub>	: <i>exp</i> → <i>exp</i> .
<i>pi</i> <sub>2</sub>	: <i>exp</i> → <i>exp</i> .
<i>let</i>	: <i>exp</i> → ( $\langle\langle id \rangle\rangle$ <i>exp</i> ) → <i>exp</i> .
<i>cconv</i>	: <i>list id</i> → <i>exp</i> → <i>exp</i> → <i>exp</i> → type.
<i>cconv_v1</i>	: <i>cconv</i> [G, X] ( <i>var</i> X) <i>Env</i> ( <i>pi</i> <sub>1</sub> <i>Env</i> ).
<i>cconv_v2</i>	: <i>cconv</i> [G, X] ( <i>var</i> Y) <i>Env</i> E ← <i>neq</i> X Y
	← <i>cconv</i> G ( <i>var</i> Y) ( <i>pi</i> <sub>2</sub> <i>Env</i> ) E.
<i>cconv_a</i>	: <i>cconv</i> G ( <i>app</i> E <sub>1</sub> E <sub>2</sub> ) <i>Env</i> ( <i>let</i> E <sub>11</sub> ( $\langle z: id \rangle$ <i>app</i> ( <i>pi</i> <sub>1</sub> ( <i>var</i> (z))) ( <i>pair</i> E <sub>21</sub> ( <i>pi</i> <sub>2</sub> ( <i>var</i> (z))))))
	← <i>cconv</i> G E <sub>1</sub> <i>Env</i> E <sub>11</sub>
	← <i>cconv</i> G E <sub>2</sub> <i>Env</i> E <sub>21</sub> .
<i>cconv_l</i>	: <i>cconv</i> G ( <i>lam</i> F <sub>1</sub> ) <i>Env</i> ( <i>pair</i> ( <i>lam</i> F <sub>2</sub> ) <i>Env</i> )
	← $\mathbf{Ix}.\mathbf{My}.$ <i>cconv</i> [G, x] (F <sub>1</sub> @x) ( <i>var</i> y) (F <sub>2</sub> @y).

Figure 16: Closure conversion translation

<i>pf</i>	: <i>list_o</i> → <i>o</i> → type.
<i>assignI</i>	: <i>pf</i> (G@x) ( <i>box</i> (x := T@x) (P@x)) ← ( $\mathbf{My}.$ <i>v.pf</i> [G@x, <i>var</i> y = T@x] (P@y)).
<i>assignE</i>	: <i>pf</i> (G@x) (Q@x)
	← <i>pf</i> (G@x) ( <i>box</i> (x := T@x) (P@x)) ← ( $\mathbf{My}.$ <i>v.pf</i> [G, <i>var</i> y = T@x, P@y] (Q@x)).

Figure 17: Representative inference rules of dynamic logic

Alternatively, we could adopt a weaker encoding in which  $lam : (var \rightarrow exp) \rightarrow exp$ , thus foregoing the benefits of built-in capture-avoiding substitution.

Second, however, in LF we cannot directly test variables for equality. Hannan [12] neither presented a concrete LF encoding nor discussed how to overcome these obstacles. Using Crary’s technique [7], we can test inequality among variables by tagging variables with distinct numerical tags, but this requires modifying all predicates in which inequality testing might be needed (see the discussion in the next section).

In  $\lambda^{\text{III}}$ , we can define closure conversion directly as a relation, as shown in Figure 16. We use a definable type of lists of identifiers *list\_id*, and define syntax for pairing, projection, and **let**. The variable inequality side-condition on the case for different variables  $x, y$  is handled using *neq*. The rest of the translation is straightforward.

**6.2. Dynamic logic.** Dynamic logic (DL) [13] is a generalization of program logics such as Hoare logic. In DL, besides ordinary propositional connectives and quantifiers, there is a syntactic class of *programs*  $\alpha$ , and a modal connective  $[\alpha]\phi$ . Such a formula has the intended interpretation, “After any terminating execution of program  $\alpha$ ,  $\phi$  necessarily holds”. Programs can in general be nondeterministic or nonterminating, so  $[\alpha]\phi$  is trivially true if  $\alpha$  diverges; on the other hand,  $[\alpha]\phi$  does not hold if there is a possible terminating execution of  $\alpha$  in a state not satisfying  $\phi$ . Thus, a DL formula  $\phi \implies [\alpha]\psi$  has the same meaning as a Hoare logic partial correctness assertion  $\{\phi\}\alpha\{\psi\}$ .

An important, but counterintuitive, aspect of dynamic logic is that variables are used both for quantification and as assignment targets in programs. As a result, it does not make sense to substitute an expression for a variable name  $x$  everywhere in its scope, because it might occur on the left-hand side of an assignment, and it would not make sense to substitute an expression there. For example,  $\forall x.[x := 0](x = 0)$  is a well-formed (and valid) formula of DL, but  $[1 := 0]1 = 0$ , the result of substituting a non-variable such as 1 for  $x$ , is nonsense.

Proof rules for the assignment operation  $x := t$  are challenging to encode in a logical framework. Honsell and Miculan [16] considered a natural deduction formulation of DL implemented in Coq. Their proof system included the following inference rules to deal with assignment:

$$\frac{\Gamma, y = t \vdash \phi[y/x] \quad (y \notin FV(\Gamma, \phi, t))}{\Gamma \vdash [x := t]\phi} :=I$$

$$\frac{\Gamma \vdash [x := t]\phi \quad \Gamma, y = t, \phi[y/x] \vdash \psi \quad (y \notin FV(\Gamma, \phi, \psi, t))}{\Gamma \vdash \psi} :=E$$

The main obstacle to encoding dynamic logic using higher-order abstract syntax is that there is no easy way to talk about distinct or fresh object variable names. To deal with the freshness side conditions, Honsell and Miculan adapted a technique introduced for encoding Hoare logic in LF by Avron, Honsell, Mason, and Pollack [20, 2]. In this technique, explicit judgments  $isin : \Pi T:\text{type}.v \rightarrow T \rightarrow \text{type}$  and  $isnotin : \Pi T:\text{type}.v \rightarrow T \rightarrow \text{type}$  are introduced to encode the property that a variable name occurs free in (does not occur free in) an object of type  $T$  (an expression, formula, program, etc.). Both LF and Coq encodings are verbose and require explicit low-level reasoning about name occurrences, freshness, and inequality.

In  $\lambda^{\text{IM}}$ , using names and dependent name types, we can encode the problematic inference rules as shown in Figure 17. Again, we use a definable type of lists of formulas  $list\_o$  for the hypotheses  $\Gamma$ .

Here, we have taken an approach that represents the context explicitly as part of the judgment, that is,  $pf : list\_o \rightarrow o \rightarrow \text{type}$ . An alternative approach to encoding hypothetical judgments, usually preferred in LF, is to encode only the conclusion via a predicate  $pf : o \rightarrow \text{type}$  and then use local  $pf$  assumptions to represent local hypotheses.

$$\begin{aligned} assignI' & : pf (box (x := T@x) (P@x)) \\ & \leftarrow (\mathbf{I}y:v. (pf (var y = T@x)) \rightarrow pf (P@y)). \\ assignE' & : pf (Q@x) \\ & \leftarrow (pf (box (x := T@x) (P@x))) \\ & \leftarrow (\mathbf{I}y:v.(pf (var y = T@x)) \rightarrow pf (P@y) \rightarrow pf (Q@x)). \end{aligned}$$

This appears correct for  $\lambda^{\text{IM}}$  as presented in this article. However, if we read these types as nominal logic formulas then their meaning does not correspond to the judgments we want to encode. The reason is that nominal logic satisfies an *equivariance* property, which is not explicitly reflected in  $\lambda^{\text{IM}}$ . Equivariance states that the validity of any proposition is preserved by applying a name-permutation to all of its arguments. In a type theory, this can be represented by introducing a swapping term  $\pi \cdot M$  such that (roughly speaking) if  $\Gamma \vdash M : A$  then  $\Gamma \vdash \pi \cdot M : \pi \cdot A$ . (This is done, in a simple type theory, for Pitts' Nominal System T [30, 31], discussed in the next section.) Representing hypothetical judgments using local implications is incorrect in full nominal logic because equivariance can be used

to break the connection between names in  $\Gamma$  and names in the conclusion; to avoid this, local assumptions have to be made explicit as an argument of the judgment. Because we view adding additional features of nominal logic (such as swapping/equivariance) to  $\lambda^{\text{PI}}$  as an important next step, we prefer to give an example that appears robust in the face of these extensions. In addition, using this approach we cannot hope to use nominal recursion or induction principles over proofs, because of the negative occurrences of  $pf$ .

Another alternative would be to represent hypotheses using  $\mathbf{V}$ -quantification or name-abstraction:

$$\begin{aligned}
\text{assign}I'' & : (pf (\text{box } (x := T@x)(P@x))) \\
& \leftarrow (\mathbf{V}y:v. \langle\langle pf (\text{var } y = T@x) \rangle\rangle pf (P@y)). \\
\text{assign}E'' & : pf (Q@x) \\
& \leftarrow (pf (\text{box } (x := T@x) (P@x))) \\
& \leftarrow (\mathbf{V}y:v. \langle\langle pf (\text{var } y = T@x) \rangle\rangle \langle\langle pf (P@y) \rangle\rangle pf (Q@x)).
\end{aligned}$$

Doing this would avoid the non-positivity issue, but would still have the other drawbacks of the ordinary local hypotheses approach discussed above. It would also require allowing name types to depend on values (including other names); we could do this by making name into a first-class kind. However, this poses both conceptual and practical problems. The conceptual problem is that name-types are usually interpreted as infinite sets of swappable atoms, which are not mixed with ordinary values. At a semantic level, it is not clear what we mean by abstracting by an ordinary data type or judgment (however, Schöpp's study [36] of nominal set semantics for Miller and Tiu's logic of generic judgments [22] may offer a solution). The practical problem is that if name-types can depend on other names, then the context restriction operation  $\Gamma \vdash a:\alpha \setminus \Gamma'$  needs to remove not only all variables introduced after  $a$ , but also all variables or names whose type depends on  $a$ . This seems workable, but makes the system considerably more complex, while it is not yet clear that the extra complexity is justified by applications. We view extending name-types to a first-class kind to be an important area for future work.

## 7. COMPARISON WITH RELATED SYSTEMS

**7.1. LF.** We argued earlier that the intuitive definition of alpha-inequality cannot be translated directly to LF. This is a somewhat subjective claim. At a technical level, the issue is that in LF, object-language variables are represented as meta-language variables, which cannot be compared directly for (in)equality. That is, we cannot simply translate the rule

$$\frac{x \neq y}{\text{var}(x) \neq_{\alpha} \text{var}(y)}$$

directly to LF in a compositional way. A naive attempt to represent this rule by declaring a type constant such as

$$a : \Pi x:\alpha. \Pi y:\alpha. \text{neq } x \ y.$$

is clearly wrong since this defines the total relation on expressions. The following proposition shows that there is no way to translate name-inequality to a binary predicate in LF that works correctly in all contexts:



```

exp : type.
lam : (exp -> exp) -> exp.
app : exp -> exp -> exp.

nat : type.
z : nat.
s : nat -> nat.
neq : nat -> nat -> type.
- : neq (s X) z.
- : neq z (s _).
- : neq (s N) (s M) <- neq N M.

bvar : exp -> nat -> type.

aneqi : nat -> exp -> exp -> type.
- : aneqi N X Y <- bvar X MX <- bvar Y MY <- neq MX MY.
- : aneqi N (app E1 E2) (app E3 E4) <- aneqi N E1 E3.
- : aneqi N (app E1 E2) (app E3 E4) <- aneqi N E2 E4.
- : aneqi N (lam E1) (lam E2) <-
  ({x : exp} bvar X N -> aneqi (s N) (E1 x) (E2 x)).
- : aneqi N X (app _ _) <- bvar X _.
- : aneqi N X (lam _) <- bvar X _.
- : aneqi N (app _ _) X <- bvar X _.
- : aneqi N (lam _) X <- bvar X _.
- : aneqi N (app _ _) (lam _).
- : aneqi N (lam _) (app _ _).

aneq : exp -> exp -> type.
aneq_i : aneq E1 E2 <- aneqi z E1 E2.

```

Figure 18: Alpha-inequivalence in LF

**Proposition 7.1.** *Let  $\Sigma$  be an LF signature,  $t : \text{type}$  a constant type in  $\Sigma$  and  $r : t \rightarrow t \rightarrow \text{type}$  be a constant in  $\Sigma$ . Then whenever  $\Gamma, x:t, y:t, \Gamma' \vdash M : r \ x \ y$  is derivable for two different variables  $x, y$ , the judgment  $\Gamma, x:t, \Gamma'[x/y] \vdash M[x/y] : r \ x \ x$  is also derivable.*

*Proof.* Direct using substitution. □

This implies that if we want to define relations involving variable inequality, we need to ensure that there are appropriate hypotheses in  $\Gamma$  that can be used to prove that variables introduced at different binding sites are distinct. For example, using Cray’s technique of adding natural number labels for bound names as they are introduced in the context [7], we can implement alpha-inequivalence as shown in Figure 18. (A similar encoding is possible using weak higher-order abstract syntax techniques, as in the Theory of Contexts [17].)

Clearly it is a subjective question whether the other advantages of LF outweigh the extra effort needed to encode judgments that do involve name-inequality. In this article, our goal has been to explore the alternative offered by nominal abstract syntax in a dependently-typed setting, not to propose a replacement for LF.

**7.2. Schöpp and Stark’s dependent type theories.** Schöpp and Stark introduced dependent type theories that capture the topos-theoretic semantics of nominal sets. (The category of nominal sets is isomorphic to the Schanuel topos, known from sheaf theory [18]). In particular, they consider both ordinary and “fresh” dependent product spaces, dependent sums, and a “free from” type of pairs  $(a, M)$  where  $a$  is a name fresh for  $M$ . The “fresh” versions of these types quantify over objects whose names are fresh for the current context; these generalize the fresh-name quantifier  $\mathbf{N}$ . The type theory is based on using bunched contexts (derived from the Logic of Bunched Implications).

Schöpp and Stark’s systems are very expressive: they can express recursive functions over nominal abstract syntax, as well as proofs by induction, as outlined earlier in this article. But they also appear quite difficult to use in an automated system. In particular, there are no results on strong normalization or decidability of equivalence and typechecking for these systems, and it does not seem easy to adapt standard results because of the use of bunched contexts. The results in this paper can be seen as a first step in this direction, focusing on a simple subsystem of theirs which captures at least some of the expressiveness of nominal abstract syntax.

**7.3. Nominal System T and related systems.** Pitts’ Nominal System T [30, 31] is a simply-typed calculus that is also an attractive starting point for a dependent nominal type theory. In contrast to SNTT or  $\lambda^{\mathbf{N}}$ , it has ordinary (non-bunched) contexts and also supports explicit name-swapping and locally-scoped names. Unfortunately, these features interact with dependent types in complex ways, making it non-obvious how to extend Nominal System T to a dependent type theory. In this section, we give an example that highlights the problem<sup>1</sup>. We give only the description of the problem, not a full formalization of a putative “Dependent Nominal System T.”

Consider a dependent version of Nominal System T with dependent pair types  $\Sigma x:A.B$  with the usual introduction and elimination rules:

$$\frac{\Gamma \vdash M : A \quad \Gamma \vdash N : B[M/x]}{\Gamma \vdash \langle M, N \rangle : \Sigma x:A.B} \quad \frac{\Gamma \vdash M : \Sigma x:A.B \quad \Gamma, x : A, y : B \vdash N : B'}{\Gamma \vdash \text{unpack } \langle x, y \rangle = M \text{ in } N : B'}$$

In Nominal System T, the  $\nu$ -binder can be pushed down through pair constructors so it is natural to expect that  $\nu a.\langle M, N \rangle$  and  $\langle \nu a.M, \nu a.N \rangle$  should be definitionally equal. But if so, then for subject reduction to hold, given a derivation of

$$\frac{\frac{\Gamma, a : \alpha \vdash M : A \quad \Gamma, a : \alpha \vdash N : B[M/x]}{\Gamma, a : \alpha \vdash \langle M, N \rangle : \Sigma x:A.B}}{\Gamma \vdash \nu a.\langle M, N \rangle : \Sigma x:A.B}$$

we should also be able to derive

$$\frac{\Gamma \vdash \nu a.M : A \quad \Gamma \vdash \nu a.N : B[\nu a.M/x]}{\Gamma \vdash \langle \nu a.M, \nu a.N \rangle : \Sigma x:A.B}$$

The first hypothesis follows immediately from  $\Gamma, a : \alpha \vdash M : A$ , but it is not obvious how to obtain the second from  $\Gamma, a:\alpha \vdash N : B[M/x]$ .

This argument certainly does not show that it is impossible to extend Nominal System T to a dependent type theory (doing so appears straightforward if we limit ourselves to

<sup>1</sup>This example was developed in informal discussions with Andrew Pitts and Stephanie Weirich

$\Pi$ -types), just that to develop further extensions we may need to be very careful about how name-restrictions interact with dependent types.

## 8. CONCLUSIONS

We have proposed a dependent nominal type theory, called  $\lambda^{\text{III}}$ . We can represent name-inequality directly in  $\lambda^{\text{III}}$ , but on the other hand must be more explicit about contexts and substitution. We also showed that (recursion-free)  $\lambda^{\text{III}}$  shares the good metatheoretic properties of the LF type theory, particularly decidability of equivalence and typechecking and existence of canonical forms.

There are several directions for future work. The main syntactic properties of the simply-typed fragment have already been verified using Nominal Isabelle/HOL [5]. We would also like to relate our approach to other techniques [27, 32, 19, 41] and further develop the foundations needed for incorporating nominal reasoning into richer type theories such as CIC, particularly the metatheory of recursion principles and locally-scoped names over nominal abstract syntax.

## ACKNOWLEDGEMENTS

Thanks to Frank Nebel, Andrew Pitts, Aaron Stump, Stephanie Weirich, and Edwin Westbrook for helpful discussions on this work.

## REFERENCES

- [1] A. Appel. *Compiling with Continuations*. Cambridge University Press, 1992.
- [2] A. Avron, F. Honsell, I. A. Mason, and R. Pollack. Using typed lambda calculus to implement formal systems on a machine. *Journal of Automated Reasoning*, 9:309–354, 1992.
- [3] A. Bucalo, F. Honsell, M. Miculan, I. Scagnetto, and M. Hofmann. Consistency of the theory of contexts. *J. Funct. Program.*, 16(3):327–372, 2006.
- [4] J. Cheney. Scrap your nameplate (functional pearl). In B. Pierce, editor, *Proceedings of the 10th International Conference on Functional Programming (ICFP 2005)*, pages 180–191, Tallinn, Estonia, 2005. ACM.
- [5] J. Cheney. A simple nominal type theory. *ENTCS*, 228:37–52, 2009. Proceedings of LFMTTP 2008.
- [6] J. Cheney, R. Vestergaard, and M. Norrish. Formalizing adequacy: a case study for higher-order abstract syntax. *Journal of Automated Reasoning*, 2011. To appear. Published online March 2011.
- [7] K. Crary. Explicit contexts in LF (extended abstract). *ENTCS*, 228:53 – 68, 2009. Proceedings of LFMTTP 2008.
- [8] J. Despeyroux, A. Felty, and A. Hirschowitz. Higher-order abstract syntax in Coq. In M. Dezani-Ciancaglini and G. Plotkin, editors, *Proc. Int. Conf. on Typed Lambda Calculi and Applications*, pages 124–138, Edinburgh, Scotland, 1995. Springer-Verlag LNCS 902.
- [9] J. Despeyroux and A. Hirschowitz. Higher-order abstract syntax with induction in Coq. In *LPAR*, pages 159–173, 1994.
- [10] M. J. Gabbay and A. M. Pitts. A new approach to abstract syntax with variable binding. *Formal Aspects of Computing*, 13:341–363, 2002.
- [11] H. Geuvers and E. Barendsen. Some logical and syntactical observations concerning the first order dependent type theory  $\lambda P$ . *Mathematical structures in computer science*, 9(4):335–360, 1999.
- [12] J. Hannan. Type systems for closure conversions. In H. R. Nielson and K. L. Solberg, editors, *Participants’ Proceedings of the Workshop on Types for Program Analysis*, pages 48–62, 1995. Technical Report DAIMI PB-493, Aarhus University.
- [13] D. Harel, D. Kozen, and J. Tiuryn. *Dynamic Logic*. MIT Press, 2000.

- [14] R. Harper, F. Honsell, and G. Plotkin. A framework for defining logics. *Journal of the Association for Computing Machinery*, 40(1):143–184, January 1993.
- [15] R. Harper and F. Pfenning. On equivalence and canonical forms in the LF type theory. *ACM Trans. Comput. Logic*, 6(1):61–101, 2005.
- [16] F. Honsell and M. Miculan. A natural deduction approach to dynamic logic. In *TYPES*, volume 1158 of *Lecture Notes in Computer Science*, pages 165–182, 1996.
- [17] F. Honsell, M. Miculan, and I. Scagnetto. Pi-calculus in (co)inductive type theory. *Theoretical Computer Science*, 253(2):239–285, 2001.
- [18] S. M. Lane and I. Moerdijk. *Sheaves in geometry and logic: a first introduction to topos theory*. Springer-Verlag, 1992.
- [19] D. R. Licata, N. Zeilberger, and R. Harper. Focusing on binding and computation. In *LICS*, pages 241–252. IEEE Computer Society, 2008.
- [20] I. A. Mason. Hoare’s logic in the LF. Technical Report ECS-LFCS-87-32, University of Edinburgh, 1987.
- [21] M. Miculan, I. Scagnetto, and F. Honsell. Translating specifications from nominal logic to CIC with the theory of contexts. In R. Pollack, editor, *Proceedings of the 3rd ACM SIGPLAN Workshop on Mechanized Reasoning about Languages with Variable Binding (MERLIN 2005)*, pages 41–49, Tallinn, Estonia, September 2005. ACM Press.
- [22] D. Miller and A. Tiu. A proof theory for generic judgments. *ACM Trans. Comput. Logic*, 6(4):749–783, 2005.
- [23] G. Nadathur and D. Miller. Higher-order logic programming. In D. M. Gabbay, C. J. Hogger, and J. A. Robinson, editors, *Handbook of Logic in Artificial Intelligence and Logic Programming*, volume 5, chapter 8, pages 499–590. Oxford University Press, 1998.
- [24] M. Odersky. A functional theory of local names. In *Proc. 21st ACM Symposium on Principles of Programming Languages*, pages 48–59, January 1994.
- [25] P. O’Hearn and D. J. Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*, 5(2):215–244, June 1999.
- [26] F. Pfenning and C. Elliott. Higher-order abstract syntax. In *Proceedings of the 1989 ACM SIGPLAN Conf. on Programming Language Design and Implementation (PLDI ’89)*, pages 199–208. ACM Press, 1989.
- [27] B. Pientka. A type-theoretic foundation for programming with higher-order abstract syntax and first-class substitutions. In *POPL*, pages 371–382, 2008.
- [28] A. M. Pitts. Nominal logic, a first order theory of names and binding. *Information and Computation*, 183:165–193, 2003.
- [29] A. M. Pitts. Alpha-structural recursion and induction. *Journal of the ACM*, 53(3):459–506, May 2006.
- [30] A. M. Pitts. Nominal system T. In *POPL*, pages 159–170, 2010.
- [31] A. M. Pitts. Structural recursion with locally scoped names. *Journal of Functional Programming*, 21(3):235–286, 2011.
- [32] A. Poswolsky and C. Schürmann. Practical programming with higher-order encodings and dependent types. In *ESOP*, number 4960 in LNCS, pages 93–107, 2008.
- [33] F. Pottier. Static name control for FreshML. In *LICS 2007*, pages 356–365, Wroclaw, Poland, July 2007.
- [34] N. Pouillard and F. Pottier. A fresh look at programming with names and binders. In *Proceedings of the 15th ACM SIGPLAN international conference on Functional programming, ICFP ’10*, pages 217–228, New York, NY, USA, 2010. ACM.
- [35] U. Schöpp. *Names and Binding in Type Theory*. PhD thesis, University of Edinburgh, 2006.
- [36] U. Schöpp. Modelling generic judgements. *Electronic Notes in Theoretical Computer Science*, 174(5):19–35, 2007.
- [37] U. Schöpp and I. Stark. A dependent type theory with names and binding. In *CSL 2004*, number 3210 in LNCS, pages 235–249, Karpacz, Poland, 2004.
- [38] C. Schürmann, J. Despeyroux, and F. Pfenning. Primitive recursion for higher-order abstract syntax. *Theor. Comput. Sci.*, 266(1–2):1–57, 2001.
- [39] M. R. Shinwell, A. M. Pitts, and M. J. Gabbay. FreshML: Programming with binders made simple. In *ICFP*, pages 263–274. ACM Press, 2003.
- [40] C. Urban, J. Cheney, and S. Berghofer. Mechanizing the metatheory of LF. *ACM Trans. Comput. Logic*, 12:15:1–15:42, January 2011.

- [41] E. Westbrook. *Higher-order encodings with constructors*. PhD thesis, Washington University in St. Louis, 2008.
- [42] E. Westbrook, A. Stump, and E. Austin. The calculus of nominal inductive constructions: an intensional approach to encoding name-bindings. In *LFMTP '09: Proceedings of the Fourth International Workshop on Logical Frameworks and Meta-Languages*, pages 74–83, New York, NY, USA, 2009. ACM.