Normalization by evaluation for call-by-push-value and polarized lambda calculus

Downloaded from: https://research.chalmers.se, 2022-04-19 22:44 UTC

Citation for the original published paper (version of record):
Normalization by evaluation for call-by-push-value and polarized lambda calculus
ACM International Conference Proceeding Series
http://dx.doi.org/10.1145/3354166.3354168

N.B. When citing this work, cite the original published paper.
Normalization by Evaluation for Call-By-Push-Value and Polarized Lambda Calculus

Andreas Abel  
Department of Computer Science and Engineering, Chalmers and Gothenburg University, Göteborg, Sweden

Christian Sattler  
School for Computer Science, University of Nottingham, Nottingham, United Kingdom

ABSTRACT

We observe that normalization by evaluation for simply-typed lambda-calculus with weak coproducts can be carried out in a weak bi-cartesian closed category of presheaves equipped with a monad that allows us to perform case distinction on neutral terms of sum type. The placement of the monad influences the normal forms we obtain: for instance, placing the monad on coproducts gives us eta-long beta-pi normal forms where pi refers to permutation of case distinctions out of elimination positions. We further observe that placing the monad on every coproduct is rather wasteful, and an optimal placement of the monad can be determined by considering polarized simple types inspired by focalization. Polarization classifies types into positive and negative, and it is sufficient to place the monad at the embedding of positive types into negative ones. We consider two calculi based on polarized types: pure call-by-push-value (CBPV) and polarized lambda-calculus, the natural deduction calculus corresponding to focalized sequent calculus. For these two calculi, we present algorithms for normalization by evaluation. We further discuss different implementations of the monad and their relation to existing normalization proofs for lambda-calculus with sums. Our developments have been partially formalized in the Agda proof assistant.

CCS CONCEPTS

• Theory of computation → Type theory; Type structures; Functional constructs; Proof theory; Categorical semantics; Operational semantics.

KEYWORDS

Evaluation, Intuitionistic Propositional Logic, Lambda-Calculus, Monad, Normalization, Polarized Logic, Semantics

1 INTRODUCTION

The idea behind normalization by evaluation (NbE) is to utilize a standard interpreter that evaluates closed terms to compute the normal form of an open term, i.e., a term that may contain free variables. The normal form is obtained by a type-directed reification procedure after evaluating the open term to a semantic value, mapping (reflecting) the free variables to corresponding unknowns in the semantics. The literal use of a standard interpreter can be achieved for the pure simply-typed lambda-calculus [9, 14] by modelling uninterpreted base types as sets of neutral (aka atomic) terms. More precisely, base types are interpreted as presheaves, or sets of neutral term families, in order to facilitate the generation of fresh variables of base type during reification of functions to lambdas. Thanks to η-equality at function types, free variables of function type can be reflected into the semantics as functions applying the variable to their reified argument, forming a neutral term. This mechanism provides us with unknowns of base and function type which can be faithfully reified to normal forms.

For the extension to sum types (logically, disjunctions, and categorically, weak coproducts), this reflection trick does no longer work. A semantic value of binary sum type is either a left or a right injection, but the decision between left or right cannot be taken at reflection time, since a variable of sum type does not provide us with such information. A literal standard interpreter for closed terms can thus no longer be used for NbE; instead, we can utilize a monadic interpreter. When the interpreter attempts a case distinction on an unknown of sum type, it asks an oracle whether the unknown is a left or a right injection. The oracle returns one of these alternatives, wrapping a new unknown in the respective injection. The communication with the oracle can be modeled in a monad $C$, which records the questions asked and the continuation of the interpreter for each of the possible answers. A monadic semantic value is thus a case tree where the inner nodes are labeled with unknowns and the leaves with non-monadic values [5].

In this article, we only consider weak sum types, lacking the universal property of coproducts. As a consequence, terms with the same denotation may have different normal forms under NbE. In particular, case trees are not normalized, allowing, e.g., redundant case splits (i.e., asking the same question twice). Further, the order of case splits is not normalized: changing the order in which the questions are asked (commuting case splits), alters the normal form. The model would need refinement for extensional sums (strong coproducts) with unique normal forms [3, 5, 7, 8, 28], i.e., where NbE decides equality of denotations.

Filinski [15] studied NbE for Moggi’s computational lambda calculus [23], shedding light on the difference between call-by-name (CBN) and call-by-value (CBV) NbE, where Danvy’s type-directed
2 NORMALIZATION BY EVALUATION FOR THE SIMPLY-TYPED LAMBDA CALCUlus WITH SUMS

In this section, we review the normalization by evaluation (NbE) argument for the simply-typed lambda calculus (STLC) with weak sums, setting the stage for the later sections. We work in a constructive type-theoretic meta-language, with the basic judgement $t : T$ meaning that object $t$ is an inhabitant of type $T$. However, to avoid confusion with object-level types such as the simple types of lambda calculus, we will refer to meta-level types as sets. Consequently, the colon : takes the role of elementhood $\in$ in set theory, and we are free to reuse the symbol $\in$ for other purposes.

2.1 Contexts and indices

We adapt a categorical aca de Bruijn style for the abstract syntax of terms, which we conceive as intrinsically well-typed. In de Bruijn style, a context $\Gamma$ is just a snoc list of simple types $\Delta$, meaning we write context extension as $\Gamma.\Delta$, and the empty context as $\varepsilon$. Membership $\Delta \subseteq \varepsilon$ and sublists relations $\Gamma \subseteq \varepsilon$ are given inductively by the following rules:

\[
\begin{align*}
\text{zero} & : \Delta \subseteq \varepsilon \\
\text{succ} & : \Delta \subseteq \varepsilon \Rightarrow \Delta \subseteq \varepsilon \\
\text{lift} & : \Delta \subseteq \varepsilon \Rightarrow \Delta.\Delta \subseteq \varepsilon \\
\text{weak} & : \Delta \subseteq \varepsilon \Rightarrow \Delta.\Delta \subseteq \varepsilon \\
\end{align*}
\]

We consider the rules as introductions of the indexed types $\ast \subseteq \ast$ and the rules names as constructors. For instance, succ zero : $\Delta \subseteq \varepsilon \Rightarrow \Delta.\Delta \subseteq \varepsilon$. If we read succ $n$ zero as unary number $n$, then $\Delta^n \subseteq \varepsilon$ is exactly the (de Bruijn) index of $\Delta$ in $\varepsilon$.

We can define
\[
\begin{align*}
id & : \Gamma \subseteq \Gamma \\
\text{sub} & : \Gamma \subseteq \Delta \Rightarrow \Delta \subseteq \Phi \Rightarrow \Gamma \subseteq \Phi
\end{align*}
\]
by recursion, meaning that the (proof-relevant) sublist relation is reflexive and transitive. Thus, lists $\Gamma$ form a category Cxt with morphisms $\tau : \Gamma \subseteq \Delta$, and the category laws hold propositionally, e.g., we have id $\tau \equiv \tau$ in propositional equality for all morphisms $\tau$. The singleton weakening wk$_1$ : $\Gamma \subseteq \Gamma.\Delta$, also written wk$^A$ or wk, is defined by wk$^\text{w} = \text{id}$.

In category theory, a presheaf $\mathfrak{A}$ over a category $\mathcal{C}$ is a contravariant functor from $\mathcal{C}$ into the category Set of sets and functions, i.e., a (covariant) functor from the category $\mathcal{C}^{\text{op}}$ with flipped morphisms to Set. In this paper, we are only interested in (covariant) functors from Cxt to Set, thus, by a presheaf we will always mean a presheaf over the category Cxt$^{\text{op}}$. For example, given any type $\Delta$,
we can consider $A\epsilon_-$ as such a presheaf, with the action on objects mapping $\Gamma$ to the set $A \in \Gamma$ of indices of $A\in \Gamma$, and the action on morphisms being reindex $: \Gamma \subseteq A \in \Gamma \rightarrow A \in \Delta$. The associated functor laws reindex id $x \equiv x$ and reindex $t_2$ (reindex $t_1$) $x$ $\equiv$ reindex $(t_1 \triangleright t_2)$ $x$ hold propositionally.

### 2.2 STLC and its normal forms

Simple types shall be distinguished into positive types $P$ and negative types $N$, depending on their root type former (for now). Function $\Rightarrow$ and product types $(\times$ and $1)$ are negative, while base types $(0)$ and sum types $(+ \text{ and } 0)$ are positive.

$$
A, B, C \ ::= \ P \mid N \quad \text{simple types}
$$

$$
P \ ::= \ 0 \mid A + B \mid 0 \quad \text{positive types}
$$

$$
N \ ::= \ 1 \mid A \times B \mid A \Rightarrow B \quad \text{negative types}
$$

Intrinsically well-typed lambda-terms, in abstract syntax, are just inhabitants $t$ of the indexed set $[A \downarrow \Gamma]$ inductively defined by the following rules.

$$
\text{var } \frac{A \in \Gamma}{A \downarrow \Gamma} \quad \text{abs } \frac{B + A \downarrow \Gamma}{A \Rightarrow B + \Gamma \downarrow A + \Gamma} \quad \text{app } \frac{A \Rightarrow B + \Gamma}{B + \Gamma}
$$

$$
\text{unit } \frac{1 \downarrow \Gamma}{A_1 \times A_2 \downarrow \Gamma} \quad \text{pair } \frac{A_1 \times A_2 \downarrow \Gamma}{A_1 \downarrow A_2 + \Gamma} \quad \text{prj}_1 \frac{A_1 \downarrow A_2 + \Gamma}{A_1 \times A_2 \downarrow \Gamma}
$$

$$
\text{inj}_1 \frac{A_1 + A_2 \downarrow \Gamma}{A_1 \downarrow A_1 + A_2 + \Gamma} \quad \text{case } \frac{A_1 + A_2 + \Gamma}{A_1 + A_2 + \Gamma} \quad \text{prj}_2 \frac{A_1 \downarrow A_1 + A_2 + \Gamma}{A_2 \downarrow A_1 + A_2 + \Gamma}
$$

$$
0 + \Gamma \quad \text{abort } \frac{B + \Gamma}{B + \Gamma} \quad \text{inj}_2 \frac{A_1 \downarrow A_1 + A_2 + \Gamma}{A_2 \downarrow A_1 + A_2 + \Gamma}
$$

The skilled eye of the reader will immediately recognize the proof rules of intuitionistic propositional logic (IPL) under the Curry-Howard isomorphism, where $A \downarrow \Gamma$ is to be read as “$A$ follows from $\Gamma$”. Using shorthand $\nu_n = \text{var}(\text{succ}^n \text{zero})$ for the $n$th variable, a term such as

$$
\text{abs } (\text{abs } (\text{pair } v_1 (\text{abs } (\text{app } v_1 v_0)))
$$

could in concrete syntax be rendered as $\lambda x. \lambda y. x (x, \lambda z. y z)$. We leave the exact connection to a printable syntax of the STLC to the imagination of the reader, as we shall not be concerned with considering concrete terms in this article.

Terms of type $A$ form a presheaf $A_{\downarrow \Gamma}$ as witnessed by the standard weakening operation

$$
\text{ren’} : \Gamma \subseteq A \downarrow \Gamma \rightarrow A \downarrow A + \Delta
$$

defined by recursion over $t : A \downarrow \Gamma$, and functor laws for ren analogously to reindex.

Normal forms$^2$ are logically characterized as those fulfilling the subformula property [14, 25]. Normal forms $[n : Nf A \Gamma]$ are mutually defined with neutral normal forms $[u : Ne A \Gamma]$. In the following inductive definition, we reuse the rule names from the term constructors.

$$
\begin{align*}
\text{var } &\frac{A \in \Gamma}{Ne A \Gamma} \quad \text{prj}_1 \frac{Ne (A_1 \times A_2) \Gamma}{Ne A_1 \Gamma} \\
\text{app } &\frac{Ne (A \Rightarrow B) \Gamma}{Ne B \Gamma} \quad \text{ne } \frac{Ne o \Gamma}{Ne o \Gamma} \\
\text{unit } &\frac{Ne 1 \Gamma}{Ne A_1 \Gamma} \quad \text{pair } \frac{Ne (A_1 \times A_2) \Gamma}{Ne (A_1 + A_2) \Gamma} \\
\text{abs } &\frac{Ne (A \Rightarrow B) \Gamma}{Ne (A \Rightarrow B) \Gamma} \quad \text{inj} \frac{Ne A_1 \Gamma}{Ne (A_1 + A_2) \Gamma} \\
\text{case } &\frac{Ne (A_1 + A_2) \Gamma}{Ne (P \Gamma, A_1) \Gamma} \quad \text{prf} \frac{Ne (P \Gamma, A_2) \Gamma}{Ne (P \Gamma) \Gamma} \\
\text{abort } &\frac{Ne 0 \Gamma}{Ne (P \Gamma) \Gamma}
\end{align*}
$$

These rules only allow the elimination of neutral; this restriction guarantees the subformula property and prevents any kind of computational (β) redex. The new rule ne embeds Ne into Nf, but only at base types o [4, Section 3.3]. Further, case distinction via case and abort is restricted to positive types $P$. As a consequence, our normal forms are $\eta$-long, meaning that any normal inhabitant of a negative type is a respective introduction (abs, unit, or pair). This justifies the attribute negative for these types: the construction of their inhabitants proceeds mechanically, without any choices. In contrast, constructing an inhabitant of a positive type involves choice: whether case distinction is required, and which introduction to pick in the end (inj$_1$ or inj$_2$).

As expected, $Ne A$ and $Nf A$ are presheaves, i. e., support reindexing with ren just as terms do. From a normal form we can extract the term via an overloaded function

$$
\begin{array}{c}
\nu_\Gamma \quad : \quad Nf A \Gamma \rightarrow A \downarrow \Gamma \\
\nu_\Gamma \quad : \quad Ne A \Gamma \rightarrow A \downarrow \Gamma
\end{array}
$$

that discards constructor ne but keeps all other constructors. This erasure function naturally commutes with reindexing, making it a natural transformation between the presheaves $Nf A \rightarrow Ne A$, resp. and $A_{\downarrow \Gamma}$. We shall simply write, for instance, $Nf A \rightarrow A_{\downarrow \Gamma}$, for such presheaf morphisms. (The point on the arrow is mnemonic for pointwise.) Slightly abusive, we shall extend this notation to $n$-ary morphisms, e. g., write $\forall A \rightarrow B \rightarrow C$ for $\forall \Gamma A \Gamma \rightarrow (B \Gamma \rightarrow C \Gamma)$.

We use the $\forall \Gamma$ quantifier as implicit dependent function type former in our meta-language, similar to the polymorphic quantifier in functional programming languages such as Haskell. We may instantiate a polymorphic function such as $f : A \rightarrow B$ silently, e. g., when $a : A \Gamma$ then $f a : B \Gamma$. For clarity, we may sometimes provide the instantiation explicitly via subscript, e. g., $f_1 : A \Gamma \rightarrow B \Gamma$ and $f_2 : a : B \Gamma$. Similarly, to introduce a polymorphic function we may provide the implicit abstraction as subscript, such as in $\lambda \Gamma a. b : A \rightarrow B \Gamma$ or $\lambda \Gamma (a : A \Gamma). b : A \rightarrow B$, or omit it, e. g., $\lambda (a : A \Gamma). b : A \rightarrow B$. 

1Here, ren is short for renaming, but in a nameless calculus we should better speak of reindexing, which could, a bit clumsily, be also abbreviated to ren.
2There is also a stronger notion of normal form, requiring that two extensionally equal lambda-terms, i. e., those that denote the same set-theoretical function, have the same normal form [5, 22, 28]. Such normal forms do not have a simple inductive definition, and we shall not consider them in this article.
Remark 1 (Positive eliminations into negative types).
While the coproduct eliminations case and abort are limited to normal forms of positive types \( P \), their extension case \( B \) and abort \( B \) to negative types is admissible, for instance:

\[
\begin{align*}
\text{abort}^B &: \text{Ne } 0 \to \text{Nf } B \\
\text{abort}^1 &: u \quad = \quad \text{unit} \\
\text{abort}^p &: u \quad = \quad \text{abort } u \\
\text{abort}^{A \times A} &: u \quad = \quad \text{pair (abort}^{A_1} u) (\text{abort}^{A_2} u) \\
\text{abort}^{A \Rightarrow B} &: u \quad = \quad \text{abs (abort}^{B} (\text{ren } \text{wk}^{A} u))
\end{align*}
\]

case generalizes analogously, with a bit of care when weakening the branches.

2.3 Normalization
Normalisation is concerned with finding a normal form \( n : \text{Nf } A \Gamma \) for each term \( t : A \Gamma \). The normal form should be sound, i.e., \( \Gamma \vdash t \Rightarrow n \vdash t \) with respect to an equational theory \( \Rightarrow \) on terms. Further, normalisation should decide, i.e., terms \( t \), \( t' \) with \( t \Rightarrow t' \) should have the same normal form \( n \). In this article, we present only the normalization function \( \text{norm} : A \Gamma \Rightarrow \text{Nf } A \Gamma \) without proving its soundness and completeness. From a logical perspective, we will compute for each derivation of \( A \Gamma \) a normal derivation \( \text{Nf } A \Gamma \).

The method normalization by evaluation (NbE)

\[
\text{norm}(t : A \Gamma) \equiv [A][t]_{\text{fresh}}^\Gamma
\]

decomposes normalization into evaluation

\[
\langle ... \rangle : (t : A \Gamma) \Rightarrow [\Gamma] \Rightarrow [A]
\]

in the identity environment

\[
\text{fresh}^\Gamma : [\Gamma] \Rightarrow [\Gamma]
\]

followed by reification

\[
\downarrow^A : [A] \Rightarrow \text{Nf } A
\]

(aka quoting). The role of evaluation is to produce from a term the corresponding semantic (i.e., meta-theoretic) function, which is finally reified to a normal form. Since we are evaluating open terms \( t \), we need to supply an environment fresh \( \Gamma \) which will map the free indices of \( t \) to corresponding unknowns. To accommodate unknowns in the semantics, types \( A \) are mapped to presheaves \( [A] \) (rather than just sets), and in particular each base type \( o \) is mapped to the presheaf \( \text{Ne } o \) with the intention that the neutrals take the role of the unknowns. The mapping \( \downarrow^A : \text{Ne } A \Rightarrow [A] \) from neutrals to unknowns is called reflection (aka unquoting), and defined mutually with reification by induction on type \( A \).

At this point, let us fix some notation for sets to prepare for some constructions of presheaves. Let \( \Gamma \) denote the unit set and (\( \Gamma \)) its unique inhabitant, \( \text{0} \) the empty set and magic: \( \text{0} \Rightarrow T \) the ex falso quod libet elimination into any set \( T \). Given sets \( S_1 \) and \( S_2 \), their Cartesian product is written \( S_1 \times S_2 \) with projections \( \pi_i : S_1 \times S_2 \Rightarrow S_i \), and their disjoint sum \( S_1 + S_2 \) with injections \( i_1 : S_1 \Rightarrow S_1 + S_2 \) and elimination \( [f_1, f_2] : S_1 + S_2 \Rightarrow T \) for arbitrary \( f_i : S_i \Rightarrow T \).

Presheaf (co)products \( \delta, 1, \oplus, \text{and } \otimes \) are constructed pointwise, e.g., \( \Gamma = 0 \), and given two presheaves \( \mathcal{A} \) and \( \mathcal{B} \), \( \mathcal{A} + \mathcal{B} ) \Gamma = \mathcal{A} + \mathcal{B} \). For the exponential of presheaves, however, we need the Kripke function space \((\mathcal{A} \Rightarrow \mathcal{B}) \Gamma = \forall \Delta. \Gamma \subseteq \Delta \Rightarrow \mathcal{A} \Delta \Rightarrow \mathcal{B} \Delta \).

We will interpret simple types \( A \) as corresponding presheaves \( [A] \). Let us start with the negative types, defining reflection \( \uparrow^A : \text{Ne } A \Rightarrow [A] \) and reification \( \downarrow^A : [A] \Rightarrow \text{Nf } A \) along the way.

\[
\begin{align*}
\downarrow^0 &= 1 \\
\downarrow^1 &= u \\
\downarrow^0(0) &= \text{unit}
\end{align*}
\]

\[
\begin{align*}
\downarrow^{A \times B} &= (\downarrow^A) \times (\downarrow^B) \\
\downarrow^{A \Rightarrow B} &= (\downarrow^A) \Rightarrow (\downarrow^B) \\
\downarrow^{A \Rightarrow B}(u) &= \lambda \Delta (\tau : \Gamma \subseteq \Delta) a. \downarrow^B (\text{app } (\text{ren } \tau) (\downarrow^A a)) \\
\downarrow^{A \Rightarrow B}(f) &= \text{abs } (\downarrow^B (\text{ren } \text{wk}^A \text{fresh}^B))
\end{align*}
\]

In the reification at function types \( \downarrow^{A \Rightarrow B} \), the renaming \( \text{wk}^A : \Gamma \subseteq \Gamma \). \( \text{Ne } A \Rightarrow [A] \) makes room for a new variable of type \( A \), which is reflected into \( [\Gamma] \) by \( \text{fresh}^\Gamma = \downarrow^A \text{f}_{\Gamma \Rightarrow \Gamma} : [\Gamma] \Rightarrow [A] \). The ability to introduce fresh variables into a context, and to use semantic objects such as \( f : [\Gamma] \Rightarrow [\Gamma] \) in such an extended context, is the reason for utilizing presheaves instead of just sets as semantic types.

Note also that in the equation for \( \downarrow^{A \Rightarrow B} \), the neutral \( u : \text{Ne } (A \Rightarrow B) \Gamma \) is transported into \( \text{Ne } (A \Rightarrow B) \Delta \) via reindexing with \( \tau : \Gamma \subseteq \Delta \), in order to be applicable to the normal form \( \downarrow^A a \) reified from the semantic value \( a : [\Gamma] \).

A direct extension of our presheaf semantics to positive types cannot work. For instance, with \( [0] = 0 \), simply \( \text{fresh}^0 : 0 \) would give us an inhabitant of the empty set, which means that reflection at the empty type would not be definable. Similarly, the setting \( [A + B] = [A] + [B] \) is refuted by \( \text{fresh}^{A + B} = [A]([A + B] + [B])([A + B]) \), which would require us to make a decision of whether \( A \) holds or \( B \) holds while only be given a hypothesis of type \( A + B \). Not even the usual interpretation of base types \( \text{[0]} = \text{Ne } 0 \) works in the presence of sums, as we would not be able to interpret the term abs (case \( v_0 v_0 : (o + o) \Rightarrow o \)) in our semantics, because \( \text{Ne } o (o + o) \) is empty. What is needed are case distinctions on neutrals in the semantics, allowing us the elimination of positive hypotheses before producing a semantic value, and we shall capture this capability in a strong monad \( C \) which can cover the cases.

Recall that a monad \( C \) on presheaves is first an endofunctor, i.e., it maps any presheaf \( \mathcal{A} \) to the presheaf \( C \mathcal{A} \) and any presheaf morphism \( f : \mathcal{A} \Rightarrow \mathcal{B} \) to the morphism map \( C f : C \mathcal{A} \Rightarrow C \mathcal{B} \) satisfying the functor laws for identity and composition. Then, there are natural transformations return \( C : \mathcal{A} \Rightarrow C \mathcal{A} (\text{unit}) \) and compose \( C : (C \mathcal{A}) \Rightarrow C \mathcal{A} (\text{multiplication}) \) satisfying the monad laws.

We are looking for a monad \( C \), called a cover monad, that takes the role of the oracle alluded to in the introduction, and offers us
the following services:

\[
\begin{align*}
n & \text{runNf}^C : C(NfP) \to NfP \\
\text{abort}^C & : Ne\ 0 \to C\ B \\
\text{case}^C_\top & : Ne\ (A_1 + A_2) \Gamma \\
& \to C\ B\ ((\Gamma, A_1)) \to C\ B\ ((\Gamma, A_2)) \to C\ B\ \Gamma
\end{align*}
\]

Method \(\text{runNf}^C\) enables us to \textit{run} a monadic computation of a normal form, \(C(NfP)\) \(\Gamma\), and delivers a normal form \(NfP\) \(\Gamma\). While \(\text{runNf}^C\) is a left inverse of \(\text{return}^C\), the converse is not true. Indeed, the information contained in \(C\) is refined and becomes part of the normal form delivered by \(\text{runNf}^C\). Technically, \((NfP, \text{runNf}^C)\) is a \textit{monad algebra} for monad \(C\). Besides \(\text{runNf}^C \circ \text{return}^C = \text{id}_{NfP}\), the square \(\text{runNf}^C \circ \text{join}^C = \text{runNf}^C \circ \text{map}^C\text{runNf}^C\) stands. This means that given a case tree whose leaves are again case trees ending in normal forms, it does not matter whether we first join the nested case trees and then assemble the normal form, or whether we first turn the inner case trees into normal forms via \text{map}^C\text{runNf}^C, and then the outer one.

Method \(\text{abort}^C\) allows us to end a computation by exhibiting an inconsistency witnessed by a neutral term \(u : Ne\ 0\ \Gamma\). Remember that, ultimately, computations in \(C\) produce a normal form extracted by \(\text{runNf}^C\). With \(\text{case}^C\) we notify the oracle that we are in an absurd case and the desired normal form can be trivially constructed by the abort-function of Remark \(1\).

Method \(\text{case}^C\) allows us, in a computation \(C\ B\ \Gamma\), to ask the oracle about a neutral term \(Ne\ (A_1 + A_2)\ \Gamma\) of sum type. We have to supply handlers for both possible answers: a computation \(C\ B\ (\Gamma, A_1)\) that can utilize an additional hypothesis of type \(A_1\) in the case of a left injection, and analogously a computation \(C\ B\ (\Gamma, A_2)\) for the case of a right injection.

\[
\begin{align*}
\llbracket a \rrbracket & = C(Ne\ a) \\
\llbracket \top \rrbracket & = \text{return}^C \\
\llbracket \bot \rrbracket & = \text{runNf}^C \circ \text{map}^C\text{ne} \\
\llbracket 0 \rrbracket & = C\ \bot \\
\llbracket \bot \rrbracket & = \text{abort}^C \\
\llbracket 1 \rrbracket & = \text{runNf}^C \circ \text{map}^C\text{magic} \\
\llbracket A + B \rrbracket & = C(\llbracket A \rrbracket \lor \llbracket B \rrbracket) \\
\llbracket i^A + B \rrbracket & = \text{case}^C\ i\ u(\text{return}^C(\text{t}_i\ \text{fresh}^A)) \\
& \quad \text{(return}^C(\text{t}_2\ \text{fresh}^B))) \\
\llbracket A + B \rrbracket & = \text{runNf}^C \circ \text{map}^C([i_j^A, i_j^B, i^B])
\end{align*}
\]

Figure 1: Interpretation of positive types.

The similarity of the monad services \(\text{abort}^C\) and \(\text{case}^C\) to the corresponding constructors for normal forms, or their generalization of Remark 1, is hard to miss. Unsurprisingly, just \textit{case trees} are a first instance of a cover monad: the free cover monad \(\text{Cov}\) defined as an inductive family with constructors \(\text{runNf}^\text{Cov}, \text{abort}^\text{Cov}\), and \(\text{case}^\text{Cov}\). One can visualize an element \(c : \text{Cov}\ (A\ \Gamma)\) as a binary case tree whose inner nodes (case) are labeled by neutral terms of sum type \(A_1 + A_2\) and its two branches by the context extensions \(A_1\) and \(A_2\), resp. Leaves are either labeled by a neutral term of empty type \(\bot\) (see abort), or by an element of \(A\) (see return). Functionality amounts to replacing the labels of the return-leaves, and the monadic bind (aka Kleisli extension) replaces these leaves by further case trees. Bind is realized via \(\text{join}^\text{Cov}\), which flattens a 2-level case tree, i.e., a case tree with case trees as leaves, into a single one. Finally, \(\text{runNf}^\text{Cov}\) is a simple recursion on the tree, replacing \(\text{case}^\text{Cov}\) and \(\text{abort}^\text{Cov}\) by the case and abort constructions on normal forms, and \(\text{return}^\text{Cov}\) by the identity.

Using the services of a generic cover monad \(C\), we can complete our semantics, see Figure 1.

Since positive types \(P\) have a monadic interpretation, there is a monad algebra \(C([P] \to [P])\), which is simply \(\text{join}^C\). It can be extended to a monad algebra \(\text{run}^A : C([A] \to [A])\) for any simple type \(A\), meaning we can run the monad, pushing its effects into \([A]\). We proceed by induction on \(A\). At negative types we can recurse pointwise at a smaller type, exploiting that values of negative types are essentially (finite or infinite) tuples.

\[
\begin{align*}
\text{run}^A & : C([A] \to [A]) \\
\text{run}^B & : c = \text{join}^C\ c \\
\text{run} & : c = () \\
\text{run}^{A \times B} & : c = (\text{run}^A(\text{map}^C\pi_1\ c),\ \text{run}^B(\text{map}^C\pi_2\ c)) \\
\text{run}^{A + B} & : c = \lambda\ A\ \tau\ a.\ \text{run}^B(\text{map}^C\ (\lambda\ \tau\ f.\ f\ \text{id}\ (\text{run}\ \tau\ a)))
\end{align*}
\]

For the case of function types \(A \to B\), we require the monad \(C\) to be \textit{strong}, which amounts to having \(\text{map}^C\ell : C\ A\Gamma \to C\ B\Gamma\) already for a "local" presheaf morphism \(\ell : (\mathcal{A} \to \mathcal{B})\Gamma\). The typings are \(c : C([A \to B] \Gamma)\) and \(\tau\ : \Gamma \subseteq \Delta\) and \(a : [A] \Delta\), and now we want to apply every function \(f : [A \to B]\) in the cover \(c\) to argument \(a\). Clearly, \(\text{map}^C\) is not applicable since it would expect a global presheaf morphism \([A \to B] \Gamma : [B] \Delta\), i.e., something that works 

\[\text{in any context. However, applying to } a : [A] \Delta\text{ can only work in context } \Delta\text{ or any extension } \tau' : \Delta \subseteq \Phi, \text{since we can transport } a \text{ to such a } \Phi \text{ via } a' : = \text{ren } \tau' a : = [A] \Phi, \text{but not to a context unrelated to } \Delta. \text{ We obtain our input to } \text{run}^B \text{ of type } C([B] \Gamma) \Gamma \text{ as an instance of } \text{map}^C\ell \text{ applied to the local presheaf morphism } (\lambda\ \tau\ f.\ f\ \text{id}\ a') : \Delta \subseteq \Phi \to [A \to B] \Phi \to [B] \Phi \text{ and the transported covers ren } c : = C([A] \to [B]) \Delta.
\]

We extend the type interpretation pointwise to contexts, i.e., \(\llbracket \ell \rrbracket = \hat{1} \rrbracket \Gamma\) \(\llbracket C[\Gamma] \rrbracket = \llbracket \Gamma \rrbracket \times \llbracket C \rrbracket\), and obtain a natural projection function lookup \((\cdot) : \Delta \to \llbracket C \rrbracket\) from the semantic environments. The evaluation function \(\llbracket \cdot : A \Gamma \rrbracket : \llbracket \Gamma \rrbracket \times \llbracket A \rrbracket\) can now be defined by recursion on \(\ell\), see Figure 2. Herein, the environment \(y\) lives in \(\llbracket \Gamma \rrbracket\Delta\), thus, \((\cdot) \Gamma \rrbracket : \llbracket C \rrbracket\Delta. \text{ For the interpretation of the binders and case we use the mutually defined } \llbracket \cdot \rrbracket\). The coproduct eliminations (\(\text{abort}\)) and (\(\text{case}\)) targeting an arbitrary semantic type \([B] \rrbracket\) are definable thanks to the weak sheaf property, i.e., the presence of pasting via \(\text{run}^B\) for any type \(B\), and strong functoriality of \(C\). It is noteworthy that the interpreter \(\llbracket \cdot \rrbracket\) does not use any of the services of the cover monad; in fact, it only requires the monad \(C\) to be strong. The interpreter is completely \textit{generic} for the \(\text{Cov}\) monadic semantics of types. This restores the spirit of \(\text{STLC}\) \(\text{NBE}\) for sum types: Take an \textit{off-the-shelf} interpreter for

\[4\text{In categorical terminology, the existence of run}\textsuperscript{A} \text{ means that all semantic types } [A] \text{ fulfill the weak sheaf condition, aka weak pasting.}\]
We have obtained a computable function \text{norm} which maps each free index to its corresponding unknown in the positive type \text{monad} \CC for normalization by evaluation. In our setting, we use a continuations \cite{5.4} \cite[Section 3.2]{15} already utilized the continuation monad \text{CC} on presheafs. Besides the free cover monad \text{CC} \cite[Section 5.4]{14} \cite[Section 3.2]{15} already utilized the continuation monad \text{CC} on presheafs. The normalization function is parametrized by an arbitrary environment \gamma: \text{A} \Rightarrow \text{B} and canonicity of intuitionistic propositional logic, derivation \text{A} \Rightarrow \text{B} means correctness of the normalization function \text{norm}(\text{t}) = \text{run}_{\text{CC}}(\text{t})\Rightarrow \text{B} for all \text{t} \in \text{A} \Rightarrow \text{B}.

\begin{align*}
\text{norm}(\text{t}) & \colonequals \text{run}_{\text{CC}}(\text{t})
\end{align*}

It is noteworthy (yet unsurprising) that \text{norm} connects continuations \text{CC} with case distinctions \text{case}_{\text{CC}} \colonequals \text{case}_{\text{CC}}(\text{u} : \text{Ne} (\text{A}_1 + \text{A}_2) \Rightarrow \text{B})\Rightarrow \text{case}_{\text{CC}}(\text{u} : \text{A}_1 \Rightarrow \text{B})\Rightarrow \text{case}_{\text{CC}}(\text{u} : \text{A}_2 \Rightarrow \text{B})\Rightarrow \text{B}

\begin{align*}
\text{case}_{\text{CC}}(\text{u} : \text{A}_1) & = \text{case}_{\text{CC}}(\text{u} : \text{A}_2) = \text{case}_{\text{CC}}(\text{u} : \text{B}) = \text{case}_{\text{CC}}(\text{u} : \text{B})
\end{align*}

The NbE algorithm using CC is comparable to Danvy’s type-directed partial evaluation \cite[Figure 8]{13}. However, Danvy uses shift-reset style continuations, which can be expressed via the continuation monad, and relies on Scheme’s gensym to produce fresh variables names rather than presheaves and the Kripke function space.

3 NORMALIZATION TO CALL-BY-PUSH VALUE

The placement of the monad \text{C} in the type semantics of the previous section is a bit wasteful: Each positive type is prefixed by \text{C}. In our grammar of normal forms, this corresponds to the ability to perform case distinctions \text{case}_{\text{CC}}(\text{t}) = \text{case}_{\text{CC}}(\text{t})\Rightarrow \text{B} at any positive type \text{B} \Rightarrow \text{B}. In fact, our type interpretation \text{B} \Rightarrow \text{B} corresponds to the translation of call-by-name (CBN) lambda-calculus into Moggi’s monadic meta-language \cite{19,23}.

It would be sufficient to perform all necessary case distinctions when transitioning from a negative type to a positive type. Introduction of the function type adds hypotheses to the context, providing material for case distinctions, but introduction of positive types does not add anything in that respect. Thus, we could focus on positive introductions until we transition back to a negative type. Such focusing is present in the call-by-value (CBV) lambda-calculus, where positive introductions only operate on values, and variables stand only for values. This structure is even more clearly spelled out in Levy’s call-by-push-value (CBPV) \cite{19}, as it comes with a deep classification of types into positive and negative ones. In the following, we shall utilize pure (i.e., effect-free) CBPV to achieve chaining of positive introductions.

3.1 Types and polarization

CBPV calls positive types \text{P} \text{value types} \text{A} and negative types \text{N} \text{computation types} \text{B} yet we shall stick to our terminology which
is common in publications on focalization. However, we shall use Thunk for switch \( \bot \) and Comp for switch \( \top \), to avoid confusion with our notion for reflection and reification.

\[
\begin{align*}
Ty^+ \ni P & := \sigma^+ \mid 1 \mid P_1 \times P_2 \mid 0 \mid P_1 + P_2 \mid \text{Thunk } N \\
Ty^- \ni N & := \sigma^- \mid \top \mid N_1 & N_2 \mid P \Rightarrow N \mid \text{Comp } P
\end{align*}
\]

CBPV uses \( U \) for Thunk and \( F \) for Comp, however, we find these names uninspiring unless you have good knowledge of the intended model. Further, CBPV [19] employs labeled sums \( \Sigma_i(P_i)_{i \leq 1} \) and labeled records \( \Pi_i(P_i)_{i \leq 1} \) up to countably infinite label sets \( I \) while we only have finite sums \( (0, +) \) and records \( (\top, \&). \) However, this difference is not essential, our treatment extends directly to the infinite case, since we are working in type theory, which allows infinitely branching inductive types. As a last difference, CBPV does not consider uninterpreted base types; in anticipation of the infinite case, since we are working in type theory, which allows infinitely branching inductive types. As a last difference, CBPV does not consider uninterpreted base types; in anticipation of the infinite case, since we are working in type theory, which allows infinitely branching inductive types.

Getting a bit ahead of ourselves, let us consider the mutually defined interpretations \( \llbracket P \rrbracket \) and \( \llbracket N \rrbracket \) of positive and negative types as presheaves (see Figure 3). This interpretation is parametrized by a strong monad \( C \) on presheaves. Semantically, we do not distinguish between positive and negative products. Notably, sum types can now be interpreted as plain (pointwise) presheaf sums. The Thunk marker is ignored, yet Comp, marking the switch from the negative to the positive type interpretation, places the monad \( C \). Positive atoms \( \sigma^+ \), standing for value types without constructors, are only inhabited by variables \( x : \sigma^+ \in \Gamma \). Negative atoms \( \sigma^- \) stand for computation types without own eliminations. Thus, their inhabitants stem only from eliminations of more complex types. They are built from positive eliminations captured in \( C \) and negative eliminations chained together as neutral \( \text{Ne } \sigma^- \), which we shall define below. The multiplication join \( \text{Comp}_C \) of the strong monad \( C \) can be extended to a monad algebra \( \text{run}^N : C[\llbracket N \rrbracket] \rightarrow \llbracket N \rrbracket \) for negative types \( N \). The construction proceeds by recursion on \( N \), exactly as in Section 2.3. This makes the effects of \( C \) available at any negative type, in other words, makes all negative types monadic.

Contexts are lists of positive types since in CBPV variables stand for values. Interpretation of contexts \( \llbracket \Gamma \rrbracket \) is again defined pointwise \( \llbracket x \rrbracket = i \) and \( \llbracket \Gamma.P \rrbracket = \llbracket \Gamma \rrbracket \times \llbracket P \rrbracket \).

### 3.2 Terms and evaluation

Value terms \( \llbracket v : \text{Val } P \Gamma \rrbracket \) or short, values, and computation terms \( \llbracket t : \text{Tm } N \Gamma \rrbracket \) or short, terms, are defined mutually by the rules in Figure 4. Values inhabit positive types \( P \) and are given by introduction rules only, whereas terms inhabit negative types \( N \) and comprise both introduction rules for negative types as well as elimination rules for both positive (split, case, abort) and negative types. Note that function application is restricted to value arguments. Values of type Thunk \( N \) are embedded by force. Further, values of type \( P \) can be embedded via \( \text{ret} \), producing a term of type Comp \( P \). Such terms are eliminated by bind which is, unlike the usual monadic bind, not only available for Comp-types but for arbitrary negative types \( N \). This is justified by the monadic character of negative types, by virtue of \( \text{run}^N \).

\[
\begin{align*}
\text{var} & : P \in \Gamma \quad \text{thunk} & : \text{Tm } N \Gamma \quad \text{unit}^+ & : \text{Val } 1 \Gamma \quad \text{pair}^+ & : \text{Val } P_1 \Gamma \times \text{Val } P_2 \Gamma \\
\text{inj}_1 & : \text{Val } P_1 \Gamma \quad \text{inj}_2 & : \text{Val } P_2 \Gamma \\
\text{ret} & : \text{Val } P \Gamma \quad \text{abs} & : \text{Tm } (\text{Comp } P) \Gamma \rightarrow \text{Tm } (\text{Comp } P) \Gamma \\
\text{unit}^- & : \text{Tm } 1 \Gamma \quad \text{pair}^- & : \text{Tm } N_1 \Gamma \times \text{Tm } N_2 \Gamma \\
\text{force} & : \text{Val } (\text{Thunk } N) \Gamma \rightarrow \text{Tm } N \Gamma \\
\text{app} & : \text{Tm } (\text{Comp } P) \Gamma \rightarrow \text{Tm } N \Gamma \rightarrow \text{Tm } N \Gamma \\
\text{bind} & : \text{Tm } (\text{Comp } P) \Gamma \rightarrow \text{Tm } N \Gamma \rightarrow \text{Tm } N \Gamma \\
\text{split} & : \text{Val } \text{Tm } (\text{Comp } (P_1 \times P_2)) \Gamma \rightarrow \text{Tm } N \Gamma \rightarrow \text{Tm } N \Gamma \\
\text{case} & : \text{Val } \text{Tm } (\text{Comp } (P_1 + P_2)) \Gamma \rightarrow \text{Tm } N \Gamma \rightarrow \text{Tm } N \Gamma \\
\text{abort} & : \text{Val } 0 \Gamma \rightarrow \text{Tm } N \Gamma
\end{align*}
\]

### Figure 4: Value and computation terms (CBPV)

Figure 5 defines interpretation of values \( \llbracket v : \text{Val } P \Gamma \rrbracket \) and terms \( \llbracket t : \text{Tm } N \Gamma \rrbracket \) and \( \llbracket N \rrbracket \rightarrow \llbracket N \rrbracket \). It is straightforward, thanks to the pioneering work of Moggi [23] and the design of CBPV by Levy [19]. Since Thunk serves only as an embedding of negative into positive types in our semantics, we interpret thunking and forcing by the identity. The eliminations split, case and abort for positive types deal now only with values, thus, need not reference...
The monad operations. The use of the monad is confined to ret and bind. Note the availability of run⁹ : Cov[N] → N at any negative type N for the interpretation of bind.

### 3.3 Normal forms and normalization

The design of normal forms for pure CBPV follows the same principles as for the STLC with sums in Section 2.2. We prevent β-redexes, i.e., eliminations of a type immediately following its introduction, by restricting the terms in elimination positions to neutrals. Due to the focused nature of CBPV, neutrals of positive type are just variables. We achieve η-long forms by only embedding neutrals of negative base type σ⁻ into normal forms. Maximal focusing for positive types is achieved by only admitting variables of base type σ⁺ in values. In the following, we present the grammar for normal forms in detail.

Positive normal forms are values v : Vnf P Γ referring only to atomic variables and whose thunks only contain negative normal forms.

<table>
<thead>
<tr>
<th>var x y</th>
<th>lookup x y</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit⁺ v y</td>
<td>()</td>
</tr>
<tr>
<td>pair⁺ z₁ z₂ y</td>
<td>(⟨z₁ y, z₂ y⟩)</td>
</tr>
<tr>
<td>inj₁ v y</td>
<td>t₁ v y</td>
</tr>
<tr>
<td>thunk t y</td>
<td>t y</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>abs t y</th>
<th>λ(t y)</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit⁻ y</td>
<td>()</td>
</tr>
<tr>
<td>pair⁻ t₁ t₂ y</td>
<td>(⟨t₁ y, t₂ y⟩)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>app t v y</th>
<th>(t y) ìd v y</th>
</tr>
</thead>
<tbody>
<tr>
<td>proj t y</td>
<td>π₁ t y</td>
</tr>
<tr>
<td>force v y</td>
<td>(v y)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>split v t y</th>
<th>λ(a₁, a₂) (t(y, a₁, a₂)) (v y)</th>
</tr>
</thead>
<tbody>
<tr>
<td>case v t₁ t₂ y</td>
<td>λ(a₁, t₁(y, a₁, a₂), a₂) : (t₂(y, a₁, a₂)) (v y)</td>
</tr>
<tr>
<td>abort v y</td>
<td>magic(v y)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ret v y</th>
<th>return⁹ v y</th>
</tr>
</thead>
<tbody>
<tr>
<td>bind u t y</td>
<td>run⁹ (map⁹ λ(t u y) u y)</td>
</tr>
</tbody>
</table>

Figure 5: Evaluation (CBPV).

Neutral normal forms Ne NΓ are negative eliminations starting from a forced Thunk rather than from variables of negative types (as those do not exist in CBPV). However, due to normality

the Thunk cannot be a thunk, but only a variable Thunk N ∈ Γ.

<table>
<thead>
<tr>
<th>force Thunk N ∈ Γ</th>
<th>prj₁ Ne(N₁ &amp; N₂)Γ Ne N₁ Γ</th>
</tr>
</thead>
<tbody>
<tr>
<td>app Ne(P → N)Γ Vnf P Γ</td>
<td>Ne N Γ</td>
</tr>
</tbody>
</table>

Variables are originally introduced by either abs or the binding of a neutral of type Comp P to a new variable of type P. Variables of composite value type can be broken down by pattern matching, introducing variables of smaller type. These positive eliminations plus bind are organized in the inductively defined strong monad Cov. In the following rules, parameter J (for "judgement") stands for an arbitrary presheaf.

<table>
<thead>
<tr>
<th>return J Γ Cov J Γ</th>
<th>bind Ne(Comp P)Γ Cov J (Γ P)</th>
</tr>
</thead>
<tbody>
<tr>
<td>split P₁ × P₂ ∈ Γ Cov J (Γ P₁ P₂)</td>
<td>abort 0 ∈ Γ Cov J Γ</td>
</tr>
<tr>
<td>case P₁ + P₂ ∈ Γ Cov J (Γ P₁) Cov J (Γ P₂)</td>
<td>Cov J Γ</td>
</tr>
</tbody>
</table>

Finally, normal forms of negative types are defined as inductive family Ne NΓ. They are generated by maximal negative introduction (abs, pair⁺, unit⁻) until a neutral atom or Comp P is reached. Then, elimination of neutrals and variables is possible through the Cov Monad until an answer can be given in form of a base neutral (Ne o⁻) or a normal value.

<table>
<thead>
<tr>
<th>ne Cov (Ne o⁻)Γ</th>
<th>ret Cov(Vnf P) Γ Nf(N Comp P)Γ</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit⁻ NF NΓ</td>
<td>pair⁻ NF N₁ Γ NF N₂ Γ</td>
</tr>
<tr>
<td>abs NF N Γ P</td>
<td>NF(N P → N)Γ</td>
</tr>
</tbody>
</table>

Note that we do not have a function run⁹Cov this time,⁵ instead, we directly employ Cov in the definition of NF at the base cases o⁻ and Comp P.

Reification ¹P : [P] → Vnf P at positive types P produces a normal value, and ¹N : [N] → NF N at negative types N a normal term. During reification of function types P → N in context Γ we need to embed a fresh variable x : P ∈ (Γ P) into [P], breaking down P to positive atoms o⁻ and negative remainders Thunk N. However, in [P] we do not have case analysis available, thus, positive reflection ¹⁺ P : P ∈ Γ → Cov [P] Γ needs to run in the monad. Luckily, we can unwind the monad using run⁹ N before we recursively reify at type N. Negative reflection ¹⁻ N : Ne N → [N] is, as before, generalized from variables to neutrals, to handle the breaking down of

⁵A trivial run⁹Cov : Cov (NF N₂) → NF N₂ for NF N₂ := α⁻ ¹ P Comp P could be given by induction on the cover, essentially being a join. However its extension to arbitrary negative types N would fail for the case of pushing a binder (bind, split or case) under an abstraction. This is because our base category Cxt of order-preserving embeddings does not permit swapping of variables in the context.
N via eliminations. In the following definition of reflection we use the abbreviation \( \text{fresh}^\Gamma : \text{Cov}[\Gamma] \subseteq \text{Cov}[\Gamma \cdot P] \).

\[
\begin{align*}
\vdash^P_\Gamma : & \quad P \in \Gamma \rightarrow \text{Cov}[P] \subseteq \Gamma \\
\vdash^\emptyset_\Gamma : & \quad x = x \\
\vdash^P_\Gamma : & \quad x = \beta \\
\vdash^P_{\Gamma \cdot P_1 \times P_2} : & \quad \text{split} \ x (\vdash^P_{\Gamma \cdot P_1 \cdot P_2 \cdot v_1} \cdot \vdash^P_{\Gamma \cdot P_1 \cdot P_2 \cdot v_0}) \\
\vdash^P_\Gamma : & \quad \text{ab} \ x \\
\vdash^P_{\Gamma \cdot P_1 \times P_2} : & \quad \text{case} \ x \ (\text{map} \ i_1 \ \text{fresh}^P_{i_1} \cdot \text{map} \ i_2 \ \text{fresh}^P_{i_2}) \\
\vdash^\text{Thunk}N_\Gamma : & \quad \text{return} \ (\text{fresh}^\text{N}_\Gamma \ (\text{force} \ x)) \\
\vdash^P_\Gamma : & \quad [\text{N}] \rightarrow \text{Vnf} \ P \\
\vdash^\emptyset : & \quad \text{var} \\
\vdash^P_{\Gamma \cdot (a_1, a_2)} : & \quad \text{pair} \ (\vdash^P_{\Gamma \cdot a_1} \cdot \vdash^P_{\Gamma \cdot a_2}) \\
\vdash^0_\Gamma : & \quad \text{magic} \\
\vdash^P_{\Gamma \cdot P_1} : & \quad \text{inj} \_1 \circ \vdash^0_{\Gamma \cdot P_1} \cdot \text{inj} \_2 \circ \vdash^0_{\Gamma \cdot P_2} \\
\vdash^\text{Thunk}N_\Gamma : & \quad \text{thunk} \circ \vdash^0_{\text{N}} \\
\end{align*}
\]

Reflection at positive pairs uses monoidal functoriality \( C \cdot A_1 \rightarrow C \cdot A_2 \rightarrow C (A_1 \times A_2) \) called # by McBride and Paterson [21, Section 7], which in our case can be defined by e.g. \( c_1 \# c_2 = \text{join} (\text{map} \ (\lambda \ n_1 a_1, \text{map} \ (\lambda \ n_2 a_2, \text{ren} (\text{tr}_2 a_1, a_2)) (\text{ren} n_1 c_2)) c_1) \).

For negative types, reflection and reification works as before:

\[
\begin{align*}
\vdash^N_\Gamma : & \quad \text{Ne} \ N \rightarrow \text{Nnf} \ N \\
\vdash^\emptyset : & \quad \text{bind} \ u \ \text{fresh}^N_{\Gamma} \\
\vdash^N_\Gamma : & \quad \text{return} \ u \\
\vdash^N_{\Gamma \cdot N_1 \& N_2} : & \quad (\vdash^N_{\Gamma \cdot N_1} \ (\text{prj}_1 u), \vdash^N_{\Gamma \cdot N_2} \ (\text{prj}_2 u)) \\
\vdash^N_\Gamma : & \quad \text{map} (\vdash^N_\Gamma \ c) \\
\vdash^N_\Gamma : & \quad \text{ne} \ c \\
\vdash^N_\Gamma : & \quad \text{unit}^- \\
\vdash^N_{\Gamma \cdot N_1 \& N_2} : & \quad \text{pair}^- (\vdash^N_{\Gamma \cdot N_1} b_1 (\vdash^N_{\Gamma \cdot N_2} b_2)) \\
\end{align*}
\]

Reflection for function types is also unchanged, except that app expects a value argument now.

\[
\begin{align*}
\vdash^P_{P \Rightarrow N} u = \lambda \ A \ a. \ \vdash^N_\Gamma \ (\text{app} \ (\text{run} \ P \ u) \ (\vdash^P_{\Gamma \cdot A} a)) \\
\vdash^P_{P \Rightarrow N} f = (\text{abs} \circ \vdash^N_{\Gamma \cdot P} \cdot \text{run}^N_{\Gamma \cdot P} \\
\quad \circ \text{map} \ (\lambda \ a. \ f \ (\text{map} \ (\lambda r \ t. \ a) \ a)) \text{fresh}^P_\Gamma \\
\end{align*}
\]

For reification of a (Kripke) function \( f : [\text{P}] \rightarrow \text{Nnf}[\text{N}] \) we extend context \( \Gamma \) to \( \Gamma \cdot P \) and create a case tree \( \text{fresh}^{\text{P}}_\Gamma : \text{Cov}[\Gamma \cdot P] \).

This time, the identity environment \( \text{fresh}^{\text{P}} : \text{Cov}[\Gamma \cdot P] \) can only be generated in the monad, due to monadic positive reflection.

\[
\begin{align*}
\text{fresh}^\text{P} : & \quad \text{return} () \\
\text{fresh}^{\Gamma \cdot P} : & \quad (\text{ren} \ \text{wk}^P \ \text{fresh}^\text{P}) \star \text{fresh}^{\text{P}}_\Gamma \\
\end{align*}
\]

Putting things together, we obtain the normalization function

\[
\text{norm} (t : \text{Tm} \ N \ \Gamma) = (\vdash^N_{\text{Nnf}} \circ \text{run}^N_{\Gamma} \circ \text{map} \ (\text{\_})) \text{fresh}^\Gamma.
\]

Taking stock, we have arrived at normal forms that eagerly introduce \((\text{Nf})\) and eliminate \((\text{Ne})\) negative types and also eagerly introduce positive types \((\text{Vnf})\). However, the elimination of positive types is still rather non-deterministic: It is possible to only partially break up a composite positive type and leave smaller, but still composite positive types for later pattern matching. The last refinement of normal forms, chaining also the positive eliminations, will be discussed in the following section.

## 4 FOCUSED INTUITIONISTIC PROPOSITIONAL LOGIC

Polarized lambda-calculus [27, 29] is a focused calculus, it eagerly employs so-called** invertible rules**: the introduction rules for negative types and the elimination rules for positive types. As a consequence of the latter, variables are either of atomic or negative type.

Types in contexts \( \Gamma, \Delta \) are of one of the forms \( \emptyset_\circ \) or \( \text{N} \).

To add a variable of positive type \( P \) to the context, we need to break it apart until only atomic and negative bits remain. This is performed by maximal pattern matching, called the left-invertible phase of focalization.6 We express maximal pattern matching on \( P \) as a strong functor \( [P] \) in the category of presheaves, mapping a presheaf \( J \) ("judgement") to \( [P] J \) and a presheaf morphism \( f : (J \Rightarrow K) \Gamma \) to \( \text{map}^P_{\Gamma} f : [P] J \Gamma \rightarrow [P] K \Gamma \). For arbitrary \( J \) and \( \Gamma \), the family \( [P] J \Gamma \) is inductively constructed by the following rules:

\[
\begin{align*}
\vdash^\text{hyp}^+ J_{\Gamma} : & \quad [J_{\Gamma} \circ \emptyset] J_\Gamma \\
\vdash^\text{hyp}^- J_{\Gamma} : & \quad J_{\text{Thunk}\ N_\Gamma} J_\Gamma \\
\vdash^\text{branch}_0 : & \quad [P] J \Gamma \rightarrow [P] J \Gamma \\
\vdash^\text{branch}_2 : & \quad [P_1 \circ P_2] J \Gamma \rightarrow [P_1 \times P_2] J \Gamma \\
\vdash^\text{split}_0 : & \quad [P_1] J \Gamma \rightarrow [P_1 \times P_2] J \Gamma \\
\vdash^\text{split}_2 : & \quad [P_2] J \Gamma \rightarrow [P_1 \times P_2] J \Gamma \\
\end{align*}
\]

Note the recursive occurrence of \( [P_2] \) as argument to \( [P_1] \) in \( \text{split}_2 \), which makes \( [P] \) a nested datatype [10]. Agda supports such nested inductive types; but note that \([P] \) is uncontroversial, since it could also be defined by recursion on \( P \). It is tempting to name \( \text{split}_2 \) "join" and \( \text{split}_0 \) "return" since \([P] \) is a graded monad on the monoid \((1, \times)\) of product types; however, this coincidence shall not matter for our further considerations.

\*Filinski [15, Section 4] achieves maximal pattern matching through an additional, ordered context \( \Theta \) for positive variables which are eagerly split.

\[\text{split}_0 : [P_1] \rightarrow [P_1 \times P_2] \]

\[\text{split}_2 : [P_2] \rightarrow [P_1 \times P_2] \]
certain future, the “proposition” \([P] \mathcal{F}\) states that \(\mathcal{F}\) should hold in the future determined by \(P\).

While in dynamic logic \(P\) would be a regular expression, our positive types represent the fragment featuring choice (0, +) and sequence (1, \(\times\)). The introduction rules for \([P] \mathcal{F}\) resemble the axioms of choice (branch0, branch2) and sequence (split0, split2) in dynamic logic.

Focalization is a technique to remove don’t-care nondeterminism from proof search, and as such, polarized lambda calculus is foremost a calculus of normal forms. These normal forms are given by four mutually defined inductive families of presheaves \(\text{Vnf} P, \text{Ne} N, \text{Cov} \mathcal{F}, \text{Nf} N\). As they are very similar to the CBPV normal forms given in the last section, we only report the differences. Values \([v : \text{Val} P \Gamma]\) are unchanged; they can refer to atomic positive values (\(\text{var}^+\)) and neutrals \(\text{Ne} N \Gamma\) start with a negative variable instead of with \(\text{abs}\). Due to the eager splitting of positive hypotheses, reflection at \(P\) now lives in the graded monad \([P]\) rather than \(\text{Cov}\). Further, as pattern matching may produce \(n \geq 0\) cases, reflection cannot simply produce a single positive semantic value; instead, one such value is needed for every branch. We implement \(\text{reflect}^P : ([P] \xrightarrow{} \mathcal{F}) \xrightarrow{} [P]\mathcal{F}\) as a higher-order function expecting a continuation \(k\) which is invoked for each generated branch with the semantic value of type \(P\) constructed for this branch, see Figure 6.

Reflecting at a positive atomic type \(\text{var}^+\) is the regular ending of a reflection pass: we call continuation \(k\) with a fresh variable \(\text{var}^+\) zero of type \(\text{var}^+\), making space for the variable using \(\text{wk}^\circ\). In case we end at type \(\text{Thunk} N\), we add a new variable \(\text{var}^-\) zero of type \(N\) and pass it to \(k\), after full \(\eta\)-expansion via \(\uparrow N\). Two more endings are possible: At type 0, we have reached an absurd case, meaning that no continuation is necessary since we can conclude with \textit{ex falso quodlibet}. At type 1, there is no need to add a new variable, as values of type 1 contain no information. We simply pass the unit value \(()\) to \(k\) in this case. Reflecting at \(P_1 + P_2\) generates two branches, which may result in several uses of the continuation \(k\). In the first branch, we recursively reflect at \(P_1\). Its continuation will receive a semantic value in \([P_1]\), which we inject via \(\iota\) into \([P_1 + P_2]\) to pass it to \(k\). The second branch proceeds analogously. Finally reflecting at \(P_1 \times P_2\) means we first have to analyze \(P_1\), and in each of the generated branches we continue to analyze \(P_2\). Thus \(\text{reflect}^P_{P_1 \times P_2}\) is passed as a continuation to \(\text{reflect}^P_{P_1}\). Each reflection phase gives us a semantic value \(a_1\) of type \(P_1\), which we combine to a tuple before passing it to \(k\). Note also that the context \(\tau_1\) created in the first phase needs to be composed with the context \(\tau_2\) of the second phase to transport \(k\) into the final context. Further, the value \(a_1\) was constructed relative to the target of \(\tau_1\) and still needs to be transported with \(\tau_2\) before being paired up with \(a_2\).

The method \(\text{reflect}^P\) replaces previous uses of \(\text{fresh}^P\) in reflection and reification at negative types.

\[
\begin{align*}
\text{reflect}^P : & \quad ([P] \xrightarrow{} \mathcal{F}) \xrightarrow{} [P]\mathcal{F} \\
\text{reflect}^e \quad k & \quad = \quad \text{hyp}^+(k \text{wk}^\circ \text{var}^+ \text{zero}) \\
\text{reflect}^\text{Thunk} N \quad k & \quad = \quad \text{hyp}^-(k \text{wk}^N (\uparrow N \text{var}^- \text{zero})) \\
\text{reflect}_0 \quad k & \quad = \quad \text{branch}_0 \\
\text{reflect}^{P_1 + P_2} \quad k & \quad = \quad \text{branch}_2 (\text{reflect}^{P_1}(\lambda \tau. k \tau \circ 1_1)) \times (\text{reflect}^{P_2}(\lambda \tau. k \tau \circ 1_2)) \\
\text{reflect}^1 \quad k & \quad = \quad \text{split}_0 (k \text{id} ()()) \\
\text{reflect}^{P_1 \times P_2} \quad k & \quad = \quad \text{split}_2 (\text{reflect}^{P_1}(\lambda \tau_1 a_1). \text{reflect}^{P_2}(\lambda \tau_2 a_2). \text{split}_0 (k (\tau_1 \uparrow \tau_2) (\text{ren} \tau_2 a_1. a_2)))
\end{align*}
\]

Figure 6: Positive reflection (polarized lambda calculus).

Due to the absence of composite positive types in contexts, the identity environment \(\text{fresh}\) can be built straightforwardly using negative reflection.

\[
\begin{align*}
\text{fresh}^\Gamma : & \quad [\Gamma] \Gamma \\
\text{fresh}^e & \quad = \quad () \\
\text{fresh}^\Gamma.a^+ & \quad = \quad (\text{ren} \text{wk}^\circ \text{fresh}^\Gamma, \text{var}^+ \text{zero}) \\
\text{fresh}^\Gamma.N & \quad = \quad (\text{ren} \text{wk}^N \text{fresh}^\Gamma, \uparrow N \text{var}^- \text{zero})
\end{align*}
\]

The terms \([\text{Tm} N \Gamma]\) of the polarized lambda calculus are the ones of CBPV minus the positive eliminations (split, case, abort), the added negative variable rule (\(\text{var}^-\)), and the necessary changes to the binders abs and bind.

\[
\begin{align*}
\text{var}^- N & \quad \in \Gamma \\
\text{bind} & \quad \in [\text{Tm} \text{Comp} P \Gamma] [\text{P} \text{P} \text{N} \Gamma]
\end{align*}
\]
Term interpretation \(\lambda() : \text{Tm} N \Gamma \rightarrow [\Gamma] \rightarrow [N]\) shall be as for CBPV except that we need to exchange the interpretation function for binders

\[\lambda() : \text{Tm} N \Gamma \rightarrow [\Gamma] \rightarrow [P] \Rightarrow [N].\]

Since a binder for \(P\) performs a maximal splitting on \(P\) and takes the form of a function defined by a case (and split) tree, applying it to a value \(v\) of type \(P\) amounts to a complete matching of \(v\) against the case tree and binding the remaining atomic and negative crumbs. This matching can be defined for a generic evaluation function of type \(\text{Ev}\mathcal{E}\) for CBPV and Polarized Lambda Calculus.

\[
\begin{align*}
\text{match} & \; x \quad \text{(hyp}\gamma e) \quad \gamma = e (y, \text{return}\ x) \\
\text{match} & \; h \quad \text{(hyp}\gamma e) \quad \gamma = e (y, b) \\
\text{match} & \; a \quad \text{branch} \quad \gamma = \text{magic}\ a \\
\text{match} & \; (a_1 a_2) \quad \text{branch} \quad \gamma = a_1 e_1 \gamma \\
\text{match} & \; (a_2 e_2) \quad \text{branch} \quad \gamma = a_2 e_2 \gamma \\
\text{match} & \; () \quad \text{split} \quad \gamma = e \gamma \\
\text{match} & \; (a_1, a_2) \quad \text{split} \quad \gamma = \text{match}\ a_1 (\text{map}(P) (\text{match}\ a_2)) \gamma
\end{align*}
\]

With instantiations \(\mathcal{E} = [N]\) and \(\lambda() : \text{Tm} N \rightarrow \text{Ev} [N]\), the interpretation \(\lambda()\) of binder \(\gamma : [P]\) \([\text{Tm} N] \Gamma\) is defined as follows:

\[
\lambda() \Gamma [\text{Tm} N] (\gamma : [P]) \Phi = \text{match}\ a (\text{map}(P) (\lambda() \Gamma [\text{Tm} N]) (\text{trim}\ \gamma))
\]

This completes the definition of the normalization function \(\text{norm}(t : \text{Tm} N \Gamma) = \downarrow N (t)_{\text{fresh}} \Gamma\).

5 CONCLUSION AND FURTHER WORK

We have defined NbE for CBPV and polarized lambda calculus, formulated with intrinsically well-typed syntax and presheaf semantics. At the heart of our development stands the notion of a cover monad, as alternative to the more common sheaf semantics, to handle sum types.

As a side result, we have proven semantically that the normal forms of both systems are logically complete, i.e., each derivable judgement \(\Gamma \vdash N\) has a normal derivation. It remains to show that NbE for these calculi is also computationally sound and complete, i.e., the computational behavior of term and normal form should agree, and normalization should decide a suitable equational theory on terms. To this end, we may switch from the category of presheaves to the category of Kripke predicates, as investigated through an Agda formalization.

Additionally, a natural question to investigate is whether known CBV- and CBV NbE algorithms can be obtained from our NbE algorithms by embedding simply-typed lambda calculus into our polarized calculi, using known CBV and CBV translations. Further, we would like to study the NbE algorithm for STLC arising from the optimal translation, i.e., the one inserting a minimal amount of \(\text{Thunk}\) and \(\text{Comp}\) transitions. Finally, we might revisit our interpretation of \(\text{Thunk}\) as a monoidal comonad as suggested by the categorical models of modal logic S4 [2].

Acknowledgments

The first author took initial inspiration from some unpublished notes by Thorsten Altenkirch titled Another topological completeness proof for intuitionistic logic received by email on 16th March 2000. Thorsten in turn credits his inspiration to an ALF proof by Thierry Coquand. Thanks to Hugo Herbelin for encouraging feedback and spotting some typos. Thanks to the anonymous referees of previous versions of this paper for the valuable feedback and remarks that helped improving the text of this article.

The first author acknowledges financial support from VR Grant 2014-04864 Termination Certificates for Dependently-Typed Programs and Proofs via Refinement Types and the EU Cost Action CA15123 EUTYPES Types for Programming and Verification.

References


[16] doi:10.1007/3-540-44802-0_21

[17] doi:10.1007/3-540-44802-0_21

[18] doi:10.1007/3-540-44802-0_21


