Linear Dependent Types
in a Call-by-Value Scenario

Ugo Dal Lago        Barbara Petit

July 25, 2012

Abstract

Linear dependent types [8] allow to precisely capture both the extensional behaviour and the time complexity of \( \lambda \)-terms, when the latter are evaluated by Krivine’s abstract machine. In this work, we show that the same paradigm can be applied to call-by-value evaluation. A system of linear dependent types for Plotkin’s PCF is introduced, called \( d\ell\text{-PCF}_V \), whose types reflect the complexity of evaluating terms in the so-called C\(\varepsilon\)K machine. \( d\ell\text{-PCF}_V \) is proved to be sound, but also relatively complete: every true statement about the extensional and intentional behaviour of terms can be derived, provided all true index term inequalities can be used as assumptions.

1 Introduction

A variety of methodologies for formally verifying properties of programs have been introduced in the last fifty years. Among them, type systems have certain peculiarities. On the one hand, the way one defines a type system makes the task of proving a given program to have a type reasonably simple and modular: a type derivation for a compound program usually consists of some type derivations for the components, appropriately glued together in a syntax-directed way (i.e. attributing a type to a program can usually be done compositionally). On the other, the specifications that can be expressed through types have traditionally been weak, although stronger properties have recently become of interest, such as security [23, 22], termination [5], monadic temporal properties [17] or resource bounds [16]. But contrary to what happens with other formal methods (e.g. model checking or program logics), giving a type to a program \( t \) is a sound but incomplete way to prove \( t \) to satisfy a specification: there are correct programs which cannot be proved such by way of typing.

In other words, the tension between expressiveness and tractability is particularly evident in the field of type systems, where certain good properties the majority of type systems enjoy (e.g. syntax-directedness) are usually considered as desirable (if not necessary), but also have their drawbacks: some specifications are intrinsically hard to verify locally and compositionally. One specific research field in which the just-described scenario manifests itself is complexity analysis, in which the specification takes the form of concrete or asymptotic bounds on the complexity of the underlying program. Many type systems have been introduced capturing, for instance, the class of polynomial time computable functions [15, 4, 3]. All of them, under mild assumptions, can be employed as tools to certify programs as asymptotically time efficient. However, a tiny slice of the polytime programs are generally typable, since the underlying complexity class \( \text{FP} \) is only characterised in a purely extensional sense — for every function in \( \text{FP} \) there is at least one typable program computing it.

Gaboardi and the first author have recently introduced [8] a type system for Plotkin’s PCF, called \( d\ell\text{-PCF}_N \), in which linearity and a restricted form of dependency in the spirit of Xi’s DML are present:
• **Linearity** makes it possible to finely control the number of times subterms are copied during the evaluation of a term \( t \), itself a parameter which accurately reflects the time complexity of \( t \) [7].

• **Dependency** allows to type distinct (virtual) copies of a term with distinct types. This gives the type system an extra flexibility similar to that of intersection types.

When mixed together, these two ingredients allow to precisely capture the extensional behaviour of \( \lambda \)-terms and the time complexity of their evaluation by Krivine’s abstract machine. Both soundness and relative completeness hold for \( d\ell \text{PCF}_N \).

One may argue, however, that the practical relevance of these results is quite limited, given that call-by-name evaluation and KAM are very inefficient: why would one be interested in verifying the complexity of evaluating concrete programs in such a setting?

In this work, we show that linear dependent types can also be applied to the analysis of call-by-value evaluation of functional programs. This is done by introducing another system of linear dependent types for Plotkin’s PCF. The system, called \( d\ell \text{PCF}_V \), captures the complexity of evaluating terms by Felleisen and Friedman’s CEK machine [12], a simple abstract machine for call-by-value evaluation. \( d\ell \text{PCF}_V \) is proved to enjoy the same good properties enjoyed by its sibling \( d\ell \text{PCF}_N \), namely soundness and relative completeness: every true statement about the extensional behaviour of terms can be derived, provided all true index term inequalities can be used as assumptions.

Actually, \( d\ell \text{PCF}_V \) is not merely a variation on \( d\ell \text{PCF}_N \): not only typing rules are different, but also the language of types itself must be modified. Roughly, \( d\ell \text{PCF}_V \) and \( d\ell \text{PCF}_N \) can be thought as being induced by translations of intuitionistic logic into linear logic: the latter corresponds to Girard’s translation \( A \leadsto B \equiv !A \multimap B \), while the former corresponds to \( A \leadsto B \equiv !(A \multimap B) \). The strong link between translations of IL into ILL and notions of reduction for the \( \lambda \)-calculus is well-known (see e.g. [13]) and has been a guide in the design of \( d\ell \text{PCF}_V \) (this is explained in Section 2.2).

2 Linear Dependent Types, Intuitively

Consider the following program:

\[
\text{dbl} = \text{fix } f.\lambda x. \quad \text{if} \quad x \quad \text{then} \quad x \quad \text{else} \quad s(f(p(x)))).
\]

In a type system like PCF [21], the term \( \text{dbl} \) receives type \( \text{Nat} \Rightarrow \text{Nat} \). As a consequence, \( \text{dbl} \) computes a function on natural numbers without “going wrong”: it takes in input a natural number, and (possibly) produces in output another natural number. The type \( \text{Nat} \Rightarrow \text{Nat} \), however, does not give any information about which specific function on the natural numbers \( \text{dbl} \) computes.

Properties of programs which are completely ignored by ordinary type systems are termination and its most natural refinement, namely termination in bounded time. Typing a term \( t \) with \( \text{Nat} \Rightarrow \text{Nat} \) does not guarantee that \( t \), when applied to a natural number, terminates. Consider, as another example, a slight modification of \( \text{dbl} \), namely

\[
\text{div} = \text{fix } f.\lambda x. \quad \text{if} \quad x \quad \text{then} \quad x \quad \text{else} \quad s(f(x))).
\]

It behaves as \( \text{dbl} \) when fed with 0, but it diverges when it receives a positive natural number as an argument. But look: \( \text{div} \) is not so different from \( \text{dbl} \). Indeed, the second can be obtained from the first by feeding not \( x \) but \( p(x) \) to \( f \). And any type system in which \( \text{dbl} \) and \( \text{div} \) are somehow recognised as being fundamentally different must be able to detect the presence of \( p \) in \( \text{dbl} \) and deduce termination from it. Indeed, sized types [5] and dependent types [24] are able to do so. Going further, we could ask the type system to be able not only to guarantee termination, but also to somehow evaluate the time or space consumption of programs. For example, we could be
interested in knowing that \( \text{dbl} \) takes a polynomial number of steps to be evaluated on any natural number, and actually some type systems able to control the complexity of higher-order programs exist. Good examples are type systems for amortised analysis [16, 14] or those using ideas from linear logic [13]: in all of them, linearity plays a key role.

\( \text{dℓPCF}_N \) combines some of the ideas presented above with the principles of bounded linear logic (BLL [13]): the cost of evaluating a term is measured by counting how many times function arguments need to be copied during evaluation, and different copies can be given distinct, although uniform, types. Making this information explicit in types permits to compute the cost step by step during the type derivation process. Roughly, typing judgements in \( \text{dℓPCF}_N \) are statements like

\[
\Gamma, \alpha \vdash \lambda x. \text{dbl} \mathord{\alpha} : !n \mathord{\alpha} \Rightarrow \text{Nat}[I(a)],
\]

where \( I \) and \( J \) depend on \( a \) and \( n \) is a natural number capturing the number of times \( t \) uses its argument. But this is not sufficient: analogously to what happens in BLL, \( \text{dℓPCF}_N \) makes types more parametric. A type like \( !n \mathord{\alpha} \Rightarrow \text{Nat}[I(a)] \) is replaced by the more parametric type \( !a \mathord{\alpha} \ldots a \mathord{\alpha} \Rightarrow \text{Nat}[I(a)] \), which tells us that the argument will be used \( a \) times, and each instance has type \( \mathord{\alpha} \mathord{\alpha} \mathord{\alpha} \ldots a \mathord{\alpha} \) where, however the variable \( a \) is instantiated with a value less than \( n \). This allows to type each copy of the argument differently but uniformly, since all instances of \( \mathord{\alpha} \) have the same \( \text{PCF} \) skeleton. This form of uniform linear dependence is actually crucial in obtaining the result which makes \( \text{dℓPCF}_N \) different from similar type systems, namely completeness. As an example, \( \text{dbl} \) can be typed as follows in \( \text{dℓPCF}_N \):

\[
\Gamma, \alpha \vdash \lambda x. \text{dbl} \mathord{\alpha} : !a \ldots a \Rightarrow \text{Nat}[2 \times a].
\]

This tells us that the argument will be used \( a \) times by \( \text{dbl} \), namely a number of times equal to its value. And that the cost of evaluation will be itself proportional to \( a \).

### 2.1 Why Another Type System?

The theory of \( \lambda \)-calculus is full of interesting results, one of them being the so-called Church-Rösser property: both \( \beta \) and \( \beta\eta \) reduction are confluent, i.e. if you fire two distinct redexes in a \( \lambda \)-term, you can always “close the diagram” by performing one or more rewriting steps. This, however, is not a local confluence result, and as such does not imply that all reduction strategies are computationally equivalent. Indeed, some of them are normalising (like normal-order evaluation) while some others are not (like innermost reduction). But how about efficiency?

On the one hand, it is well known that optimal reduction is indeed possible [18], even if it gives rise to high overheads [1]. On the other, call-by-name can be highly inefficient. Consider, as an example, the composition of \( \text{dbl} \) with itself:

\[
\text{dbl}^2 = \lambda x. \text{dbl} (\text{dbl} \mathord{x}).
\]

This takes quadratic time to be evaluated in the KAM: the evaluation of \( (\text{dbl} \mathord{a}) \) is repeated a linear number of times, whenever it reaches the head position. This actually can be seen from within \( \text{dℓPCF}_N \), since

\[
\Gamma, \alpha \vdash \lambda x. \text{dbl} \mathord{\alpha} : !a \ldots a \Rightarrow \text{Nat}[4 \times a].
\]

where both \( I \) and \( J \) are quadratic in \( a \). Call-by-value solves this problem, at the price of not being normalising. Indeed, eager evaluation of \( \text{dbl}^2 \) when fed with a natural number \( n \) takes linear time in \( n \). The relative efficiency of call-by-value evaluation, compared to call-by-name, is not a novelty: many modern functional programming languages (like OCaml and Scheme) are based on it, while very few of them evaluate terms in call-by-name order.

For the reasons above, we strongly believe that designing a type system in the style of \( \text{dℓPCF}_N \), but able to deal with eager evaluation, is a step forward applying linear dependent types to actual programming languages.
2.2 Call-by-Value, Call-by-Name and Linear Logic

Various notions of evaluation for the $\lambda$-calculus can be seen as translations of intuitionistic logic (or of simply-typed $\lambda$-calculi) into Girard’s linear logic. This correspondence has been investigated in the specific cases of call-by-name (CBN) and call-by-value (CBV) reduction (e.g. see the work of Maraist et al. [19]). In this section, we briefly introduce the main ideas behind the correspondence, explaining why linear logic has guided the design of $d\ell$PCFV.

The general principle in such translations, is to guarantee that whenever a term can possibly be duplicated, it must be mapped to a box in the underlying linear logic proof. In the CBN translation (also called Girard’s translation), any argument to functions can possibly be substituted for a variable and copied, so arguments are banged during the translation:

\[(A \Rightarrow B)^* = (\exists! A^* \Rightarrow B)^*\]

Adding the quantitative bound on banged types (as explained in the previous section) gives rise to the type $(\exists! \sigma \Rightarrow \tau)$ for functions (written $[a < 1] : \sigma \Rightarrow \tau$ in [5]). In the same way, contexts are banged in the CBN translation: a typing judgement in $d\ell$PCF$_N$ have the following form:

\[x_1 : !a_{1 < 1} \sigma_1, \ldots, x_n : !a_{n < 1} \sigma_n \vdash t : \tau.\]

In the CBV translation, $\beta$-reduction should be performed only if the argument is a value. Thus, arguments are not automatically banged during the translation but values are, so that the $\beta$-reduction remains blocked until the argument reduces to a value. In the $\lambda$-calculus values are functions, hence the translation of the intuitionistic arrow becomes

\[(A \Rightarrow B)^{\circ} = (\exists! A^{\circ} \Rightarrow B^{\circ}).\]

Function types in $d\ell$PCF$_V$ then become $!a_{i < 1} (\sigma \Rightarrow \tau)$, and a judgement has the form $x_1 : \sigma_1, \ldots, x_n : \sigma_n \vdash t : \tau$. The syntax of types varies fairly much between $d\ell$PCF$_N$ to $d\ell$PCF$_V$, and consequently the two type systems are different, although both of them are greatly inspired by linear logic.

In both cases, however, the “target” of the translation is not the whole of ILL, but rather a restricted version of it, namely BLL, in which the complexity of normalisation is kept under control by shifting from unbounded, infinitary, exponentials to finitary ones. For example, the BLL contraction rule allows to merge the first I copies of A, and the following J ones into the first $I + J$ copies of A:

\[\Gamma, !a_{i < 1} A, !a_{i < 1} A[1 + a/a] \vdash B\]
\[\Gamma, x : !a_{i < 1} A \vdash B\]

We write $\sigma \vartriangleright \tau = !a_{i < 1} A$ if $\sigma = !a_{i < 1} A$ and $\tau = !a_{i < 1} A[1 + a/a]$. Any time a contraction rule is involved in the CBV translation of a type derivation, a sum $\psi$ appears at the same place in the corresponding $d\ell$PCF$_V$ derivation. Similarly, the dereliction rule allows to see any type as the first copy of itself:

\[\Gamma, A[0/a] \vdash B\]
\[\Gamma, !a_{i < 1} A \vdash B\]

hence any dereliction rule appearing in the translation of a typing judgement tells us that the corresponding type is copied once. Both contraction and dereliction appear while typing an application in $d\ell$PCF$_V$: the PCF typing rule

\[\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash u : A\]
\[\Gamma \vdash tu : B\]

corresponds to the following ILL proof:

\[\frac{z : A^\circ \Rightarrow B^\circ \vdash z : A^\circ \Rightarrow B^\circ}{\vdash (\exists! A^\circ \Rightarrow B^\circ) \vdash z : A^\circ \Rightarrow B^\circ} \text{ der}\]
\[\vdash (\exists! A^\circ \Rightarrow B^\circ) \vdash z : A^\circ \Rightarrow B^\circ\]
\[\Gamma \vdash t^\circ : A^\circ \Rightarrow B^\circ\]
\[\vdash (t^\circ = t^\circ) \text{ der}\]
\[\vdash (t^\circ = t^\circ) \vdash t^\circ u^\circ : B^\circ\]
\[\Gamma \vdash t^\circ u^\circ : B^\circ\]
\[\vdash (t^\circ = t^\circ) \text{ der}\]
\[\vdash (t^\circ = t^\circ) \vdash t^\circ u^\circ : B^\circ\]
\[\Gamma \vdash t^\circ u^\circ : B^\circ\]
which becomes the following, when appropriately decorated according to the principles of BLL (writing $A_0$ and $B_0$ for $A(0/a)$ and $B(0/a)$):

\[
\begin{aligned}
\text{der} & \quad \frac{z : A_0 \to B_0 \vdash z : A_0 \to B_0}{\Gamma \vdash t : A_0 \to B_0 \vdash z : A_0 \to B_0} \quad \Gamma \vdash t : A_0 \to B_0 \\
\text{der} & \quad \frac{\Gamma \vdash t : A_0 \to B_0}{\Gamma \vdash \lambda x. t : A_0}
\end{aligned}
\]

This CBV translation of the application rule hence leads to the typing rule for applications in $\text{d/PCF}_V$:

\[
\begin{aligned}
\Gamma \vdash K t : !_{\sigma < 1} (\sigma \to \tau) & \quad \Delta \vdash H u : \sigma [0/a] \\
\Gamma, x : \sigma \vdash K t : \tau & \\
\sum_{\sigma < 1} \Gamma \vdash 1^\tau \sum_{\sigma < 1} K \lambda x. t : !_{\sigma < 1} (\sigma \to \tau)
\end{aligned}
\]

One may wonder what $I$ represents in this typing rule, and more generally in a judgement such as

\[
\Gamma \vdash K t : !_{\sigma < 1} A.
\]

This is actually the main new idea of $\text{d/PCF}_V$: such a judgement intuitively means that the value to which $t$ reduces will be used $I$ times by the environment. If $t$ is applied to an argument $u$, then $t$ must reduce to an abstraction $\lambda x.s$, that is destructed by the argument without being duplicated. In that case, $I = 1$, as indicated by the application typing rule. On the opposite, if $t$ is applied to a function $\lambda x.u$, then the type of this function must be of the form (up to a substitution of $b$) $!_{\sigma < 1} (l_{\sigma < 1} A \to \tau)$. This means that $\lambda x.u$ uses $I$ times its arguments, or, that $x$ can appear at most $I$ times in the reducts of $u$.

This suggests that the type derivation of a term is not unique in general: whether a term $t$ has type $!_{\sigma < 1} A$ or $!_{\sigma < 1} A$ depends on the use we want to make of $t$. This intuition will direct us in establishing the typing rules for the other PCF constructs (namely conditional branching and fixpoints).

### 3  $\text{d/PCF}_V$, Formally

In this section, the language of programs and a type system $\text{d/PCF}_V$ for it will be introduced formally. While programs are just terms of a fairly standard $\lambda$-calculus (which is very similar to Plotkin’s PCF), types may include so-called index terms, which are first-order terms denoting natural numbers by which one can express properties about the extensional and intentional behaviour of programs.

#### 3.1  Index Terms and Equational Programs

Syntactically, index terms are built either from function symbols from a given untyped signature $\Theta$ or by applying any of two special term constructs:

\[
I, J, K ::= a \mid f(I_1, \ldots, I_n) \mid \sum_{\sigma < 1} J \mid \bigotimes_a^{1 \leq J} K.
\]

Here, $f$ is a symbol of arity $n$ from $\Theta$ and $a$ is a variable drawn from a set $V$ of index variables. We assume the symbols 0, 1 (with arity 0) and +, − (with arity 2) are always part of $\Theta$. An index term in the form $\sum_{\sigma < 1} I$ is a bounded sum, while one in the form $\bigotimes_a^{1 \leq J} K$ is a forest cardinality. For every natural number $n$, the index term $n$ is just $1 + 1 + \ldots + 1$, $n$ times.
Index terms are meant to denote natural numbers, possibly depending on the (unknown) values of variables. Variables can be instantiated with other index terms, e.g. $I/J/a$. So, index terms can also act as first order functions. What is the meaning of the function symbols from $\Theta$? It is the one induced by an equational program $E$. Formally, an equational program $E$ over a signature $\Theta$ is a set of equations in the form $I = J$ where both $I$ and $J$ are index terms. We are interested in equational programs guaranteeing that, whenever symbols in $\Theta$ are interpreted as partial functions over $\mathbb{N}$ and 0, 1, + and $-$ are interpreted in the usual way, the semantics of any function symbol $f$ can be uniquely determined from $E$. This can be guaranteed by, for example, taking $E$ as an Herbrand-Gödel scheme [20] or as an orthogonal constructor term rewriting system [2]. The definition of index terms is parametric on $\Theta$ and $E$: this way one can tune our type system from a highly undecidable but truly powerful machinery down to a tractable but less expressive formal system.

What about the meaning of bounded sums and forest cardinalities? The first is very intuitive: the value of $\sum_{a=0}^{I} J$ is simply the sum of all possible values of $J$ with $a$ taking the values from 0 up to $I$, excluded. Forest cardinalities, on the other hand, require some effort to be described. Informally, $\sum_{a}^{I} J K$ is an index term denoting the number of nodes in a forest composed of $J$ trees described using $K$. All the nodes in the forest are (uniquely) identified by natural numbers. These are obtained by consecutively visiting each tree in pre-order, starting from $I$. The term $K$ has the role of describing the number of children of each forest node, e.g. the number of children of the node 0 is $K[0/a]$. More formally, the meaning of a forest cardinality is defined by the following two equations:

\[
\begin{align*}
\sum_{a}^{I} 0 K &= 0 \\
\sum_{a}^{I+1} 1 J K &= \left( \sum_{a}^{I} J K \right) + 1 + \left( \sum_{a}^{I+1} \sum_{a}^{I+1} J K[K/a] \right)
\end{align*}
\]

The first equation says that a forest of 0 trees contains no nodes. The second one tells us that a forest of $J + 1$ trees contains:

- The nodes in the first $J$ trees;
- plus the nodes in the last tree, which are just one plus the nodes in the immediate subtrees of the root, considered themselves as a forest.

To better understand forest cardinalities, consider the following forest comprising two trees:

```
It is well described by an index term $K$ with a free index variable $a$ such that $K[1/a] = 3$; $K[n/a] = 2$ for $n \in \{2, 8\}$; $K[n/a] = 1$ when $n \in \{0, 6, 9, 11\}$; and $K[n/a] = 0$ when $n \in \{3, 4, 5, 7, 10, 12\}$. That is, $K$ describes the number of children of each node. Then $\sum_{a}^{0} 2 K = 13$ since it takes into account the entire forest; $\sum_{a}^{2} 1 K = 8$ since it takes into account only the leftmost tree; $\sum_{a}^{2} 1 K = 5$ since it takes into account only the second tree of the forest; finally, $\sum_{a}^{2} 1 K = 6$ since it takes into account only the three trees (as a forest) within the dashed rectangle.

One may wonder what is the role of forest cardinalities in the type system. Actually, they play a crucial role in the treatment of recursion, where the unfolding of recursion produces a tree-like
structure whose size is just the number of times the (recursively defined) function will be used globally. Note that the value of a forest cardinality could also be undefined. For instance, this happens when infinite trees, corresponding to diverging recursive computations, are considered.

The expression \([I]_{\rho} \vdash E\) denotes the meaning of I, defined by induction along the lines of the previous discussion, where \(\rho : V \rightarrow \mathbb{N}\) is an assignment and \(E\) is an equational program giving meaning to the function symbols in I. Since \(E\) does not necessarily interpret such symbols as total functions, and moreover, the value of a forest cardinality can be undefined, \([I]_{\rho}\) can be undefined itself. A constraint is an inequality in the form \(I \leq J\). Such a constraint is true (or satisfied) in an assignment \(\rho\) if \([I]_{\rho}\) and \([J]_{\rho}\) are both defined and the first is smaller or equal to the latter. Now, for a subset \(\phi\) of \(V\), and for a set \(\Phi\) of constraints involving variables in \(\phi\), the expression

\[\phi; \Phi \models_{E} I \leq J\]

denotes the fact that the truth of \(I \leq J\) semantically follows from the truth of the constraints in \(\Phi\).

To denote that \(I\) is well defined for \(E\) and any valuation \(\rho\) satisfying \(\Phi\), we may write \(\phi; \Phi \models_{E} I \Downarrow\) instead of \(\phi; \Phi \models_{E} I \equiv I\).

### 3.2 Programs

Values and terms are generated by the following grammar:

\[
\begin{align*}
\text{Values:} & \quad v, w ::= \text{nat} \mid \lambda x.t \mid \text{fix } t \\
\text{Terns:} & \quad s, t, u ::= x \mid v \mid tu \mid s(t) \mid p(t) \\
& \quad \mid \text{ifz } t \text{ then } u \text{ else } s
\end{align*}
\]

Terms can be typed with a well-known type system called PCF: types are those generated by the basic type \texttt{nat} and the binary type constructor \Rightarrow. Typing rules are standard (see [9]). A notion of (weak) call-by-value reduction \(\rightarrow_{v}\) can be easily defined: take the rewriting rules in Figure 1 and close them under all applicative contexts. A term \(t\) is said to be a program if it can be given the PCF type \texttt{nat} in the empty context. The multiplicative size \(\|t\|\) of a term \(t\) is defined as follows:

\[
\begin{align*}
\|\text{nat}\| &= \|\lambda x.t\| = \|\text{fix } t\| = 0 \\
\|x\| &= 2 \\
\|tu\| &= \|t\| + \|u\| + 2 \\
\|s(t)\| &= \|t\| + 2 \\
\|p(t)\| &= \|t\| + 2 \\
\|\text{ifz } t \text{ then } u \text{ else } s\| &= \|t\| + \|u\| + \|s\| + 2.
\end{align*}
\]

Notice that the multiplicative size of a term \(t\) is less or equal than its size \(|t|\) (which is defined inductively, similarly to \(|t|\), except for values: \(|\text{nat}| = 2\), and \(|\text{fix } t| = |\lambda x.t| = |t| + 2\)). Values are not taken into account by the multiplicative size. Indeed, the evaluation of terms (cf. Section 3.4) consists first in scanning a term until a value is reached (and the cost of this step is measured by the multiplicative size). Then this value is either destructed (e.g. when a lambda abstraction is given an argument), either duplicated (e.g. when it is itself an argument of a lambda abstraction). The cost of this second step will be measured by the type system \texttt{dPCF}_V.
instances of \( \text{Nat} \) above: suppose that \( a < 1 \) and \( b < 1 \) are in \( \text{Nat} \). Moreover, the condition \( a < 1 \) says that \( a \) consists of all the instances of the linear type \( A \) where the variable \( a \) is successively instantiated with the values from 0 to 1−1, i.e. \( A\{0/a\}, \ldots, A\{1−1/a\} \). For those readers who are familiar with linear logic, and in particular with BLL, the modal type \( a < 1 \) · \( A \) is a generalisation of the BLL formula \( l_{n < p} A \) to arbitrary index terms. As such it can be thought of as representing the type \( A\{0/a\} \otimes \cdots \otimes A\{1−1/a\} \). The language of types

The Language of Types

The type system \( \text{dPFC} \) can be seen as a refinement of PCF obtained by a linear decoration of its type derivations. *Linear and modal types* are defined as follows:

\[
A, B ::= \quad \sigma \rightarrow \tau \quad \text{linear types} \\
\sigma, \tau ::= \quad [a < 1] \cdot A \mid \text{Nat}[1, J] \quad \text{modal types}
\]

where \( I, J \) range over index terms and \( a \) ranges over index variables. Modal types need some comments. Natural numbers are freely duplicable, so \( \text{Nat}[1, J] \) is modal by definition. As a first approximation, \( [a < 1] \cdot A \) can be thought of as a universal quantification of \( A \), and so \( a \) is bound in the linear type \( A \). Moreover, the condition \( a < 1 \) says that \( a \) consists of all the instances of the linear type \( A \) where the variable \( a \) is successively instantiated with the values from 0 to 1−1, i.e. \( A\{0/a\}, \ldots, A\{1−1/a\} \). For those readers who are familiar with linear logic, and in particular with BLL, the modal type \( a < 1 \) · \( A \) is a generalisation of the BLL formula \( l_{n < p} A \) to arbitrary index terms. As such it can be thought of as representing the type \( A\{0/a\} \otimes \cdots \otimes A\{1−1/a\} \). The language of types

\[
\text{Nat}[1] \text{ is syntactic sugar for } \text{Nat}[1, I]. \text{ In the typing rules we are going to define, modal types need to be manipulated in an algebraic way. For this reason, two operations on modal types need to be introduced. The first one is a binary operation } \varpi \text{ on modal types. Suppose that } \sigma = [a < 1] \cdot A\{a/c\} \text{ and that } \tau = [b < J] \cdot A\{1 + b/c\}. \text{ In other words, } \sigma \text{ consists of the first } I \text{ instances of } A, i.e. } A\{0/c\}, \ldots, A\{I−1/c\} \text{ while } \tau \text{ consists of the next } J \text{ instances of } A, i.e. } A\{1 + 0/c\}, \ldots, A\{1 + J−1/c\}. \text{ Their sum } \sigma \varpi \tau \text{ is naturally defined as a modal type consisting of the first } I + J \text{ instances of } A, i.e. } [c < I + J] \cdot A. \text{ Furthermore, } \text{Nat}[1, I] \varpi \text{Nat}[1, J] \text{ is just } \text{Nat}[1, J]. \text{ An operation of bounded sum on modal types can be defined by generalising the idea above: suppose that }
\]
\[
\sigma = [b < J] \cdot A\{b + \sum_{d < a} J\{d/a\}/c\}.
\]
Then its \textit{bounded sum} \( \sum_{n=1}^{a} \sigma \) is just \([c < \sum_{n=1}^{a} J \cdot A].\) Finally, \( \sum_{n=1}^{a} \text{Nat}[J, K] = \text{Nat}[J, K] \), provided \( a \) is not free in \( J \) nor in \( K \).

\textbf{Subtyping} Central to \( \mathcal{d} \mathcal{P} \mathcal{C} \mathcal{F}_V \) is the notion of subtyping. An inequality relation \( \sqsubseteq \) between \( (\text{linear or modal}) \) types can be defined using the formal system in Figure 2. This relation corresponds to lifting index inequalities at the type level. Please observe that \( \sqsubseteq \) is a pre-order, \( i.e., \) a reflexive and transitive relation.

\textbf{Typing} A typing judgement is of the form

\[
\phi; \Phi; \Gamma \triangleright_{\text{K}} t : \tau,
\]

where \( K \) is the \textit{weight} of \( t \), that is (informally) the maximal number of substitutions involved in the \textit{cbv} evaluation of \( t \). \( \Phi \) is a set of constraints \( (c.f. \text{Section 3.1}) \) that we call the \textit{index context}, and \( \Gamma \) is a context assigning a modal type to (at least) each free variable of \( t \). Both sums and bounded sums are naturally extended from modal types to contexts \( (\text{with, for instance,} \{x : \sigma; y : \tau\} \cup \{x : \sigma', z : \tau'\} = \{x : \sigma \cup \sigma'; y : \tau; z : \tau'\}) \). There might be free index variables in \( \Phi, \Gamma, \tau \) and \( K \), all of them from \( \phi \). Typing judgements can be derived from the rules of Figure 3.

Derivation rules for abstractions and applications have been informally presented in Section 3.2. The other ones are then intuitive, except the derivation rule for typing \( \text{fix}\, x.t \), that is worth an explanation: to simplify, assume we want to type only one copy of its type (that is, \( K = 1 \)). To compute the weight of \( \text{fix}\, x.t \), we need to know the number of times \( t \) will be copied during the evaluation, that is the number of nodes in the tree of its recursive calls. This tree is described by \( I \) (as explained in Section 3.1), since each occurrence of \( x \) in \( t \) stands for a recursive call. It has, say, \( H = \sum_{b=1}^{9} 1 \) nodes. At each node \( b \) of this tree, the \( a^{th} \) occurrence of \( x \) will be replaced by the \( a^{th} \) son of \( b \), \( i.e. \), by \( b + 1 + \sum_{b=1}^{a} 1 \). The types have to match, and that is what the second premise expresses. Finally, the type of \( \text{fix}\, x.t \) is the type of the “main” copy of \( t \), at the root of the tree \( (i.e., \) at \( b = 0 \)). The weight counts all the recursive calls \( (i.e., \) \( H \)) plus the weight of each copy of \( t \) \( (i.e., \) the weight of \( t \) for each \( b < H \)).

Last, the subsumption rule allows to relax the precision standards of a typing judgement. One can also restrict the inequalities on indexes to equalities in this rule, and thereby construct only \textit{precise} typing judgements. Observe that the set of all rules but this one is syntax directed. Moreover the subsumption rule preserves the \( \text{PCF} \) skeleton of the types, and so the type system is itself syntax directed \textit{up to} index inequalities.

\textbf{3.4 An Abstract Machine for \textit{PCF}}

The call-by-value evaluation of \( \text{PCF} \) terms can be faithfully captured by an abstract machine in the style of \textit{CEK} \cite{9}, which will be introduced in this section.

The internal state of the \( \text{CEK}_{\text{PCF}} \) machine consists of a closure and a stack, interacting following a set of rules. Formally, a \textit{value closure} is a pair \( v \equiv \langle v; \xi \rangle \) where \( v \) is a value and \( \xi \) is an \textit{environment}, itself a list of assignments of value closures to variables:

\[
\xi ::= \emptyset | (x \mapsto v) \cdot \xi.
\]
A closure is a pair \( \langle t; \xi \rangle \) where \( t \) is a term (and not necessarily a value). Stacks are terms from the following grammar:

\[
\pi ::= \emptyset | \text{fun}(v, \pi) | \text{arg}(c, \pi) \\
| \text{fork}(t, u, \xi, \pi) | s(\pi) | p(\pi).
\]

A process \( P \) is a pair \( c \cdot \pi \) of a closure and a stack.

Processes evolve according to a number of rules. Some of them (see Figure 4) describe how the CEK\textsubscript{PCF} machine evolves when the first component of the process is a value closure. Other rules (see Figure 5) prescribe the evolution of CEK\textsubscript{PCF} in all the other cases.

The following tells us that CEK\textsubscript{PCF} is an adequate methodology to evaluate PCF terms:

**Proposition 3.1 (Adequacy)** If \( t \) is a PCF term of type \( \text{Nat} \), then \( t \rightarrow^* v \) if \( \langle t; \emptyset \rangle \rightarrow^* \langle t; \xi \rangle \) iff \( (\langle B; \emptyset \rangle \rightarrow^* \emptyset) \).
In this section, some metatheoretical results about df/PCF will be presented. More specifically, type derivations are shown to be modifiable in many different ways, all of them leaving the underlying term unaltered. These manipulations, described in Section 5.1, form a basic toolkit which is essential to achieve the main results of this paper, namely intentional soundness and completeness (which are presented in Section 5.2 and Section 5.4). Types are preserved by call-by-value reduction, as proved in Section 5.2.
Figure 7: Typing derivation of mult

Figure 8: dfPCF\textsubscript{Y}: Lifting Typing to Stacks
5.1 Manipulating Type Derivations

First of all, the constraints \( \Phi \) in index, subtyping and typing judgements can be made stronger without altering the rest:

**Lemma 5.1 (Strengthening)** If \( \phi; \Psi \vdash_\varepsilon \Phi \), then the following implications hold:
1. If \( \phi; \Phi \vdash_\varepsilon I \equiv J \), then \( \phi; \Psi \vdash_\varepsilon I \equiv J \);
2. If \( \phi; \Phi \vdash_\varepsilon \sigma \subseteq \tau \), then \( \phi; \Psi \vdash_\varepsilon \sigma \subseteq \tau \);
3. If \( \phi; \Phi; \Gamma \vdash_\varepsilon t : \sigma \), then \( \phi; \Psi; \Gamma \vdash_\varepsilon t : \sigma \).

**Proof.** Point 1 is a trivial consequence of transitivity of implication in logic. Point 2 can be proved by induction on the structure of the proof of \( \phi; \Phi \vdash_\varepsilon \sigma \subseteq \tau \), using point 1. Point 3 can be proved by induction on a proof of \( \phi; \Phi; \Gamma \vdash_\varepsilon t : \sigma \), using points 1 and 2.

Strengthening is quite intuitive: whatever appears on the right of \( \vdash_\varepsilon \) should hold for all values of the variables in \( \phi \) satisfying \( \Phi \), so strengthening corresponds to making the judgement weaker.

Fresh term variables can be added to the context \( \Gamma \), leaving the rest of the judgement unchanged:

**Lemma 5.2 (Context Weakening)** \( \phi; \Phi; \Gamma \vdash_\varepsilon t : \tau \) implies \( \phi; \Phi; \Gamma, \Delta \vdash_\varepsilon t : \tau \).

**Proof.** Again, this is an induction on the structure of a derivation for \( \phi; \Phi; \Gamma \vdash_\varepsilon t : \tau \).

Another useful transformation on type derivations consists in substituting index variables for defined index terms.

**Lemma 5.3 (Index Substitution)** If \( \phi; \Phi \vdash_\varepsilon I \downarrow \), then the following implications hold:
1. If \( (a, \varphi); \Phi, \Psi \vdash_\varepsilon J \equiv K \), then \( (a, \varphi); \Phi, \Psi \{1/a\} \vdash_\varepsilon J \{1/a\} \equiv K \{1/a\} \);
2. If \( (a, \varphi); \Phi, \Psi \vdash_\varepsilon \sigma \subseteq \tau \), then \( (a, \varphi); \Phi, \Psi \{1/a\} \vdash_\varepsilon \sigma \{1/a\} \subseteq \tau \{1/a\} \);
3. If \( (a, \varphi); \Phi, \Psi, \Gamma \vdash_\varepsilon t : \sigma \), then \( (a, \varphi); \Phi, \Psi \{1/a\}; \Gamma \{1/a\} \vdash_\varepsilon \Gamma \{1/a\} \vdash_\varepsilon t : \sigma \{1/a\} \).

**Proof.**
1. Assume that \( \phi; \Phi \vdash_\varepsilon I \downarrow \) and \( (a, \varphi); \Phi, \Psi \vdash_\varepsilon J \equiv K \), and let \( \rho \) be an assignment satisfying \( \Phi, \Psi \{1/a\} \). In particular, \( \rho \) satisfies \( \Phi \), thus \( \|I\|_\rho^\varepsilon = \|H\|_{\rho,a \rightarrow n}^\varepsilon \). Hence \( (a, \varphi, \rho \mapsto n) \) satisfies \( \Phi, \Psi \), and then it also satisfies \( J \equiv K \). So \( \|J \{1/a\}\|_{\rho}^\varepsilon = \|H\|_{\rho,a \rightarrow n}^\varepsilon \leq \|K\|_{\rho,a \rightarrow n}^\varepsilon = \|K\{1/a\}\|_{\rho}^\varepsilon \), and \( \rho \) satisfies \( J \{1/a\} \equiv K \{1/a\} \).
2. By induction on the subtyping derivation, using 1
3. By induction on the typing derivation, using 1 and 2.

Observe that the only hypothesis is that \( \phi; \Phi \vdash_\varepsilon I \downarrow \) (definition in Section 3.1): we do not require \( I \) to be a value of \( a \) that satisfies \( \Psi \). If it does not the constraints in \( \Phi, \Psi \{1/a\} \) become inconsistent, and the obtained judgements are vacuous.

5.2 Subject Reduction

What we want to prove in this subsection is the following result:

**Proposition 5.4 (Subject Reduction)** If \( t \rightarrow_\varphi u \) and \( \phi; \Theta \vdash_\varepsilon t : \tau \), then \( \phi; \Phi; \Theta \vdash_\varepsilon u : \tau \).

Subject Reduction can be proved in a standard way, by going through a Substitution Lemma, which only needs to be proved when the term being substituted is a value. Preliminary to the Substitution Lemma are two auxiliary results stating that derivations giving types to values can, if certain conditions hold, be split into two, or put in parametric form:

**Lemma 5.5 (Splitting)** If \( \phi; \Phi; \Gamma \vdash_\varepsilon v : \tau \uplus \tau_2 \), then there exist two indexes \( N_1, N_2 \), and two contexts \( \Gamma_1, \Gamma_2 \), such that \( \phi; \Phi; \Gamma_1 \vdash_\varepsilon v : \tau_1 \), and \( \phi; \Phi \vdash_\varepsilon N_1 + N_2 \leq M \) and \( \phi; \Phi \vdash_\varepsilon \Gamma \uplus \Gamma_2 \).
Hence we can conclude with $\Gamma$ by Lemma 5.1 and derive

$$\frac{(a, \phi); (a < I, \Phi); \Delta, x : \sigma \vdash K \tau t : \tau}{\phi; \Phi \vdash \Gamma \subseteq \sum_{a < I} \Delta}$$

with $\tau_1 \cdot \tau_2 = [a < I] \cdot \sigma \vdash \Gamma$ and $M = I + \sum_{a < I} K$. Hence $I = I_1 + I_2$, and $\tau_1 = [a < I_1] \cdot \sigma \vdash \Gamma$, and $\tau_2 = [a < I_2] \cdot \sigma \{b / a\} \vdash \Gamma \{b / a\}$. Since $(a, \phi); (a < I, \Phi) \vdash E (a, \phi ; I, \Phi)$, we can strengthen the hypothesis in (3) by Lemma 5.3 and derive

$$\frac{(a, \phi); (a < I, \Phi); \Delta, x : \sigma \vdash K \tau t : \tau}{\phi; \Phi; \sum_{a < I} \Delta \vdash \sum_{a < I} K \lambda x.t : [a < I] \cdot \sigma \vdash \Gamma}$$

On the other hand, we can substitute $a$ with $a + I_1$ in (3) by Lemma 5.3 and derive

$$\frac{(a, \phi); (a < I_2, \Phi); \Delta(a + I_1/a), x : \sigma(a + I_1/a) \vdash K(a + I_1/a) \tau t : \tau(a + I_1/a)}{\phi; \Phi; \sum_{a < I_2} \Delta(a + I_1/a) \vdash \sum_{a < I_1} K(a + I_1/a) \lambda x.t : [a < I] \cdot \sigma(a + I_1/a) \vdash \Gamma}$$

Hence we can conclude with $\Gamma_1 = \sum_{a < I_1} \Delta$, $\Gamma_2 = \sum_{a < I_2} \Delta(a + I_1/a)$, and $N_1 = I_1 + \sum_{a < I_1} K$ and $N_2 = I_2 + \sum_{a < I_2} K(a + I_1/a)$.

Now, if $v = \text{fix } x.t$, then its typing judgement derives from

$$\frac{(b, \phi); (b < H, \Phi); \Delta, x : [a < I] \cdot A \vdash \Delta \tau t : [a < I] \cdot B}{\phi; \Phi \vdash E \Gamma \geq H \geq \sum_{a < H} K}$$

with $\tau_1 \cdot \tau_2 = [a < K] \cdot C$, and $M = H + \sum_{a < H} I$. Hence $K = K_1 + K_2$, with $\tau_1 = [a < K_1] \cdot C$, and $\tau_2 = [a < K_2] \cdot C(a + K_1/a)$. Let $H_1 = \sum_{a < H} K_1 I$ and $H_2 = \sum_{a < H} K_2 I$. Then $H_1 + H_2 = \sum_{a < H} K I$, and $H_2$ is also equal to $\sum_{a < H} K I$. Just like the previous case, we can strengthen the hypothesis in (5), (7), and (8) and derive

$$\frac{(b, \phi); (b < H_1, \Phi); \Delta, x : [a < I] \cdot A \vdash \Delta \tau t : [a < I] \cdot B}{(a, b, \phi); (a < I, b < H_1, \Phi) \vdash E B \{0/a\} \{(\sum_{a < H} K_1 I + b + 1/b) \} \subseteq A}$$

and get

$$\frac{(a, \phi); (a < I, b < H_2, \Phi) \vdash E B \{0/a\} \{(\sum_{a < H} K_2 I + b + 1/b) \} \subseteq A \{b + 1/b\}}{(a, b, \phi); (a < I, b < H_2, \Phi) \vdash E B \{0/a\} \{(\sum_{a < H} K_2 I + b + 1/b) \} \subseteq A \{b + 1/b\}}$$

Moreover, if we substitute $b$ with $b + H_2$ in (7) and we strengthen the constraints (since $b$ implies $\phi; b < H_2 \vdash E \Phi ; b + H_1 < H$), we get

$$\frac{(a, b, \phi); (a < I, b < H_2, \Phi) \vdash E B \{0/a\} \{(\sum_{a < H} K_2 I + b + 1/b) \} \subseteq A \{b + 1/b\}}{(a, b, \phi); (a < I, b < H_2, \Phi) \vdash E B \{0/a\} \{(\sum_{a < H} K_2 I + b + 1/b) \} \subseteq A \{b + 1/b\}}$$

But $(\sum_{a < H} K_2 I + b + 1/b) \subseteq A \{b + 1/b\}$, and so $B \{0/a\} \{(\sum_{a < H} K_2 I + b + 1/b) \} \subseteq A \{b + 1/b\}$. Finally, by substituting also $b$ with $b + H_1$ in (8) we can derive

$$\frac{(a, \phi); (a < K_2, \Phi) \vdash E B \{0/a\} \{(\sum_{a < H} K_2 I + b + 1/b) \} \subseteq C \{a + K_1/a\}}{(a, \phi); (a < K_2, \Phi) \vdash E B \{0/a\} \{(\sum_{a < H} K_2 I + b + 1/b) \} \subseteq C \{a + K_1/a\}}$$
Given Lemma 5.7, proving Proposition 5.4 is routine: the only two nontrivial cases are those where the fired redex is a \( \beta \)-redex or the unfolding of a recursively-defined function, and both consist in a fixing a variable \( x \) that is in the context of the rule. Observe how Subject Reduction already embeds a form of extensional soundness for \( \mathcal{D} \text{-PCF}_V \), since types are preserved by reduction. As an example, if one builds a type derivation for \( \vdash^{\mathcal{E}}_M t : \text{Nat}[2,7] \), then the normal form of \( t \) (if it exists) is guaranteed to be a constant between 2 and 7. Observe, on the other hand, than nothing is known about the complexity of the underlying computational process yet, since the weight \( I \) does not necessarily decrease along reduction. This is the topic of the following section.

5.3 Intentional Soundness

In this section, we prove the following result:

**Theorem 5.8 (Intensional soundness)** For any term \( t \), if

\[ \vdash^{\mathcal{E}}_H t : \text{Nat}[I, J] \]

then \( t \downarrow^m \mathbb{N} \) where \( n \leq |t| \cdot (|H|)^{\mathcal{E}} + 1 \) and \( |H|^{\mathcal{E}} \leq m \leq |J|^{\mathcal{E}} \).

Roughly speaking, this means that \( \mathcal{D} \text{-PCF}_V \) also gives us some sensible information about the time complexity of evaluating typable \( \text{PCF} \) programs. The path towards Theorem 5.8 is not too short:
it is necessary to lift $d{\textbf{PCF}}_V$ to a type system for closures, environments and processes, as defined in Section 3.3. Actually, the type system can be easily generalised to closures by the rule below:

$$
\phi; \Phi; x_1 : \sigma_1, \ldots, x_n : \sigma_n \vdash^z_{\bar{K}} t : \tau \\
\phi; \Phi \vdash^z_{\bar{K} + \sum_{i < n} l_i} v_i : \sigma_i \\
\phi; \Phi \vdash^z_{\bar{K} + \sum_{i < n} l_i} \langle t; \{x_1 \mapsto v_1; \ldots; x_n \mapsto v_n\} \rangle : \tau
$$

Lifting everything to stacks, on the other hand, requires more work, see Figure 8. We say that it is necessary to lift $\phi; \Phi$ to be acceptable for $\sigma$ with type $\tau$ with cost $I$ (notation: $\phi; \Phi \vdash^z_{\bar{K}} \pi : (\sigma, \tau)$) when it interacts well with closures of type $\sigma$ to produce a process of type $\tau$. Indeed, a process can be typed as follows:

$$
\phi; \Phi \vdash^z_{\bar{K}} \pi : (\sigma, \tau) \\
\phi; \Phi \vdash^z_{\bar{K}} c : \sigma \\
\phi; \Phi \vdash^z_{\bar{K} + I} c \star \pi : \tau
$$

This way, also the notion of weight has been lifted to processes, with the hope of being able to show that it strictly decreases at every evaluation step. Apparently, this cannot be achieved in full: sometimes the weight of a process does not change, but in that case another parameter is guaranteed to decrease, namely the process size. The size $|c \star \pi|$ of $c \star \pi$, is defined as $|c| + |\pi|$, where:

- The size $|c|$ of a closure $\langle t; \xi \rangle$ is the multiplicative size of $t$ (cf. Section 5.2).
- The size of $|\pi|$ is the sum of the sizes of all closures appearing in $\pi$ plus the number of occurrences of symbols (different from $\circ$ and fun) in $\pi$.

The formal definition of $|c \star \pi|$ is given in Figure 9.

The size of a process decreases by any evaluation steps, except the two ones performing a substitution (1) and (2). However, these two reduction rules make the weight of a process decrease, as formalised by the following proposition. By the way, these are the cases in which a box is opened up in the underlying linear logic proof.

**Proposition 5.9 (Weighted Subject Reduction)** Assume $P > R$ and $\phi; \Phi \vdash^z_{\bar{K}} P : \tau$. Then $\phi; \Phi \vdash^z_{\bar{K}} R : \tau$ and

- either $\phi; \Phi \vdash^z_{\bar{K}} I = J$ and $|P| > |R|$, or $\phi; \Phi \vdash^z_{\bar{K}} I > J$ and $|P| + |s| > |R|$, where $s$ is a term appearing in $P$.

**Proof.** 1. If $P > R$ with a non substitution rule (any rule of Figure 3 or Figure 5 except (1) and (2)), then it is easy to check that $|P| > |R|$. Moreover, in all these cases $P$ and $R$ have the same type and the same weight. We detail some cases:

---

**Figure 9: Size of processes**
• If \( P = v \star \text{arg}(c, \pi) \succ c \star \text{fun}(\nu, \pi) = R \), then the typing of \( P \) derives from

\[
\begin{align*}
\phi; \Phi &\vdash^c c : \sigma_0(0/a) \\
\phi; \Phi &\vdash^\pi \pi : ([\tau_0(0/a), \tau] \\
\phi; \Phi &\vdash \sigma \subseteq [a < 1] \cdot (\sigma_0 \to \tau_0) \\
\phi; \Phi &\vdash \eta = J = H + L \\
\phi; \Phi &\vdash^\pi \text{arg}(c, \pi) : (\sigma, \tau) \\
\phi; \Phi &\vdash^\pi v : \sigma \\
\phi; \Phi &\vdash \eta = J + K
\end{align*}
\]

Hence since subtyping is derivable (Lemma 5.5) we can derive for \( R \):

\[
\begin{align*}
\phi; \Phi &\vdash^c c : \sigma_0(0/a) \\
\phi; \Phi &\vdash^\pi \pi : ([\tau_0(0/a), \tau] \\
\phi; \Phi &\vdash \eta = J = H + L + K
\end{align*}
\]

• If \( P = \langle tu; \xi \rangle \succ \langle t; \xi \rangle \star \text{arg}(\langle u; \xi \rangle, \pi) = R \), then the typing of \( P \) derives from

\[
\begin{align*}
\phi; \Phi; x_1 : \mu_1, \ldots, x_n : \mu_n &\vdash^\pi t : [a < N] \cdot \kappa \to \eta \\
\phi; \Phi; x_1 : \eta_1, \ldots, x_n : \eta_n &\vdash^\eta \eta : [\tau_0(0/a), \kappa] \\
\phi; \Phi &\vdash \sigma_1 \subseteq \mu_i \cup \eta_i \\
\phi; \Phi &\vdash\eta \eta \subseteq [0/a] \subseteq \sigma \\
\phi; \Phi &\vdash^\pi \text{arg}(tu; \xi) : \sigma \\
\phi; \Phi &\vdash^\pi \mu_i : \sigma_i \\
\phi; \Phi &\vdash^\pi \eta_i : \tau_i \\
\phi; \Phi &\vdash \eta = J + K + \sum_i J_i \\
\phi; \Phi &\vdash^\pi \langle tu; \xi \rangle : \sigma \\
\phi; \Phi &\vdash^\pi \eta = J + K + \sum_i J_i \\
\phi; \Phi &\vdash^\pi \eta = J + H + K + \sum_i J_i \\
\phi; \Phi &\vdash^\pi \langle tu; \xi \rangle \succ \langle t; \xi \rangle \star \text{arg}(\langle u; \xi \rangle, \pi) = R
\end{align*}
\]

In particular, since subtyping is derivable, \( \phi; \Phi \vdash^\pi \nu_i : \mu_i \cup \eta_i \) for each \( i \). By Lemma 5.5 (that can be trivially extended to closures), it means that there are some \( X_i, N_i \) such that

\[
\begin{align*}
\phi; \Phi &\vdash^\mu \nu_i : \mu_i \\
\phi; \Phi &\vdash^\eta \nu_i : \eta_i \\
\phi; \Phi &\vdash \eta = J + M_i + N_i = J_i \\
\phi; \Phi &\vdash^\pi \text{arg}(\langle u; \xi \rangle, \pi) : \kappa \to \eta
\end{align*}
\]

Hence both these judgements are derivable:

\[
\begin{align*}
\phi; \Phi; x_1 : \mu_1, \ldots, x_n : \mu_n &\vdash^\pi t : [a < 1] \cdot \kappa \to \eta \\
\phi; \Phi &\vdash^\eta \nu_i : \mu_i \\
\phi; \Phi &\vdash^\eta \nu_i : \tau_i \\
\phi; \Phi &\vdash^\pi \text{arg}(\langle u; \xi \rangle, \pi) : \kappa \to \eta
\end{align*}
\]

and

\[
\begin{align*}
\phi; \Phi; x_1 : \eta_1, \ldots, x_n : \eta_n &\vdash^\pi \eta : [\tau_0(0/a), \kappa] \\
\phi; \Phi &\vdash^\eta \nu_i : \tau_i \\
\phi; \Phi &\vdash^\pi \text{arg}(\langle u; \xi \rangle, \pi) : \kappa \to \eta
\end{align*}
\]

Hence we can derive the following typing judgement for \( R \) (notice that subtyping is derivable for the stacks, with contravariance in the first type):

\[
\begin{align*}
\phi; \Phi &\vdash^\pi \text{arg}(\langle u; \xi \rangle, \pi) : ([a < 1] \cdot \kappa \to \eta, \tau) \\
\phi; \Phi &\vdash \eta = J + H + \sum_i N_i \\
\phi; \Phi &\vdash \eta = J + H + \sum_i (M_i + N_i) \\
\phi; \Phi &\vdash \eta = K + J + H + \sum_i (M_i + N_i) \\
\phi; \Phi &\vdash^\pi \langle tu; \xi \rangle \succ \langle t; \xi \rangle \star \text{arg}(\langle u; \xi \rangle, \pi) = R
\end{align*}
\]

2. If \( P \succ R \) with a substitution rule...

Splitting and parametric splitting play a crucial role here, once appropriately generalised to value closures.
Given Proposition 5.9, Theorem 5.8 is within reach: the natural number \(|s|\) in Proposition 5.9 cannot be greater than the size of the term \(t\) we start from, since the only “new” terms created along reduction are constants in the form \(n\) (which have null size).

### 5.4 (Relative) Completeness

In this section, we will prove some results about the expressive power of \(d/\text{PCF}_V\), seen as a tool to prove intentional (but also extensional) properties of PCF terms. Actually, \(d/\text{PCF}_V\) is extremely powerful: every first-order PCF program computing the function \(f : \mathbb{N} \rightarrow \mathbb{N}\) in a number of steps bounded by \(g : \mathbb{N} \rightarrow \mathbb{N}\) can be proved to enjoy these properties by way of \(d/\text{PCF}_V\), provided two conditions are satisfied:

- On the one hand, the equational program \(E\) needs to be universal, meaning that every partial recursive function is expressible by some index terms. This can be guaranteed, as an example, by the presence of a universal program in \(E\).
- On the other hand, all true statements in the form \(\phi; \Phi \vdash E I \leq J\) must be “available” in the type system for completeness to hold. In other words, one cannot assume that those judgements are derived in a given (recursively enumerable) formal system, because this would violate Gödel’s Incompleteness Theorem. In fact, ours are completeness theorems relative to an oracle for the truth of those assumptions, which is precisely what happens in Floyd-Hoare logics [6].

#### PCF Typing

The first step towards completeness is quite easy: propositional type systems in the style of PCF for terms, closures, stacks and processes need to be introduced. All of them can be easily obtained by erasing the index information from \(d/\text{PCF}_V\). As an example, the typing rule for the application looks like

\[
\frac{\Gamma \vdash \text{PCF} \, \ell : \alpha \Rightarrow \beta \quad \Gamma \vdash \text{PCF} \, u : \alpha}{\Gamma \vdash \text{PCF} \, \ell u : \beta}
\]

while processes can be typed by the following rule

\[
\frac{\vdash \text{PCF} \, \pi : (\alpha, \beta) \quad \vdash \text{PCF} \, \epsilon : \alpha}{\vdash \text{PCF} \, \epsilon \cdot \pi : \beta}
\]

Given any type \(\sigma\) (respectively any type derivation \(\delta\)) of \(d/\text{PCF}_V\), the PCF type (respectively, the PCF type derivation) obtained by erasing all the index information will be denoted by \([\sigma]\) (respectively, by \([\delta]\)). Of course both terms and processes enjoy subject reduction theorems with respect to PCF typing, and their proofs are much simpler than those for \(d/\text{PCF}_V\). As an example, given a type derivation \(\delta\) for \(\vdash \text{PCF} \, P : \text{Nat}\) (we might write \(\delta \triangleright \vdash \text{PCF} \, P : \text{Nat}\)) and \(P > R\), a type derivation \(\delta'\) for \(\vdash \text{PCF} \, R : \text{Nat}\) can be easily built by manipulating in a standard way \(\delta\); we write \(\delta > \delta'\).

#### Weighted Subject Expansion

The key ingredient for completeness is a dualisation of Weighted Subject Reduction:

**Proposition 5.10 (Weighted Subject Expansion)** Suppose that \(\delta \triangleright \vdash \text{PCF} \, P : \alpha\), that \(\delta > \delta'\), and that \(\theta' \triangleright \phi; \Phi \vdash \text{PCF} \, R : \tau\) where \([\theta'] = \delta'\). Then there is

\[
\theta \triangleright \phi; \Phi \vdash \text{PCF} \, \ell : \tau
\]

with \([\theta] = \delta\) and \(\phi; \Phi \vdash \text{PCF} \, J \leq I + 1\). Moreover, \(\theta\) can be effectively computed from \(\delta, \theta'\) and \(\delta'\).

Proving Proposition 5.10 requires a careful analysis of the evolution of the CEK\(_{\text{PCF}}\) machine, similarly to what happened for Weighted Subject Reduction. But while in the latter it is crucial to be able to (parametrically) split type derivations for terms (and thus closures), here we need to be able to join them:
sequence of processes

Observe that the Joining Lemma requires the two type derivations to be joined to have the same completeness result, namely one about programs (which are terms of type $\text{PCF}$). It should be now clear that one can reach the following:

Completeness for Programs We now have all the necessary ingredients to obtain a first completeness result, namely one about programs (which are terms of type $\text{Nat}$). Suppose that $t$ is a $\text{PCF}$ program such that $t \rightarrow^* m$, where $m$ is a natural number. By Proposition 5.11 there is a sequence of processes

where $P_1 = (\langle t \rangle, \varnothing) * \varnothing$ and $P_n = (\langle m \rangle, \varnothing) * \varnothing$. Of course, $\vdash P_i : \text{Nat}$ for every $i$. For obvious reasons, $\vdash P_i : \text{Nat}[m]$. Moreover, by Weighted Subject Expansion, we can derive each of $\vdash_{\text{PCF}} P_i : \text{Nat}[m]$, until we reach $\vdash_{\text{PCF}} P_1 : \text{Nat}[m]$, where $I_1 \leq n$ (see Figure 10 for a graphical representation of the above argument). It should be now clear that one can reach the following:

Theorem 5.13 (Completeness for Programs) Suppose that $t \vdash_{\text{PCF}} t : \text{Nat}$, that $t \Downarrow^k \mathbb{M}$ and that $E$ is universal. Then, $\vdash_{\text{PCF}} t : \text{Nat}[m]$, where $k \leq n$.

Uniformisation and Completeness for Functions Completeness for programs, however, is not satisfactory: the fact (normalising) $\text{PCF}$ terms of type $\text{Nat}$ can all be analysed by $d$-$\text{PCF}_V$ is not so surprising, and other type systems (like non-idempotent intersection types $\text{IM}$) have comparable expressive power. Suppose we want to generalise relative completeness to first-order functions: we would like to prove that every term $t$ having a $\text{PCF}$ type $\text{Nat} \Rightarrow \text{Nat}$ (which terminates...
when fed with any natural number) can be typed in $\text{dPCF}_V$. How could we proceed? First of all, observe that the argument in Figure 10 could be applied to all instances of $t$, namely to all terms in $\{tn \mid n \in \mathbb{N}\}$. This way one can obtain, for every $n \in \mathbb{N}$, a type derivation $\delta_n$ of

$$
\Gamma \vdash I_n t : [a < J_n] \cdot \text{Nat}[K_n] \rightarrow \text{Nat}[H_n]
$$

where $J_n$ can be assumed to be 1, while $K_n$ can be assumed to be $n$. Moreover, the problem of obtaining $\delta_n$ from $n$ is recursive, i.e., can be solved by an algorithm. Surprisingly, the infinitely many type derivations in $\{\delta_n \mid n \in \mathbb{N}\}$ can be turned into one:

**Proposition 5.14 (Uniformisation of type derivations)** Suppose that $E$ is universal and that $\{\delta_n\}_{n \in \mathbb{N}}$ is a recursively enumerable class of type derivations satisfying the following constraints:

1. For every $n \in \mathbb{N}$, $\theta_n \vdash I_n t : \sigma_n$;
2. all derivations have the same skeleton

Then there is a type derivation $\theta \vdash a; \emptyset \vdash I_n t : \sigma$ such that $\Gamma \vdash I\{n/a\} = I_n$ and $\Gamma \vdash \sigma\{n/a\} = \sigma_n$ for all $n$.

Uniformisation of type derivations should be seen as an extreme form of joining: not only a finite number of type derivations for the same term can be unified into one, but even any recursively enumerable class of them can. Again, the universality of $E$ is crucial here. We are now ready to give the following:

**Theorem 5.15 (Completeness for functions)** Suppose that $\varphi \vdash \text{Nat} \Rightarrow \text{Nat}$, that $t_{\mathbb{N}} \models \phi_n$ $m_n$ for all $n \in \mathbb{N}$ and that $E$ is universal. Then, there is an index $H$ such that $a; \emptyset ; \emptyset \vdash I [b < 1] \cdot \text{Nat}[a] \rightarrow \text{Nat}[H]$, where $\Gamma \vdash \text{Nat}\{n/a\} \leq k_n$ and $\Gamma \vdash H\{n/a\} = m_n$.

6 Further Developments

Relative completeness of $\text{dPCF}_V$, especially in its stronger form (Theorem 5.15) can be read as follows. Suppose that a (sound), finitary formal $C$ system deriving judgements in the form $\Theta; \Phi \vdash I \leq J$ is fixed and “plugged” into $dPCF_V$. What you obtain is a sound, but necessarily incomplete formal system, due to Gödel’s incompleteness. However, this incompleteness is only due to $C$ and not to the rules of $dPCF_V$, which are designed so as to reduce the problem of proving properties of programs to checking inequalities over $E$ without any loss of information.

In this scenario, it is of paramount importance to devise techniques to automatically reduce the problem of checking whether a program satisfies a given intentional or extensional specification to the problem of checking whether a given set of inequalities over an equational program $E$ hold. Indeed, many techniques and concrete tools are available for the latter problem (take, as an example, the immense literature on SMT solving), while the same cannot be said about the former problem. The situation, in a sense, is similar to the one in the realm of program logics for imperative programs, where logics are indeed very powerful [8], and great effort have been directed to devise efficient algorithms generating weakest preconditions [10].

Actually, at the time of writing, the authors are actively involved in the development of relative type inference algorithms for both $\text{dPCF}_N$ and $\text{dPCF}_V$, which can be seen as having the same role as algorithms computing weakest preconditions. This is however out of the scope of this paper.

7 Conclusions

Linear dependent types are shown to be applicable to the analysis of intentional and extensional properties of functional programs when the latter are call-by-value evaluated. More specifically, soundness and relative completeness results are proved for both programs $a$ and functions. This generalises previous work by Gaboardi and the first author [5], who proved similar results in

20
the call-by-name setting. This shows that linear dependency not only provides an expressive formalism, but is also robust enough to be adaptable to calculi whose notions of reduction are significantly different (and more efficient) than normal order evaluation.

Topics for future work include some further analysis about the applicability of linear dependent types to languages with more features, including some form of inductive data types, or ground type references.

References


