Correctness of Non-determinism Analyses in a Parallel-Functional Language*

Clara Segura and Ricardo Peña

20 March 2003

Technical Report n° 131-03
Departamento de Sistemas Informáticos y Programación
Universidad Complutense de Madrid, Spain

Abstract. The presence of non-determinism in the parallel-functional language Eden creates some problems. Several non-deteminism analyses have been developed to determine when an Eden expression is sure to be deterministic, and when it may be non-deterministic. The correctness of these analyses had not been proved yet as there was not a formally defined denotational semantics for Eden including non-determinism. In this paper we define a "maximal" denotational semantics for Eden in the sense that the set of possible values produced by an expression is bigger than the actual one. This semantics is enough to prove the correctness of the analyses. We provide the abstraction and concretisation functions relating the concrete and abstract values so that the determinism property is adequately captured. Finally we prove the correctness of the analyses with respect to the previously defined semantics.

1 Introduction

The presence of non-determinism in the parallel-functional language Eden creates some problems [6]: It affects the referential transparency of programs [3, 10] and invalidates some optimizations done in the Glasgow Haskell Compiler (GHC) [9]. Three non-determinism analyses have been defined to determine when an Eden expression is sure to be deterministic, and when it may be non-deterministic [6, 7]. They have been formally related and compared with respect to expresiveness and efficiency [4, 5].

However the correctness of these analyses had not been proved yet as there was not a formally defined denotational semantics for Eden including non-determinism. The first contribution of this paper is the definition of such a denotational semantics. It is a *plural* semantics in the style of [11] but with higher order and algebraic types incorporated. The domains of values are defined by means of Hoare powerdomains considering that the behaviour of the non-deterministic operator is near to angelic non-determinism. It is not the actual semantics of Eden but an upper approximation to it in the sense that the set of possible values produced by an expression is bigger than the actual one. This semantics is enough to prove the correctness of the analyses.

Then, we provide the abstraction and concretisation functions relating the concrete and abstract values so that the determinism property is adequately

* Work partially supported by the Spanish project TIC 2000-0738.

captured. Finally we prove the correctness of the analyses with respect to the previously defined semantics.

The plan of the paper is as follows. In Section 2 we describe Eden and the non-determinism analyses that have been defined for it. In Section 3 we present the denotational semantics including non-determinism. Finally, in Section 4 correctness of the analyses is formally proved.

2 Non-determinism Analyses for Eden

2.1 Eden in a nutshell

The parallel-functional language Eden extends the lazy functional language Haskell by constructs to explicitly define and communicate processes. The three main new concepts are *process abstractions*, *process instantiations* and the non-deterministic process abstraction `merge`.

A *process abstraction* expression `process x -> e` of type `Process a b` defines the behaviour of a process having the formal parameter `x::a` as input and the expression `e::b` as output. An instantiation is achieved by using the predefined infix operator `(#) :: Process a b -> a -> b`. Process abstractions of type `Process a b` can be compared to functions of type `a -> b`, the main difference being that the former, when instantiated, are executed in parallel. Process instantiations can be compared to function applications: Each time an expression `e1 # e2` is evaluated, a new parallel process is created to evaluate `(e1 e2)`.

The evaluation of an expression `e1 # e2` leads to the dynamic creation of a process together with its interconnecting communication channels. The instantiating or *parent process* will be responsible for evaluating and sending `e2` via an implicitly generated channel, while the new *child process* will evaluate first the expression `e1` until a process abstraction `process x -> e` is obtained and then the application `(\ x -> e) e2`, returning the result via another implicitly generated channel. The instantiation protocol deserves some attention: (1) Closure `e1` together with the closures of all the free variables referenced there (its whole environment) are *copied*, in the current evaluation state (possibly unevaluated), to a new processor, and the child process is created there to evaluate the expression `(\ x -> e) e2`, where `e2` must be remotely received. (2) Expression `e2` is eagerly evaluated in the parent process. The resulting full normal form data is communicated to the child process as its input argument. (3) The normal form of the value `(\ x -> e) e2` is sent back to the parent. For input or output tuples, independent concurrent threads are created to evaluate each component.

Processes communicate via *unidirectional channels* which connect one writer to exactly one reader. Once a process is running, only fully evaluated data objects are communicated. The only exceptions are lists, which are transmitted in a *stream*-like fashion, i.e. element by element. Each list element is first evaluated to full normal form and then transmitted. Concurrent threads trying to access input which is not available yet, are temporarily suspended. This is the only way in which Eden processes synchronize.

Lazy evaluation is changed to eager evaluation in two cases: Processes are eagerly instantiated, and instantiated processes produce their output even if it

is not demanded. These modifications aim at increasing the parallelism degree and at speeding up the distribution of the computation. In general, a process is implemented by several threads concurrently running in the same processor, so that different values can be produced independently. The concept of a virtually shared global graph does not exist. Each process evaluates its outputs autonomously.

Non-determinism is introduced in Eden by means of a predefined process abstraction `merge :: Process [[a]] [a]` which *fairly* interleaves a set of input lists, to produce a single non-deterministic list. Its implementation immediately copies to the output list any value appearing at any of the input lists. So, `merge` can profitably be used to quickly react to requests coming in an unpredictable order from a set of processes. This feature is essential in reactive systems and very useful in some deterministic parallel algorithms. Eden is aimed at both types of applications.

2.2 A simplified language

In the next section a denotational semantics is defined for a simplified version of Eden, see Figure 1, in order to prove correctness of several non-determinism analyses. The language is an extended simplification of Core-Haskell [8], a simple functional language with second-order polymorphism. As Eden is an extension of Haskell, it is obviously polymorphic. But in order to simplify the rest of the paper, we have removed this aspect of the language. So there are neither type abstractions nor type applications.

A program is a list of possibly recursive bindings from variables to expressions. Such expressions include variables, lambda abstractions, applications of a functional expression to an atom, tuples, constructor applications, and also *case* and *let* expressions. We will use v to denote a variable, k to denote a literal, and x to denote an atom (a variable or a literal). Constructor applications are saturated.

The variables contain type information, so we will not write it explicitly in the expressions. When necessary, we will write $e :: t$ to make explicit the type of an expression. A type may be a basic type K, a tuple type $(t_1, \ldots, t_m)$, an algebraic (sum) type T[1], or a functional type $t_1 \to t_2$.

Process abstractions **process** $v \to e$ and process instantiations $e \# x$ do not appear in the language. This simplification of the language is motivated by an approximation to the semantics explained in Section 3.2. When an unevaluated non-deterministic free variable is duplicated in two different processes, it may happen that the actual value computed by each process is different. However, within the same process, a variable is evaluated at most once and its value is shared thereafter. Consequently this means that variables are *definite* (each occurrence denotes the same single value) within the same process and are not definite (different occurrences may denote different values) within different processes. In general, in Eden the *unfoldability* property does not hold (a variable cannot be replaced by its definition, i.e. $[\![(\lambda x.e)\ e']\!]\ \rho \neq [\![e[e'/x]]\!]\ \rho$), except in

[1] Defined by **data** $T = C_1\ t_{11} \ldots t_{1n_1} \mid \ldots \mid C_m\ t_{m1} \ldots t_{mn_m}$.

$$
\begin{array}{lll}
prog \rightarrow bind_1; \ldots; bind_m & & \\
bind \rightarrow \quad v = expr & & \{\text{non-recursive binding}\} \\
\quad | \ \textbf{rec}\ v_1 = expr_1; \ldots; v_m = expr_m & & \{\text{recursive binding}\} \\
expr \rightarrow \quad expr\ x & & \{\text{application to an atom}\} \\
\quad | \ \lambda v.expr & & \{\text{lambda abstraction}\} \\
\quad | \ \textbf{case}\ expr\ \textbf{of}\ alts & & \{case \text{ expression}\} \\
\quad | \ \textbf{let}\ bind\ \textbf{in}\ expr & & \{let \text{ expression}\} \\
\quad | \ (x_1, \ldots, x_m) & & \{\text{tuple}\} \\
\quad | \ C\ x_1 \ldots x_m & & \{\text{saturated constructor application}\} \\
\quad | \ x & & \{\text{atom: variable } v \text{ or literal } k\} \\
\quad | \ merge_t & & \{\text{non-determinism operator}\} \\
alts \rightarrow \quad Calt_1; \ldots; Calt_m; [Deft] & m \geq 0 & \\
\quad | \ Lalt_1; \ldots; Lalt_m; [Deft] & m \geq 0 & \\
\quad | \ TAlt & & \\
TAlt \rightarrow (v_1, \ldots, v_m) \rightarrow expr & m \geq 0 & \{\text{tuple alternative}\} \\
Calt \rightarrow C\ v_1 \ldots v_m \rightarrow expr & m \geq 0 & \{\text{algebraic alternative}\} \\
Lalt \rightarrow k \rightarrow expr & & \{\text{primitive alternative}\} \\
Deft \rightarrow v \rightarrow expr & & \{\text{default alternative}\}
\end{array}
$$

Fig. 1. A simplified version of a parallel functional language

the case that the unfolded expression is deterministic. This is a consequence of having definite variables within a process.

So, there are some ocurrences that surely have the same value but others may have different values. The following example illustrates this situation. Assume ne is a non-deterministic expression:

$$
\begin{array}{l}
\textbf{let}\ v = ne \\
\textbf{in}\ (p_1\ v)\#v + (p_2\ v)\#v
\end{array}
$$

The second and fourth ocurrences of v necessarily have the same value as they are evaluated in the parent process. However the first and third occurrences may have different values as v is copied twice and evaluated in two children processes. So, an upper approximation is obtained by considering that

- All the ocurrences of each variable may have a different value, i.e. all the variables are non-definite.
- All functions behave as processes, and consequently all function applications behave as process instantiations. Consequently, we will only have syntactical lambda abstractions and function applications with the semantics of process abstractions and process instantiations.

The semantics defined in Section 3.2 will make these assumptions.

As polymorphism is omitted, the `merge` operator is monomorphic, so we consider the existence of an instance $merge_t$ for every type t. Aditionally we simplify this operator so that it merges just two lists of values: $merge_t : [t] \rightarrow [t] \rightarrow [t]$. Eden's `merge` is more convenient since it may receive as arguments any finite number of lists, but it can be simulated by the simplified one, $merge_t$.

2.3 Motivation for the analyses

The non-deterministic process `merge` may be used to create non-deterministic expressions and to define non-deterministic funcions. Subsection 2.4 introduces several analyses to detect at compile time these non-deterministic expressions. The analyses annotate the expressions with a mark which, in the simplest case is just d or n. The first one means that the expression is *sure* to be deterministic, while the second one means that it *may be* non-deterministic. So, a possible better name for these analyses would be *determinism* analyses because the sure value is the deterministic one. We found at least three motivations for developing these analyses:

In the one hand, to annotate the places in the text where equational reasoning may be lost due to the presence of non-determinism. This is important in an optimizing compiler such as that of Eden built on top of GHC [8]. A lot of internal transformations such as *inlining* or *full laziness* are done on the assumption that it is always possible to replace equals by equals. This is not true when the expressions involved are non-deterministic. For instance, the full laziness transformation moves a binding out of a lambda when it does not depend on the lambda argument. So, the expression

$$\begin{array}{l}\textbf{let } f = \lambda x.\ \textbf{let } y = e_1 \\ \qquad\qquad\quad \textbf{in } e_2 \\ \textbf{in } \ e_3\end{array}$$

when e_1 does not depend on x is transformed to

$$\begin{array}{l}\textbf{let } y = e_1 \\ \textbf{in } \ \textbf{let } f = \lambda x.e_2 \\ \qquad \textbf{in } e_3\end{array}$$

If e_1 is non-deterministic, this transformation restricts the set of values the expression may evaluate to, as now expression e_1 is evaluated only once instead of many times.

A second motivation is to be able to implement in the future a semantics for Eden, different from the currently implemented one, in which all variables will be guaranteed to be definite, i.e. they will denote the same value in all the processes. To this aim, when a non-deterministic binding is to be copied to a newly instantiated process, the runtime system will take care of previously evaluating the binding to normal form. Doing this evaluation for all bindings would make Eden more eager than needed and would decrease the amount of parallelism as more work would be done in parent processes. So, it is important to do this evaluation only when it is known that the binding is possibly non-deterministic.

A third motivation could be to be able to inform the programmer of the deterministic expressions of the program. In this way, the part of the program where equational reasoning is still posssible would be clearly determined. To this aim, a first step is doing the analysis at the core language level. A translation of the annotations to source level would also be required in order to provide the programmer with meaningful information. For the moment we have not implemented this translation.

2.4 A hierarchy of analyses

Three non-determinism analyses have been developed to determine when an Eden expression is sure to be deterministic and when it may be non-deterministic. In [6], two different abstract interpretation based analyses were presented and compared with respect to expresiveness and efficiency. The first one $[\![\cdot]\!]_1$ was efficient (linear) but not very powerful, and the second one $[\![\cdot]\!]_2$ was powerful but less efficient (exponential). In [7] an intermediate analysis $[\![\cdot]\!]_3$ and its implementation (written in Haskell) were described. Such analysis is a compromise between power and efficiency (cubic). Its definition is based on the second analysis $[\![\cdot]\!]_2$. The improvement in efficiency is obtained by speeding up the fixpoint calculation by means of a widening operator *wop*, and by using an easily comparable representation of functions. By choosing different operators we obtain different variants of the analysis $[\![\cdot]\!]_3^{wop}$. The paper describes one particular variant $[\![\cdot]\!]_3^{\mathcal{W}}$ in detail.

In [4] and [5], the three analyses were formally related so that they become totally ordered by increasing cost and precision. In [5] it was shown that all variants of the third analysis are safe approximations to the second analysis. In [4] it was shown that the first analysis is only a safe aproximation to those variants of the third analysis satisfying a particular property. In Figure 2 we illustrate the relation between the first analysis, the second analysis and some variants of the third analysis. In [5] an example was given to show the differences in precision between $[\![\cdot]\!]_1$, $[\![\cdot]\!]_2$ and $[\![\cdot]\!]_3^{\mathcal{W}}$.

In this paper we only summarize the second analysis as we are going to prove its correctness with respect to Eden semantics. The previous results lead us to correctness of the whole hierarchy of analyses with respect to Eden semantics.

In Figure 3 the abstract domains for $[\![\cdot]\!]_2$ are shown. There is a domain *Basic* with two values: d represents *determinism* and n *possible non-determinism*, with the ordering $d \sqsubseteq n$. This is the abstract domain corresponding to basic types and algebraic types. The abstract domains corresponding to a tuple type and a function/process type are respectively the cartesian product of the components' domains and the domain of continuous functions between the domains of the argument and the result. In [6] polymorphism was also included, but in this paper we do not treat it.

In Figure 5 the abstract interpretation for this analysis is shown. It is an abstract interpretation based analysis in the style of [1]. We outline here only some cases. The interpretation of a tuple is the tuple of the abstract values of the components. Functions are interpreted as abstract functions. So, applications are interpreted as abstract functions applications. The interpretation of a constructor application belongs to *Basic*, obtained as the least upper bound (lub) of the components' abstract values. But each component $x_i :: t_i$ has an abstract value belonging to D_{2t_i}, that must be first *flattened* to a basic abstract value. This is done by a function called *flattening function* $\phi_t : D_{2t} \to \mathit{Basic}$, defined in Figure 4. The idea is to flatten the tuples (by applying the lub operator) and to apply the functions to deterministic arguments.

In a recursive **let** expression the fixpoint can be calculated by using Kleene's ascending chain. We have three different kinds of *case* expressions (for tuple,

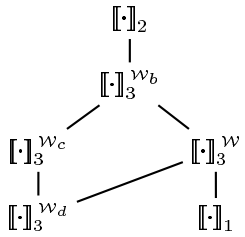

Fig. 2. A hierarchy of analyses

$Basic = \{d, n\}$ where $d \sqsubseteq n$
$D_{2K} = D_{2T} = Basic$
$D_{2(t_1,\ldots,t_m)} = D_{2t_1} \times \ldots \times D_{2t_m}$
$D_{2t_1 \to t_2} = [D_{2t_1} \to D_{2t_2}]$

Fig. 3. Abstract domains for the second analysis

$\phi_t : D_{2t} \to Basic$
$\phi_K = \phi_T = id_{Basic}$
$\phi_{(t_1,\ldots,t_m)}(e_1, \ldots, e_m) = \bigsqcup_i \phi_{t_i}(e_i)$
$\phi_{t_1 \to t_2}(f) = \phi_{t_2}(f(\mu_{t_1}(d)))$

$\mu_t : Basic \to D_{2t}$
$\mu_K = \mu_T = id_{Basic}$
$\mu_{(t_1,\ldots,t_m)}(b) = (\mu_{t_1}(b), \ldots, \mu_{t_m}(b))$
$\mu_{t_1 \to t_2}(b) = \begin{cases} \lambda z \in D_{2t_1}.\mu_{t_2}(n) \text{ if } b = n \\ \lambda z \in D_{2t_1}.\mu_{t_2}(\phi_{t_1}(z)) \text{ if } b = d \end{cases}$

Fig. 4. Functions ϕ_t and μ_t

algebraic types and primitive types). The more complex one is the algebraic *case*. Its abstract value is non-deterministic if either the discriminant or any of the expressions in the alternatives is non-deterministic. Note that the abstract value of the discriminant e, let us call it b, belongs to *Basic*. That is, when it was interpreted, the information about the components was lost. We want now to interpret each alternative's right hand side in an extended environment with abstract values for the variables $v_{ij} :: t_{ij}$ in the left hand side of the alternative. We do not have such information, but we can safely approximate it by using the *unflattening function* $\mu_t : Basic \to D_{2t}$ defined in Figure 4. Given a type t, it *unflattens* a basic abstract value and produces an abstract value in D_{2t}. The idea is to obtain the best safe approximation both to d and n in a given domain. The flattening and unflattening functions are mutually recursive. In [6] they were explained in detail and an example was given to illustrate their definitions. They have some interesting properties (e.g. they are a Galois insertion pair [2]), studied in [5, 4].

3 A Denotational Semantics for Non-determinism

3.1 The domain of values

To capture the idea of a non-deterministic value, the traditional approach is to make a expression to denote a *set* of values. This is obvious for basic types such as integers, but things get more complex when we move to structured types such as functions or tuples. Should a functional expression denote a set of functions or a function from sets to sets? Should a tuple expression denote a set of tuples or a tuple of sets? Additionally, the denoted values should constitute a domain. In the literature, three powerdomains with different properties have been proposed: Hoare, Smyth and Plotkin powerdomains [11]. The first one models *angelic* or

$$
\begin{array}{l}
[\![v]\!]_2\ \rho_2 = \rho_2(v) \\
[\![k]\!]_2\ \rho_2 = d \\
[\![(x_1,\ldots,x_m)]\!]_2\ \rho_2 = ([\![x_1]\!]_2\ \rho_2,\ldots,[\![x_m]\!]_2\ \rho_2) \\
[\![C\ x_1 \ldots x_m]\!]_2\ \rho_2 = \bigsqcup_i \phi_{t_i}([\![x_i]\!]_2\ \rho_2) \text{ where } x_i :: t_i \\
\\
[\![e\ x]\!]_2\ \rho_2 = ([\![e]\!]_2\ \rho_2)\ ([\![x]\!]_2\ \rho_2) \\
[\![\lambda v.e]\!]_2\ \rho_2 = \lambda z \in D_{2t_v}.[\![e]\!]_2\ \rho_2\ [v \mapsto z] \text{ where } v :: t_v \\
[\![merge_t]\!]_2\ \rho_2 = \lambda z_1 \in Basic.\lambda z_2 \in Basic.n \\
[\![\textbf{let } v = e \textbf{ in } e']\!]_2\ \rho_2 = [\![e']\!]_2\ \rho_2\ [v \mapsto [\![e]\!]_2\ \rho_2] \\
[\![\textbf{let rec } \overline{\{v_i = e_i\}} \textbf{ in } e']\!]_2\ \rho_2 = [\![e']\!]_2\ (fix\ (\lambda\rho_2'.\rho_2\ \overline{[v_i \mapsto [\![e_i]\!]_2\ \rho_2']})) \\
[\![\textbf{case } e \textbf{ of } (v_1,\ldots,v_m) \to e']\!]_2\ \rho_2 = [\![e']\!]_2\ \rho_2\ \overline{[v_i \mapsto \pi_i([\![e]\!]_2\ \rho_2)]} \\
[\![\textbf{case } e \textbf{ of } \overline{C_i\ \overline{v_{ij}} \to e_i}; [v \to e']]\!]_2\ \rho_2 = \begin{cases} \mu_t(n) \text{ if } [\![e]\!]_2\ \rho_2 = n \\ \bigsqcup_i [\![e_i]\!]_2\ \rho_{2i}\ [\ \sqcup [\![e']\!]_2\ \rho_2'\ ] \text{ otherwise} \end{cases} \\
\qquad \text{where } \rho_{2i} = \rho_2\ \overline{[v_{ij} \mapsto \mu_{t_{ij}}(d)]}, v_{ij} :: t_{ij}, e_i :: t \\
\qquad\qquad \rho_2' = \rho_2\ [v \mapsto d] \\
[\![\textbf{case } e \textbf{ of } \overline{k_i \to e_i};\ [v \to e']]\!]_2\ \rho_2 = \begin{cases} \mu_t(n) \text{ if } [\![e]\!]_2\ \rho_2 = n \\ \bigsqcup_i [\![e_i]\!]_2\ \rho_2\ [\ \sqcup [\![e']\!]_2\ \rho_2'\ ] \text{ otherwise} \end{cases} \\
\qquad \text{where } e_i :: t, \rho_2' = \rho_2\ [v \mapsto d]
\end{array}
$$

Fig. 5. Abstract interpretation $[\![\cdot]\!]_2$

bottom-avoiding nondeterminism (in which bottom is never chosen unless it is the only option), the second one models *demonic* non-determinism (it chooses bottom whenever it is a possible option) and the third one models *erratic* non-determinism (in which bottom is an option as the other ones).

Regarding structured domains we have chosen a functional expression to denote a single function from sets to sets. In this sense, the following two bindings

$$
\begin{array}{l}
f_1 = head(merge_{Int \to Int}[\lambda x.0][\lambda x.1]) \\
f_2 = \lambda x.head(merge_{Int}[0][1])
\end{array}
$$

will both denote the function $\lambda x.\{0, 1, \bot\}$. That is, the information whether the non-deterministic decision is taken at binding evaluation time or at function application time is lost. Non-deterministic decisions are deferred as much as possible; in this example to function application time. This is consistent with the plural semantics we have adopted for our language in Section 3.2: Several ocurrences of the same variable (let us say f_1) may represent different values.

Regarding the selection of powerdomain, we have decided to use Hoare's one. This is consistent with the implementation of `merge` in Eden: If one of the input lists is blocked (i.e., it denotes $\bot$), `merge` will still produce an output list by copying values from the non-blocked list. Only if both lists are blocked will the output list be blocked. Nevertheless, `merge` will terminate only when both input lists terminate. This behaviour is very near to angelic non determinism. If D is a domain, $\mathcal{P}(D)$ will denote the Hoare powerdomain of D. First, a preorder relation is defined in $P(D)$ (all subsets of D) as follows:

$$
A \sqsubseteq_{P(D)} B \quad \textit{iff} \quad \forall a \in A.\exists b \in B.a \sqsubseteq_D b \tag{1}
$$

$A_K = \mathcal{P}([\![K]\!])$ where $[\![Int]\!] = \mathbb{Z}_\perp$
$A_{(t_1,\ldots,t_m)} = A_{t_1} \times \ldots \times A_{t_m}$
$A_T = \mathcal{P}([\![T]\!])$
where $[\![T]\!] = \oplus_{i=1}^{m}(C_i \times \times_{j=1}^{n_i} A_{t_{ij}})_\perp$, **data** $T = C_1\ t_{11} \ldots t_{1n_1} \mid \ldots \mid C_m\ t_{m1} \ldots t_{mn_m}$
$A_{t_1 \to t_2} = [A_{t_1} \to A_{t_2}]$

Fig. 6. Domain of values

This preorder relation induces an equivalence relation $\equiv \stackrel{\text{def}}{=} \sqsubseteq \cap \sqsupseteq$ identifying sets such as $\{0, 1, \perp\}$ and $\{0, 1\}$. Hoare powerdomain is the quotient $\mathcal{P}(D) \stackrel{\text{def}}{=} (P(D) - \emptyset)/\equiv$. A property enjoyed by all elements of a Hoare powerdomain is that they are downwards closed, i.e. $\forall x \in A. y \sqsubseteq_D x \Rightarrow y \in A$.

In Figure 6, the domains of semantic values for every type are defined. Notice that, for basic and constructed types, the domains consist of sets of values while for tuples and functions, the domains consist of single values. In the definition for constructed types, $\oplus$ denotes the coalesced sum of (lifted) domains. Sets of values are needed for the constructed types because non-deterministic values of such types may contain several different constructors. However, those with only one constructor could be treated as tuples.

If the constructed type is recursive, notice that the recursive ocurrences denote sets of values. For instance, a non-deterministic list would consist of a set of lists. A non-empty list of this set would consist of a head value and a tail value formed by a set of lists.

3.2 A maximal semantics: non-definite variables

In Figure 7 a denotational semantics for Eden is given. There $\{v\}^*$ denotes the downwards closure of a value, i.e. a set of values containing all values below v. The environment ρ maps variables of type t to values of their corresponding non-deterministic domains A_t. The semantic function $[\![.]\!]$ maps an expression of type t and an environment ρ to a value in A_t. The only expression introducing sets of values is $merge_t$. Its behaviour is that of a lambda abstraction returning all the possible interleavings of all pairs of input lists. The detail of the auxiliar function *mergeS* is given in Figure 8.

These decisions configure a plural semantics for Eden as every ocurrence of the same variable within an expression is mapped to *all* possible values for that variable (see definitions for **let** and lambda in Figure 7). This is not the actual semantics of Eden, but just a safe upper approximation to it in the sense that the set of possible values produced by an expression is bigger than the actual one. As an example, the expression **let** $f = head(merge_{Int \to Int}[\lambda x.0]\ [\lambda x.1])$ **in** $(f\ 3) + (f\ 4)$ in fact may only produce the values 0 or 2 while the approximated semantics will say that it may also produce the value 1. It is *maximal* in the sense that all variables are considered non definite, while in the actual semantics only those variables duplicated in different processes may be non definite if they are non deterministic. Notice that with this approximated semantics unfoldability holds although in the actual semantics this is not true.

$[\![v]\!]\ \rho = \rho(v)$
$[\![k]\!]\ \rho = \{k\}^*$
$[\![(x_1,\ldots,x_m)]\!]\ \rho = ([\![x_1]\!]\ \rho,\ldots,[\![x_m]\!]\ \rho)$
$[\![C\ x_1 \ldots x_m]\!]\ \rho = \{C\ [\![x_1]\!]\ \rho \ldots [\![x_m]\!]\ \rho\}^*$
$[\![\lambda v.e]\!]_2\ \rho = \lambda s \in A_{t_v}.[\![e]\!]\ \rho\ [v \mapsto s]$ where $v :: t_v$
$[\![e\ x]\!]\ \rho = ([\![e]\!]\ \rho)\ ([\![x]\!]\ \rho)$
$[\![merge_t]\!]\ \rho = \lambda s_1 \in A_{[t]}.\lambda s_2 \in A_{[t]}.\bigcup\{mergeS\ l_1\ l_2 \mid l_1 \in s_1, l_2 \in s_2\}$
$[\![\textbf{let}\ v = e\ \textbf{in}\ e']\!]\ \rho = [\![e']\!]\ \rho\ [v \mapsto [\![e]\!]\ \rho]$
$[\![\textbf{let rec}\ \overline{\{v_i = e_i\}}\ \textbf{in}\ e']\!]\ \rho = [\![e']\!]\ (fix\ (\lambda\rho'.\rho\ \overline{[v_i \mapsto [\![e_i]\!]\ \rho']}))$
$[\![\textbf{case}\ e\ \textbf{of}\ (v_1,\ldots,v_m) \to e']\!]\ \rho = [\![e']\!]\ \rho\ \overline{[v_i \mapsto \pi_i([\![e]\!]\ \rho)]}$
$[\![\textbf{case}\ e\ \textbf{of}\ \overline{C_i\ \overline{v_{ij}} \to e_i}; [v \to e']]\!]\ \rho =$
$\begin{cases} \bot_{A_t} \text{ if } [\![e]\!]\ \rho = \bot_{A_T} \\ \bigsqcup_{A_t}\{[\![e_k]\!]\ \rho\overline{[v_{kj} \mapsto s_{kj}]}^{m_k} \mid C_k\ \overline{s_{kj}}^{m_k} \in [\![e]\!]\ \rho\} [\sqcup \bigsqcup_{A_t}\{[\![e']\!]\ \rho[v \to s \mid s \in [\![e]\!]\ \rho\}] \text{ otherwise} \end{cases}$
$[\![\textbf{case}\ e\ \textbf{of}\ \overline{k_i \to e_i};\ [v \to e']]\!]\ \rho = \begin{cases} \bot_{A_t} \text{ if } [\![e]\!]\ \rho = \bot_{A_T} \\ \bigsqcup_{k_i \in [\![e]\!]_\rho}\ [\![e_i]\!]\ \rho\ [\ \sqcup \bigsqcup_{A_t}\{[\![e']\!]\ \rho[v \mapsto s] \mid s \in [\![e]\!]\ \rho\}\ ] \text{ otherwise} \end{cases}$

Fig. 7. A denotational semantics for Eden

The reason for this maximal semantics is that, if we are able to show the correctness of the analysis with respect to it, then the analysis will be correct with respect to the actual semantics. We remind that the sure value is the deterministic one. If the analysis detects an expression as deterministic then it should be semantically deterministic .

An exception is the algebraic **case** expression where the variables in the right hand side of the alternatives are definite. The discriminant's value is a set that may contain different constructors, so we have to take the least upper bound of all the alternatives' values that match them. As the discriminant is inmediately evaluated, the non-deterministic decission is inmediately taken so that all the ocurrences of the same variable in the right hand side have the chosen value.

For example, let a type **data** $Fool = C\ Int \mid C'\ Int$ and the values $s_1 = \{\bot, C\{0,\bot\}, C'\{0,\bot\}\}$, $s_2 = \{\bot, C\{1,\bot\}, C\{0,\bot\}\}$ and $s_2' = \{\bot, C\{1,\bot\}, C\{0,\bot\}, C\{0,1,\bot\}\}$. Let an expression $e' =$ **case** e **of** $C\ v \to v + v; C'\ v' \to v' + 4$. If $[\![e]\!]\ \rho = s_1$, then $[\![e']\!]\ \rho = \{0, 4, \bot\}$. Notice that s_2 and s_2' are different: If $[\![e]\!]\ \rho = s_2$ then $[\![e']\!]\ \rho = \{0, 2, \bot\}$, but if $[\![e]\!]\ \rho = s_2'$, then $[\![e']\!]\ \rho = \{0, 1, 2, \bot\}$. This is because the variables in the right hand side of a **case** alternative are definite. We could have chosen another option when building the environments for the right hand sides: If there were several values with the same constructor then we could take the least upper bound of the components so that the variables would be non-definite:

$[\![\textbf{case}\ e\ \textbf{of}\ \overline{C_i\ \overline{v_{ij}} \to e_i}; [v \to e']]\!]\ \rho =$
$\begin{cases} \bot_{A_t} \text{ if } [\![e]\!]\ \rho = \bot_{A_T} \\ \bigsqcup_{A_t}\{[\![e_k]\!]\ \rho\overline{[v_{kj} \mapsto \bigsqcup s_{kj}]}^{m_k} \mid C_k\ \overline{s_{kj}}^{m_k} \in [\![e]\!]\ \rho\} [\sqcup \bigsqcup_{A_t}\{[\![e']\!]\ \rho[v \to s \mid s \in [\![e]\!]\ \rho\}] \text{ otherwise} \end{cases}$

With this alternative version then, both when $[\![e]\!]\ \rho = s_2$ and when $[\![e]\!]\ \rho = s_2'$, we would have $[\![e']\!]\ \rho = \{0, 1, 2, \bot\}$ because v is bound to $\{0,\bot\} \sqcup \{1,\bot\} = \{0, 1, \bot\}$. We have chosen the first option because it is nearer to the actual semantics. The rest of the rules are self-explanatory.

$$
\begin{array}{l}
\mathit{mergeS}\ \bot\ \bot = \{\bot\} \\
\mathit{mergeS}\ \bot\ l_2 = \{l_2 +\!\!+ \bot\}^* \\
\mathit{mergeS}\ l_1\ \bot = \{l_1 +\!\!+ \bot\}^* \\
\mathit{mergeS}\ [\,]\ [\,] = \{[\,]\}^* \\
\mathit{mergeS}\ [\,]\ l_2 = \{l_2\}^* \\
\mathit{mergeS}\ l_1\ [\,] = \{l_1\}^* \\
\mathit{mergeS}\ (s_1 : l_1)\ (s_2 : l_2) = \{s_1 : (\bigcup_{l' \in l_1} \mathit{mergeS}\ l'\ (s_2 : l_2)), s_2 : (\bigcup_{l' \in l_2} \mathit{mergeS}\ (s_1 : l_1)\ l_2)\}^* \\
\quad \text{where} \\
\quad \bot +\!\!+ \bot = \bot \\
\quad [\,] +\!\!+ \bot = \bot \\
\quad (xs : xss) +\!\!+ \bot = xs : \{xss' +\!\!+ \bot \mid xss' \in xss\}
\end{array}
$$

Fig. 8. Non-determinism semantics

$$
\begin{array}{l}
\mathit{det}_K(s) = \mathit{unit}(s) \\
\quad \text{where} \\
\quad \mathit{unit}(\{\bot\}) = \mathit{true} \\
\quad \mathit{unit}(\{z, \bot\}) = \mathit{true} \\
\quad \mathit{unit}\_ = \mathit{false} \\
\mathit{det}_{(t_1,\ldots,t_m)}((s_1, \ldots, s_m)) = \bigwedge_{i=1}^{m} \mathit{det}_{t_i}(s_i) \\
\mathit{det}_T(s) = \begin{cases} \bigwedge_{i=1}^{m} \mathit{det}_{t_i}(\sqcup\{s_i \mid C\ s_1 \ldots s_m \in s, s_i :: t_i\}) \text{ if } \mathit{one}(s) \\ \mathit{false} \quad \text{otherwise} \end{cases} \\
\quad \text{where}\ \ \mathit{one}(s) = (s = \{\bot\}) \vee (\exists C. \forall s' \in s. s' \neq \bot \Rightarrow s' = C\ s_1 \ldots s_m) \\
\mathit{det}_{t_1 \to t_2}(f) = \forall s \in A_{t_1}. \mathit{det}_{t_1}(s) \Rightarrow \mathit{det}_{t_2}(f(s))
\end{array}
$$

Fig. 9. Semantic definition of determinism

4 Capturing the Determinism Meaning

4.1 Deterministic values

In this section we are proving that the second analysis is correct with respect to the denotational semantics presented in the previous section (see Theorem 2). In order to establish the correctness predicate we need first to define the semantic property we want to capture, that is the determinism of an expression. In Figure 9 the boolean functions det_t are defined. Given $s \in A_t$, $\mathit{det}_t(s)$ tells us whether s is a deterministic value or not. A value of type K is deterministic if it is a set with at most one element different from $\bot$ (as $\bot$ belongs to each $s \in A_K$), which is established by the function *unit*. A tuple is deterministic if each component is deterministic. A constructed value $s \in A_T$ is deterministic if its elements different from $\bot$ (again $\bot$ belongs to each $s \in A_T$) have the same constructor, which is established by the function *one*, and additionally the least upper bound of the values in each component is deterministic. For example, values s_1, s_2 and s_2' defined in Section 3.2 are non-deterministic: The first one because it has two different constructors, and the other two because the least upper bound of the first component, $\{0, 1, \bot\}$, is not deterministic.

Finally, a function is deterministic if given a deterministic argument it produces a deterministic result.

Functions det_t have some properties that will be useful in order to prove that the analysis is correct. The first property is quite intuitive: All the values below a deterministic value are also deterministic, just by how the order is defined in the domains.

Proposition 1 *For each type t, and $s, r \in A_t$: $det_t(s) \wedge r \sqsubseteq s \Rightarrow det_t(r)$.*

This proposition can be proved by structural induction on t and on the number of constructors of the values in s (for more details, see Appendix A). The second property is necessary to prove continuity of the abstraction function defined in the following section.

Proposition 2 *For each type t, and $\{s_i\}_{i \in I}$ such that $s_i \in A_t$ and $\forall i \in I. s_i \sqsubseteq s_{i+1}$:*

$$det_t(\bigsqcup_{i \in I} s_i) \Leftrightarrow \bigwedge_{i \in I} det_t(s_i)$$

This proposition can be easily proved by structural induction on t and on the number of constructors of the values in $\bigsqcup_{i \in I} s_i$.

4.2 Abstraction and concretisation functions

In this section we define the abstraction Λ_t and concretisation Γ_t functions that relate the abstract and concrete domains, following the ideas in [1]. We will prove that they are a Galois connection, a crucial property in the correctness proof.

The function Λ_t is just an extension of a function α_t to Hoare sets by applying it to each element of the set and taking the least upper bound. So we will call abstraction function also to α_t. In Figure 10 the abstraction function is defined. With this function we want to abstract the determinism behaviour of the concrete values. It loses information, i.e. several concrete values may have the same abstract value. In Figure 11 the concretisation function is defined. For each abstract value, it returns all the concrete values that can be approximated by that abstract value. They are mutually recursive. We will prove that Λ_t and Γ_t are a Galois connection, which implies that for each concrete value there may be several abstract approximations but there exists only one best (least) approximation.

A value of type K or T is abstracted to d only if it is deterministic. The abstraction of a tuple is the tuple of the abstractions. The abstraction of a function f of type $t_1 \to t_2$ is a little more involved. It is an abstract function taking an argument $z \in D_{2t_1}$. Such z represents several concrete values $s_1 \in \Gamma_t(z)$ whose abstract images are $\alpha_{t_2}(f(s_1))$. So the abstraction of the result is the least upper bound of these abstract images.

The concretisation function is defined in such a way that it builds a Galois connection with Λ_t. The concretisation Γ_t of the basic abstract value d is the set of deterministic concrete values (when $t = K$ or $t = T$), and the concretisation of n is the whole corresponding Hoare powerdomain ($\mathcal{P}(A_K)$ or $\mathcal{P}(A_T)$). The concretisation of a tuple is the set of tuples whose components are abstracted to the abstract components. The concretisation of an abstract function $f^{\#}$ is

$$\alpha_t : A_t \to D_{2t}$$
$$\alpha_K(s) = \begin{cases} d & \text{if } det_K(s) \\ n & \text{otherwise} \end{cases}$$
$$\alpha_{(t_1,\ldots,t_m)}((s_1,\ldots,s_m)) = (\alpha_{t_1}(s_1),\ldots,\alpha_{t_m}(s_m))$$
$$\alpha_T(s) = \begin{cases} d & \text{if } det_T(s) \\ n & \text{otherwise} \end{cases}$$
$$\alpha_{t_1\to t_2}(f) = \lambda z \in D_{2t_1}.\bigsqcup_{s_1\in\Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1))$$

$$\Lambda_t : \mathcal{P}(A_t) \to D_{2t}$$
$$\Lambda_t(S) = \bigsqcup_{s\in S} \alpha_t(s)$$

Fig. 10. Abstraction function

$$\Gamma_t : D_{2t} \to \mathcal{P}(A_t)$$
$$\Gamma_K(b) = \begin{cases} \{s \in A_K \mid unit(s)\} & \text{if } b = d \\ \mathcal{P}(A_K) & \text{if } b = n \end{cases}$$
$$\Gamma_{(t_1,\ldots,t_m)}((z_1,\ldots,z_m)) = \{(s_1,\ldots,s_m) \mid \alpha_{t_i}(s_i) \sqsubseteq z_i \forall i \in \{1..m\}\}$$
$$\Gamma_T(b) = \begin{cases} \{s \in A_T \mid det_T(s)\} & \text{if } b = d \\ \mathcal{P}(A_T) & \text{if } b = n \end{cases}$$
$$\Gamma_{t_1\to t_2}(f^\#) = \{f \in A_{t_1\to t_2} \mid \forall s \in A_{t_1}.\alpha_{t_2}(f(v)) \sqsubseteq f^\#(\alpha_{t_1}(s))\}$$

Fig. 11. Concretisation function

again more involved. It is a set of concrete functions such that the abstraction of its behaviour on a concrete argument s is safely approximated (it is less or equal than) by the behaviour of the abstract function on the abstraction of the argument.

In the following proposition we prove that Γ_t is well defined, i.e. it produces downwards closed sets of concrete values. So it is not necessary to close any set.

Proposition 3 *For each type t, Γ_t is well defined.*

This proposition can be easily proved by definition (see Appendix A).

We now prove some properties that will be useful below. First we prove that the abstraction and concretisation functions are continuous.

Proposition 4 *For each type t, functions α_t, Λ_t and γ_t are continuous.*

For Γ_t it is enough to prove (by structural induction on t) that it is monotone because its domain is finite. For Λ_t we just need the conmutativity and associativity properties of $\sqcup$ in the Hoare powerdomain. In the case of α_t we can use structural induction on t.

The important result in this section is Theorem 1, shown below, but this is equivalent to the following proposition that will be used in the correctness proof quite often.

Proposition 5 *For each type t, $z \in D_{2t}$, and $s \in A_t$: $s \in \Gamma_t(z) \Leftrightarrow \alpha_t(s) \sqsubseteq z$.*

This proposition can be proved by structural induction on t (see Appendix A).

Theorem 1. *For each type t, Λ_t and Γ_t are a Galois connection, i.e.*

$$\Lambda_t \cdot \Gamma_t \sqsubseteq id_{D_{2t}}$$
$$\Gamma_t \cdot \Lambda_t \sqsupseteq id_{\mathcal{P}_{(A_t)}}$$

Finally we present an interesting property that only holds when the concrete domains of basic and algebraic types have at least two elements different from $\perp$. In the following proposition we show that α_t is surjective, i.e. each abstract value is the abstraction of a concrete value, which in particular belongs to the concretisation of that abstract value. This means that Λ_t and Γ_t are a Galois insertion ($\Lambda_t \cdot \Gamma_t = id_{D_{2t}}$).

Proposition 6 *If all $[\![K]\!]$ and $[\![T]\!]$ have at least two elements different from $\perp$, then for each type t and $z \in D_{2t}$, there exists $s \in \Gamma_t(z)$ such that $\alpha_t(s) = z$.*

This can also be proved by structural induction on t (see Appendix A). If the theorem hypothesis about $[\![K]\!]$ and $[\![T]\!]$ does not hold then it is easy to see that all the concrete values are abstracted to d and none to n. In fact we are avoiding the *Unit* type. However this property is not necessary in the correctness proof.

4.3 A proof of correctness

In this subsection we prove that the second analysis is correct with respect to the denotational semantics: When the analysis tells that an expression is deterministic, then the concrete value produced by the denotational semantics is deterministic (otherwise we do not know anything about it). We have to formally describe this intuition. On the one hand, we said in Section 2 that $\mu_t(d)$ is the best safe approximation to d in a given domain, so the analysis tells us that an expression is deterministic when its abstract value is less or equal than $\mu_t(d)$. On the other hand the determinism of a concrete value is established by det_t. So, the main result of the paper is expressed as follows.

Theorem 2. *Let ρ and ρ_2 be two environments, such that for each variable $x :: t_x$, $\alpha_{t_x}(\rho(x)) \sqsubseteq \rho_2(x)$. Then for each expression $e :: t$:*

$$[\![e]\!]_2\ \rho_2 \sqsubseteq \mu_t(d) \Rightarrow det_t([\![e]\!]\ \rho)$$

This is proved in two parts written as Propositions 7 and 8, shown below. The first one tells us that all the values whose abstraction is below $\mu_t(d)$ are semantically deterministic. The second one asserts that the analysis is an upper approximation to the abstraction of the concrete semantics. The theorem is then inmediately obtained.

Proposition 7 *For each type t, and $s \in A_t$: $\alpha_t(s) \sqsubseteq \mu_t(d) \Leftrightarrow det_t(s)$.*

This proposition can be proved by structural induction on t (see Appendix A). We need Proposition 5 and also some properties already proved in [4, 5].

Proposition 8 *Let ρ and ρ_2 be two environments, such that for each variable $x :: t_x$, $\alpha_{t_x}(\rho(x)) \sqsubseteq \rho_2(x)$. Then for each expression $e :: t$: $\alpha_t([\![e]\!])\ \rho \sqsubseteq [\![e]\!]_2\ \rho_2$.*

This proposition can be proved by structural induction on e (see Appendix A). We need Propositions 5 and 7, and some properties proved in [4, 5]. Additionally we need Lemmas 9 and 10, shown below. The first one tells us that α_t reflects the bottom element, and the second one says that the denotational semantics we have defined is monotone with respect to the environments. Both can be proved by structural induction, on t the first one and on e the second one.

Lemma 9 *For each type t, $\alpha_t(\bot_{A_t}) = \bot_{D_{2t}}$.*

Lemma 10 *Let $s, s' \in A_t$ such that $s \sqsubseteq s'$. Then, for each expression e, variable v of type t, and environment ρ, $[\![e]\!]\ \rho[v \to s] \sqsubseteq [\![e]\!]\ \rho'[v \to s']$.*

5 Conclusions and Future Work

We have proved the correctness of a whole hierarchy of non-determinism analyses for the parallel-functional language Eden. In order to do this, we have defined first a denotational semantics for Eden where non-determinism is represented.

We have chosen to use a plural semantics in which non-deterministic choices for variables are deferred as much as possible. A semantics nearer to the actual one (within a single process) would have been a singular one in which environments map variables to single values. This would reflect the fact that non-deterministic choices are done at binding evaluation time instead of at each variable ocurrence. For instance, a let-bound variable will get its value the first time it is evaluated and this value will be shared thereafter by all its ocurrences. In order to consider all the possible values the variable can have, we build one environment for each of them:

$$[\![\mathbf{let}\ v = e\ \mathbf{in}\ e']\!]\ \rho = \bigsqcup_{z \in [\![e]\!]\ \rho} [\![e']\!]\ \rho[v \mapsto z]$$

The same would be true for case-bound and lambda-bound variables. We have tried to define this singular semantics and things go wrong when trying to give semantics to mutually recursive definitions. The traditional fixpoint computation by using Kleene's ascending chain gives a semantics more plural than expected. For instance, in the definition

$$\begin{array}{ll} \mathbf{letrec} & f = \mathit{head}(\mathit{merge}\ [g]\ [\lambda x.0]) \\ & g = \mathit{head}(\mathit{merge}\ [f]\ [\lambda x.1]) \\ \mathbf{in} & (f, g) \end{array}$$

Kleene's ascending chain will compute the following set of possible environments:

$$\begin{array}{rl} \overline{\rho} = \{ & \{f \mapsto \lambda x.\{\bot\},\ g \mapsto \lambda x.\{\bot\}\}, \\ & \{f \mapsto \lambda x.\{0\}^*,\ g \mapsto \lambda x.\{1\}^*\}, \\ & \{f \mapsto \lambda x.\{0\}^*,\ g \mapsto \lambda x.\{0\}^*\}, \\ & \{f \mapsto \lambda x.\{1\}^*,\ g \mapsto \lambda x.\{1\}^*\}, \\ & \{f \mapsto \lambda x.\{1\}^*,\ g \mapsto \lambda x.\{0\}^*\}\ \} \end{array}$$

However, the lazy evaluation of the expression will never produce the fifth possibility. In [11] a singular semantics for a small non-deterministic recursive functional language was defined. The problem with fixpoints did not arise there because the language was extremely simple: only one recursive binding was allowed in the program and this had to be to a lambda abstraction. Additionally, the language was only first-order. The problem arises when there are at least two mutually recursive bindings to non normal-form expressions. In order to define a real singular semantics, we think that an operational approach should be taken. In this way, the actual lazy evaluation with its updating of closures and sharing of expressions could be appropriately modeled. We forsee to do it as future work.

Another extension of the present work is to include polymorphism in the language, in the semantics and in the proof of correctness. The analyses originally presented in [6, 7] already included this aspect.

References

1. G. L. Burn, C. L. Hankin, and S. Abramsky. The Theory of Strictness Analysis for Higher Order Functions. In *Programs as Data Objects*, volume 217 of *LNCS*, pages 42–62. Springer-Verlag, October 1986.
2. P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Conference Record of the 6th Annual ACM Symposium on Principles on Programming Languages*, pages 269–282. ACM, 1979.
3. R. J. M. Hughes and J. O'Donnell. Expressing and Reasoning About Non-Deterministic Functional Programs. In *Functional Programming: Proceedings of the 1989 Glasgow Workshop*, pages 308–328. Springer-Verlag, 1990.
4. R. Peña and C. Segura. A Comparison between three Non-determinism Analyses in a Parallel-Functional Language. In *Primeras Jornadas sobre Programación y Lenguajes, PROLE'01*, pages 263–277, 2001.
5. R. Peña and C. Segura. Three Non-determinism Analyses in a Parallel-Functional Language. Technical Report 117-01, Dep. Sistemas Informáticos y Programación, Universidad Complutense de Madrid, Spain, 2001. (http://dalila.sip.ucm.es/miembros/clara/publications.html).
6. R. Peña and C. Segura. Non-Determinism Analysis in a Parallel-Functional Language. In *Selected Papers of the 12th International Workshop on Implementation of Functional Languages, IFL'00*, volume 2011 of *LNCS*, pages 1–18. Springer-Verlag, 2001.
7. R. Peña and C. Segura. A Polynomial Cost Non-Determinism Analysis. In *Selected papers of the 13th International Workshop on Implementation of Functional Languages, IFL'01*, volume 2312 of *LNCS*, pages 121–137. Springer-Verlag, 2002.
8. S. L. Peyton Jones, C. V. Hall, K. Hammond, W. D. Partain, and P. L. Wadler. The Glasgow Haskell Compiler: A Technical Overview. In *Joint Framework for Inf. Technology, Keele, DTI/SERC*, pages 249–257, 1993.
9. S. L. Peyton Jones and A. L. M. Santos. A Transformation-based Optimiser for Haskell. *Science of Computer Programming 32(1-3):3-47*, September 1998.
10. H. Søndergaard and P. Sestoft. Referential Transparency, Definiteness and Unfoldability. *Acta Informatica*, 27(6):505–517, May 1990.
11. H. Søndergaard and P. Sestoft. Non-Determinism in Functional Languages. *Computer Journal*, 35(5):514–523, October 1992.

A Proofs of the propositions

Proof 1 *(Proposition 1) This proposition can be proved by structural induction on t and the number of constructors of the values in s.*

- $t = K$.
$$\begin{aligned} det_t(s) &\Rightarrow unit(s) \ \{\text{by definition of } det_t\} \\ &\Rightarrow unit(r) \ \{\text{as } r \sqsubseteq s\} \\ &\Rightarrow det_t(r) \ \{\text{by definition of } det_t\} \end{aligned}$$
- $t = (t_1, \ldots, t_m)$. *This case is trivial by definition of det_t and by induction hypothesis on each component type t_i.*
- $t = T$. *If $det_t(s)$ then $one(s)$ and, by definition, $det_{t_i}(\sqcup\{s_i \mid C\ s_1 \ldots s_m \in s, s_i :: t_i\})$ for each $i \in \{1..m\}$. As $r \sqsubseteq s$, trivially $one(s) \Rightarrow one(r)$.*
  For the same reason $\sqcup\{s_i \mid C\ s_1 \ldots s_m \in r, s_i :: t_i\} \sqsubseteq \sqcup\{s_i \mid C\ s_1 \ldots s_m \in s, s_i :: t_i\}$, where the values in $\sqcup\{s_i \mid C\ s_1 \ldots s_m \in s, s_i :: t_i\}$ have one constructor less than those in s. So, by induction hypothesis on each t_i we have that $det_{t_i}(\sqcup\{s_i \mid C\ s_1 \ldots s_m \in r, s_i :: t_i\})$ for each $i \in \{1..m\}$.
- $t = t_1 \to t_2$. *If $det_t(f)$ then by definition of det_t we have that*
$$\forall s \in A_{t_1}.det_{t_1}(s) \Rightarrow det_{t_2}(f(s)) \quad (1)$$
  Let $f' \sqsubseteq f$. We have to prove that
$$\forall s \in A_{t_1}.det_{t_1}(s) \Rightarrow det_{t_2}(f'(s))$$
  Let $s \in A_{t_1}$ such that $det_{t_1}(s)$. Then $det_{t_2}(f(s))$ by (1). As $f' \sqsubseteq f$, by induction hypothesis on t_2 we have trivially that $det_{t_2}(f'(s))$.

□

Proof 2 *(Proposition 3) We have to prove that for each t, and $z \in D_{2t}$, $\Gamma_t(s) \in \mathcal{P}(A_t)$, i.e. $\Gamma_t(s)$ is downwards closed. We prove this by distinguising one case for each type t. No induction is necessary.*

- $t = K$. *This case is trivial by definition of unit and Γ_K.*
- $t = (t_1, \ldots, t_m)$. *Let $(s_1, \ldots, s_m) \in \Gamma_t(z_1, \ldots, z_m)$ and let $(s'_1, \ldots, s'_m) \sqsubseteq (s_1, \ldots, s_m)$.*
  This means that
$$\begin{aligned} \alpha_{t_i}(s'_i) &\sqsubseteq \alpha_{t_i}(s_i) \ \{\text{by monotonicity of } \alpha_t\} \\ &\sqsubseteq z_i \qquad \{\text{by def. of } \Gamma_t\} \end{aligned}$$
  which implies that $(s'_1, \ldots, s'_m) \in \Gamma_t(z_1, \ldots, z_m)$ by definition of Γ_t.
- $t = T$. *We distinguish two cases. Let $s \in \Gamma_T(n)$. If $r \sqsubseteq s$, then trivially $r \in Gamma_T(n) = \mathcal{P}(A_T)$.*
  Let $s \in \Gamma_T(d)$, then $det_T(s)$. As $r \sqsubseteq s$, by Proposition 1, $det_T(r)$ as well, which implies that $r \in \Gamma_T(d)$.

– $t = t_1 \to t_2$. *Let* $f \in \Gamma_t(f^\#)$. *This implies that*

$$\forall s \in A_{t_1}.\alpha_{t_2}(f(s)) \sqsubseteq f^\#(\alpha_{t_1}(s)) \quad (1)$$

Let $f' \sqsubseteq f$. *We have that, given* $s \in A_{t_1}$

$$\begin{array}{rl} \alpha_{t_2}(f'(s)) \sqsubseteq \alpha_{t_2}(f(s)) & \{\text{by monotonicity of } \alpha_t\} \\ \sqsubseteq f^\#(\alpha_{t_1}(s)) & \{\text{by (1)}\} \end{array}$$

So, $f' \in \Gamma_t(f^\#)$.

□

Proof 3 *(Proposition 5) This proposition can be proved by structural induction on* t.

– $t = K$.
  - (⇒). *If* $z = n$, *then trivially* $\alpha_t(s) \sqsubseteq n$, *as* n *is the top of Basic.*
    If $z = d$, *then if* $s \in \Gamma_K(d)$, *by definition of* Γ_t, *we have that* $unit(s)$ *which implies that* $\alpha_K(s) = d$ *by definition of* α_t.
  - (⇐). *If* $z = d$, $\alpha_K(s) \sqsubseteq d$ *implies* $unit(s)$, *so* $s \in \Gamma_K(d)$ *by definition of* Γ_t.
    If $z = n$, *then trivially* $s \in \Gamma_K(n) = \mathcal{P}(A_K)$.

– $t = (t_1, \ldots, t_m)$.

$$\begin{array}{rl} (s_1, \ldots, s_m) \in \Gamma_t(z_1, \ldots, z_m) \Leftrightarrow \forall i \in \{1..m\}.\alpha_{t_i}(s_i) \sqsubseteq z_i & \{\text{by definition of } \Gamma_t\} \\ \Leftrightarrow \alpha_t(s_1, \ldots, s_n) \sqsubseteq (z_1, \ldots, z_m) & \{\text{by definition of } \alpha_t\} \end{array}$$

– $t = T$.
  - (⇒). *If* $z = n$, *then trivially* $\alpha_t(s) \sqsubseteq n$, *as* n *is the top of Basic.*
    If $z = d$, *then if* $s \in \Gamma_T(d)$, *by definition of* Γ_t, *we have that* $det_T(s)$ *which implies that* $\alpha_T(s) = d$ *by definition of* α_t.
  - (⇐). *If* $z = d$, $\alpha_T(s) \sqsubseteq d$ *implies* $det_T(s)$, *so* $s \in \Gamma_T(d)$ *by definition of* Γ_t.
    If $z = n$, *then trivially* $s \in \Gamma_T(n) = \mathcal{P}(A_T)$.

– $t = t_1 \to t_2$.
  - (⇒). *Let* $f \in \Gamma_t(f^\#)$. *Then,*

$$\forall s \in A_{t_1}.\alpha_{t_2}(f(s)) \sqsubseteq f^\#(\alpha_{t_1}(s)) \quad (1)$$

Let $z \in D_{2t}$. *We have to prove that* $\alpha_t(f)(z) \sqsubseteq f^\#(z)$. *By definition,* $\alpha_t(f)(z) = \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(s_1)$.
If $s_1 \in \Gamma_{t_1}(z)$, *then by* (1) $\alpha_{t_2}(f(s_1)) \sqsubseteq f^\#(\alpha_{t_1}(s_1))$. *So*

$$\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(s_1) \sqsubseteq \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} f^\#(\alpha_{t_1}(s_1)) \quad (2)$$

But, by induction hypothesis on t_1, *if* $s_1 \in \Gamma_{t_1}(z)$ *then* $\alpha_{t_1}(s_1) \sqsubseteq z$, *so by (2) and monotonicity of* $f^\#$ *we have that* $\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(s_1) \sqsubseteq f^\#(z)$.

- ($\Leftarrow$). *If* $\alpha_t(f) \sqsubseteq f^\#$, *then by definition of* α_t,

$$\forall z \in D_{2t_1} \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(s_1) \sqsubseteq f^\#(z) \quad (1)$$

Let $s \in A_{t_1}$. *We have to prove that* $\alpha_{t_2}(f(s)) \sqsubseteq f^\#(\alpha_{t_1}(s))$.
As $\alpha_{t_1}(s) \in D_{2t_1}$, *by (1) we have that* $\bigsqcup_{s_1 \in \Gamma_{t_1}(\alpha_{t_1}(s))} \alpha_{t_2}(s_1) \sqsubseteq f^\#(\alpha_{t_1}(s))$.
By induction hypothesis, trivially $s \in \Gamma_{t_1}(\alpha_{t_1}(s))$, *so*

$$\alpha_{t_2}(f(s)) \sqsubseteq \bigsqcup_{s_1 \in \Gamma_{t_1}(\alpha_{t_1}(s))} \alpha_{t_2}(s_1) \sqsubseteq f^\#(\alpha_{t_1}(s))$$

□

Proof 4 *(Proposition 6) We can prove this proposition by structural induction on* t.

- $t = K$. *If* $z = d$, *then* $s = \{\bot\} \in \Gamma_K(d)$ *holds that* $\alpha_K(s) = d$. *If* $z = n$, *then* $s = [\![K]\!] \in \Gamma_K(n)$ *holds that* $\alpha_K(s) = n$ *whenever* $[\![K]\!]$ *has at least two elements different from* $\bot$.
- $t = (t_1, \ldots, t_m)$. *Let* $z = (z_1, \ldots, z_m)$. *By induction hypothesis on each* t_i, *then for each* $i \in \{1..m\}$ *there exists* $s_i \in \Gamma_{t_i}(z_i)$ *such that* $\alpha_{t_i}(s_i) = z_i$. *So,* $s = (s_1, \ldots, s_m)$ *holds that* $\alpha_t(s) = z$ *by definition of* α_t.
- $t = T$. *If* $z = n$, *then* $s = [\![T]\!] \in \Gamma_t(n)$ *holds that* $\alpha_t(s) = n$ *whenever* $[\![T]\!]$ *has at least two elements different from* $\bot$.
  If $z = d$ *then* $s = \{\bot\} \in \Gamma_t(d)$ *holds that* $\alpha_t(s) = d$ *trivially.*
- $t = t_1 \to t_2$. *Let* $f^\# \in D_{2t}$; *we are looking for* $f \in \Gamma_t(f^\#)$ *such that* $\alpha_t(f) = f^\#$.
  For each $r \in A_{t_1}$, $\alpha_{t_1}(r) \in D_{2t_1}$ *and* $f^\#(\alpha_{t_1}(r)) \in D_{2t_2}$. *By induction hypothesis on* t_2, *there exists* $s_r \in \Gamma_{t_2}(f^\#(\alpha_{t_1}(r)))$ *such that* $\alpha_{t_2}(s_r) = f^\#(\alpha_{t_1}(r))$.
  Let us take $f = \lambda r \in D_{2t_1}.s_r$, *where* $s_r \in \Gamma_{t_2}(f^\#(\alpha_{t_1}(r)))$ *and* $\alpha_{t_2}(s_r) = f^\#(\alpha_{t_1}(r)))$ *(we have just proved there exists one that holds that).*
  We have that

$$\alpha_t(f) = \lambda z \in D_{2t_1}. \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) = \lambda z \in D_{2t_1}. \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(s_{1r})$$

  where $s_{1r} \in \Gamma_{t_2}(f^\#(\alpha_{t_1}(s_1)))$ *and* $\alpha_{t_2}(s_{1r}) = f^\#(\alpha_{t_1}(s_1))$. *We want to prove that given* $z \in D_{2t_1}$, $\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(s_{1r}) = f^\#(z)$, *i.e. that* $\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} f^\#(\alpha_{t_1}(s_1)) = f^\#(z)$:
  - ($\sqsubseteq$). *Each* $s_1 \in \Gamma_{t_1}(z)$ *holds that* $\alpha_{t_1}(s_1) \sqsubseteq z$ *by Proposition 5, so* $f^\#(\alpha_{t_1}(s_1)) \sqsubseteq f^\#(z)$ *by monotonicity of* $f^\#$. *Consequently,*

$$\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} f^\#(\alpha_{t_1}(s_1)) \sqsubseteq f^\#(z)$$

- ($\sqsupseteq$). *As* $z \in D_{2t_1}$, *by induction hypoythesis on* t_1, *there exists* $s_z \in \Gamma_{t_1}(z)$ *such that* $\alpha_{t_1}(s_z) = z$. *So*

$$f^{\#}(z) = f^{\#}(\alpha_{t_1}(s_z)) \sqsubseteq \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} f^{\#}(\alpha_{t_1}(s_1))$$

□

Proof 5 *(Proposition 7) We can prove this proposition by structural induction on* t.

- $t = K$. *We have trivially that*

$$\alpha_K(s) \sqsubseteq \mu_K(d) = d \Leftrightarrow det_K(s)$$

- $t = (t_1, \ldots, t_m)$. *We have that*

$$\begin{array}{lll} \alpha_t((s_1,\ldots,s_m)) \sqsubseteq \mu_t(d) \Leftrightarrow \alpha_{t_i}(s_i) \sqsubseteq \mu_{t_i}(d) \ \ \forall i \in \{1..m\} & \{\text{by definition of } \alpha_t \text{ and } \mu_t\} \\ \Leftrightarrow det_{t_i}(s_i) \ \ \forall i \in \{1..m\} & \{\text{by induction hypothesis on } t_i\} \\ \Leftrightarrow det_t((s_1,\ldots,s_m)) & \{\text{by definition of } det_t\} \end{array}$$

- $t = T$. *This case is similar to the basic case* $t = K$.
- $t = t_1 \to t_2$.
  - ($\Rightarrow$).*If* $\alpha_t(f) \sqsubseteq \mu_t(d)$, *then*

$$\forall z \in D_{2t_1}. \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) \sqsubseteq \mu_{t_2}(\phi_{t_1}(z)) \quad (1)$$

We have to prove that $\forall s \in A_{t_1}.det_{t_1}(s) \Rightarrow det_{t_2}(f(s))$. *So, let* $s \in A_{t_1}$ *such that* $det_{t_1}(s)$. *By induction hypothesis on* t_1 *then*

$$\alpha_{t_1}(s) \sqsubseteq \mu_{t_1}(d) \quad (2)$$

In order to prove $det_{t_2}(f(s))$, *it is enough to prove that* $\alpha_{t_2}(f(s)) \sqsubseteq \mu_{t_2}(d)$ *by induction hypothesis on* t_2. *Let us try this:*

$$\begin{array}{ll} \alpha_{t_2}(f(s)) \sqsubseteq \bigsqcup_{s_1 \in \Gamma_{t_1}(\alpha_{t_1}(s))} \alpha_{t_2}(f(s_1)) & \{\text{as } s \in \Gamma_{t_1}(\alpha_{t_1}(s))\} \\ \sqsubseteq \mu_{t_2}(\phi_{t_1}(\alpha_{t_1}(s))) & \{\text{by (1) when } z = \alpha_{t_1}(s)\} \\ \sqsubseteq \mu_{t_2}(\phi_{t_1}(\mu_{t_1}(d))) & \{\text{by (2) and monotonicity}\} \\ = \mu_{t_2}(d) & \{\text{as } \phi_t \cdot \mu_t = id_{Basic}\} \end{array}$$

  - ($\Leftarrow$). *If* $det_t(f)$ *then*

$$\forall s \in A_{t_1}.det_{t_1}(s) \Rightarrow det_{t_2}(f(s)) \quad (1)$$

We have to prove that

$$\forall z \in D_{2t_1}. \bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) \sqsubseteq \mu_{t_2}(\phi_{t_1}(z))$$

Let $z \in D_{2t_1}$. *We distinguish two cases.*

* $z \sqsubseteq \mu_{t_1}(d)$. *In this case* $\phi_{t_1}(z) = d$ (2) *because* $\phi_t \cdot \mu_t = id_{Basic}$ *(Proposition 1(b) in [4]).*
We have that

$$\begin{array}{lll} s_1 \in \Gamma_{t_1}(z) \Rightarrow \alpha_{t_1}(s_1) \sqsubseteq z & & \{\text{by Proposition 5}\} \\ \Rightarrow \alpha_{t_1}(s_1) \sqsubseteq \mu_{t_1}(d) & & \{\text{as } z \sqsubseteq \mu_{t_1}(d)\} \\ \Rightarrow det_{t_2}(f(s_1)) & & \{\text{by (1)}\} \\ \Rightarrow \alpha_{t_2}(f(s_1)) \sqsubseteq \mu_{t_2}(d) & & \{\text{by i.h. on } t_2\} \\ \Rightarrow \alpha_{t_2}(f(s_1)) \sqsubseteq \mu_{t_2}(\phi_{t_1}(d)) & & \{\text{by (2)}\} \end{array}$$

* $z \not\sqsubseteq \mu_{t_1}(d)$. *In this case* $\phi_{t_1}(z) = n$ (2′) *(by Proposition 2 in [4],* $\forall z \in D_{2t}.z \sqsubseteq \mu_t(d) \Leftrightarrow \phi_t(z) = d$*). We have to prove that* $\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(f(s_1)) \sqsubseteq \mu_{t_2}(n)$*, which holds trivially as* $\mu_t(n)$ *is the top element in* D_{2t} *(Proposition 1(d) in [4]).*

□

Proof 6 *(Proposition 8) This proposition can be proved by structural induction on* e*.*

– $e = k :: K$. *We have that*

$$\begin{array}{lll} \alpha_K([\![k]\!]\ \rho) = \alpha_K(\{k, \bot\}) & & \{\text{by def. of } [\![\cdot]\!]\} \\ = d & & \{\text{by def. of } \alpha_K\} \\ = [\![k]\!]_2\ \rho_2 & & \{\text{by def. of } [\![\cdot]\!]_2\} \end{array}$$

– $e = v :: t$. *In this case*

$$\begin{array}{lll} \alpha_t([\![v]\!]\ \rho) = \alpha_t(\rho(v)) & & \{\text{by def. of } [\![\cdot]\!]\} \\ \sqsubseteq \rho_2(v) & & \{\text{hypothesis of the theorem}\} \\ = [\![v]\!]_2\ \rho_2 & & \{\text{by def. of } [\![\cdot]\!]_2\} \end{array}$$

– $e = (x_1, \ldots, x_m) :: (t_1, \ldots, t_m)$.

$$\begin{array}{lll} \alpha_{(t_1,\ldots,t_m)}([\![(x_1, \ldots, x_m)]\!]\ \rho) = (\alpha_{t_1}([\![x_1]\!]\ \rho), \ldots, \alpha_{t_m}([\![x_m]\!]\ \rho)) & & \{\text{by def. of } \alpha_t \text{and } [\![\cdot]\!]\} \\ \sqsubseteq ([\![x_1]\!]_2\ \rho_2, \ldots, [\![x_m]\!]_2\ \rho_2) & & \{\text{by i.h. on each } t_i\} \\ = [\![(x_1, \ldots, x_m)]\!]_2\ \rho_2 & & \{\text{by def. of } [\![\cdot]\!]_2\} \end{array}$$

– $e = C\ x_1 \ldots x_m :: T$. *In this case*

$$\begin{array}{lll} \alpha_T([\![C\ x_1 \ldots x_m]\!]\ \rho) = \alpha_T(\{C\ ([\![x_1]\!]\ \rho) \ldots ([\![x_m]\!]\ \rho)\}^*) & & \{\text{by def. of } [\![\cdot]\!]\} \\ = \begin{cases} d & \text{if } det_T(\{C\ ([\![x_1]\!]\ \rho) \ldots ([\![x_m]\!]\ \rho)\}^*) \\ n & \text{otherwise} \end{cases} & & \end{array}$$

We want to prove that $\alpha_T([\![C\ x_1 \ldots x_m]\!]\ \rho) \sqsubseteq [\![C\ x_1 \ldots x_m]\!]_2\ \rho_2$*. We distinguish two cases.*
If $\alpha_T([\![C\ x_1 \ldots x_m]\!]\ \rho) = d$ *then it is trivial, as* d *is the bottom element in Basic.*
If $\alpha_T([\![C\ x_1 \ldots x_m]\!]\ \rho) = n$*, then* $\neg det_T(\{C\ ([\![x_1]\!]\ \rho) \ldots ([\![x_m]\!]\ \rho)\}^*)$*. In* $\{C\ ([\![x_1]\!]\ \rho) \ldots ([\![x_m]\!]\ \rho)\}^*$ *there is just one constructor, so the only possibility for it to be non-deterministic, is that there exists* $i \in \{1..m\}$ *such*

that $\neg det_{t_i}(\sqcup\{s_j \mid C\ s_1 \ldots s_m \in \{C\ (\llbracket x_1 \rrbracket\ \rho) \ldots (\llbracket x_m \rrbracket\ \rho)\}^*\})$*, i.e. such that* $\neg det_{t_i}(\llbracket x_i \rrbracket\ \rho)$*. But, by Proposition 5, this implies that* $\alpha_{t_i}(\llbracket x_i \rrbracket\ \rho) \not\sqsubseteq \mu_{t_i}(d)$*. This implies that* $\phi_{t_i}(\alpha_{t_i}(\llbracket x_i \rrbracket\ \rho)) = n$ (1) *(by Proposition 2 in [4]), so*

$$\begin{array}{lll} \llbracket C\ x_1 \ldots x_m \rrbracket_2\ \rho_2 = \bigsqcup_{j=1}^{m} \phi_{t_j}(\llbracket x_j \rrbracket_2\ \rho_2) & \{\text{by def. of } \llbracket\cdot\rrbracket_2\} \\ \sqsupseteq \bigsqcup_{j=1}^{m} \phi_{t_j}(\alpha_{t_j}(\llbracket x_j \rrbracket\ \rho)) & \{\text{by i.h. on each } t_j \text{and monotonicity}\} \\ = n & \{\text{by (1)}\} \end{array}$$

– $e = \lambda v.e' :: t_1 \to t_2$*. On the one side*

$$\begin{array}{ll} \alpha_{t_1 \to t_2}(\llbracket \lambda v.e' \rrbracket\ \rho) = \alpha_{t_1 \mapsto t_2}(\lambda s \in A_{t_1}.\llbracket e' \rrbracket\ \rho[v \mapsto s]) & \{\text{by def. of } \llbracket\cdot\rrbracket\} \\ = \lambda z \in D_{2t_1}.\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(\llbracket e' \rrbracket\ \rho[v \mapsto s_1]) & \{\text{by def. of } \alpha_t\} \end{array}$$

On the other side

$$\llbracket e \rrbracket_2\ \rho_2 = \lambda z \in D_{2t_1}.\llbracket e' \rrbracket_2\ \rho_2[v \mapsto z]$$

Let $z \in D_{2t_1}$*. We have to prove that*

$$\bigsqcup_{s_1 \in \Gamma_{t_1}(z)} \alpha_{t_2}(\llbracket e' \rrbracket\ \rho[v \mapsto s_1]) \sqsubseteq \llbracket e' \rrbracket_2\ \rho_2[v \mapsto z]$$

If $s_1 \in \Gamma_{t_1}(z)$ *then* $\alpha_{t_1}(s_1) \sqsubseteq z$ *by Proposition 5, so* $\rho[x \mapsto s_1]$ *and* $\rho_2[v \mapsto z]$ *hold the theorem hypothesis about the environments. We can then apply induction hypothesis on* e' *and obtain*

$$\alpha_{t_2}(\llbracket e' \rrbracket\ \rho[v \mapsto s_1]) \sqsubseteq \llbracket e' \rrbracket_2\ \rho_2[v \mapsto z]$$

and inmediately holds what we wanted.

– $e = merge_t :: [t] \to [t] \to [t]$*. This case is trivial as* $\llbracket merge_t \rrbracket_2\ \rho_2$ *is the top element in the corresponding abstract domain.*

– $e =$ **let** $v = e_1$ **in** $e_2 :: t$*, where* $e_1 :: t_1$ *and* $e_2 :: t$*. Applying induction hypothesis on* e_1 *we have that* $\alpha_{t_1}(\llbracket e_1 \rrbracket\ \rho) \sqsubseteq \llbracket e_1 \rrbracket_2\ \rho_2$*, so* $\rho[v \mapsto \llbracket e_1 \rrbracket\ \rho]$ *and* $\rho_2[v \mapsto \llbracket e_1 \rrbracket_2\ \rho_2]$ *hold the hypothesis theorem. Consequently:*

$$\begin{array}{ll} \alpha_t(\llbracket e \rrbracket\ \rho) = \alpha_t(\llbracket e_2 \rrbracket\ \rho[v \mapsto \llbracket e_1 \rrbracket\ \rho]) & \{\text{by def. of } \llbracket\cdot\rrbracket\} \\ \sqsubseteq \llbracket e_2 \rrbracket_2\ \rho_2[v \mapsto \llbracket e_1 \rrbracket_2\ \rho_2] & \{\text{by i.h. on } e_2\} \\ = \llbracket e \rrbracket_2\ \rho_2 & \end{array}$$

– $e =$ **letrec** $\overline{v_i = e_i}$ **in** $e' :: t$*, where* $e_i :: t_i$ *and* $e' :: t$*. By definition of* $\llbracket\cdot\rrbracket$ *and* $\llbracket\cdot\rrbracket_2$ *we have to prove that*

$$\alpha_t(\llbracket e' \rrbracket\ (fix\ (\lambda\rho'.\rho\ \overline{[v_i \mapsto \llbracket e_i \rrbracket\ \rho']}))) \sqsubseteq \llbracket e' \rrbracket_2\ (fix(\lambda\rho_2'.\rho_2\ \overline{[v_i \mapsto \llbracket e_i \rrbracket_2\ \rho_2']}))$$

We could apply induction hypothesis on e' *if the environmets*

$$A = fix\ (\lambda\rho'.\rho\ \overline{[v_i \mapsto \llbracket e_i \rrbracket\ \rho']})$$

and

$$B = fix(\lambda\rho_2'.\rho_2\ \overline{[v_i \mapsto \llbracket e_i \rrbracket_2\ \rho_2']})$$

holded the hypothesis theorem, i.e. for each variable $v :: t_v$, $\alpha_{t_v}(A(v)) \sqsubseteq B(v)$.
Both the concrete and abstract domains are pointed cpos, so

$$A = \bigsqcup_{n \in I\!N} (\lambda \rho'.\rho\ \overline{[v_i \mapsto [\![e_i]\!]\ \rho']})^n(\rho_0)$$

and

$$B = \bigsqcup_{n \in I\!N} (\lambda \rho_2'.\rho_2\ \overline{[v_i \mapsto [\![e_i]\!]_2\ \rho_2']})^n(\rho_{02})$$

where for each variable $v :: tv$, $\rho_0(v) = \bot_{A_{tv}}$ *and* $\rho_{02}(v) = \bot_{D_{2tv}}$. *Let us call* $G = \lambda \rho'.\rho\ \overline{[v_i \mapsto [\![e_i]\!]\ \rho']}$ *and* $F = \lambda \rho_2'.\rho_2\ \overline{[v_i \mapsto [\![e_i]\!]_2\ \rho_2']}$. *We are going to prove that*

$$\forall n \in I\!N. \forall v :: tv. \alpha_{tv}(G^n(\rho_0)(v)) \sqsubseteq F^n(\rho_{02})(v) \quad (1)$$

Then we will have that

$$\bigsqcup_{n \in I\!N} \alpha_{tv}(G^n(\rho_0)(v)) \sqsubseteq \bigsqcup_{n \in I\!N} F^n(\rho_{02})(v)$$

As α_t *is continuous and* $G^n(\rho_0)(v)$ *is an ascending chain then*

$$\alpha_{tv}(\bigsqcup_{n \in I\!N} G^n(\rho_0)(v)) \sqsubseteq \bigsqcup_{n \in I\!N} F^n(\rho_{02})(v)$$

and we would have finished.
We prove (1) by induction on n. *If* $n = 0$, *it is trivial by Lemma 9.*
If $n > 0$, *the induction hypothesis says that*

$$\forall v :: tv. \alpha_{tv}(G^n(\rho_0)(v)) \sqsubseteq F^n(\rho_{02})(v) \quad (2)$$

i.e. $G^n(\rho_0)$ *and* $F^n(\rho_{02})$ *hold the hypothesis theorem.*
We have to prove that

$$\forall v :: tv. \alpha_{tv}(G^{n+1}(\rho_0)(v)) \sqsubseteq F^{n+1}(\rho_{02})(v)$$

where $G^{n+1} = G \cdot G^n$ *and* $F^{n+1} = F \cdot F^n$.
Let $v :: tv$. *We distinguish two cases. If* $v \neq v_i\ \forall i$, *then*

$$\alpha_{tv}(G^{n+1}(\rho_0)(v)) = \alpha_{tv}(\rho(v)) \sqsubseteq \rho_2(v) = F^{n+1}(\rho_{02}(v))$$

If there is any v_i *such that* $v = v_i$, *then*

$$\begin{array}{lll} \alpha_{tv}(G^{n+1}(\rho_0)(v)) = \alpha_{tv}([\![e_i]\!]\ (G^n(\rho_0))) & & \{\text{by def. of } G\} \\ \sqsubseteq [\![e_i]\!]_2\ (F^n(\rho_{02})) & & \{\text{by (2) and i.h. on } e_i\} \\ = F^{n+1}(\rho_{02})(v) & & \{\text{by def. of } F\} \end{array}$$

– $e = \textbf{case}\ e_1\ \textbf{of}\ (v_1, \ldots, v_m) \to e_2 :: t$ *where* $e_1 :: (t_1, \ldots, t_m)$. *By induction hypothesis on* e_1 *and definition of* α_t, *the environments* $\rho\ \overline{[v_i \mapsto \pi_i([\![e_1]\!]\ \rho)]}$ *and* $\rho_2\ \overline{[v_i \mapsto \pi_i([\![e_1]\!]_2\ \rho_2]}$ *hold the theorem hypothesis, so we can apply induction hypothesis on* e' *and trivially obtain what we want.*

– $e = \textbf{case}\ e'\ \textbf{of}\ \overline{C_i\ \overline{v_{ij}} \to e_i}; [v \to e''] :: t$, *where* $e' :: T$ *and* $e_i, e'' :: t$.
By definition

$$[\![e]\!]\ \rho = \begin{cases} \bot_{A_t} \text{ if } [\![e']\!]\ \rho = \bot_{A_T} \\ \bigsqcup_{A_t}\{[\![e_k]\!]\ \overline{\rho[v_{kj} \mapsto s_{kj}]}^{m_k} \mid C_k\ \overline{s_{kj}}^{m_k} \in [\![e]\!]\ \rho\}[\sqcup\bigsqcup_{A_t}\{[\![e']\!]\ \rho[v \to s \mid s \in [\![e]\!]\ \rho\}] \text{ otherwise} \end{cases}$$

So we distinguish two cases. If $[\![e']\!]\ \rho = \bot_{A_T}$, *it is trivial as* $\alpha_t(\bot_{A_t}) = \bot_{D_{2t}}$ *by Lemma 9.*
Otherwise, by induction hypothesis on e' *we have that for each* $\alpha_T([\![e']\!]\ \rho) \sqsubseteq [\![e']\!]_2\ \rho_2$. *We distinguish again two cases. If* $[\![e']\!]_2\ \rho_2 = n$ *then it is trivial, as* $[\![e]\!]_2\ \rho_2 = \mu_t(n)$ *which is the top in* D_{2t}. *If* $[\![e']\!]_2\ \rho_2 = d$, *then* $\alpha_T([\![e']\!]\ \rho) = d$, *so* $det_T([\![e']\!]\ \rho)$ *by Proposition 7. This means that in* $[\![e']\!]\ \rho$ *there is at most a unique constructor* C_k *and that for each* $i \in \{1..m_k\}$

$$det_{t_{ki}}(\sqcup\{s_i \mid C_k\ s_1 \ldots s_{m_k} \in [\![e']\!]\ \rho)$$

which implies by Proposition 7 that

$$\alpha_{t_{ki}}(\sqcup\{s_i \mid C_k\ s_1 \ldots s_{m_k} \in [\![e']\!]\ \rho) \sqsubseteq \mu_{t_{ki}}(d) \quad (1)$$

This implies that

$$\begin{aligned}
&\alpha_t(\textstyle\bigsqcup_{A_t}\{[\![e_k]\!]\ \overline{\rho[v_{kj} \mapsto s_{kj}]}^{m_k} \mid C_k\ \overline{s_{kj}}^{m_k} \in [\![e']\!]\ \rho\}[\sqcup\bigsqcup_{A_t}\{[\![e'']\!]\ \rho[v \to s \mid s \in [\![e']\!]\ \rho\}] \\
&\sqsubseteq \alpha_t([\![e_k]\!]\ \overline{\rho[v_{kj} \mapsto \bigsqcup s_{kj}]}^{\,\mid C_k\ \overline{s_{kj}}^{m_k} \in [\![e']\!]\ \rho|^{m_k}})\ [\sqcup[\![e'']\!]\ \rho[v \mapsto \bigsqcup s \mid s \in [\![e']\!]\ \rho\}] \\
&\quad \{\text{by Lemma 10}\} \\
&\sqsubseteq [\![e_k]\!]_2\ \rho_2\overline{[v_{kj} \mapsto \mu_{kj}(d)]}^{m_k}\ \sqcup [[\![e'']\!]_2\ \rho_2[v \mapsto d]] \\
&\quad \{\text{by (1) and i.h. on } e_k \text{ and } e''\} \\
&\sqsubseteq \bigsqcup_i [\![e_i]\!]_2\ \rho_2\overline{[v_{ij} \mapsto \mu_{t_{ij}}(d)]}^{m_i}[\ \sqcup [\![e'']\!]_2\ \rho_2[v \mapsto d]]
\end{aligned}$$

– $e = \textbf{case}\ e'\ \textbf{of}\ \overline{k_i \to e_i};\ [v \to e'']$. *This case is very similar to the algebraic case so we do not repeat it here.*

□