Electronic Notes in Theoretical Computer Science 11 (1998)
URL: http://www.elsevier.nl/locate/entcs/volume11.html 18 pages

# Guarded induction on final coalgebras

Duško Pavlović [1]

*COGS, University of Sussex, Brighton, and*
*Kestrel Institute, Palo Alto*

**Abstract**

We make an initial step towards a categorical semantics of guarded induction. While ordinary induction is usually modelled in terms of the least fixpoints and the initial algebras, guarded induction is based on the *unique* fixpoints of certain operations, called guarded, on the *final* coalgebras. So far, such operations were treated syntactically [3,8,9,23]. We analyse them categorically. Guarded induction appears as couched in coinductively constructed domains, but turns out to be reducible to coinduction only in special cases.

The applications of the presented analysis span across the gamut of the applications of guarded induction — from modelling computation to solving differential equations. A subsequent paper [26] will provide an account of some domain theoretical aspects, which are presently left implicit.

> "In order to establish that a proposition $\phi$ follows from other propositions $\phi_1, \ldots, \phi_q$, it is enough to build a proof term $e$ for it, using not only natural deduction, case analysis and already proven lemmas, but also using the proposition we want to prove recursively, provided such a recursive call is guarded by introduction rules. We call this proof principle the 'guarded induction principle'."
>
> — Th. Coquand [8, sec. 2.3]

## 1 Introduction

Coinduction is usually presented and studied as dual to induction: if induction is interpreted in terms of the universal property of initial algebras, coinduction arises from the couniversal property of final coalgebras [12,15,16,24,28,29]. A bit like in the case of monads and comonads, the symmetry, with one side more familiar, opens an easier access to the other side. It provides a very rich

[1] A part of this paper was prepared while I enjoyed the hospitality of the Theory and Formal Methods Section at the Department of Computing, Imperial College, London.

source of parallel concepts and techniques [28] — but unfortunately goes only as far as it goes.

In fact, the most interesting conceptual distinctions often begin to surface only when the symmetry starts breaking down. Going back to monads and comonads, recall, e.g., how the free algebras for a monad form an algebra classifier (the clone), whereas the cofree coalgebras for a comonad do not seem to either classify or "coclassify" anything meaningful. And indeed, the former turns out to be the foundation of a rich mathematical theory, capturing algebraic varieties by *functorial semantics* [21,22], whereas the latter remains a symptom of the fundamental fact that this theory does not have a dual: coalgebras for comonads on toposes tend to form toposes again, rather than "covarieties".

The present paper is an effort towards analysing an observed asymmetry of induction and coinduction: *coinductively constructed objects conspicuously often come about as domains on which we perform inductive constructions.* Not only models of computation, but even the universes of such models tend to be coinductively constructed — apparently *in order to* accomodate induction [1]. On the other hand, some basic structures of real analysis can be captured in a similar setting, with induction embedded in a coinductively defined domain [27].

### *1.1 Guarded induction is induction*

In the simplest cases, this interplay of induction and coinduction is easy to understand. Take, e.g., the product functor $\Sigma \times (-) : \mathsf{Set} \longrightarrow \mathsf{Set}$. Its final coalgebra is the set $\Sigma^\omega$ of infinite streams in $\Sigma$, with the structure map

$$\langle \mathrm{head}, \mathrm{tail} \rangle : \Sigma^\omega \longrightarrow \Sigma \times \Sigma^\omega$$

In this destructor form, it accomodates the *stream induction*, where head takes care for the base case, and tail for the step. However, using inverse of $\langle \mathrm{head}, \mathrm{tail} \rangle$, the constructor $\mathrm{cons} : \Sigma \times \Sigma^\omega \longrightarrow \Sigma^\omega$ — sometimes abbreviated by $a.x = \mathrm{cons}(a, x)$ — the inductive definition

$$\begin{aligned} \mathrm{head}(x) &= a \\ \mathrm{tail}(x) &= x \end{aligned} \tag{1}$$

becomes the basic guarded equation

$$x = a.x \tag{2}$$

The prefixing $a.(-) : \Sigma^\omega \longrightarrow \Sigma^\omega$ is the simplest kind of a guarded operation. Its unique fixpoint is the unique solution of the corresponding inductive system (1).

This surely looks like a very simple example, but it is very typical. For instance, an interesting bit of differential equations can be hidden behind it. Take $\Sigma$ to be the set $\mathbb{R}$ of real numbers. The final coalgebra $\Sigma^\omega$ then contains

the set $\mathbb{A}$ of analytic functions: every $f \in \mathbb{A}$ can indeed be represented as the stream $[f(0), f'(0), f''(0), \ldots]$. As observed by M.H. Escardó[2] [27], the $\langle \text{head}, \text{tail} \rangle$-structure restricts to $\mathbb{A}$ in the form

$$\begin{aligned} \text{head}(f) &= f(0) \\ \text{tail}(f) &= f' \end{aligned}$$

while its inverse becomes

$$\text{cons}(a, g) = a + \textstyle\int_0^x g\, dt$$

It is not hard to see that the coalgebra $\mathbb{A}$ is final for all $\langle h, t \rangle : A \longrightarrow \mathbb{R} \times A$ such that for every $\alpha \in A$ there is some $x > 0$ with

$$\textstyle\sum_{n=0}^{\infty} \frac{ht^n(\alpha)}{n!} x^n < \infty$$

An inductive definition in terms of head and tail now becomes an initial value problem, while a guarded equation like (2) becomes the corresponding integral equation.

The first guarded equations, introduced in CCS [23, sec. 3.2], were of a similar kind, e.g.

$$x = a.x + bc.x \tag{3}$$

The operation $+$ can be understood as the union of non-wellfounded sets [2]. Formally, it is the inverse of the structure map

$$\ni : \mathcal{V} \longrightarrow \wp\mathcal{V}$$

which makes the class $\mathcal{V}$ of non-wellfounded sets into a final coalgebra for the powerset functor $\wp : \mathsf{SET} \longrightarrow \mathsf{SET}$. The map $\ni$ assigns to each element of $\mathcal{V}$ the set of its elements. We write $x \ni y$ instead of $y \in \ni(x)$.

If non-wellfounded sets are presented as (irredundant) trees [25], it becomes clear that $\ni$ supports the *tree induction*. Equations like (3) are solved by a combination of the stream and the tree induction, which one might call *labelled tree induction*. It is supported by the class $\mathcal{V}_\Sigma$ of $\Sigma$-labelled non-wellfounded sets — or synchronisation trees. The map

$$\twoheadrightarrow \; : \mathcal{V}_\Sigma \longrightarrow \wp(\Sigma \times \mathcal{V}_\Sigma)$$

makes this class into a final coalgebra for the functor $\wp_\Sigma = \wp(\Sigma \times -) : \mathsf{SET} \longrightarrow \mathsf{SET}$. The inverse of $\twoheadrightarrow$ is the composite of the constructors $+$ and cons. Guarded equation (3) is just the constructor version of the system

$$\begin{aligned} x &\xrightarrow{a}\!\!\!\!\rightarrow x \\ x &\xrightarrow{b}\!\!\!\!\rightarrow y \xrightarrow{c}\!\!\!\!\rightarrow x \end{aligned}$$

In general, guarded induction seems to be a form of induction supported by final coalgebras — but written not in terms of their inverses, in the constructor

[2] and perhaps also by C.A.R. Hoare [13], who writes respectively $\alpha_0$ and $\alpha'$ for the head and the tail of a trace $\alpha$

form. Unravelling the destructor form in principle discloses the base case, and sheds some light on the mystery of proofs "using the proposition we want to prove" [8], or of "induction without the base case" [24]; yet it surely does not resolve it. Even if we translate all guarded equations (2) into definitions with an inductive base (1), it will still remain unclear — *why do final coalgebras support such induction at all?*

Here and in [26], we shall analyse some structural undercurrents that seem to be pointing to an answer. The first idea that comes to mind is that *the unique homomorphisms to a final coalgebra should somehow yield the unique fixpoints of guarded operations on it.* In other words, guarded induction should be based on coinduction. We shall see that this idea covers only a very small part of guarded operations used in practice; yet it does provide an intuitive starting point.

### *1.2 Outline of the paper*

The simple operations where guarded induction boils down to coinduction are analysed in section 2. An abstract, semantic notion of *prefixing* follows, applicable to fixpoints of an arbitrary functor. Of course, in all relevant particular cases, the usual, syntactic notion of prefixing is captured. Only the fixpoints of the prefixing operations, or some standard constants, can be constructed coinductively.

The central idea of the paper is presented in section 3. We propose a categorical notion of a guard, a structure that can be carried by operations on arbitrary coalgebras. On a final coalgebra, though, an operation can have at most one guard, *and* is completely determined by it. In a way, the guard displays the inductive nature of the corresponding guarded operation, as well as the inductive construction of its unique fixpoint.

So we end up with two methods for constructing unique fixpoints of operations on final coalgebras: one direct, based on their couniversal property, the other inductive, and more general. Can such basic tools lead up to a discipline of *coinductive programming*, where programs, real functions and other infinitary objects would be extracted as fixpoints from specifications written in the form of guarded equations? Section 4 plays with this idea, investigating the compositionality of the prefixing and of the guarded operations.

## 2 Prefixing

**Lemma 2.1** *Let $F : \mathbb{C} \longrightarrow \mathbb{C}$ be a functor and $\Upsilon$ its fixpoint, i.e. an object of $\mathbb{C}$, given together with an isomorphism*

$$\Upsilon \underset{\delta}{\overset{\varrho}{\underset{\cong}{\rightleftarrows}}} F\Upsilon$$

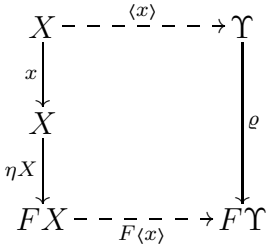
*Furthermore, let $\eta : \mathrm{id} \longrightarrow F$ be an arbitrary natural transformation, and $\partial$*

*the composite*

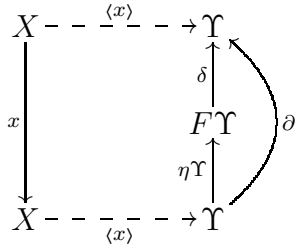
$$\partial : \Upsilon \xrightarrow{\eta\Upsilon} F\Upsilon \xrightarrow{\delta} \Upsilon$$

*The following commutativity conditions are then equivalent.*

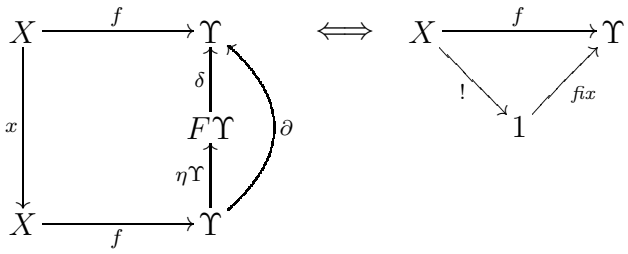
**(a)** $\forall x \exists! \langle x \rangle.$




**(b)** $\forall x \exists! \langle x \rangle.$




**(c)** $\exists fix \forall x f.$




**Remark.** Without mentioning the terminal object, (c) can be equivalently reformulated

$$\forall X \; \exists fix_X : X \longrightarrow \Upsilon \; \forall x : X \longrightarrow X \; \forall f : X \longrightarrow \Upsilon.$$
$$\partial \circ f \circ x = f \iff f = fix_X$$

It follows that

$$\forall u : X \longrightarrow Y. \;\; fix_X = fix_Y \circ u$$

**Proof of lemma 2.1.** (a⇔b): By the naturality of $\eta$, (a) is equivalent with

$$\varrho \circ \langle x \rangle = \eta\Upsilon \circ \langle x \rangle \circ x \tag{4}$$

Composing both sides of this equation with $\delta$ yields (b). The other way around, composing both sides of (b), i.e. $\partial \circ \langle x \rangle \circ x = \langle x \rangle$, with $\varrho$ yields (4), and hence (a).

(b⇒c): Since $\partial \circ \langle \mathrm{id}_1 \rangle = \langle \mathrm{id}_1 \rangle$ and $! \circ x = !$, we have $\partial \circ \langle \mathrm{id}_1 \rangle \circ ! \circ x = \langle \mathrm{id}_1 \rangle \circ !$. By the uniqueness part of (b), this implies $\langle x \rangle = \langle \mathrm{id}_1 \rangle \circ !$, for every $x$. (c) thus holds with $fix = \langle \mathrm{id}_1 \rangle$.

(c⇒b) is easy. □

**Definition 2.2** An operation[3] $\partial : \Upsilon \longrightarrow \Upsilon$ on a fixpoint $\Upsilon$ of $F$ (as in lemma 2.1) is *prefixing* if the composite

$$\eta\Upsilon : \Upsilon \xrightarrow{\partial} \Upsilon \xrightarrow{\varrho} F\Upsilon$$

can be extended to a natural transformation

$$\eta : \mathrm{id} \longrightarrow F$$

The *prefix* is the component $\eta 1 : 1 \longrightarrow F1$.

**Corollary 2.3** *If $\varrho : \Upsilon \longrightarrow F\Upsilon$ is the final coalgebra, then each prefixing operation $\partial : \Upsilon \longrightarrow \Upsilon$ has a unique fixpoint $fix : 1 \longrightarrow \Upsilon$.*

**Proof.** By the assumption that it is prefixing, $\partial$ induces $\eta : \mathrm{id} \longrightarrow F$. Since $\varrho : \Upsilon \longrightarrow F\Upsilon$ is the final $F$-coalgebra, condition (a) from lemma 2.1 is satisfied. The equivalent condition (c) yields the desired fixpoint $fix : 1 \longrightarrow \Upsilon$. In fact, it is just the coalgebra homomorphism from the prefix $\eta 1 : 1 \longrightarrow F1$ to $\varrho : \Upsilon \longrightarrow F\Upsilon$.

While $\partial : \Upsilon \longrightarrow \Upsilon$ may extend to various natural transformations $\eta : \mathrm{id} \longrightarrow F$, they must all have the same prefix component $\eta 1 : 1 \longrightarrow F1$. Indeed, by the naturality of $\eta$ and the definition of $\eta\Upsilon$, we have

$$\eta 1 \circ ! = F! \circ \eta\Upsilon = F! \circ \varrho \circ \partial$$

But $! : \Upsilon \longrightarrow 1$ is surely an epi, because it is split by *fix* (be it unique or not). So $\partial$ induces a unique prefix $\eta 1$, and $\eta 1$ induces a unique fixpoint *fix*. □

**Examples.** Consider again the set of streams $\Upsilon = \Sigma^\omega$. With the structure map $\varrho = \langle \mathrm{head}, \mathrm{tail} \rangle$, it is the final coalgebra of the functor $FX = \Sigma \times X$. By definition 2.2, an operation $\partial : \Sigma^\omega \longrightarrow \Sigma^\omega$ is prefixing if the map $\eta\Upsilon = \varrho \circ \partial$ can be extended to a natural transformation $\eta$. In particular, the component $\eta 1$ determines some $a \in \Sigma$ such that for every $x$, the square

$$\begin{array}{ccc} 1 & \xrightarrow[\langle a, \mathrm{id} \rangle]{\eta 1 \,=} & \Sigma \times 1 \\ {\scriptstyle x}\downarrow & & \downarrow{\scriptstyle \Sigma \times x} \\ \Sigma^\omega & \xrightarrow[\langle \mathrm{head}, \mathrm{tail} \rangle \circ \partial]{\eta\Upsilon \,=} & \Sigma \times \Sigma^\omega \end{array}$$

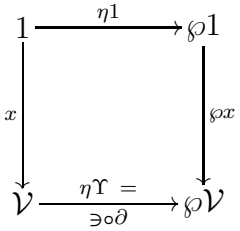
commutes. But $\mathrm{head} \circ \partial(x) = a$ and $\mathrm{tail} \circ \partial(x) = x$ together imply that $\partial$ must be the usual prefixing

$$\partial(x) = a.x$$

The induced natural transformation $\eta$ has the components $\eta X = \langle a \circ !, \mathrm{id} \rangle : X \longrightarrow \Sigma \times X$.

[3] Like in algebra, an $n$-ary operation is simply an arrow $X^n \longrightarrow X$. Presently, we only consider unary operations, i.e. endomorphisms; yet we call them operations in anticipation of later algebraic developments.

For $F = \wp\mathcal{O}$ and its greatest fixpoint $\Upsilon = \mathcal{V}$, consider a similar square.




$\eta 1$ can now pick either $\emptyset$ or $1 \in \wp 1$. This yields two prefixing operations on $\mathcal{V}$

$$\partial^0(x) = \emptyset$$
$$\partial^1(x) = \{x\}$$

They respectively extend to $\eta^0 : \mathrm{id} \longrightarrow \wp\mathcal{O}$, the components of which take everything to $\emptyset$, and $\eta^1 : \mathrm{id} \longrightarrow \wp\mathcal{O}$, where $\eta^1_X : X \longrightarrow \wp\mathcal{O}X$ takes $x \in X$ to the singleton $\{x\} \in \wp\mathcal{O}X$.

Combining the above two examples, one gets the class of synchronisation trees $\mathcal{V}_\Sigma$, as the greatest fixpoint of $F = \wp\mathcal{O}_\Sigma$. The prefixing operations on it are in the form

$$\partial^a(x) \xrightarrow{a} x$$

one for each $a \in \Sigma$, and moreover the constant $\partial^0(x) = \emptyset$.

The prefixing operations, of course, cover a very small part of the operations with unique fixpoints. Obviously, every constant $\partial : \Upsilon \longrightarrow 1 \longrightarrow \Upsilon$ has a unique fixpoint, but very few of them extend to natural transformations. On the coalgebra $\mathbb{A}$ of analytic functions, the prefixing equations $y = \mathrm{cons}(a, y)$ correspond to the trivial initial value problems, in the form

$$y(0) = a$$
$$y' \quad = y$$

A bit less trivially, every composite of prefixing operations still has a unique fixpoint — like e.g.

$$\partial^{bc}(x) \xrightarrow{b} \partial^c(x) \xrightarrow{c} x$$

does. Such composites usually fail to be prefixing operations with respect to $F$, but we shall see in section 4 that they are prefixing with respect to $F^2$.

Finally, there are many interesting operations with unique fixpoints that cannot be obtained even as composites of prefixing operations. For instance,

$$\partial^{a,bc}(x) = a.x + bc.x$$

on $\mathcal{V}_\Sigma$. Or simply

$$\partial^\infty(x) = \infty$$

on $\mathcal{V}$, where $\infty = \{\infty\}$ is the non-wellfounded set containing itself as the only element. We shall see that $\mathcal{V}$ is a final $\wp\mathcal{O}^n$-coalgebra for every $n$, yet there is

no way of extending $\partial^\infty$ to a natural transformation $\mathrm{id} \longrightarrow \wp\mathcal{O}^n$ for any $n$.

Operations like $\partial^{a,bc}$ and $\partial^\infty$ are essentially more general than the prefixing.

# 3 Guarded operations

*3.1 Cones and coalgebras*

In a category $\mathbb{C}$ with a final object 1, every functor $F : \mathbb{C} \longrightarrow \mathbb{C}$ induces a tower $\nu F$, like on

$$
\begin{array}{lcl}
\nu F & = & 1 \xleftarrow{\ !\ } F1 \xleftarrow{\ F!\ } F^2 1 \xleftarrow{\ F^2!\ } F^3 1 \xleftarrow{\ F^3!\ } \cdots \\
 & & \uparrow{\scriptstyle !} \quad \uparrow{\scriptstyle F!} \quad \uparrow{\scriptstyle F^2!} \quad \uparrow{\scriptstyle F^3!} \\
\Xi & = & X \xrightarrow[\xi]{} FX \xrightarrow[F\xi]{} F^2 X \xrightarrow[F^2\xi]{} F^3 X \xrightarrow[F^3\xi]{} \cdots
\end{array}
\tag{5}
$$

while every coalgebra $\xi : X \longrightarrow FX$ induces a tower $\Xi$. Hence the cone $p = p^\xi : X \longrightarrow \nu F$, with the components

$$
\begin{array}{ll}
p_0 & : X \xrightarrow{\ !\ } 1 \\
p_{i+1} & : X \xrightarrow{\ \xi\ } FX \xrightarrow{Fp_i} F^{i+1}1
\end{array}
\tag{6}
$$

If $F^\omega 1$ is defined to be the limit of $\nu F$, the cone $p$ factorizes through $p_\omega : X \longrightarrow F^\omega 1$. On the other hand, $F^{\omega+1}1 = FF^\omega 1$ comes with an obvious cone to $\nu F$ as well, which induces $F^{\omega+1}1 \xrightarrow{F^\omega!} F^\omega 1$. Proceeding in this way, the tower $\nu F$ and the cone $p$ can both be extended transfinitely.

If $\nu F$ ever becomes stationary, in the sense that for some ordinal $\alpha$, the arrow $\delta : F^{\alpha+1}1 \xrightarrow{F^\alpha!} F^\alpha 1$ is an isomorphism, then $\Upsilon = F^\alpha 1$ will be the final $F$-coalgebra, with the inverse $\varrho : \Upsilon \longrightarrow F\Upsilon$ of $\delta$ as the structure map [19,30].

Of course, $\nu F$ will surely become stationary at $\alpha$ if $F$ preserves the limits of the towers of length $\alpha$. In fact, if $F : \mathbb{C} \longrightarrow \mathbb{C}$ does not preserve such limits, but $\mathbb{C}$ is a concrete category with objects bounded by some inaccessible cardinal $\kappa$, then $F$ can usually be extended to a larger category $\widehat{\mathbb{C}}$, containing $\mathbb{C}$ as a full subcategory, *and* having the limits of $\kappa$-towers. The extension of $F$ to $\widehat{\mathbb{C}}$ is then defined as to preserve such limits — and hence to have the greatest fixpoint. The familiar construction [2] of the universe of non-wellfounded sets as the greatest fixpoint of (the extension of) the powerset functor $\wp\mathcal{O} : \mathsf{Set} \longrightarrow \mathsf{Set}$ (to the category $\mathsf{SET}$ of classes) can be viewed as an example of this method [4, prop. 1.3].

Alternatively, if the $F$-images of the finite objects are finite, and $\mathbb{C}$ has the limits of the countable towers, then one can take the finitary restriction $F_{\mathrm{fin}} : \mathbb{C}_{\mathrm{fin}} \longrightarrow \mathbb{C}_{\mathrm{fin}}$ of $F$ and then extend it to $F_{\mathrm{fin}} : \mathbb{C} \longrightarrow \mathbb{C}$, but in such a way that the limits of the countable towers are preserved. Applied to the powersets $\wp\mathcal{O} : \mathsf{Set} \longrightarrow \mathsf{Set}$, this method of *modifying* a functor leads to the finite powersets $\wp\mathcal{O}_{\mathrm{fin}} : \mathsf{Set} \longrightarrow \mathsf{Set}$. Note that this is, in fact, just a variant of the previous method of *extending* a functor as to preserve the limits of $\kappa$-towers: here, indeed, $F_{\mathrm{fin}}$ gets extended as to preserve the limits of the

$\aleph_0$-towers [4].

In any case, the preceding discussion shows that the following assumption causes no significant loss of generality, as it can usually be enforced with enough inaccessible cardinals (or Grothendieck universes), and often even without them.

**Assumption.** In the sequel, the functor $F$ will be assumed to preserve the limits of $\kappa$-towers, for some fixed $\kappa$, so that its greatest fixpoint $\Upsilon$ comes about as the limit $F^\kappa 1$, where the $\kappa$-tower $\nu F$ stabilizes.

As pointed out before, the coalgebra structure $\varrho : \Upsilon \longrightarrow F\Upsilon$ is obtained as the inverse of the stabilizing isomorphism $\delta : F^\kappa 1 \longrightarrow FF^\kappa 1$. The cone $p : \Upsilon \longrightarrow \nu F$, induced as in (6) by $\xi = \varrho$, will in this case be a limit cone.

On the other hand, taking (5) with $X = 1$, any $\xi : 1 \longrightarrow F1$ induces a corresponding tower $\Xi$ as a "splitting" of $\nu F$. For each $i < \kappa$, (5) now gives a cone $\upsilon_i : F^i 1 \longrightarrow \nu F$, with $\upsilon_{i+1} \circ F^i\xi = \upsilon_i$. Since $\Upsilon$ is the limit of $\nu F$, these cones induce $u_i : F^i 1 \longrightarrow \Upsilon$, satisfying $u_{i+1} \circ F^i\xi = u_i$.

Since each $u_i$ is defined as the factorisation of the cone $\upsilon_i : F^i 1 \longrightarrow \nu F$ through the limit cone $p : \Upsilon \longrightarrow \nu F$, the arrow $p_m \circ u_n : F^n 1 \longrightarrow F^m 1$ must be the $m$-th component of $\upsilon^n$, that is

$$p_m \circ u_n \quad = \quad \begin{cases} F^{m-1}\xi \circ \cdots \circ F^n\xi & \text{if } m > n \\ \mathrm{id} & \text{if } m = n \\ F^m! \circ \cdots \circ F^{n-1}! & \text{if } m < n \end{cases} \tag{7}$$

In particular,

**Lemma 3.1** *For a final $F$-coalgebra $\Upsilon$, all limit cone components $p_i : \Upsilon \longrightarrow F^i 1$ are split epi, as soon as there is some arrow $1 \longrightarrow F1$.*

**Remark.** Algebras $FX \longrightarrow X$ and coalgebras $X \longrightarrow FX$ are clearly a glorification [5] of post-fixpoints $x \geq f(x)$ and pre-fixpoints $x \leq f(x)$ in posets. Initial algebras correspond to the least post-fixpoints; final coalgebras to the greatest pre-fixpoints. As it is well known, they turn out to be proper fixpoints in each case: the Knaster-Tarski theorem [18,31] tells this for lattices, the Lambek lemma [20] for categories.

On the other side, there is the Kleene theorem for lattices [17], which says that the least fixpoint of a monotone map $f$ is the stationary point of the (possibly transfinite) tower $0 \leq f(0) \leq f^2(0) \leq \cdots \leq f^\omega(0) \cdots$; and that its greatest fixpoint is the stationary point of $1 \geq f(1) \geq f^2(1) \geq \cdots \geq f^\omega \cdots$. The glorifications in terms of diagrams like (5) are mostly in [30].

[4] Although $\aleph_0$ is often explicitly, by definition, excluded from the class of inaccessible cardinals, it actually possesses both of the relevant closure properties: for all $\zeta < \aleph_0$ holds $2^\zeta < \aleph_0$ and $|\cup\zeta| < \aleph_0$.

[5] In more glorious times, categorical generalisations came to be called glorifications!

*3.2 Guards*

Let us now introduce a class of operations $\partial$ more general than those analysed in section 2.

**Definition 3.2** A *guard* of an operation $\partial : X \longrightarrow X$ with respect to a coalgebra $\xi : X \longrightarrow FX$ is a family $\eta = \langle \eta_0, \eta_1, \eta_2 \ldots \rangle$, such that the squares

(8)
$$\begin{array}{ccc} F^i 1 & \xleftarrow{p_i} & X \\ {\scriptstyle \eta_i}\downarrow & & \downarrow{\scriptstyle \partial} \\ X & & \downarrow{\scriptstyle \xi} \\ F^{i+1}1 & \xleftarrow[Fp_i]{} & FX \end{array}$$

commute for all $i \geq 0$, with $p_i$ constructed as in (6). An operation $\partial$ is said to be *guarded* if there is some guard $\eta$ for it.

**Remark.** By definition (6) of $p_i$, square (8) commutes if and only if

(9)
$$\begin{array}{ccc} F^i 1 & \xleftarrow{p_i} & X \\ {\scriptstyle \eta_i}\downarrow & & \downarrow{\scriptstyle \partial} \\ F^{i+1}1 & \xleftarrow[p_{i+1}]{} & X \end{array}$$

commutes.

**Proposition 3.3** *Every prefixing operation is guarded.*

**Proof.** If the composite $\varrho \circ \partial : \Upsilon \longrightarrow F\Upsilon$ extends to a natural transformation $\eta : \mathrm{id} \longrightarrow F$, then the family consisting of $\eta_i = \eta F^i 1$ constitutes a guard of $\partial$ with respect to $\varrho$. □

**Examples.** The constant operation $\partial^\infty(x) = \infty$ on the class $\mathcal{V}$ of non-wellfounded sets is guarded by the maps $\eta_i : \wp^i 1 \longrightarrow \wp^{i+1} 1$, such that

$$\begin{aligned} \eta_0 \quad &= 1 \\ \eta_{i+1}(x) &= \{\eta_i\} \end{aligned}$$

On the other hand, the operation $\partial^{a,b}(x) = a.x + b.x$ on $\mathcal{V}_\Sigma$ is guarded by $\eta_i : \wp^i_\Sigma 1 \longrightarrow \wp^{i+1}_\Sigma 1 = \wp(\Sigma \times \wp^i_\Sigma 1)$, where

$$\eta_i(x) = \{\langle a, x\rangle, \langle b, x\rangle\}$$

Finally, $\partial^{bc}(x) = bc.x$ is not just prefixing on the class $\mathcal{V}_\Sigma$ viewed as the fixpoint of $\wp^2_\Sigma$. More importantly, it is also guarded on $\mathcal{V}_\Sigma$ as a $\wp_\Sigma$-coalgebra,

with the guard

$$\begin{aligned}\eta_0 &= \{b\}\\ \eta_{i+1}(x) &= \{\langle b, \{\langle c, \overline{x}\rangle\}\rangle\}\end{aligned}$$

where $\overline{x}$ is the truncation, i.e. the image of $x$ by $\wp^i_\Sigma! : \wp^{i+1}_\Sigma 1 \longrightarrow \wp^i_\Sigma 1$. In a general setting, such guards will be discussed in section 4.

On the coalgebra $\mathbb{A}$ of analytic functions, guarded operations are exactly those that can be approximated by polynomials. Diagram (9) tells that the $(i+1)$-st order approximation of $\partial(f)$ is completely determined by the $i$-th order approximation of $f$. The component $\eta_i$ expresses that determination.

In fact, guarded induction on $\mathbb{A}$ actually boils down to the power series method of solving ordinary differential equations. First of all, if $\partial : \mathbb{A} \longrightarrow \mathbb{A}$ is guarded, then $p_1 \circ \partial = \eta_0 \circ p_0$ means that it must be in the form

$$\partial(y) = \mathrm{cons}\,(\eta_0, h(y))$$

where $h = \mathrm{tail} \circ \partial$. The equation $y = \partial(y)$ thus turns out to be an initial value problem in the general form

$$\begin{aligned}y(0) &= \eta_0\\ y' &= h(x, y)\end{aligned} \tag{10}$$

When $h$ is an analytic function, the analytic solution

$$y(x) = \textstyle\sum_{i=0}^{\infty} y_i x^i$$

can always be determined recursively:

$$\begin{aligned}y_0 &= \eta_0\\ y_{i+1} &= \eta_{i+1}(y_0, \ldots, y_i)\end{aligned}$$

where $\eta_{i+1}$ is a polynomial with the coefficients derived from the power expansion of $h$, *viz* its coefficients of order $\leq i+1$. This clearly yields a guard, and corresponds to guarded induction, as described in the next section. Concrete examples can be found in any textbook on differential equations; an explanation how to derive $\eta_{i+1}$ in [7, sec. 4.8].

For the initial value problems in several dimensions, i.e. involving *partial* derivatives, the power series method is even more important. The fundamental existence theorem, due to Kowalevskaya and Cauchy, is essentially based on a recursive construction of a power series solution in several variables (cf. [14, ch. 3], or [11, ch. 4,6]). This is a striking example of guarded induction in classical mathematics.

The set $\mathbb{A}_2$ of real analytic functions in two variables embeds, in the obvious way, into the set $\mathbb{R}^{\omega\times\omega}$ of "two dimensional streams", or infinite matrices. This set carries two different final coalgebra structures $\langle \mathrm{head}, \mathrm{tail}\rangle : \mathbb{R}^{\omega\times\omega} \longrightarrow$

$\mathbb{R}^\omega \times \mathbb{R}^{\omega\times\omega}$, which restrict to $\mathbb{A}_2 \subseteq \mathbb{R}^{\omega\times\omega}$ and $\mathbb{A} \subseteq \mathbb{R}^\omega$ as follows:

$$\begin{aligned} \mathrm{head}_x(f) &= f(0,y) & \mathrm{head}_y(f) &= f(x,0) \\ \mathrm{tail}_x(f) &= f'_x & \mathrm{tail}_y(f) &= f'_y \end{aligned}$$

The two dimensional Cauchy problems induce equations in this signature. Similarly as in the one dimensional case, one shows that the induced equations are indeed guarded with respect to a suitable coalgebra. On the other hand, there are guarded equations that do not reduce to the Cauchy form in any obvious way. In any case, as a consequence of the general result in the next section, each of them has a unique analytic solution.

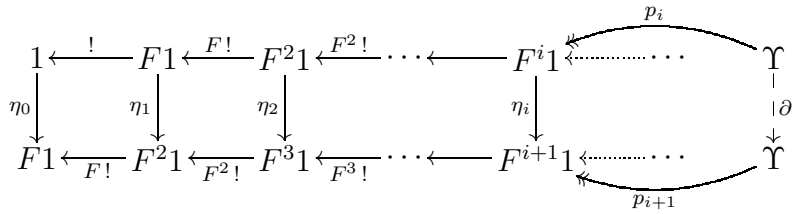
### *3.3 Guarded operations on final coalgebras and their fixpoints*

As explained in 3.1, when $\Upsilon$ is the final coalgebra for $F$, it is natural to assume that $p : \Upsilon \longrightarrow \nu F$ is a limit cone. This means, of course, that the arrows $p_i : \Upsilon \longrightarrow F^i 1$ are jointly monic.

On the other hand, if there is a guarded operation on $\Upsilon$, each $p_i : \Upsilon \longrightarrow F^i 1$ will be a split epi. Indeed, a guard $\eta$ supplies an arrow $\eta_0 : 1 \longrightarrow F1$, so that the hypotheses of lemma 3.1 are fulfilled.

One consequence is that the commutativity of (8), with $X = \Upsilon$, implies that $\partial : \Upsilon \longrightarrow \Upsilon$, together with $\varrho : \Upsilon \longrightarrow F\Upsilon$, uniquely determines each component $\eta_i$ of its guard $\eta$.

Another consequence is that, conversely, the guard $\eta$ uniquely determines the operation $\partial$. Indeed, when all $p_i$ are epi, then all squares on the diagram




must commute. The operation $\partial$ can thus be recovered from $\eta$ as the limit factorisation of the cone $\eta \circ p : \Upsilon \longrightarrow \nu F$.

We have thus proved that

**Proposition 3.4** *An operation $\partial$ on a final coalgebra $\Upsilon$ has at most one guard $\eta$. When it exists, the guard $\eta$ completely determines the operation $\partial$.*

For an operation on a final coalgebra, being guarded is thus a *property*, rather than additional structure!

The upshot is that this property ensures the unique fixpoints.

**Proposition 3.5** *A guarded operation on a final coalgebra has a unique fixpoint.*

**Proof.** If $\partial : \Upsilon \longrightarrow \Upsilon$ is guarded by $\eta$, its fixpoint $\mathit{fix} : 1 \longrightarrow \Upsilon$ is induced

by the cone with the components

$$\begin{aligned} \mathit{fix}_0 &: 1 \longrightarrow 1 \\ \mathit{fix}_{i+1} &: 1 \xrightarrow{\mathit{fix}_i} F^i 1 \xrightarrow{\eta_i} F^{i+1} 1 \end{aligned}$$

These arrows indeed form a cone $1 \longrightarrow \nu F$, because $F^i! \circ \eta_i = \eta_{i-1} \circ F^{i-1}!$ implies $F^i! \circ \mathit{fix}_{i+1} = \mathit{fix}_i$.

On the other hand, the $(i+1)$-st component of the cone corresponding to $\partial \circ \mathit{fix} : 1 \longrightarrow \Upsilon$ is

$$\begin{aligned} p_{i+1} \circ \partial \circ \mathit{fix} &= \eta_i \circ p_i \circ \mathit{fix} \\ &= \eta_i \circ \mathit{fix}_i \\ &= \mathit{fix}_{i+1} \end{aligned}$$

Hence $\partial \circ \mathit{fix} = \mathit{fix}$.

Towards the uniqueness, suppose $\partial \circ f = f : X \longrightarrow \Upsilon$. Writing $p_i \circ f$ as $f_i$, we have

$$\begin{aligned} f_{i+1} &= p_{i+1} \circ f \\ &= p_{i+1} \circ \partial \circ f \\ &= \eta_i \circ p_i \circ f \\ &= \eta_i \circ f_i \end{aligned}$$

Since $f_0$ is obviously $! : X \longrightarrow 1$,

$$f_i = \mathit{fix}_i \circ !$$

follows by induction over $i$. □

**Remark.** If a coalgebra is not final, a guarded operation may not have a fixpoint, or may have many. E.g., the universe $V$ of *wellfounded* sets is not only a coalgebra, but even a fixpoint of the powerset functor $\wp$ — but initial, rather than final. Anyway, the operation $\partial^1(x) = \{x\}$ is still prefixing with respect to it — but does not have any fixpoints, as they would have to be non-wellfounded. In a sense that will be explained in [26], adjoining fixpoints of guarded operations leads directly to final coalgebras.

## 4 Towards coinductive programming: the composites

Roughly, the idea of coinductive programming is that infinite objects — be it processes, abstract machines, or real numbers — can be specified over coinductively defined domains, final coalgebras. However, while inductive programming generally boils down to unique homomorphisms from initial algebras [6], coinductive programming will probably be more about guarded operations and their fixpoints, than about coalgebras and homomorphisms. This tendency is

already clear in process calculus and real analysis [27], and is illustrated by the examples in sections 2 and 3.

In any case, the main task is now, as always in programming, to systematically decompose complex objects into simple parts; and to compose simple specifications as to solve complex problems. As a first step towards developing a toolkit needed for the practice of coinductive programming, we shall now briefly analyse the ways in which respectively the prefixing and the guarded operations compose. It turns out that each of the classes is closed under the composition, the latter in a much stronger sense.

For any $n \geq 1$ and the $n$-tuple composite $F^n$ of $F : \mathbb{C} \longrightarrow \mathbb{C}$, each $F$-coalgebra $\xi : X \longrightarrow FX$ gives rise to an $F^n$-coalgebra

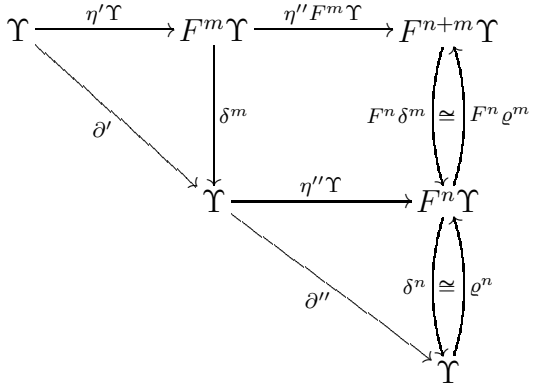
$$\xi^n : X \xrightarrow{\xi} FX \xrightarrow{F\xi} F^2X \xrightarrow{F^2\xi} \cdots \xrightarrow{F^{n-1}\xi} F^nX \tag{11}$$

Clearly, if $\xi = \varrho$ is an isomorphism making $X$ into a fixpoint of $F$, then $\varrho^n$ is an isomorphism too, making $X$ into a fixpoint of $F^n$.

### *4.1 Composite prefixing*

**Lemma 4.1** *Let $\Upsilon$ be a fixpoint of $F$, as in lemma* 2.1. *If $\partial' : \Upsilon \longrightarrow \Upsilon$ is a prefixing operation with respect to $F^m$ and $\partial'' : \Upsilon \longrightarrow \Upsilon$ with respect to $F^n$, then $\partial'' \circ \partial'$ is a prefixing operation with respect to $F^{m+n}$.*

**Proof.** By assumption, there are natural transformations $\eta' : \mathrm{id} \longrightarrow F^m$ and $\eta'' : \mathrm{id} \longrightarrow F^n$, such that $\eta'\Upsilon = \varrho^m \circ \partial'$ and $\eta''\Upsilon = \varrho^n \circ \partial''$. If $\delta^m$ and $\delta^n$ are the respective inverses of $\varrho^m$ and $\varrho^n$, the following diagram must commute.




It shows that $\varrho^{m+n} \circ \partial'' \circ \partial'$ appears as the $\Upsilon$-component of the natural transformation $\eta''F^m \circ \eta' = F^n\eta' \circ \eta'' : \mathrm{id} \longrightarrow F^{n+m}$. □

**Lemma 4.2** *With the assumption from section* 3.1, *the greatest fixpoints of $F$ and of its $n$-tuple composite $F^n$ coincide. If $\varrho : \Upsilon \longrightarrow F\Upsilon$ is the final $F$-coalgebra, then the final $F^n$-coalgebra is $\varrho^n : \Upsilon \longrightarrow F^n\Upsilon$* (11).

**Proof.** If $\nu F$ (5) stabilizes at $\kappa$, i.e. if $\delta : FF^\kappa 1 \xrightarrow{F^\kappa !} F^\kappa 1$ is an isomorphism, then $\Upsilon = F^\kappa 1 \cong F^\alpha 1$ for all $\alpha \geq \kappa$. But the tower $\nu F^n$, consisting of each

$n$-th entry of $\nu F$, will then stabilize at $F^{n\beta}$, where $\beta$ is the smallest ordinal such that $n\beta \geq \kappa$. The greatest fixpoint of $F^n$ is thus $F^{n\beta}1 \cong F^\kappa 1 = \Upsilon$.

(Chasing through the structure maps is left to the reader.) □

**Remark.** Without the "Kleene assumption" from 3.1, a final $F^n$-coalgebra still yields a final $F$-coalgebra, but not the other way around: see [10].

**Corollary 4.3** *If $\varrho : \Upsilon \longrightarrow F\Upsilon$ is a final coalgebra as above, then any composite of prefixing operations with respect to it has a unique fixpoint.*

**Proof.** By lemma 4.1, a composite of $n$ prefixing operations with respect to $F$ will be a prefixing operation with respect to $F^n$. By lemma 4.2, the final $F$-coalgebra $\varrho : \Upsilon \longrightarrow F\Upsilon$ yields the final $F^n$-coalgebra $\varrho^n : \Upsilon \longrightarrow F^n\Upsilon$. Applying corollary 2.3 (i.e. the constructions preceding it), we get the unique fixpoint of the composite prefixing as the unique coalgebra homomorphism to $\varrho^n$. □

### *4.2 Composite guards*

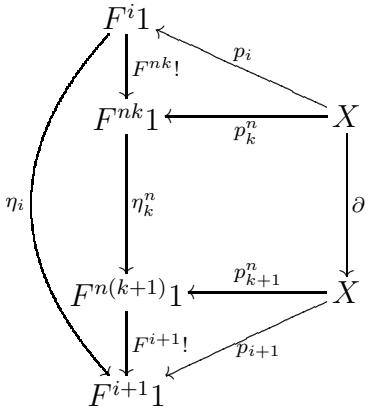
Similarly as above, a composite of $n$ operations guarded with respect to $\xi$ is guarded with respect to $\xi^n$. The point is now that it is also guarded with respect to $\xi$ itself.

**Proposition 4.4** *An operation $\partial : X \longrightarrow X$ is guarded with respect to $\xi : X \longrightarrow FX$ as soon as it is guarded with respect to any of $\xi^n : X \longrightarrow F^nX$, for $n \geq 1$.*

**Proof.** Given a guard $\eta^n = \langle \eta^n_0, \eta^n_1, \eta^n_2, \ldots \rangle$ of $\partial : X \longrightarrow X$ with respect to $\xi^n : X \longrightarrow F^nX$, a guard $\eta = \langle \eta_0, \eta_1, \eta_2, \ldots \rangle$ with respect to $\xi : X \longrightarrow FX$ will have the components

$$\eta_i = F^{i+1}! \circ \eta^n_k \circ F^{nk}!$$

(12)




where $nk \leq i < n(k+1)$ and $k$ runs along the natural numbers. To show that the extracted family constitutes a guard, we must show that the above diagram commutes.

The square clearly does, by the assumption that $\eta^n$ is a guard.

The arrow $p^n_k$ is a component of the cone $p^n : X \longrightarrow \nu F^n$, induced by $\xi^n$ and (5–6). Clearly, $p^n$ is a subcone of $p : X \longrightarrow \nu F$, and in particular

$$p^n_k = p_{nk}$$

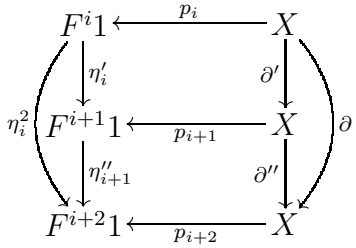
The triangles on the above diagram thus commute, because $p$ is a cone. □

**Corollary 4.5** *A composite of guarded operations is guarded with respect to the same coalgebra.*

**Proof.** Let $\partial'$ be guarded by $\eta'$, and $\partial''$ by by $\eta''$, both with respect to $\xi : X \longrightarrow FX$. Then by (9), $\partial = \partial'' \circ \partial'$ is guarded with respect to $\xi^2 : X \longrightarrow F^2X$ by the family $\eta^2$, the components of which are

$$\eta^2_i = \eta''_{i+1} \circ \eta'_i$$

(13)




Proposition 4.4 now tells that $\partial$ is also guarded with respect to $\xi : X \longrightarrow FX$.

The argument clearly carries over to all finite composites. □

## 5 Conclusion

We have characterised and analysed two classes of operations on final coalgebras, both with unique fixpoints. The *prefixing* operations, and their composites, allow a direct construction of fixpoints as coalgebra homomorphisms. On the other hand, the richer class of *guarded* operations, and their composites, only allows step-wise *approximation* of fixpoints — an infinite, but inductive, and therefore effective procedure.

Some logical consequences of this *induction within coinduction* will be analysed in [26], but full understanding will probably require more work. The proposed notion of guard does seem to be capturing a bulk of the effective approximation procedures, but some forms of coinductive programming, especially those arising from calculus, seem to require further refinements.

**Acknowledgement.** Thanks are due to Jan Rutten, for providing many valuable comments. In particular, he has informed me that a version of corollary 2.3, with a slightly different proof, will appear in a revised version of his extensive report on universal coalgebra [28], which is currently being prepared for *Theoret. Comput. Sci.*

## References


[1] S. Abramsky and D. Pavlovic, Process Categories as Fixpoints *(in preparation)*

[2] P. Aczel, *Non-Well-Founded Sets*. Lecture Notes 14 (CSLI 1988)

[3] R.M. Amadio and S. Coupet-Grimal, Analysis of a guard condition in type theory. Rapport 245, Laboratoire d'Informatique Marseille

[4] M. Barr, Terminal coalgebras for endofunctors on sets. *Theoret. Comput. Sci.* 114(1993) 299-315, additions and corrections 124(1994) 189–192

[5] J. Barwise and L.S. Moss, *Vicious Circles* (CSLI 1996)

[6] R. Bird and O. de Moor, *Algebra of Programming.* (Prentice Hall 1997)

[7] G. Birkhoff and G.-C. Rota, *Ordinary Differential Equations* (John Wiley and Sons 1959, third ed. 1978)

[8] Th. Coquand, Infinite Objects in Type Theory. In: *Types for Proofs and Programs*, Lecture Notes in Computer Science 806 (Springer 1993)

[9] E.W. Dijkstra, *A Discipline of Programming* (Prentice-Hall 1976)

[10] P.J. Freyd, Algebraically complete categories. In: *Category Theory, Como 1990* (A. Carboni et al., eds.) Lecture Notes in Mathematics 1488 (Springer 1991) 95–104

[11] P.R. Garabedian, *Partial Differential Equations* (John Wiley & Sons 1964)

[12] H. Geuvers, Inductive and coinductive types with iteration and recursion *(extended notes for a talk, 1992)*

[13] C.A.R. Hoare, *Communicating Sequential Processes* (Prentice-Hall 1985)

[14] F. John, *Partial Differential Equations* (Springer 1971, fourth ed. 1982)

[15] B. Jacobs, Mongruences and cofree coalgebras. In: *Algebraic Methodology and Software Technology (AMAST 1995)* (V.S. Alagar and M. Nivat, eds.) Lecture Notes in Computer Science 936 (Springer 1995) 245–260

[16] B. Jacobs and J. Rutten, A tutorial on (co)algebras and (co)induction, *Bulletin of EATCS* 62(1997) 229–259

[17] S.C. Kleene, *Introduction to Metamathematics* (North-Holland 1952)

[18] B. Knaster, Un théorème sur les fonctions d'ensambles. *Annales de la Soc. Polonaise Math.* 6(1928) 133–134

[19] J. Lambek, A fixpoint theorem for complete categories. *Math. Zeitschr.* 103(1968) 151–161

[20] J. Lambek, Subequalizers. *Canadian Math. Bull.* 13(1970) 337–349

[21] F.W. Lawvere, Functorial semantics of algebraic theories. *Proc. Nat. Acad. Sci. U.S.A.* 50(1963) 869–873

[22] E.G. Manes, *Algebraic Theories* (Springer 1974)

[23] R. Milner, *Communication and Concurrency* (Prentice Hall 1989)

[24] L.S. Moss and N. Danner, On the Foundations of Corecursion. *J. of the IGPL* 5(1997) 231–257

[25] D. Pavlović, Convenient categories of processes and simulations I: modulo strong bisimilarity. In: *Category Theory and Computer Science '95* (D. Pitt et al., eds.) Lecture Notes in Computer Science 953 (Springer 1995) 3–24

[26] D. Pavlović, Semantics of guarded induction *(in preparation)*

[27] D. Pavlović and M.H. Escardó, Calculus in coinductive form. University of Sussex Report CS 97/5, pp. 9 (to appear in the proceedings of LICS '98)

[28] J. Rutten, Universal coalgebra: a theory of systems. CWI Report CS-R9652, pp. 55

[29] J. Rutten and D. Turi, Initial algebra and final coalgebra semantics for concurrency. In: *A Decade of Concurrency* (J.W. de Bakker et al., eds.) Lecture Notes in Computer Science 803 (Springer 1994) 530–582

[30] M.B. Smyth and G.D. Plotkin, The category theoretic solution of recursive domain equations. *SIAM J. Comp.* 11(1982) 761–783

[31] A. Tarski, A lattice-theoretic fixpoint theorem and its applications. *Pacific J. of Math.* 5(1955) 285–309