Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science

L.G.L.T. Meertens

Paramorphisms

Computer Science/Department of Algorithmics & Architecture Report CS-R9005 February

Paramorphisms

Lambert Meertens
CWI, Amsterdam, & University of Utrecht

0 Context

This paper is a small contribution in the context of an ongoing effort directed towards the design of a calculus for constructing programs. Typically, the development of a program contains many parts that are quite standard, requiring no invention and posing no intellectual challenge of any kind. If, as is indeed the aim, this calculus is to be usable for constructing programs by completely formal manipulation, a major concern is the amount of labour currently required for such non-challenging parts.

On one level this concern can be addressed by building more or less specialised higher-level theories that can be drawn upon in a derivation, as is usual in almost all branches of mathematics, and good progress is being made here. This leaves us still with much low-level laboriousness, like administrative steps with little or no algorithmic content. Until now, the efforts in reducing the overhead in low-level formal labour have concentrated on using equational reasoning together with specialised notations to avoid the introduction of dummy variables, in particular for "canned induction" in the form of promotion properties for homomorphisms—which have turned out to be ubiquitous. Recent developments and observations strongly suggest that further major gains in the proof methods are possible. One of the most promising developments is that it has become apparent that often a lengthy administrative calculation can be replaced by a single step by simply considering the types concerned. In the context of mechanical support for formal

Report CS-R9005
Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

program construction, this can be mechanised in conjunction with mechanical type inference.

The present paper is concerned with another contribution to avoiding formal overhead, less dramatic, but probably still important, namely a generalisation of homomorphisms on initial data types, dubbed *paramorphisms*. While often much leverage is obtained by using homomorphisms, the occasions are also ample where the gain of the homomorphism approach is less clear. It will be shown below that for a class of functions that are not themselves homomorphisms, but that satisfy a similar simple recursive pattern, a short-cut can be made, resulting in properties that are very similar to well-known properties of homomorphisms, such as the promotion properties. The recursive pattern involved is well known: it is essentially the same as the standard pattern used in the so-called elimination rules for a data type in constructive type theory (see, e.g., [1]). The specific investigation of which these results form a part is not complete; rather, it has barely begun. There is some evidence that the approach can be generalised to other recursive patterns, possibly giving rise to a more elegant theory than expounded in this snapshot.

A few words are in order on the proof methods used here, and on the notation. The current pace of development of proof methods is so rapid that, although I valiantly tried to use the best techniques I knew in constructing the proofs in this paper, I now think of them as being thoroughly outdated. This is mainly due to the work of Roland Backhouse and his crew at Groningen University; using their techniques, some of the lenghthier proofs given here, requiring mildly excruciating symbol manipulation, can be presented in one or two extremely simple calculation steps! Since there is, at the time of writing, no published account of these developments, I have refrained from updating the proofs.

As to the notation, I have taken the liberty (as in all my other papers in this area) to conduct some further notational experiments. While deviation from "established" notation is hard on the reader, most current notations were clearly not designed with a view to the exigencies of calculation. Where notation is concerned, an attempt has been made to make this paper reasonably self-contained. However, not all non-standard notations are formally introduced—namely when their meaning can be inferred from the context.

A convention here, as well as in [8], is to treat values of type A as nullary functions of type $A \longleftarrow \mathbf{1}$. This makes it possible to denote function application unambiguously as function composition, for which the symbol $\bullet$ is used. Within functional expressions this operator has the lowest precedence.

1 The problem

Structural induction is the traditional technique for proving the equality of two functions that are defined on an inductively defined domain. Such functional equalities can also be proved by calculation in an equational proof style. This is based on the fact that, under a suitably chosen algebraic viewpoint, these functions are homomorphisms whose source algebra (an "algebraic data type") is initial. It is then possible to invoke elementary algebraic tools that replace the induction proofs (GOGUEN[4]). In particular, the *Unique Extension Property* and the *Promotion Theorem* for that source algebra provide the same proof-theoretic power as structural induction.

An examination of the proof obligations under the two approaches—traditional induction and algebra—reveals that they are ultimately identical. Thus it would seem that nothing is gained by using the homomorphic approach. However, the reduction in the labour needed to record the full proof is striking, especially when combined with a dummy-free style.

The explanation of this phenomenon is simple. A proof by structural induction follows a fixed ritual, that is repeated for each next proof. In the algebraic theorems, this proof has been given once and for all; what remains as the applicability condition is the heart of the matter. Moreover, the adoption of the algebraic viewpoint makes it possible to give concise notations for inductively defined functions[7, 2, 3], reducing the formal labour further.

The straightforward algebraic approach fails, however, when the definitional pattern of a function does not mimic the structural pattern of its domain. There is a standard trick that often makes it possible to apply the algebraic methods in such cases: 'tuple' the function concerned together with the identity function, thus giving another function that *is* a homomorphism. Unfortunately, this method entails much formal overhead, making it less attractive for practical use.

In this paper we develop a generic extension of the theory that caters for a slightly more general class of definitional patterns. The term 'generic' here means that the theory applies to all inductively defined data types.

2 A simple example

A simple inductive data type is formed by the naturals, with a unary constructor succ and a nullary constructor 0. Consider the following pattern of functional equations (with a function dummy F):

$$(1) \qquad \Pi(F) := (F \bullet \mathsf{succ} = s \bullet F) \wedge (F \bullet \mathsf{0} = z) \quad .$$

This pattern has two yet unbound function variables, a unary $s \in A \longleftarrow A$ and a nullary $z \in A \longleftarrow \mathbf{1}$, where A is some type. Given bindings for s and z, a function satisfying Π is a homomorphism from the algebra of the naturals with signature (succ, 0) to the algebra on A with signature $(s,\ z)$. Since the algebra of naturals is defined as the initial algebra in this category, there exists—by the definition of 'initial'—*exactly one* such homomorphism for each choice of $(s,\ z)$. Therefore this is a means for defining functions on the naturals. Moreover, given two functions $f,\ g \in A \longleftarrow \mathcal{N}$, we have

$$f = g \quad \Leftarrow \quad \Pi(f) \wedge \Pi(g) \quad .$$

This is the *Unique Extension Property* for the naturals. It can be seen that the task of proving one functional equality is replaced by the obligation of proving two times (for this data type) two such equalities, which however tend to be simpler. To invoke this instrument, a suitable instantiation of s and z must be chosen, but if one of the two functions is inductively defined, not only is the necessary instantiation known, but we also have for free that that function satisfies Π.

After having established $\Pi(f)$ and $\Pi(g)$, the induction approach to conclude to $f = g$ still has to go through the following ritual steps:

Basis:

$$\begin{array}{ll} & f \bullet \mathsf{0} = g \bullet \mathsf{0} \\ \equiv & \qquad \{(1)\text{: } \Pi(f),\ \Pi(g)\} \\ & z = z \end{array}$$

$$\begin{array}{ll}
\equiv & \qquad \{\text{reflexivity of } =\} \\
 & \mathsf{true} \quad .
\end{array}$$

Step:

$$\begin{array}{ll}
 & f \bullet \mathsf{succ} \bullet n \;=\; g \bullet \mathsf{succ} \bullet n \\
\equiv & \qquad \{(1)\text{: } \Pi(f),\ \Pi(g)\} \\
 & s \bullet f \bullet n \;=\; s \bullet g \bullet n \\
\Leftarrow & \qquad \{\text{Leibniz}\} \\
 & f \bullet n \;=\; g \bullet n \\
\equiv & \qquad \{\text{Induction Hypothesis}\} \\
 & \mathsf{true} \quad .
\end{array}$$

End of ritual steps.

The more complicated the inductive construction of the data type, the longer these rites.

Of course, in many cases the proof of the equality of two functions can be given purely equationally without appealing to either induction or these algebraic tools—otherwise no proof would be possible at all, since the common proof obligation has the shape of a set of functional equalities. Somewhat surprisingly, it turns out that often such a proof can also be substantially shortened by appealing to the Unique Extension Property.

Not all functions on the naturals are homomorphisms. Attempts to prove a (valid) functional equality for a non-homomorphic function by appeal to the Unique Extension Property are doomed to fail, and, in fact, even for homomorphisms success is not guaranteed. An example is the factorial function *fac* : there exists no *simple* function s such that $\Pi(\mathit{fac})$ holds. However, there are simple functions $\oplus$ and z such that $\Pi\Pi(\mathit{fac})$ holds, where $\Pi\Pi$ is the pattern given by

$$\Pi\Pi(F) \;:=\; (F \bullet \mathsf{succ} \;=\; F \otimes\hat{}\ \mathsf{id}) \wedge (F \bullet \mathsf{0} \;=\; z) \quad .$$

(Here $\otimes$ is a binary function; between two functions returning naturals $\otimes\hat{}$ then denotes the application of $\otimes$ to the results of these functions.) The instantiation that gives the factorial function is that in which $\otimes$ is taken to be the operation such that $m \otimes n \;=\; m \times (\mathsf{succ} \bullet n)$, and z is 1.

Like Π before, $\Pi\Pi$ has a unique solution for each choice for the unbound functions, in this case $\oplus$ and z. So the following is a valid statement:

$$f \;=\; g \quad\Leftarrow\quad \Pi\Pi(f) \wedge \Pi\Pi(g) \quad .$$

This can be shown to follow from the Unique Extension Property. But the proof of this is (even for a simple type like the naturals) non-obvious, lengthy, and in fact a new ritual that can be avoided by a properly designed extension of the theory.

3 Functors

Category theory provides some concepts that have proven indispensable in the formulation of generic theory, paramount among which is the notion of a functor. We give a treatment here slightly geared towards our purposes. In particular, we handle only the unary case, although the type constructors $\|$ and ⧺ introduced below are also (binary) functors.

A functor is a pair of functions, one acting on types, and one on functions, with some further properties as stated below.

The application of a functor is denoted as a postfix operation. A functor $\dagger$ assigns to each type A a type $A\dagger$, and to each function $f \in A \longleftarrow B$ a function $f\dagger \in A\dagger \longleftarrow B\dagger$, where the latter mapping preserves function composition and identity; more precisely:

(2) $\qquad (f \bullet g)\dagger \;=\; f\dagger \bullet g\dagger \quad ,$

(3) $\qquad \mathsf{id}\dagger \;=\; \mathsf{id} \quad .$

Equality (2) requires that $f \bullet g$ is well-typed; this is viewed as a well-formedness condition that applies in general to all constituents of functional expressions, and is from now on left implicit. In denoting an identity function, as in (3), its type is not stated, but in any context id is assumed to have a specific type, and so (3) stands for as many equalities as there are types.

An appeal to these equalities will be indicated in the justification of a proof step by "$\dagger$ is a functor".

An important type constructor is $\|$. In category theory this is usually denoted by $\times$. It has a corresponding action on functions. (In [8] I used different notations for $\|$ on types and on functions, which was a bad idea.) It is informally defined by:

$$
\begin{array}{lcl}
A \,\|\, B & := & \text{“the type whose elements are the pairs } (a, b) \\
 & & \quad \text{for } a \in A \text{ and } b \in B, \\
f \,\|\, g & := & \text{“the function that, applied to a pair } (a, b), \\
 & & \quad \text{returns the pair } ((f \bullet a), (g \bullet b)).
\end{array}
$$

We have the usual “projection functions” from $A \,\|\, B$ to A and B, which are denoted as:

$$
\begin{array}{l}
\ll \,\in\, A \longleftarrow A \,\|\, B \quad , \\
\gg \,\in\, B \longleftarrow A \,\|\, B \quad ,
\end{array}
$$

We also need the combinator that combines two functions $f \in A \longleftarrow C$ and $g \in B \longleftarrow C$ into one function

$$f \Uparrow g \in A \,\|\, B \longleftarrow C \quad .$$

(The usual category-theory notation is (f, g).)

The relevant properties that we shall have occasion to use are:

$$
\begin{array}{lrcl}
(4) & F \Uparrow G \bullet H & = & (F \bullet H) \Uparrow (G \bullet H) \\
(5) & f \,\|\, g \bullet F \Uparrow G & = & (f \bullet F) \Uparrow (g \bullet G) \\
(6) & \ll \bullet\, F \Uparrow G & = & F \\
(7) & \gg \bullet\, F \Uparrow G & = & G \\
(8) & \ll \Uparrow \gg & = & \mathsf{id} \quad .
\end{array}
$$

A fact that we shall also use is that any mapping $\Uparrow F$, i.e., mapping a function f with the same domain as F to the function $f \Uparrow F$, is a bijection (since composition to the left with $\ll$ undoes the mapping), so that

$$(9) \qquad f = g \;\equiv\; f \Uparrow F = g \Uparrow F \quad .$$

For discussing the application of the theory we need the dual type constructor $\Downarrow$, which forms the “disjoint” or “tagged” union. The usual category-theory notation is $+$. Informally,

$$\begin{array}{lcl} A \mathbin{\|\!\!\!\vee} B & := & \text{“the type whose elements are the union of the} \\ & & \quad \text{elements of } A \text{ and } B\text{, tagged with the origin} \\ & & \quad \text{of an element (left or right)”,} \end{array}$$

$$\begin{array}{lcl} f \mathbin{\|\!\!\!\vee} g & := & \text{“the function that, for a left-tagged value a} \\ & & \quad \text{returns the left-tagged value } f \bullet \text{a, and for a} \\ & & \quad \text{right-tagged value } b \text{ the right-tagged value} \\ & & \quad g \bullet b\text{”.} \end{array}$$

There are “injection functions” from each of A and B to $A \mathbin{\|\!\!\!\vee} B$, which are not needed here, and a combinator that combines two functions $f \in C \longleftarrow A$ and $g \in C \longleftarrow B$ into one function

$$f \mathbin{\|\!\!\!\diamond} g \in C \longleftarrow A \mathbin{\|\!\!\!\vee} B \quad ,$$

which amounts to applying f to left-tagged, and g to right-tagged values, thereby loosing the tag information. (The usual category-theory notation is $[f,\ g]$.) There are similar (but dual) properties to those given for $\|$ and friends, which are not listed here since they will not be used.

From functors and $\|$ and $\mathbin{\|\!\!\!\vee}$, we can form new functors. Functors can be formed by the composition of two functors, which is denoted by juxtaposition:

$$\begin{array}{lcl} A(\dagger\ddagger) & := & (A\dagger)\,\ddagger \quad , \\ f\,(\dagger\ddagger) & := & (f\dagger)\,\ddagger \quad . \end{array}$$

If B is some type, $\|\,B$ and $\mathbin{\|\!\!\!\vee} B$ are functors, defined by

$$\begin{array}{lcl} A(\,\|\,B) & := & A\,\|\,B \quad , \\ f\,(\,\|\,B) & := & f\,\|\,\mathsf{id} \quad , \end{array}$$

and

$$\begin{array}{lcl} A(\,\mathbin{\|\!\!\!\vee} B) & := & A \mathbin{\|\!\!\!\vee} B \quad , \\ f\,(\,\mathbin{\|\!\!\!\vee} B) & := & f \mathbin{\|\!\!\!\vee} \mathsf{id} \quad . \end{array}$$

Combining this, we have, e.g., that $(\,\|\,B)(\,\mathbin{\|\!\!\!\vee}\mathbf{1})$ is a functor, with

$$A((\,\|\,B)(\,\mathbin{\|\!\!\!\vee}\mathbf{1})) = (A\,\|\,B) \mathbin{\|\!\!\!\vee}\mathbf{1} \quad .$$

4 Types as initial fixed points

The treatment in this section is mainly based on work by MALCOLM[6, 5]. Functors can be used to characterise a class of algebras with compatible signatures. If $\dagger$ is a functor, it characterises the class of algebras $(A,\ \phi)$, in which A is some type and the signature is

$$\phi \in A \longleftarrow A\dagger \quad .$$

(For simplicity, we do not consider here the possibility of laws on the algebra. The theory developed here applies, nevertheless, equally to algebras with laws.)

For example, in the algebra of naturals $(\mathcal{N},\ \mathsf{succ} \mathbin{\nabla} 0)$ the signature has type

$$\mathsf{succ} \mathbin{\nabla} 0 \in \mathcal{N} \longleftarrow \mathcal{N} \mathbin{+\!\!\!\!\|} \mathbf{1} \quad ,$$

(which is equivalent to: $(\mathsf{succ} \in \mathcal{N} \longleftarrow \mathcal{N}) \wedge (0 \in \mathcal{N} \longleftarrow \mathbf{1})$), so it belongs to the class characterised by the functor $\mathbin{+\!\!\!\!\|}\mathbf{1}$.

If $(A,\ \phi)$ and $(B,\ \psi)$ are two $\dagger$-algebras, then $h \in A \longleftarrow B$ is called a *homomorphism* between these algebras when:

$$\phi \bullet h\dagger \ = \ h \bullet \psi \quad .$$

We introduce a concise notation for the homomorphic property:

$$(10) \qquad F \in \phi \xleftarrow{\ \dagger\ } \psi \ := \ \phi \bullet F\dagger \ = \ F \bullet \psi \quad .$$

An algebra is called *initial* in the class of $\dagger$-algebras if there is a unique homomorphism from it to each algebra in the class. If two algebras in the same class are initial, they are isomorphic: each can be obtained from the other by renaming. We assume that we can fix some representative, which is then called *the* initial algebra. For all functors introduced in this paper the class of algebras has an initial element. The initial algebra for $\dagger$ is denoted by $\mu(\dagger)$.

If we have

$$(L,\ \mathsf{in}) \ = \ \mu(\dagger) \quad ,$$

then it can be shown (only for the lawless case!) that L and $L\dagger$ are isomorphic, which is the reason to call the type L the initial *fixed point* of $\dagger$.

So the naturals can be defined by:

$$(\mathcal{N},\ \mathsf{succ} \mathbin{\triangledown\!\!\!\!|}\ 0) \ := \ \mu(\ \mathbin{+\!\!\!\!\|}\mathbf{1}) \quad .$$

The non-empty "snoc" lists over the base type A can likewise be defined by:

$$(A*,\ \mathbin{-\!\!\!\!\prec} \mathbin{\triangledown\!\!\!\!|} \Box) \ := \ \mu((\,\|\,A)(\ \mathbin{+\!\!\!\!\|}\mathbf{1})) \quad .$$

Let $(L,\ \mathsf{in})$ be the initial algebra $\mu(\dagger)$ for some functor $\dagger$. A function $\phi \in A \longleftarrow A\dagger$ determines uniquely an algebra $(A,\ \phi)$, and therefore a unique homomorphism $h \in\ A \longleftarrow L$, that is, a function h satisfying

$$h \in \phi \xleftarrow{\dagger} \mathsf{in} \quad .$$

Denote it by $(\!|\phi|\!)$. It is useful to have a term for these homomorphisms whose domain is an initial algebra, and to this end we coin the term *catamorphism*. So we now have the following characterisation of catamorphisms:

CATAMORPHISM:

(11) $\qquad h \ = \ (\!|\phi|\!) \ \ \equiv \ \ h \in \phi \xleftarrow{\dagger} \mathsf{in} \quad ,$

which we shall also invoke in the equivalent version

(12) $\qquad h \ = \ (\!|\phi|\!) \ \ \equiv \ \ \phi \bullet h\dagger \ = \ h \bullet \mathsf{in} \quad ,$

obtained by unfolding definition (10), and in the weaker version

(13) $\qquad \phi \bullet (\!|\phi|\!)\dagger \ = \ (\!|\phi|\!) \bullet \mathsf{in} \quad ,$

obtained by taking $h \ := \ (\!|\phi|\!)$.

The following two are now (almost) immediate:

UNIQUE EXTENSION PROPERTY (UEP):

$$f \ = \ g \quad \Leftarrow \quad (f \in \phi \xleftarrow{\dagger} \mathsf{in}) \wedge (g \in \phi \xleftarrow{\dagger} \mathsf{in}) \quad .$$

IDENTITY CATAMORPHISM:

(14) $\quad ([\mathsf{in}]) \;=\; \mathsf{id} \;\in\; L \longleftarrow L \quad .$

Another easy consequence is:

PROMOTION:

$$([\phi]) \;=\; f \bullet ([\psi]) \quad \Leftarrow \quad f \in \phi \overset{\dagger}{\longleftarrow} \psi \quad .$$

All functions defined on an initial type that have a left inverse are catamorphisms. For let $f \in A \longleftarrow L$ and $g \in L \longleftarrow A$ be two functions. Then

(15) $\quad f \;=\; ([f \bullet \mathsf{in} \bullet g\dagger]) \quad \Leftarrow \quad g \bullet f \;=\; \mathsf{id} \quad .$

Proof.

$$
\begin{array}{ll}
 & f \;=\; ([f \bullet \mathsf{in} \bullet g\dagger]) \quad . \\
\equiv & \qquad \{(12)\text{: Catamorphism}\} \\
 & f \bullet \mathsf{in} \bullet g\dagger \bullet f\dagger \;=\; f \bullet \mathsf{in} \\
\equiv & \qquad \{\mathsf{id} \text{ is identity of } \bullet\} \\
 & f \bullet \mathsf{in} \bullet g\dagger \bullet f\dagger \;=\; f \bullet \mathsf{in} \bullet \mathsf{id} \\
\equiv & \qquad \{(2,3):\ \dagger \text{ is a functor}\} \\
 & f \bullet \mathsf{in} \bullet (g \bullet f)\dagger \;=\; f \bullet \mathsf{in} \bullet \mathsf{id}\dagger \\
\Leftarrow & \qquad \{\text{Leibniz}\} \\
 & g \bullet f \;=\; \mathsf{id} \quad .
\end{array}
$$

End of proof.

A function $f \in A \longleftarrow L$ need not be a catamorphism, but the result of tupling it with the identity function, namely $f \Uparrow \mathsf{id} \in A \,||\, L \longleftarrow L$, always is, for it has, by (7), a left inverse $\gg$. So, by instantiating (15), we obtain:

FIRST TUPLING LEMMA:

(16) $\quad f \Uparrow \mathsf{id} \;=\; ([f \Uparrow \mathsf{id} \bullet \mathsf{in} \bullet \gg\dagger]) \quad .$

5 Paramorphisms

Throughout this and the next section $(L,\ \mathsf{in})$ denotes the initial algebra $\mu(\dagger)$ for some functor $\dagger$.

Define, for $\phi \in A \longleftarrow (A \parallel L)\dagger$,

(17) $\quad \surd\phi \ := \ \phi \Uparrow (\mathsf{in} \bullet \gg\!\dagger) \ \in A \parallel L \longleftarrow (A \parallel L)\dagger \quad .$

The notation $\surd\phi$ introduced here serves merely as a shorthand and is purely local to this section.

Define, furthermore, for ϕ as above,

(18) $\quad [\![\phi]\!] \ := \ \ll \bullet \llparenthesis \surd\phi \rrparenthesis \ \in A \longleftarrow L \quad .$

Functions expressed in this form will be called *paramorphisms*. The actual notation used here is provisional, but is chosen to be reminiscent of the notation $\llparenthesis \phi \rrparenthesis$ used for catamorphisms.

We have seen that a function $\phi \in A \longleftarrow A\dagger$ determines a function of type $A \longleftarrow L$ with certain important properties, namely the catamorphism $\llparenthesis \phi \rrparenthesis$, and also that not all functions with source type L can be obtained this way, since not all are catamorphisms.

A function $\phi \in A \longleftarrow (A \parallel L)\dagger$ also determines a function of type $A \longleftarrow L$, namely $[\![\phi]\!]$. Not only are, as we shall see, *all* functions with source type L expressible in this form, but—somewhat surprisingly in the light of the generality—it will also turn out that we still have properties that are very similar to the Unique Extension Property and the Promotion rule.

First we show the generality of the construction by determining, for a given $f \in A \longleftarrow L$, a function ϕ such that $f \ = \ [\![\phi]\!]$:

$$
\begin{array}{ll}
 & f \\
= & \qquad \{(6)^{\smile}\colon\ F \ = \ \ll \bullet F \Uparrow G\} \\
 & \ll \bullet f \Uparrow \mathsf{id} \\
= & \qquad \{(16)\text{: First Tupling Lemma}\} \\
 & \ll \bullet \llparenthesis f \Uparrow \mathsf{id} \bullet \mathsf{in} \bullet \gg\!\dagger \rrparenthesis \\
= & \qquad \{(4)\colon\ F \Uparrow G \bullet H \ = \ (F \bullet H) \Uparrow (G \bullet H)\}
\end{array}
$$

$$
\begin{array}{ll}
 & \ll \bullet (\!|(f \bullet \mathsf{in} \bullet \gg\dagger) \Uparrow (\mathsf{in} \bullet \gg\dagger)|\!) \\
= & \qquad \{\phi := f \bullet \mathsf{in} \bullet \gg\dagger\} \\
 & \ll \bullet (\!|\phi \Uparrow (\mathsf{in} \bullet \gg\dagger)|\!) \\
= & \qquad \{(17)\text{: } \surd\phi\} \\
 & \ll \bullet (\!|\surd\phi|\!) \\
= & \qquad \{(18)\text{: } [\![\phi]\!]\} \\
 & [\![\phi]\!] \quad .
\end{array}
$$

Remember that (16), used in the second step in this calculation, was based on expressing the injective function $f \Uparrow \mathsf{id}$ as a catamorphism. So for the particular instantiation of ϕ used above we could as easily prove that $\gg \bullet (\!|\surd\phi|\!) = \mathsf{id}$. However, the validity of this functional equality is not dependent on the instantiation of ϕ:

CLAIM: For $\phi \in A \longleftarrow (A \,\|\, L)\dagger$,

(19) $\quad \gg \bullet (\!|\surd\phi|\!) = \mathsf{id} \in L \longleftarrow L \quad .$

Proof. First we reduce the functional equality to another one:

$$
\begin{array}{ll}
 & \gg \bullet (\!|\surd\phi|\!) = \mathsf{id} \\
\equiv & \qquad \{(14)\text{: Identity catamorphism}\} \\
 & \gg \bullet (\!|\surd\phi|\!) = (\!|\mathsf{in}|\!) \\
\equiv & \qquad \{(12)\text{: Catamorphism}\} \\
 & \mathsf{in} \bullet (\gg \bullet (\!|\surd\phi|\!))\dagger = \gg \bullet (\!|\surd\phi|\!) \bullet \mathsf{in} \quad .
\end{array}
$$

The last equality is proved thus:

$$
\begin{array}{ll}
 & \mathsf{in} \bullet (\gg \bullet (\!|\surd\phi|\!))\dagger \\
= & \qquad \{(2)\text{: } \dagger \text{ is a functor}\} \\
 & \mathsf{in} \bullet \gg\dagger \bullet (\!|\surd\phi|\!)\dagger \\
= & \qquad \{(7)^{\smile}\text{: } G = \gg \bullet F \Uparrow G\} \\
 & \gg \bullet \phi \Uparrow (\mathsf{in} \bullet \gg\dagger) \bullet (\!|\surd\phi|\!)\dagger \\
= & \qquad \{(17)\text{: } \surd\phi\} \\
 & \gg \bullet \surd\phi \bullet (\!|\surd\phi|\!)\dagger
\end{array}
$$

$=$ $\qquad \{(13)\text{: Catamorphism (weak version)}\}$

$\quad \gg \bullet (\!|\sqrt{\phi}|\!) \bullet \mathsf{in} \quad .$

End of proof.

(Remark. It is likely that a one-step proof of this claim could be given, based on theory about some "generically defined" functions being uniquely determined by their types. As far as I am aware, the currently developed theory is not yet powerful enough for this.)

The result just proved can be nicely combined with the definition of $[[\phi]]$, giving:

SECOND TUPLING LEMMA:

(20) $\qquad [[\phi]] \Uparrow \mathsf{id} \;=\; (\!|\sqrt{\phi}|\!) \quad .$

Proof.

$\quad [[\phi]] \Uparrow \mathsf{id}$

$=$ $\qquad \{(19)\text{: above claim}\}$

$\quad [[\phi]] \Uparrow (\gg \bullet (\!|\sqrt{\phi}|\!))$

$=$ $\qquad \{(18)\text{: } [[\phi]]\}$

$\quad (\ll \bullet (\!|\sqrt{\phi}|\!)) \Uparrow (\gg \bullet (\!|\sqrt{\phi}|\!))$

$=$ $\qquad \{(4)^{\smile}\text{: } (F \bullet H) \Uparrow (G \bullet H) \;=\; F \Uparrow G \bullet H\}$

$\quad \ll \Uparrow \gg \bullet (\!|\sqrt{\phi}|\!)$

$=$ $\qquad \{(8)\text{: } \ll \Uparrow \gg \;=\; \mathsf{id}\}$

$\quad (\!|\sqrt{\phi}|\!) \quad .$

End of proof.

We are now ready to obtain the central result, namely a unique characterisation for paramorphisms. From it the other, calculationally possibly more important, properties follow easily.

PARAMORPHISM:

(21) $\qquad f \;=\; [[\phi]] \;\;\equiv\;\; \phi \bullet (f \Uparrow \mathsf{id})\dagger \;=\; f \bullet \mathsf{in} \quad .$

Proof.

$$f \;=\; [[\phi]]$$

$$\equiv \qquad \{(9)\text{: } {\Uparrow} F \text{ is a bijection}\}$$

$$f \Uparrow \mathsf{id} \;=\; [[\phi]] \Uparrow \mathsf{id}$$

$$\equiv \qquad \{(20)\text{: Second Tupling Lemma}\}$$

$$f \Uparrow \mathsf{id} \;=\; (\!|\surd\phi|\!)$$

$$\equiv \qquad \{(12)\text{: Catamorphism}\}$$

$$\surd\phi \bullet (f \Uparrow \mathsf{id})\dagger \;=\; f \Uparrow \mathsf{id} \bullet \mathsf{in}$$

$$\equiv \qquad \{(17)\text{: } \surd\phi\}$$

$$\phi \Uparrow (\mathsf{in} \bullet \gg\dagger) \bullet (f \Uparrow \mathsf{id})\dagger \;=\; f \Uparrow \mathsf{id} \bullet \mathsf{in}$$

$$\equiv \qquad \{(4)\text{: } F \Uparrow G \bullet H \;=\; (F \bullet H) \Uparrow (G \bullet H) \text{ (both sides)}\}$$

$$(\phi \bullet (f \Uparrow \mathsf{id})\dagger) \Uparrow (\mathsf{in} \bullet \gg\dagger \bullet (f \Uparrow \mathsf{id})\dagger) \;=\; (f \bullet \mathsf{in}) \Uparrow (\mathsf{id} \bullet \mathsf{in})$$

$$\equiv \qquad \{(2)^{\smile}\text{: } \dagger \text{ is a functor}\}$$

$$(\phi \bullet (f \Uparrow \mathsf{id})\dagger) \Uparrow (\mathsf{in} \bullet (\gg \bullet f \Uparrow \mathsf{id})\dagger) \;=\; (f \bullet \mathsf{in}) \Uparrow (\mathsf{id} \bullet \mathsf{in})$$

$$\equiv \qquad \{(7)\text{: } \gg \bullet F \Uparrow G \;=\; G\}$$

$$(\phi \bullet (f \Uparrow \mathsf{id})\dagger) \Uparrow (\mathsf{in} \bullet \mathsf{id}\dagger) \;=\; (f \bullet \mathsf{in}) \Uparrow (\mathsf{id} \bullet \mathsf{in})$$

$$\equiv \qquad \{(3)^{\smile}\text{: } \dagger \text{ is a functor; } \mathsf{id} \text{ is identity (both sides)}\}$$

$$(\phi \bullet (f \Uparrow \mathsf{id})\dagger) \Uparrow \mathsf{in} \;=\; (f \bullet \mathsf{in}) \Uparrow \mathsf{in}$$

$$\equiv \qquad \{(9)^{\smile}\text{: } {\Uparrow} F \text{ is a bijection}\}$$

$$(\phi \bullet (f \Uparrow \mathsf{id})\dagger) \;=\; f \bullet \mathsf{in} \quad .$$

End of proof.

The substitution $f := [[\phi]]$ gives the weaker version

$$(22) \qquad \phi \bullet ([[\phi]] \Uparrow \mathsf{id})\dagger \;=\; [[\phi]] \bullet \mathsf{in} \quad .$$

The uniqueness gives us:

UEP FOR PARAMORPHISMS:

$$f \;=\; g \quad \Leftarrow \quad (\phi \bullet (f \Uparrow \mathsf{id})\dagger \;=\; f \bullet \mathsf{in}) \wedge (\phi \bullet (g \Uparrow \mathsf{id})\dagger \;=\; g \bullet \mathsf{in}) \quad .$$

Whereas for catamorphisms the unique characterisation involves a condition of the same form as for the promotion law, here we find a divergence. The analogon of the promotion law for paramorphisms is:

PARAMORPHISM PROMOTION:

(23) $$[\![\phi]\!] \;=\; f\bullet[\![\psi]\!] \quad\Leftarrow\quad \phi\bullet(f\parallel\mathsf{id})\dagger \;=\; f\bullet\psi \quad .$$

Proof.

$$
\begin{array}{ll}
 & [\![\phi]\!] \;=\; f\bullet[\![\psi]\!] \\
\equiv & \qquad \{(21)\text{: Paramorphism}\} \\
 & \phi\bullet((f\bullet[\![\psi]\!])\Uparrow\mathsf{id})\dagger \;=\; f\bullet[\![\psi]\!]\bullet\mathsf{in} \\
\equiv & \qquad \{\mathsf{id}\text{ is identity of }\bullet\} \\
 & \phi\bullet((f\bullet[\![\psi]\!])\Uparrow(\mathsf{id}\bullet\mathsf{id}))\dagger \;=\; f\bullet[\![\psi]\!]\bullet\mathsf{in} \\
\equiv & \qquad \{(5)^{\smile}\text{: } (f\bullet F)\Uparrow(g\bullet G) \;=\; f\parallel g\bullet F\Uparrow G\} \\
 & \phi\bullet(f\parallel\mathsf{id}\bullet[\![\psi]\!]\Uparrow\mathsf{id})\dagger \;=\; f\bullet[\![\psi]\!]\bullet\mathsf{in} \\
\equiv & \qquad \{(2)\text{: } \dagger\text{ is a functor}\} \\
 & \phi\bullet(f\parallel\mathsf{id})\dagger\bullet([\![\psi]\!]\Uparrow\mathsf{id})\dagger \;=\; f\bullet[\![\psi]\!]\bullet\mathsf{in} \\
\equiv & \qquad \{(22)^{\smile}\text{: Paramorphism (weak version)}\} \\
 & \phi\bullet(f\parallel\mathsf{id})\dagger\bullet([\![\psi]\!]\Uparrow\mathsf{id})\dagger \;=\; f\bullet\psi\bullet([\![\psi]\!]\Uparrow\mathsf{id})\dagger \\
\Leftarrow & \qquad \{\text{Leibniz}\} \\
 & \phi\bullet(f\parallel\mathsf{id})\dagger \;=\; f\bullet\psi \quad .
\end{array}
$$

End of proof.

6 Relationship with catamorphisms

We shall see now two ways in which paramorphisms and catamorphisms are related.

Firstly, paramorphisms can be viewed as a generalisation of catamorphisms, in the sense that the characterisation for catamorphisms, (12), follows formally from that for paramorphisms, (21). To show this we have to express a catamorphism as a paramorphism. The crucial result is:

(24) $$h \;=\; [\![\phi\bullet\ll\dagger]\!] \quad\Leftarrow\quad \phi\bullet h\dagger \;=\; h\bullet\mathsf{in} \quad .$$

Proof.

$$
\begin{array}{ll}
 & h \;=\; [\![\phi \bullet \ll\dagger]\!] \\
\equiv & \qquad \{(21)\text{: Paramorphism}\} \\
 & \phi \bullet \ll\dagger \;\bullet (h \Uparrow \mathsf{id})\dagger \;=\; h \bullet \mathsf{in} \\
\equiv & \qquad \{(2)\text{: } \dagger \text{ is a functor}\} \\
 & \phi \bullet (\ll \bullet\, h \Uparrow \mathsf{id})\dagger \;=\; h \bullet \mathsf{in} \\
\equiv & \qquad \{(6)\text{: } \ll \bullet\, F \Uparrow G \;=\; F\} \\
 & \phi \bullet h\dagger \;=\; h \bullet \mathsf{in} \quad .
\end{array}
$$

End of proof.

The right-hand side of (24) is precisely the equivalent of $h \;=\; (\![\phi]\!)$ figuring in (12); in other words, considering paramorphisms as primitive, $[\![\phi \bullet \ll\dagger]\!]$ can be viewed as a new definition of the catamorphism $(\![\phi]\!)$. With this definition, then, (24) states the same as (12).

Secondly, note that the condition in the rule for paramorphism promotion, (23), can be expressed as a homomorphic property, namely as follows. Let $\ddagger$ denote the functor $(\;\|\, L)\dagger$, that is,

$$
\begin{array}{llcll}
(25) & A\ddagger & = & (A \,\|\, L)\,\dagger & , \\
(26) & f\ddagger & = & (f \,\|\, \mathsf{id})\,\dagger & .
\end{array}
$$

Then

$$
\begin{array}{ll}
 & f \in \phi \xleftarrow{\ddagger} \psi \\
\equiv & \qquad \{(10)\text{: homomorphic property}\} \\
 & \phi \bullet f\ddagger \;=\; f \bullet \psi \\
\equiv & \qquad \{(26)\} \\
 & \phi \bullet (f \,\|\, \mathsf{id})\dagger \;=\; f \bullet \psi \quad ,
\end{array}
$$

which is precisely the condition of (23). So a "parapromotable" function with respect to $\dagger$ is a true homomorphism in the category of $\ddagger$-algebras.

Put $(M,\ \mathsf{IN}) \;:=\; \mu(\ddagger)$, in which we use IN as notation for the constructor to avoid confusion with the constructor in of L. We have $\mathsf{IN} \in M \longleftarrow M\ddagger$, or, equivalently, expanding $\ddagger$ by means of (25),

$$
\mathsf{IN} \in M \longleftarrow (M \,\|\, L)\dagger \quad .
$$

Therefore IN has a type that makes the form $[\![\mathsf{IN}]\!]$ meaningful. We give a name to this paramorphism:

$$(27)\qquad \mathit{preds} := [\![\mathsf{IN}]\!] \;\in M \longleftarrow L \quad .$$

Now it turns out that all paramorphisms can be formed from this particular one by the composition with a catamorphism on the type M. To make explicit that these catamorphisms are defined on the initial ‡-algebra, rather than the †-algebra as until now, we write them as $(\![\phi]\!)_\ddagger$. The result is then:

$$[\![\phi]\!] \;=\; (\![\phi]\!)_\ddagger \bullet \mathit{preds} \quad .$$

Proof.

$$\begin{array}{cl}
 & [\![\phi]\!] \;=\; (\![\phi]\!)_\ddagger \bullet \mathit{preds} \\
\equiv & \qquad \{(27)\text{: } \mathit{preds}\} \\
 & [\![\phi]\!] \;=\; (\![\phi]\!)_\ddagger \bullet [\![\mathsf{IN}]\!] \\
\Leftarrow & \qquad \{(23)\text{: Paramorphism promotion}\} \\
 & \phi \bullet ((\![\phi]\!)_\ddagger \,\|\, \mathsf{id})\dagger \;=\; (\![\phi]\!)_\ddagger \bullet \mathsf{IN} \\
\equiv & \qquad \{(26)^{\smile}\text{: } \ddagger\} \\
 & \phi \bullet (\![\phi]\!)_\ddagger\ddagger \;=\; (\![\phi]\!)_\ddagger \bullet \mathsf{IN} \\
\equiv & \qquad \{(13)\text{: Catamorphism (weak version)}\} \\
 & \mathsf{true} \quad .
\end{array}$$

End of proof.

With this as a basis, it is trivial to prove the promotion rule (23) for paramorphisms.

To conclude, we examine what this means for the initial example, the factorial function *fac*. Here $L := \mathcal{N}$, which is obtained by taking the initial fixed point of $\dagger := \Vert\!\!\!\curlyvee\mathbf{1}$. Putting

$$\begin{array}{lcl}
\otimes & := & \times \bullet (\mathsf{id} \,\|\, \mathsf{succ}) \quad , \\
1 & := & \mathsf{succ} \bullet 0 \quad ,
\end{array}$$

the recursive definition pattern of *fac* can be expressed as

$$\otimes \mathbin{\text{⇟}} 1 \bullet (\mathit{fac} \Uparrow \mathsf{id}) \mathbin{\text{⫲}} \mathsf{id} \;=\; \mathit{fac} \bullet \mathsf{succ} \mathbin{\text{⇟}} 0 \quad ,$$

which equivales, by (21),

$$\mathit{fac} \;=\; [\![\otimes \mathbin{\text{⇟}} 1]\!] \quad .$$

We have, further, $\ddagger \;=\; (\,\|\,\mathcal{N})(\mathbin{\text{⫲}}\mathbf{1})$. Then (M, IN) is $(\mathcal{N}*, \mathbin{\text{⤙}} \mathbin{\text{⇟}} \square)$, the algebra of the finite lists of naturals, and thus $\mathit{preds} \in \mathcal{N}* \longleftarrow \mathcal{N}$. It satisfies, by (21) with the proper instantiations, the pattern

$$\mathbin{\text{⤙}} \mathbin{\text{⇟}} \square \bullet (\mathit{preds} \Uparrow \mathsf{id}) \mathbin{\text{⫲}} \mathsf{id} \;=\; \mathit{preds} \bullet \mathsf{succ} \mathbin{\text{⇟}} 0 \quad ,$$

which in a more traditional style can be expressed as

$$\begin{array}{lcl} \mathit{preds} \bullet \mathsf{succ} \bullet n & = & (\mathit{preds} \bullet n) \mathbin{\text{⤙}} n \\ \mathit{preds} \;\bullet\; \mathsf{0} & = & \square \quad , \end{array}$$

or, informally, $\mathit{preds} \bullet n \;=\; [0, 1, \ldots, n-1]$. Catamorphisms on snoc-lists are also known as left-reduces, and another way of writing $(\![\otimes \mathbin{\text{⇟}} 1]\!)$ is $\otimes \not\rightarrow_1$ (Bird[2, 3]). Thus,

$$\mathit{fac} \;=\; \otimes \not\rightarrow_1 \bullet \mathit{preds} \quad .$$

References

[1] Roland Backhouse, Paul Chisholm, Grant Malcolm, and Erik Saaman. Do-it-yourself type theory. *Formal Aspects of Computing*, 1:19–84, 1989.

[2] Richard S. Bird. An introduction to the theory of lists. In M. Broy, editor, *Logic of Programming and Calculi of Discrete Design*, volume F36 of *NATO ASI Series*, pages 5–42. Springer–Verlag, 1987.

[3] Richard S. Bird. Lectures on constructive functional programming. In M. Broy, editor, *Constructive Methods in Computing Science*, volume F55 of *NATO ASI Series*, pages 151–216. Springer–Verlag, 1989.

[4] J. A. Goguen. How to prove inductive hypotheses without induction. In W. Bibel and R. Kowalski, editors, *Proc. 5th Conference on Automated Deduction*, pages 356–373. Springer-Verlag, 1980. LNCS 87.

[5] Grant Malcolm. Factoring homomorphisms. Technical Report Computing Science Notes CS 8908, Department of Mathematics and Computing Science, University of Groningen, 1989.

[6] Grant Malcolm. Homomorphisms and promotability. In J.L.A. van de Snepscheut, editor, *Mathematics of Program Construction*, pages 335–347. Springer-Verlag, 1989. LNCS 375.

[7] Lambert Meertens. Algorithmics–towards programming as a mathematical activity. In J. W. de Bakker, M. Hazewinkel, and J.K. Lenstra, editors, *Proceedings of the CWI Symposium on Mathematics and Computer Science*, volume 1 of *CWI Monographs*, pages 289–334. North–Holland, 1986.

[8] Lambert Meertens. Constructing a calculus of programs. In J.L.A. van de Snepscheut, editor, *Mathematics of Program Construction*, pages 66–90. Springer-Verlag, 1989. LNCS 375.