Induction and Recursion on Datatypes

$\boxed{\text{DRAFT}}$

Roland Backhouse
Henk Doornbos
Department of Mathematics and Computing Science,
Eindhoven University of Technology,
P.O. Box 513,
5600 MB Eindhoven,
The Netherlands.

July 28, 1993

1 Introduction

A central element in any programming algebra is the definition of programs as solutions of (recursive) equations. A central element in any programming algebra's metatheory is thus the characterisation of classes of equations that have unique solutions, first, because uniqueness guarantees well-definedness and, second, because it affords much stronger calculational properties than does mere existence of solutions.

Unicity is typically established by an inductive argument —more often than not by induction over the datatype natural number. In this paper we introduce a notion of induction over an arbitrary datatype and go on to show how the notion is used to establish unicity of a certain (broad) class of equations.

Our overall goal is to develop a *calculational* theory of mathematical induction. That is we want to be able to *calculate* relations on which inductive arguments may be based using laws that relate admitting induction to the mechanisms for constructing datatypes. We also want to incorporate such calculations into a methodology for *calculating* inductive hypotheses rather than leaving their creation to inspired guesswork. This is a bold aim, in view of the vast amount of knowledge and experience that already exists on proof by induction, but recent advances in the rôle played by Galois connections in the calculus of relations have led us to speculate that significant progress can be made in the short term.

The theory developed in this paper is general and not specific to any particular datatype. We define a notion of F-reductivity (so called in order to avoid confusion with existing notions of inductivity), where F stands for a "relator", and show that F-reductive relations always exist, whatever the value of F. We also give laws for constructing reductive relations from existing reductive relations. We conclude the paper by introducing the dual notion of F-*in*ductivity and briefly contrast it with F-*re*ductivity.

The organisation of this note is as follows. In section 2 we give a very brief introduction to the relational calculus. In section 3 the notion of reductivity is defined. This notion is a generalisation of well-foundedness, or inductivity. Then in section 4 we define a class of equations and prove that an equation from that class has a unique solution if one of its components enjoys a reductivity property. The next two sections 5 and 6 are devoted to showing how reductive relations can be constructed. In section 7 we define structural induction, give a class of equations and prove that an equation from that class has at most one solution if a certain component of the equation admits structural induction.

2 Preliminaries

In this section we give a brief introduction to the relational calculus We use the notation and calculational style as introduced in [2]. Apart from the introduction we also mention some results from the theory of Galois connections, because we need them for the introduction of some of the operators.

2.1 Basic operators and relators

A binary relation on a set $\mathcal{A}$ is a subset of the cartesian product $\mathcal{A} \times \mathcal{A}$. In other words a relation is an element of the powerset $\mathcal{P}(\mathcal{A} \times \mathcal{A})$. Therefore, the first axiom is that the relations form a complete lattice. The top of this lattice is denoted by $\top\!\!\top$, its interpretation being the total relation $\mathcal{A} \times \mathcal{A}$. The bottom, denoted by $\perp\!\!\perp$, has as interpretation the empty relation. We write $\sqsubseteq$ for the order on the lattice and $\sqcup$ and $\sqcap$ for the join and the meet, respectively.
Relations can be composed in the usual way:

$$x(R \circ S)y \;\equiv\; \exists(z : x(R)z : z(S)y)$$

This composition is associative and has as unit the identity relation, so we have as an axiom ($\mathcal{A}$,I,$\circ$) is a monoid. The interpretation of I is the identity relation: $x(I)y \;\equiv\; x \,=\, y$. The sections $R\circ$ and $\circ R$ distribute over arbitrary joins. As a consequence $\circ$ is monotonic in both its arguments with respect to $\sqsubseteq$. From now on if we say that an operator is monotonic it is to be understood that this is with respect to $\sqsubseteq$.
The reverse $R\cup$ of a relation R is interpreted as $x(R\cup)y \;\equiv\; y(R)x$. We have as an axiom:

(1) $\quad R\cup \sqsubseteq S \;\equiv\; R \sqsubseteq S\cup$

A consequence of this axiom is that reverse is its own inverse: $R\cup\cup \,=\, R$. Furthermore it follows that reverse distributes over arbitrary meets and joins. So we also have $\top\!\!\top\cup \,=\, \top\!\!\top$, $\perp\!\!\perp\cup \,=\, \perp\!\!\perp$ and reverse is monotonic.
Reverse and composition are related by the axiom:

(2) $\quad (R \circ S)\cup \,=\, S\cup \circ R\cup$

We also have $I\cup \,=\, I$; it is not very difficult to prove this from (1) and (2).
An important concept is that of relator. A function F from relations to relations is a relator if

(a) $\quad F$ is monotonic
(b) $\quad F$ distributes over $\circ$
(c) $\quad F.I \sqsubseteq I$
(d) $\quad (F.R)\cup \,=\, F.(R\cup)$

In the sequel F, G and H will denote relators.

2.2 Galois connections

The concept of Galois connection is well-known, see e.g. [5, 6], but perhaps not as well known as it deserves to be. Given two preorders $\sqsubset$ and $<$, two functions, f and g say, form a Galois connection if the following formula holds for all x and y.

(3) $\quad f.x < y \;\equiv\; x \sqsubset g.y \quad .$

Function f will be called the lower adjoint and function g the upper adjoint. (These names are chosen because (3) is a special case of the categorical notion of adjoint situation.) Galois connections are interesting because as soon as we recognise one we get a large number of properties of the adjoints for free, so to speak. First of all, we have the two *cancellation properties* $x \sqsubseteq g.(f.x)$ and $f.(g.y) < y$. These are obtained by instantiating (3) in such a way that either the lefthand or the righthand side becomes true. Furthermore we have that if the two orders are complete lattices (which is the case for the inclusion $\sqsubseteq$ on relations) the lower adjoint distributes over arbitrary joins and the upper adjoint distributes over arbitrary meets.
Another important fact is that if a function on a complete lattice distributes over arbitrary joins then it has an upper adjoint and, conversely, if it distributes over arbitrary meets then it has a lower adjoint. This fact allows us to define new operators: e.g. if we have that G is a function that distributes over arbitrary joins then we know that there is a function $G^\sharp$ with properties

(4) $\quad G.A \sqsubseteq B \equiv A \sqsubseteq G^\sharp.B \quad$ and $\quad G.(G^\sharp.A) \sqsubseteq A.$

For a complete account of the theory of Galois connections, including proofs of the properties mentioned here, see [1].

2.3 Monotypes and the domain operators

Following [2] we call relations R that satisfy $R \sqsubseteq I$ monotypes. Monotypes will be denoted by uppercase identifiers A, B, C. In the relational model of the calculus monotypes are partial identity relations and can be identified with subsets of the universe $\mathcal{A}$. Therefore we write $x \in A$ as a shorthand for $x(A)x$. An important fact is that the meet and the composition coincide on monotypes: $A \sqcap B = A \circ B$.
A relation R induces two monotypes: the right domain, denoted by $R>$, and the left domain, denoted by $R<$. The interpretations are:

$$x \in R< \;\equiv\; \exists(y : \;: x(R)y) \quad \text{and} \quad x \in R> \;\equiv\; \exists(y :: y(R)x),$$

so they can indeed be interpreted as domain operators on relations. The domain operators are defined by the Galois connections

$$R> \sqsubseteq A \equiv R \sqsubseteq \top\!\!\top \circ A \quad \text{and} \quad R< \sqsubseteq A \equiv R \sqsubseteq A \circ \top\!\!\top$$

That these are definitions at all follows from the fact that $\top\!\!\top\circ$ and $\circ\top\!\!\top$ both distribute over arbitrary meets of monotypes. An immediate consequence is that the domain operators, being lower adjoints, distribute over arbitrary joins and therefore are monotonic. Another property is:

(5) $\quad R< \circ R = R = R \circ R> \quad .$

2.4 The monotype factor

The monotype factor is defined by the Galois connection

(6) $\quad (R \circ A)< \sqsubseteq B \equiv A \sqsubseteq R\backslash B \quad .$

That this is a proper definition follows again from the theory of Galois connections and the join-distributivity properties of composition and the domain operators. It should be noted that $R\backslash B$ is a monotype. The interpretation of $R\backslash B$ is the following:

(7) $\quad x \in R\backslash B \equiv \forall(y : y(R)x : y \in B) \quad .$

Because this operator plays an important role in the remainder of this note we give, for referential purposes, a rather long list of properties. All of these are rather easy to prove using the defining Galois connection and the properties of the domain operator documented in [2].
First note that the function $R\backslash$, being an upper adjoint, distributes over arbitrary meets of monotypes. Because the meet on monotypes coincides with the composition it follows that $R\backslash$ distributes over $\circ$.

From (6) we obtain the cancellation property:

(8) $\quad (R \circ R\backslash B)< \sqsubseteq B \quad .$

Often this property is used in a slightly different form:

(9) $\quad R \circ R\backslash B \sqsubseteq B \circ R \quad .$

It can be shown that if R is a monotype (8) can be strengthened to an equality.

(10) $\quad A \circ A\backslash B \;=\; A \circ B$

(We call (10) the rule of modus ponens. The reason is that if monotypes are interpreted as predicates then, when restricted to monotypes only, the operator $\circ$ and the operator $\backslash$ are interpreted as conjunction and implication, respectively. Thus (10) is the statement $A \;\wedge\; A{\Rightarrow}B \quad\equiv\quad A \wedge B$.) Another version of the cancellation property that is sometimes useful is:

(11) $\quad R> \circ R\backslash A \sqsubseteq (A \circ R)> \quad .$

If R is a functional relation this inclusion can be strengthened to an equality:

(12) $\quad R \circ R^{\cup} \sqsubseteq I \qquad \Rightarrow \qquad R> \circ R\backslash A \;=\; (A \circ R)> \quad .$

From associativity of composition we obtain:

(13) $\quad R\backslash(S\backslash A) \;=\; (S \circ R)\backslash A \quad .$

Combining (10) and (13) we get the following:

(14) $\quad A \circ R\backslash B \;=\; A \circ (R \circ A)\backslash B \quad .$

Another fact is that relators distribute over the monotype factor in the sense that

(15) $\quad F.(R\backslash A) \sqsubseteq F.R \backslash F.A \quad .$

Finally we mention the monotonicity properties of the monotype factor; we have: $R\backslash$ is monotonic and $\backslash A$ is anti monotonic. This concludes our short introduction to the monotype factor. For a more extensive treatment the reader is referred to [4].

2.5 Yet another factor

To give a nice proof of the main theorem of this note, it is convenient to define a second factor operation. Recall that the function $R\circ$ from specs to specs distributes over all joins. Clearly, if this function is restricted to a function from *monotypes* to specs it still distributes over arbitrary joins. Therefore, its upper adjoint exists.

Definition 16 (Second factor) The function $R\backslash\!\!\backslash$ from specs to monotypes is defined by the following Galois connection:

$$A \sqsubseteq R\backslash\!\!\backslash S \equiv R{\circ}A \sqsubseteq S \quad .$$

□

The important cancellation rule is:

(17) $\quad R \circ R\backslash\!\!\backslash S \sqsubseteq S \quad .$

2.6 The induction principle

Now we have all the machinery to define the induction principle in the spec calculus. A more or less standard definition is: relation R admits induction if and only if:

(18) $\forall(y : \forall(x : x(R)y : x \in A) : y \in A) \Rightarrow \forall(y : \; : y \in A)$ for all sets A.

To arrive at a definition without dummies we first notice that $\forall(y : \, : y \in A)$, the (understood) domain of y being I, can be rewritten as $I \sqsubseteq A$. Furthermore, we see that the expression in the domain of the antecedent,$\forall(x : x(R)y : x \in A)$, is just $y \in R\backslash A$, see (7). So the notion of admitting induction can be drastically simplified to: relation R admits induction if and only if

(19) $R\backslash A \sqsubseteq A \Rightarrow I \sqsubseteq A$, for all monotypes A.

Property (19) is, in our view, a very attractive calculational formulation of the notion of admitting induction. Note first its compactness. Now note its form: it is a rule for establishing that a property (A) is universal ($I \sqsubseteq A$). The mechanism to do so is to establish a property that is formally much weaker, namely $R\backslash A \sqsubseteq A$. The proof of $R\backslash A \sqsubseteq A$ is what is usually called the induction step, and $R\backslash A$ is the induction hypothesis.
In the next section this definition will be generalised.

2.7 Natural transformations for monotypes

From category theory the concept "natural transformation" is well known. In this paper we need the following variant.

Definition 20 Let R be a spec and let F and G be relators. We say that $R \in F \overset{\cdot}{\leftsquigarrow} G$ if and only if for all monotypes A:

$$R \circ G.A \sqsubseteq F.A \circ R \quad .$$

□

An, for the calculations in the rest of this paper important, observation is that $R \in F \overset{\cdot}{\leftsquigarrow} G$ can also be expressed using the monotype factor.

Lemma 21

$$R \in F \overset{\cdot}{\leftsquigarrow} G \equiv \forall(A : A \sqsubseteq I : G.A \sqsubseteq R\backslash F.A)$$

Proof:

$$\begin{array}{ll}
 & G.A \sqsubseteq R\backslash F.A \\
\equiv & \quad \{ \quad \text{factors: (6)} \quad \} \\
 & (R \circ G.A)^{<} \sqsubseteq F.A \\
\equiv & \quad \{ \quad \text{domains: } X^{<} \sqsubseteq A \;\; \equiv \;\; X \sqsubseteq A \circ X \quad \} \\
 & R \circ G.A \sqsubseteq F.A \circ R \circ G.A \\
\equiv & \quad \{ \quad (\Rightarrow)\text{: } G.A \sqsubseteq I;\ (\Leftarrow)\text{: } G.A \circ G.A = G.A \quad \} \\
 & R \circ G.A \sqsubseteq F.A \circ R
\end{array}$$

□

3 F-reductivity

This section is begun by giving a compact point-free definition of the notion of F-*reductive* spec (where F is a relator). This definition generalises the notion of a well-founded spec (relation).

Following its definition we present a theorem giving alternative characterisations of the notion. These alternative characterisations help to justify its relevance and usefulness. In later sections we amplify on this aspect by considering several (abstract and concrete) applications.

Definition 22 (F-reductivity) Spec R is said to be F-*reductive* if and only if it enjoys the property:

(23) $\mu(R\backslash \bullet F) = I$.

□

Theorem 24 (Characterisations of F-reductivity) The following are all equivalent:

(a) R is F-reductive
(b) $\forall(A : A \sqsubseteq I : R\backslash F.A \sqsubseteq A \Rightarrow I \sqsubseteq A)$
(c) $\forall(A : A \sqsubseteq I : R\backslash F.A = A \Rightarrow R{>} \sqsubseteq A)$

The proof is by mutual implication. That (a) implies (b) is an immediate consequence of the Knaster-Tarski fixpoint theorem. The implication (b)$\Rightarrow$(c) is also easy: by reflexivity of $\sqsubseteq$ and the fact that $R{>} \sqsubseteq I$. The more difficult step is that from (c) to (a); we show the (formally) stronger: clause (c) implies that *every* fixpoint of the function $R\backslash \bullet F$ is I. Assume :

$$R\backslash F.A = A \quad ,$$

i.e. A is a fixpoint of $R\backslash \bullet F$, and (c). Then

$$\begin{array}{ll}
 & I = A \\
\Leftarrow & \{ \quad A \sqsubseteq I, \text{ assumption} \quad \} \\
 & I \sqsubseteq R\backslash F.A \\
\equiv & \{ \quad \text{factors: (6)} \quad \} \\
 & R{<} \sqsubseteq F.A \\
\equiv & \{ \quad \text{domains: (5)} \quad \} \\
 & (R \circ R{>}){<} \sqsubseteq F.A \\
\equiv & \{ \quad \text{factors: (6)} \quad \} \\
 & R{>} \sqsubseteq R\backslash F.A \\
\equiv & \{ \quad \text{assumption} \quad \} \\
 & R{>} \sqsubseteq A \\
\Leftarrow & \{ \quad \text{(c)} \quad \} \\
 & R\backslash F.A = A \\
\equiv & \{ \quad \text{assumption} \quad \} \\
 & \mathit{true}
\end{array}$$

This completes the proof.
□

Of the three different forms of the definition of F-reductive the first is clearly the most compact, and hence the most suited to abstract reasoning about the notion. The second form is closest to the way proof by induction is normally presented. The third alternative, because it is formally weaker than the other two, is often useful to *prove* that a given spec is F-reductive.
Comparing 24 (b) with (19) one sees that F-reductivity is a generalisation of well-foundedness: I-reductivity is the same as well-founded. One may wonder why we use the term reductivity instead of inductivity. The reason is that the term F-inductivity seems to be reserved traditionally for the notion to be introduced in section 7.

4 Hylomorphisms

A spec is said to be a *hylomorphism* if it is the least solution to the equation

$$X :: \qquad X = S \circ F.X \circ R$$

for some specs R and S, and such an equation is called a hylo equation. The reason why such equations are interesting is that they represent a recursion pattern that occurs frequently in practice. Consider, for instance, the program known as "merge sort". In that case R represents the "splitting" step, $F.X$ the recursive call, and S the "merge" step. Also the hylo equation generalises many of the defining equations of the "morphisms" from the "squiggol" literature. Examples are catamorphisms (see e.g. [9]) defined as the unique solution of

(25) $X \;::\; \qquad X = f \circ F.X \circ out \quad ,$

and paramorphisms (see [8]), which have as defining equation:

(26) $X \;::\; \qquad X = f \circ I \vartriangle F.X \circ out \quad .$

(In fact, the name hylomorphisms for the least solution of a hylo equation appears in [7].)
Typically such an equation will not have a unique solution. The purpose of this section is to show, however, that it does have a unique solution, whatever the value of S, in the case that R is an F-reductive spec.

Theorem 27 (Hylomorphism UEP) Let S be an arbitrary spec and R be an F-reductive spec. Then the equation

(28) $X \;::\; \qquad X = S \circ F.X \circ R$

has a unique solution.

Proof That equation (28) has a solution follows from the fact that $S \circ F.X \circ R$ is a monotonic function of X and the Knaster-Tarski theorem. So we need only show that there is at most one solution; therefore assume:

(a) $X = S \circ F.X \circ R$, and
(b) $Y = S \circ F.Y \circ R$.

Now it suffices to prove $X \sqsubseteq Y$.

$$
\begin{array}{ll}
 & X \sqsubseteq Y \\
\equiv & \qquad \{ \quad \text{definition 16} \quad \} \\
 & I \sqsubseteq X \mathbin{\backslash\!\!\backslash} Y \\
\Leftarrow & \qquad \{ \quad R \text{ is } F\text{-reductive} \quad \} \\
 & R \backslash F.(X \mathbin{\backslash\!\!\backslash} Y) \sqsubseteq X \mathbin{\backslash\!\!\backslash} Y \\
\equiv & \qquad \{ \quad \text{definition 16} \quad \} \\
 & X \circ R \backslash F.(X \mathbin{\backslash\!\!\backslash} Y) \sqsubseteq Y \\
\equiv & \qquad \{ \quad \text{assumption (a)} \quad \} \\
 & S \circ F.X \circ R \circ R \backslash F.(X \mathbin{\backslash\!\!\backslash} Y) \sqsubseteq Y \\
\Leftarrow & \qquad \{ \quad \text{factor cancellation: (9)} \quad \} \\
 & S \circ F.X \circ F.(X \mathbin{\backslash\!\!\backslash} Y) \circ R \sqsubseteq Y \\
\Leftarrow & \qquad \{ \quad \text{relators distr. over } \circ \text{ ; cancellation (17)} \quad \}
\end{array}
$$

$S \circ F.Y \circ R \sqsubseteq Y$

$\equiv \qquad \{ \quad$ assumption (b) $\quad \}$

$true$

$\square$

5 Basic F-reductive specs

We have seen that the notion of F-reductivity is an important one. It is therefore desirable to be able to *construct* specs enjoying this property. Remarkably, it is always possible to turn a given spec into an F-reductive spec by restricting it by a certain monotype.

Theorem 29 For any spec R the spec $R \circ \mu(R\setminus \bullet F)$ is F-reductive.

Proof: Let $\aleph$ be $\mu(R\setminus \bullet F)$. By theorem 24 we have to show for any monotype A:

$$(R \circ \aleph)\setminus F.A \; = \; A \;\Rightarrow\; (R \circ \aleph)> \,\sqsubseteq A \quad .$$

This is done in the following calculation.

$(R \circ \aleph)> \,\sqsubseteq A$

$\Leftarrow \qquad \{ \quad$ domains: $(R \circ A)< \,\sqsubseteq A \quad \}$

$\aleph \sqsubseteq A$

$\equiv \qquad \{ \quad$ monotypes: $\circ$ and $\sqcap$ coincide $\quad \}$

$\aleph \sqsubseteq \aleph \circ A$

$\Leftarrow \qquad \{ \quad$ Knaster-Tarski $\quad \}$

$R\setminus F.(\aleph \circ A) \sqsubseteq \aleph \circ A$

$\equiv \qquad \{ \quad$ $R\setminus$ and F distribute over $\circ \quad \}$

$R\setminus F.\aleph \circ R\setminus F.A \; \sqsubseteq \; \aleph \circ A$

$\equiv \qquad \{ \quad$ $R\setminus F.\aleph \; = \; \aleph$; monotypes: $\circ$ and $\sqcap$ coincide $\quad \}$

$\aleph \circ R\setminus F.A \; \sqsubseteq \; A$

$\equiv \qquad \{ \quad$ factors: (14) $\quad \}$

$\aleph \circ (R \circ \aleph)\setminus F.A \; \sqsubseteq \; A$

$\Leftarrow \qquad \{ \quad$ $\aleph \sqsubseteq I \quad \}$

$(R \circ \aleph)\setminus F.A \; \sqsubseteq \; A$

$\square$

A straightforward corollary of this theorem is:

Corollary 30 Let $X \; = \; S \circ F.X \circ R$ and $\aleph \; = \; \mu(R\setminus \bullet F)$,. Then $X \circ \aleph$ is the unique solution of

(31) $Y{::} \quad Y \; = \; S \circ F.Y \circ R \circ \aleph \quad .$

Proof: That (31) has a unique solution follows from theorems 27 and 29. Furthermore, $X \circ \aleph$ is a solution:

$X \circ \aleph$

$$
\begin{array}{ll}
= & \{ \quad X = S \circ F.X \circ R \quad \} \\
& S \circ F.X \circ R \circ \aleph \\
= & \{ \quad \aleph = R \backslash\!\!\downarrow F.\aleph, \text{ hence: } (R \circ \aleph)^{<} \sqsubseteq F.\aleph \quad \} \\
& S \circ F.(X \circ \aleph) \circ R \circ \aleph
\end{array}
$$

□

Another easy consequence is that for any relator F there is an F-reductive relation:

Corollary 32 μF is F-reductive.

Proof: Instantiate R in theorem 29 to I and observe that $I \backslash\!\!\downarrow$ is the identity function.
□

6 New F-reductive specs from old

This section is intended to show how given an F-reductive spec other reductive specs can be constructed. The first construction is simple enough:

Theorem 33 If R is F-reductive and $S \sqsubseteq R$ then S is F-reductive

Proof: Immediate from theorem 24 (b) and the monotonicity properties of the monotype factor.

□

The next two theorems can be used to change the "kind of reductivity", i.e. to construct F-reductive specs from G-reductive specs.

Theorem 34 Let Q be G-reductive and $\alpha \in F \dot{\leftsquigarrow} \mathsf{I}$. Then $F.Q \circ \alpha$ is $F \bullet G$-reductive.

Proof:

$$
\begin{array}{ll}
& I \sqsubseteq A \\
\Leftarrow & \{ \quad Q \text{ is } G\text{-reductive} \quad \} \\
& Q \backslash\!\!\downarrow G.A \sqsubseteq A \\
\Leftarrow & \{ \quad \alpha \in F \dot{\leftsquigarrow} \mathsf{I} \text{ lemma 21} \quad \} \\
& \alpha \backslash\!\!\downarrow F.(Q \backslash\!\!\downarrow G.A) \sqsubseteq A \\
\Leftarrow & \{ \quad \text{factors and relators: (15)} \quad \} \\
& \alpha \backslash\!\!\downarrow (F.Q \backslash\!\!\downarrow F.G.A) \sqsubseteq A \\
\equiv & \{ \quad \text{factors: (13)} \quad \} \\
& (F.Q \circ \alpha) \backslash\!\!\downarrow A \sqsubseteq A
\end{array}
$$

□

A typical use of theorems (33) and (34) is: R is F-reductive follows from the fact that there is a well-founded relation Q and a relation $\alpha \in F \dot{\leftsquigarrow} \mathsf{I}$ such that $R \sqsubseteq F.Q \circ \alpha$.
Another F-reductivity theorem is:

Theorem 35 Let R be F-reductive, $\alpha \in H \bullet G \dot{\leftsquigarrow} G \bullet F$ and G a relator that distributes over all joins of monotypes. Then $\alpha \circ G.R$ is H-reductive.

Proof: We aim to prove (c) in theorem 24 with the instatiations $R := \alpha \circ G.R$ and $F := H$.

$$
\begin{array}{ll}
 & (\alpha \circ G.R)> \sqsubseteq A \\
\Leftarrow & \{ \quad \text{domains} \quad \} \\
 & G.I \sqsubseteq A \\
\equiv & \{ \quad G \text{ distributes over all joins} \quad \} \\
 & I \sqsubseteq G^\sharp.A \\
\Leftarrow & \{ \quad R \text{ is } F\text{-reductive} \quad \} \\
 & R \backslash F.(G^\sharp.A) \sqsubseteq G^\sharp.A \\
\equiv & \{ \quad G \text{ distributes over all joins} \quad \} \\
 & G.(R \backslash F \,.\, G^\sharp.A) \sqsubseteq A \\
\Leftarrow & \{ \quad \text{relators and factors: (15)} \quad \} \\
 & G.R \backslash G \,.\, F \,.\, G^\sharp.A \sqsubseteq A \\
\Leftarrow & \{ \quad \alpha \in H \bullet G \dot{\leftsquigarrow} G \bullet F \text{ ; lemma 21} \quad \} \\
 & G.R \backslash (\alpha \backslash H.G.G^\sharp.A) \sqsubseteq A \\
\Leftarrow & \{ \quad \text{factors: (13); cancellation (4)} \quad \} \\
 & (\alpha \circ G.R) \backslash H.A \sqsubseteq A
\end{array}
$$

□

Some applications are given in [3].
The restriction on relator G in this theorem is rather severe. However, there is one important class of relators satisfying it: the sections of the (cartesian) product relator. This enables us to define functions that are not defined on an "inductive" domain but on the product of such a domain and another domain (such as the summation function on pairs of natural numbers or the concatenation function on pairs of lists) as the unique solution of a hylo equation.
Another example of a relator that distributes over any join is of course the identity relator, so we have the following corollary of theorem 35.

Corollary 36 If R is F-reductive and $\alpha \in H \dot{\leftsquigarrow} F$ then $\alpha \circ R$ is H-reductive.

Proof: Instantiate theorem 35 with the (join-distributive) identity relator.
□

Using this corollary (together with corollary 32) it is straightforward to prove that equations such as the "paramorphism" equation

$$X \quad :: \quad X \;=\; R \circ I \vartriangle F.X \circ \mu F$$

have unique solutions.

7 Structural induction

As we have seen, the concept of F-reductivity allows one to show that a hylo equation has a unique solution. However, sometimes one wishes to prove that equations of another type always have unique solutions.
For instance, a relation on lists can be defined by an equation of the form:

$$(37) \quad X \quad :: \quad X \;=\; X \circ \varphi< \;\wedge\; X \circ \varphi \;=\; R \circ F.X \quad ,$$

where φ is the usual algebra: $[\text{-}] \triangledown ([\,] \triangledown \mathit{concat})$. If X solves (37), simple calculus (using that φ is functional) gives $X \;=\; \varphi \circ F.X \circ \varphi^\cup$. So, we might hope that we can show that (37) has a unique solution using F-reductivity of $\varphi\cup$. However, it turns out that this is not possible. It can be shown that both $\varphi<$ and $\varphi< \circ \top\!\top \circ \varphi<$ solve $X \;::\; X = \varphi \circ F.X \circ \varphi\cup$. Hence, $\varphi\cup$ is *not* F-reductive. Therefore, to show that (37) has a unique solution, another technique is needed. Now it is well known that relations like $[\text{-}] \triangledown ([] \triangledown \mathit{concat})$ admit structural induction over their domain and that this method of induction allows one to prove that equations of the form (37) have at most one solution. Therefore we need to formalise this the method of induction in our calculus. This then is done in the following definition

Definition 38 (F-inductivity) We say that relation R is F-inductive if and only if for all monotypes A:

(39) $(R \circ F.A)< \sqsubseteq A \Rightarrow R< \sqsubseteq A$.

□

Although structural induction in itself is not sufficient to show that (37) has a unique solution, it can be used to prove that there is at most one solution.

Theorem 40 If φ is an F-inductive relation such that $\varphi< = \varphi \circ \varphi\cup$ and, moreover, $S \in G \overset{\cdot}{\leftsquigarrow} F$, then the equation

(41) $X \;::\; X = X \circ \varphi< \wedge X \circ \varphi = R \circ G.X \circ S$

has at most one solution.

Proof: Assume X and Y solve (41). It is sufficient to show $X \sqsubseteq Y$

$$
\begin{array}{ll}
 & X \sqsubseteq Y \\
\equiv & \{ \quad X = X \circ \varphi< \quad \} \\
 & \varphi< \sqsubseteq X \backslash Y \\
\Leftarrow & \{ \quad \varphi \text{ admits } F\text{-structural induction} \quad \} \\
 & (\varphi \circ F.(X \backslash Y))< \sqsubseteq X \backslash Y \\
\Leftarrow & \{ \quad \text{domains} \quad \} \\
 & X \circ \varphi \circ G.(X \backslash Y) \circ \varphi\cup \sqsubseteq Y \\
\equiv & \{ \quad X \text{ and } Y \text{ solve (41); } \varphi< = \varphi \circ \varphi\cup \quad \} \\
 & R \circ G.X \circ S \circ F.(X \backslash Y) \circ \varphi\cup \sqsubseteq Y \circ \varphi \circ \varphi\cup \\
\Leftarrow & \{ \quad S \in G \overset{\cdot}{\leftsquigarrow} F \quad \} \\
 & R \circ G.X \circ G.(X \backslash Y) \circ S \sqsubseteq Y \circ \varphi \\
\Leftarrow & \{ \quad \text{cancellation} \quad \} \\
 & R \circ G.Y \circ S \sqsubseteq Y \circ \varphi \\
\equiv & \{ \quad Y \text{ solves (41)} \quad \} \\
 & \mathit{true}
\end{array}
$$

□

For conditions under which equations like (37) do have solutions, see Voerman's thesis.

7.1 Connections between inductive and reductive

The notions of inductivity and reductivity are of course not totally unconnected and in this section we mention two such connections. The first can be read as: the converse of an inductive injection is reductive.

Theorem 42 If R is an F-inductive relation such that $R^{\cup} \circ R \sqsubseteq I$, then $R^{\cup}$ is F-reductive

Proof: We aim to prove (c) in theorem (24).

$$
\begin{array}{ll}
 & R^{\cup}{>} \sqsubseteq A \\
\equiv & \qquad \{ \qquad X{<} \;=\; X^{\cup}{>} \quad \} \\
 & R{<} \sqsubseteq A \\
\Leftarrow & \qquad \{ \qquad R \text{ is } F\text{-inductive, definition 39} \quad \} \\
 & (R \circ F.A){<} \sqsubseteq A \\
\equiv & \qquad \{ \qquad X{<} \;=\; X^{\cup}{>}\text{; distribution properties of } \cup \quad \} \\
 & (F.A \circ R^{\cup}){>} \sqsubseteq A \\
\equiv & \qquad \{ \qquad \text{assumption: } R^{\cup} \circ R^{\cup\cup} \sqsubseteq I\text{; (12) with } R := R^{\cup} \quad \} \\
 & R^{\cup}{>} \circ R^{\cup} \backslash F.A \;\sqsubseteq\; A \\
\Leftarrow & \qquad \{ \qquad R^{\cup}{>} \sqsubseteq I \quad \} \\
 & R^{\cup} \backslash F.A \;=\; A
\end{array}
$$

□

The second connection between inductivity and reductivity might be interpreted as: the converse of a total, reductive co-algebra is inductive.

Theorem 43 Let R be an F-reductive relation such that $R{<} \sqsubseteq F.R{>}$. Then $R^{\cup}$ is F-inductive.

Proof:

$$
\begin{array}{ll}
 & R^{\cup}{<} \sqsubseteq A \\
\equiv & \qquad \{ \qquad X{<} \;=\; X^{\cup}{>} \quad \} \\
 & R{>} \sqsubseteq A \\
\equiv & \qquad \{ \qquad \text{factors (6)} \quad \} \\
 & I \sqsubseteq R{>} \backslash A \\
\Leftarrow & \qquad \{ \qquad R \text{ is } F\text{-reductive} \quad \} \\
 & R \backslash F.(R{>} \backslash A) \sqsubseteq R{>} \backslash A \\
\Leftarrow & \qquad \{ \qquad \text{factors (6) and (15)} \quad \} \\
 & R{>} \circ R \backslash (F.R{>} \backslash F.A) \sqsubseteq A \\
\equiv & \qquad \{ \qquad \text{factors (13)} \quad \} \\
 & R{>} \circ (F.R{>} \circ R) \backslash F.A \;\sqsubseteq\; A \\
\equiv & \qquad \{ \qquad \text{assumption: } R{<} \sqsubseteq F.R{>} \quad \} \\
 & R{>} \circ R \backslash F.A \;\sqsubseteq\; A \\
\Leftarrow & \qquad \{ \qquad \text{factors (11)} \quad \} \\
 & (F.A \circ R){>} \sqsubseteq A \\
\equiv & \qquad \{ \qquad X{<} \;=\; X^{\cup}{>} \quad \} \\
 & (R^{\cup} \circ F.A){<} \sqsubseteq A
\end{array}
$$

□

Because μF is a monotype we have $\mu F < \;\sqsubseteq\; F \,.\, \mu F >$ so we get from theorem 43 and corollary 32 the following result.

Corollary 44 For any relator F the relation μF is F-inductive.

□

8 Future work

In this paper we have given two different induction principles over arbitrary datatypes and gave two classes of equations that can be proved to have unique solutions using those induction principles. A topic for future research is: are there other classes of equations such that one of the induction principles can be used to give uniqueness proofs? A particularly interesting class seems to be formed by equations of the form:

(45) $X \;::\; \quad X \;=\; R \circ F.X \circ G.X \circ S \quad .$

(For instance the Ackermann function satisfies an equation of this form.)
Another problem is how to weaken the restriction on α in corollary 36. This is important because it turns out that for some applications the requirement $\alpha \in H \dot{\leftsquigarrow} F$ is simply too strong.
Also it has still to be investigated how two reductive relations can be combined into one, thereby generalising the result that, under certain conditions, the join of two well-founded relations is well-founded again.

Acknowledgement:

We owe a great debt to the team spirit in the Eindhoven Mathematics of Program Construction group. The inspiration for the notion of F-reductivity came from Oege de Moor during an extended visit he made to Eindhoven in October 1992.

References

[1] C.J. Aarts. Galois connections presented calculationally. Afstudeer verslag (Graduating Dissertation), Department of Computing Science, Eindhoven University of Technology, 1992.

[2] C.J. Aarts, R.C. Backhouse, P. Hoogendijk, T.S. Voermans, and J. van der Woude. A relational theory of datatypes. In preparation: copies of draft available on request, September 1992.

[3] R.C. Backhouse. Constructive lattice theory. Eindhoven University of Technology, Department of Computing Science., July 1993.

[4] R.C. Backhouse and J. van der Woude. Demonic operators and monotype factors. Eindhoven University of Technology, Department of Computing Science, Computing Science Note No. 92/11, (To appear in Mathematical Structures in Computer Science), May 1992.

[5] Garrett Birkhoff. *Lattice Theory*, volume 25 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, Rhode Island, 3rd edition, 1967.

[6] B. A. Davey and H. A. Priestly. *Introduction to Lattices and Order*. Cambridge Mathematical Textbooks. Cambridge University Press, first edition, 1990.

[7] Maarten M. Fokkinga. *Law and Order in Algorithmics*. PhD thesis, Universiteit Twente, The Netherlands, 1992.

[8] L. Meertens. Paramorphisms. *Formal Aspects of Computing*, 4(5):413–424, 1992.

[9] E. Meijer, M.M. Fokkinga, and R. Paterson. Functional programming with bananas, lenses, envelopes and barbed wire. In *FPCA91: Functional Programming Languages and Computer Architecture*, volume 523 of *LNCS*, pages 124–144. Springer-Verlag, 1991.