A Calculational Approach to Mathematical Induction

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

March 1994
Revised April 1996

Abstract

Several concise formulations of mathematical induction are presented and proven equivalent. The formulations are expressed in variable-free relation algebra and thus are in terms of relations only, without mentioning the related objects. It is shown that the induction principle in this form, when combined with the explicit use of Galois connections, lends itself very well for use in calculational proofs. Two non-trivial examples are presented. The first is a proof of a Newman's lemma. The second is a calculation of a condition under which the union of two well-founded relations is well-founded. In both cases the calculations lead to generalisations of the known results. In the case of the latter example, one lemma generalises three different conditions.

The idea of formal reasoning — by which we mean the manipulation of uninterpreted formulae according to prescribed syntactic rules — seems to split the computing community into two distinct and opposing schools. There are the enthusiasts who fervently advocate its use, arguing its effectiveness and reliability, and there are the sceptics who dismiss it, arguing that it ignores the creative process in the discovery of new facts or the design of new systems. Whilst ourselves belonging very much to the enthusiasts we are nevertheless of the opinion that, at this point in time, the sceptics can muster much bigger artillery than we enthusiasts. There are two problems. First, the formal methods community is too concerned with the issue of (a posteriori) *verification* of software rather than harnessing formal methods to the much harder task of its *construction*. Second, it is not sufficiently recognised that formal methods must combine *precision* with *concision*. Too often formal systems are large and complex, involving complex rules with large numbers of parameters, and even the simplest specifications stretch over several pages of text. Like programming languages of old, formal systems of today too often belong to the problem domain rather than the solution domain.

Induction illustrates the issue well. An inductive proof typically involves a creative step, namely the invention of the inductive hypothesis. There then follows a verification according to well-defined (and well-known) mathematical principles. Formal reasoning is undoubtedly effective in the verification step, but in most cases it plays a very subordinate rôle (if any at all) in the creative step. Formal reasoning is a service industry and not a production industry.

Or is it? We would argue that formal reasoning *can* contribute significantly to the creative aspects of computing (and mathematics in general) if much more emphasis is given to the search for crisp and compact (but of course still precise) formulations of the fundamental concepts we use in our everyday work.

This paper argues the use of variable-free relation algebra [25] to formulate the fundamental notions of well-foundedness and admitting induction. By doing so one obtains much compacter formulae than the pointwise formulae with which we are all familiar. As a result it is easier to understand the relationship between the two notions and to recognise the circumstances in which they are applicable. More importantly, the invention of inductive hypotheses can be reduced to purely syntactic considerations.

The paper is organised around several different but equivalent formalisations of "is well-founded" and "admits induction". It is well known that the two notions are equivalent but proofs of that fact invariably entail the use of complementation. Our goal is to see what can be learnt by studying the two notions individually and with respect to each other in the context of a relation algebra in which complementation is not permitted. For each of the two notions we first recall the usual pointwise definition and then reformulate their definitions more concisely in the point-free style of relation algebra. Then we proceed to formulate a yet more concise definition which we show equivalent to the original formulation. In order to show the advantages of concision we prove that admits-induction implies well-foundedness even in the absence of negation, and we show the equivalence of well-foundedness to the notion of "definiteness" introduced in [3] as an abstraction of the (absence of) the empty word property in regular algebra. With the understanding so gained we proceed to tackle the construction of a proof of Newman's lemma [20], a lemma that is much exploited in the construction of term rewriting systems but is regarded as difficult to prove (as evidenced by the fact that it has been used to demonstrate the power of theorem proving systems). We demonstrate that the proof of the lemma becomes straightforward by reducing it to purely syntactic considerations. Finally, we consider the difficult problem of determining conditions under which the union of two well-founded relations is itself well-founded. Here we calculate a single condition that subsumes three conditions that have previously been regarded as distinct.

Our concern is, first and foremost, the calculational *method*. Economy of calculation is considerably enhanced if one is able to recognise recurring patterns and formulate them as basic concepts. In this case the basic concept underlying many of the calculation steps is the notion of a Galois connection [21]. The paper could also be seen as a demonstration of how important it is to identify Galois connections in the development of a theory.

1 The Algebraic Framework

In this section we provide a short introduction to *relation algebra*, the axiomatic calculus of relations due to (among others) de Morgan, Schröder and Tarski. Full accounts appear in several monographs (see, for example, [24, 25]); we will make do with just a summary of precisely those properties we need in our calculations.

Throughout the rest of this article capital letters R, S, T, U will denote elements of a relation algebra. Implicit in the presentation of the axioms and other rules is that such variables are universally quantified.

1.1 The Lattice Structure

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 $\bot\!\!\bot$, has as interpretation the empty relation. We write $\subseteq$ for the lattice ordering and $\cup$ and $\cap$ for the join (supremum) and the meet (infimum) operators, respectively. We further assume that join distributes universally over meet, and, vice-versa, meet distributes universally over join.

For the join operator we have

$$(1)\qquad R{\cup}S \subseteq T \;\equiv\; R{\subseteq}T \wedge S{\subseteq}T \quad .$$

The interpretation of join is set union: $x[\![R{\cup}S]\!]y \equiv x[\![R]\!]y \vee x[\![S]\!]y$. Similarly, meet satisfies

$$(2)\qquad T \subseteq R{\cap}S \;\equiv\; T\subseteq R \wedge T\subseteq S \quad .$$

Its interpretation is set intersection: $x[\![R{\cap}S]\!]y \equiv x[\![R]\!]y \wedge x[\![S]\!]y$. The interpretation of the ordering relation is: $[\![R{\subseteq}S]\!] \equiv \forall(x,y{:}\,x[\![R]\!]y{:}\,x[\![S]\!]y)$.

1.2 The Monoid Structure

Relations can be composed in the usual way:

$$x[\![R{\circ}S]\!]y \equiv \exists(z{:}\,x[\![R]\!]z{:}\,z[\![S]\!]y) \quad .$$

Composition is associative and has as unit the identity relation, so we have as an axiom $(\circ, I)$ 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 $\subseteq$. From now on if we say that an operator is monotonic it is to be understood that this is with respect to $\subseteq$.

1.3 The Converse Structure

The converse $R^\cup$ of a relation R is interpreted as $x[\![R^\cup]\!]y \equiv y[\![R]\!]x$. We have as an axiom:

(3) $\qquad R^\cup \subseteq S \equiv R \subseteq S^\cup$.

A consequence of this axiom is that converse is its own inverse: $R^{\cup\cup} = R$. Furthermore it follows that converse distributes over arbitrary meets and joins. So we also have $\top\!\!\top^\cup = \top\!\!\top$, $\bot\!\!\bot^\cup = \bot\!\!\bot$, and converse is monotonic.

Reverse and composition are related by the axiom:

(4) $\qquad (R \circ S)^\cup = S^\cup \circ R^\cup$.

We also have $I^\cup = I$; it is not difficult to prove this from (3) and (4).

1.4 The Modular Identity

The next axiom acts as an interface between all three structures.

$$R \circ S \cap T \subseteq R \circ U \;\Leftarrow\; S \cap R^\cup \circ T \subseteq U \quad .$$

Following Freyd and Scedrov [15] we call the rule the *modular identity*. The earliest reference we know of to the rule is [22] where it is given the name "Dedekind's formula" (in French "formel Dedekind") because of its relationship to the modular identity (for groups) formulated by Dedekind.

We make no explicit use of this rule. The rule is however needed to establish the properties of the domain operators stated in section 4.

1.5 Remarks

This completes the axiomatisation of (non-complemented) relation algebra. Note that, although binary relations form a model of the complete set of axioms, there are also important models of subsets of the set of axioms. For instance, the axioms for the lattice structure and the monoid structure are modelled by *regular algebra*, the algebra of sets of strings over a finite alphabet: the join and meet operations are set union and set intersection, respectively, I is the set containing the empty word, and $\circ$ is concatenation of strings extended in the usual way to sets of strings. Some of our calculations — those exploiting only the lattice and monoid structures — are thus appropriate to this algebra.

In order to maintain a clear distinction between relation algebra as presented above and the particular model of the algebra given by the set of binary relations over some universe $\mathcal{U}$ we will henceforth refer to elements of the algebra as *specs*.

A major advantage of algebraic calculation is that it is easy to trace the properties exploited within a proof. Our division of the axiom system into substructures is intended to better organise the discussion of such issues.

2 Galois Connections

2.1 Basics

The concept of a Galois connection is "well known", see e.g. [6, 8], but perhaps not as well known as it should be. The combination of two preorders $(A, \leq)$ and $(B, \preceq)$, and two functions, $f \in A \leftarrow B$ and $g \in B \leftarrow A$, forms a Galois connection if the following formula holds for all $x \in B$ and $y \in A$.

(5) $\quad f.x \leq y \equiv x \preceq g.y$.

Function f will be called the *lower adjoint* and function g the *upper adjoint*. (These names are chosen because (5) is a special case of the categorical notion of adjoint situation.) Galois connections are interesting because as soon as we recognise one we can immediately deduce a number of useful properties of the adjoints. First of all, we have the two *cancellation properties* $x \preceq g.(f.x)$ and $f.(g.y) \leq y$. These are obtained by instantiatiating (5) 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 specs) the lower adjoint distributes over arbitrary joins and the upper adjoint distributes over arbitrary meets. Conversely, if a function on a complete lattice distributes over arbitrary joins then it has an upper adjoint; dually, if it distributes over arbitrary meets then it has a lower adjoint. This fact will allow us to define the operators of the next subsection.

Finally, Galois-connected functions can be composed to form new Galois connections. To be precise, if the quadruple $(A, \leq_A)$, $(B, \leq_B)$, $f \in A \leftarrow B$ and $g \in B \leftarrow A$ forms a Galois connection and the quadruple $(B, \leq_B)$, $(C, \leq_C)$, $h \in B \leftarrow C$ and $k \in C \leftarrow B$ also forms a Galois connection then so does the quadruple $(A, \leq_A)$, $(C, \leq_C)$, $f \bullet h \in A \leftarrow C$ and $k \bullet g \in C \leftarrow A$. (Here and elsewhere we use the symbol "$\bullet$" for function composition.)

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

We have already seen several examples of Galois connections: (1), (2), and (3) are all instances of (5). To see this for (1), define $f.T = (T, T)$, take for $\leq$ the lattice ordering $\subseteq$ and for $\preceq$ the product ordering $\subseteq \times \subseteq$. Then (1) can be rewritten as $\cup.(R, S) \subseteq T \equiv (R, S) \preceq f.T$. See [14] for an illustration of how the use of this Galois connection considerably enhances calculations with the supremum operator.

A particularly interesting example of a Galois connection is (3): it states that converse is its own upper and lower adjoint, so the join and meet distribution properties of converse follow immediately. Notice also that the fact that converse is its own inverse follows from the two cancellation properties $R^{\cup\cup} \subseteq R$ and $R \subseteq R^{\cup\cup}$.

The assumption that meet distributes over arbitrary joins is equivalent to the existence of a family of Galois connections. To be more specific, for each spec R, there is a function $(R\cap)^\sharp$ that is upper adjoint to the function $(R\cap)$. That is, for all specs S and T, a function $(R\cap)^\sharp$ exists such that

$$R \cap S \subseteq T \;\equiv\; S \subseteq (R\cap)^\sharp.T \quad .$$

(Of course, if the relation algebra is complemented, with complement operator $\neg$, then $(R\cap)^\sharp.T = \neg R \cup T$. The assumption we have made is, however, weaker.) Dually, that join distributes over arbitrary meets is equivalent to the existence, for each spec R, of a function $(R\cup)^\flat$ that is lower adjoint to the function $(R\cup)$. That is, for all specs S and T, a function $(R\cup)^\flat$ exists such that

$$(R\cup)^\flat.T \subseteq S \equiv T \subseteq R\cup S \quad .$$

As we shall see, we do not need to know a closed formula for either $(R\cap)^\sharp$ or $(R\cup)^\flat$, only their existence is required.

2.2 Factors

Recall that composition is universally join-distributive. This, according to the theory of Galois connections just outlined, is equivalent to the existence of two binary operators $\backslash$ and $/$ (pronounced under and over, respectively) defined by the rules:

(6) $$R \subseteq S\backslash T \equiv S\circ R \subseteq T \quad ,$$

(7) $$R \subseteq S/T \equiv R\circ T \subseteq S \quad .$$

These two operators have been given a variety of names in the literature, the oldest being the right and left *residual* operators [10]. We prefer Conway's [7] terminology viz. right and left *factor* operators.

Straightforward consequences of these definitions are the *cancellation* properties

$$R\circ R\backslash S \subseteq S \quad ,$$

$$R/S\circ S \subseteq R \quad .$$

Given the interpretations of composition and inclusion in the relational model it is straightforward to derive the interpretations of the two factor operators. Specifically, we have:

$$x[\![R\backslash S]\!]y \equiv \forall(w\colon w[\![R]\!]x\colon w[\![S]\!]y) \quad .$$

Similarly we have the interpretation:

$$x[\![R/S]\!]y \equiv \forall(z\colon y[\![S]\!]z\colon x[\![R]\!]z) \quad .$$

2.3 Pseudo-Inverses

If two functions are inverses of each other then they are Galois connected. Suppose the inverse functions are F and G. Then we have, for all x in the domain of F, and y in the domain of G,

$$F.x = y \;\equiv\; x = G.y \quad .$$

The two poset orderings needed to establish the connection are the trivial orderings whereby the only ordered elements are equal elements.

This observation has no significance whatsoever for a study of inverse functions: nothing can be gained in such a study by instantiating general theorems about Galois connections that is not predicted by much simpler, direct calculations using the fact that a composition of the one function followed by the other is an identity function. The main benefit that is gained from the observation is that it can suggest properties that one might investigate of Galois-connected functions. An important example is that inverse functions have "inverse" algebraic properties. The exponential function, for instance, has as its inverse the logarithmic function, and

$$\exp(-x) \;=\; \frac{1}{\exp x} \qquad \text{and} \qquad \exp(x+y) \;=\; \exp x \cdot \exp y$$

whereas

$$-\ln x \;=\; \ln(\frac{1}{x}) \qquad \text{and} \qquad \ln x + \ln y \;=\; \ln(x \cdot y) \quad .$$

In general, if F and G are inverse functions then, for any functions h and k of appropriate type,

$$\forall(x :: \; F.(h.x) \;=\; k.(F.x)) \quad\equiv\quad \forall(y :: \; h.(G.y) \;=\; G.(k.y)) \quad .$$

More generally, and expressed at function level, if (F_0, G_0) and (F_1, G_1) are pairs of inverse functions, then for all functions h and k of appropriate type,

$$(8) \qquad F_0 \bullet h \;=\; k \bullet F_1 \quad\equiv\quad h \bullet G_1 \;=\; G_0 \bullet k \quad .$$

The generalisation to Galois connections takes the following form. Suppose, for $i = 0, 1$, $(\mathcal{A}_i, \subseteq_{\mathcal{A}_i})$ and $(\mathcal{B}_i, \subseteq_{\mathcal{B}_i})$ are posets and $(F_i \in \mathcal{A}_i \leftarrow \mathcal{B}_i,\; G_i \in \mathcal{B}_i \leftarrow \mathcal{A}_i)$ are Galois-connected pairs of functions. Let $h \in \mathcal{B}_0 \leftarrow \mathcal{B}_1$ and $k \in \mathcal{A}_0 \leftarrow \mathcal{A}_1$ be arbitrary monotonic functions. Then

$$(9) \qquad F_0 \bullet h \;\dot{\subseteq}\; k \bullet F_1 \quad\equiv\quad h \bullet G_1 \;\dot{\subseteq}\; G_0 \bullet k \quad .$$

(The ordering, $\dot{\subseteq}$, on functions is the usual pointwise extension of the lattice ordering. That is $f \dot{\subseteq} g \;\equiv\; \forall(x :: \; f.x \subseteq g.x)$. Subscripts have been omitted since they can be inferred from the type information.)

As a useful aide mémoire to property (9) we suggest the slogan "Galois-connected functions have pseudo-inverse algebraic properties".

An amusing application of (9) is afforded by the associativity of composition. Highlighting the quantification with respect to the middle variable, thus

$$\forall(S:: (R\circ S)\circ T = R\circ(S\circ T)) \quad ,$$

we have, for all R and T,

$$(R\circ)\bullet(\circ T) = (\circ T)\bullet(R\circ) \quad .$$

We conjecture that the corresponding upper adjoints commute in the same way. Four applications of (9) are needed. First,

$$\begin{array}{ll} & (R\circ)\bullet(\circ T)\ \dot{\subseteq}\ (\circ T)\bullet(R\circ) \\ \equiv & \qquad \{ \qquad (9) \quad \} \\ & (\circ T)\bullet(R\backslash)\ \dot{\subseteq}\ (R\backslash)\bullet(\circ T) \\ \equiv & \qquad \{ \qquad (9) \quad \} \\ & (R\backslash)\bullet(/T)\ \dot{\subseteq}\ (/T)\bullet(R\backslash) \quad . \end{array}$$

Then two further applications of (9) establish the dual property:

$$(R\backslash)\bullet(/T)\ \dot{\supseteq}\ (/T)\bullet(R\backslash) \quad .$$

Thus equality has been established. Reintroducing the variable S we have,

$$R\backslash(S/T) = (R\backslash S)/T \quad ,$$

for all R, S and T.

In fact we seldom explicitly instantiate (9), preferring to use it as a guide to the discovery of useful algebraic properties. Several examples occur in this article. Another example of a pseudo-inverse property is the property $I\backslash R = R$ which is pseudo-inverse to the fact that I is a left unit of composition. That I is a right unit of composition has pseudo-inverse $R/I = R$. Two examples which are particularly important are the pseudo-inverses of the monotonicity of composition, namely that $\backslash$ and $/$ are both monotone in their "upper" argument (i.e. the second argument in the case of $\backslash$ and the first in the case of $/$) and anti-monotone in their "lower" argument.

The final example concerns the *right domain* function $(X \mapsto \top\!\!\top\circ X)$ and its pseudo-inverse, the *right polar* function $(X \mapsto \top\!\!\top\backslash X)$. Specifically, $(X \mapsto \top\!\!\top\circ X)$ is a closure operator, i.e.

$$R\subseteq \top\!\!\top\circ S \equiv \top\!\!\top\circ R\subseteq \top\!\!\top\circ S \quad ,$$

and its pseudo-inverse is an interior operator:

$$R\supseteq \top\!\!\top\backslash S \equiv \top\!\!\top\backslash R\supseteq \top\!\!\top\backslash S \quad .$$

(The term "polarity" was coined by Birkhoff [6].) The proofs are by mutual implication and use only the lattice and monoid structures of a relation algebra.

3 Galois Connections and Fixed Points

One reason why it is important to identify Galois connections early in the development of a theory is the extraordinary usefulness of the theorem we call the "fusion theorem" relating Galois connections and fixed points. This section presents the theorem and then illustrates its use in proving some properties of a regular algebra. For a more complete account of fixed point calculus see [19].

3.1 Fusion

Suppose h is an endofunction on some set partially ordered by the relation $\preceq$. A *fixed point* of h is an element x of the domain of h such that $x = h.x$. A *prefix point* of h is an element x of the domain of h such that $h.x \preceq x$. A *postfix point* of h is an element x of the domain of h such that $x \preceq h.x$. Noting that a postfix point with respect to the ordering $\preceq$ is a prefix point with respect to the converse ordering $\succeq$, we can restrict attention to prefix points. Properties of postfix points are then obtained by turning the ordering around.

For the purposes of this paper it suffices to restrict our attention to the consideration of complete lattices. In such a context we may apply the Knaster-Tarski fixed point theorem with which we assume familiarity. We use the theorem in the following form: every monotonic endofunction, f , on a complete lattice has a least prefix point, denoted here by μf , and a greatest postfix point, denoted here by νf , and both of these are fixed points of the function f .

Let $(A, \leq)$ and $(B, \preceq)$ be complete lattices, and $g \in A \leftarrow A$ and $h \in B \leftarrow B$ be monotonic endofunctions. We denote the least prefix point of g by μg and the least prefix point of h by μh. The question we ask is: given function $f \in B \leftarrow A$ under what conditions can we establish a relationship between μg and μh?

It is easy to derive a condition under which $\mu h \preceq f.\mu g$. Specifically:

$$
\begin{array}{ll}
 & \mu h \preceq f.\mu g \\
\Leftarrow & \qquad \{ \quad \text{definition of } \mu h \quad \} \\
 & h.(f.\mu g) \preceq f.\mu g \\
\Leftarrow & \qquad \{ \quad \text{by definition of } \mu g ,\ g.\mu g \leq \mu g \\
 & \qquad\qquad \bullet \quad f \text{ is monotonic} \quad \} \\
 & h.(f.\mu g) \preceq f.(g.\mu g) \\
\Leftarrow & \qquad \{ \quad y := \mu g \quad \} \\
 & \forall (y :: h.(f.y) \preceq f.(g.y)) \ .
\end{array}
$$

We have thus derived that, for all monotonic functions f ,

(10) $\mu h \preceq f.\mu g \Leftarrow \forall (y :: h.(f.y) \preceq f.(g.y))$.

Property (10) is *not* by itself at all interesting: the weakening in the last step of its proof is very coarse. The property becomes interesting, however, when we combine it with the assumption that f is the upper adjoint in a Galois connection. Suppose that this is so and let $f^\flat$ denote its lower adjoint. (So $f^\flat \in A \leftarrow B$.) Then we recognise in the premise of (10) one side of the "pseudo-invertability" of the algebraic properties of Galois-connected functions — see (9), and we can calculate as follows:

$f^\flat.\mu h \leq \mu g$

$\equiv$ { $(f^\flat, f)$ is a Galois connection }

$\mu h \preceq f.\mu g$

$\Leftarrow$ { (10) — the functions in a Galois connection are necessarily monotonic }

$\forall(y{::}\ h.(f.y) \preceq f.(g.y))$

$\equiv$ { Galois-connected functions have pseudo-inverse algebraic properties: (9) with $F_0,F_1,G_0,G_1,h,k := f^\flat,f^\flat,f,f,h,g$ }

$\forall(x{::}\ f^\flat.(h.x) \leq g.(f^\flat.x))$.

We thus conclude:

(11) $\quad f^\flat.\mu h \leq \mu g \Leftarrow \forall(x{::}\ f^\flat.(h.x) \leq g.(f^\flat.x))$.

This theorem we call the *basic fusion theorem*. (The superscript $\flat$ in the statement of the theorem is intended to remind you of the requirement that the function $f^\flat$ be a lower adjoint in a Galois connection.)

A final step in this investigation is to enquire when the inclusion in the left side of (11) can be strengthened to an equality. By making the substitutions $f, g, h := f^\flat, h, g$ in (10) we obtain immediately

(12) $\quad \mu g \leq f^\flat.\mu h \Leftarrow \forall(x{::}\ g.(f^\flat.x) \leq f^\flat.(h.x))$.

Combining (11) and (12) we obtain the theorem we call the *fusion theorem*:

(13) $\quad f^\flat.\mu h = \mu g \Leftarrow \forall(x{::}\ f^\flat.(h.x) = g.(f^\flat.x))$.

(There is a stronger fusion theorem demanding only that $f^\flat$ be continuous and bottom strict rather than the lower adjoint in a Galois connection —the difference is finite distributivity— but proofs that we know of are substantially more complicated, and we know of no application where the additional strength is needed. More widely known is an incomparable theorem in which all three functions are required to be continuous.)

3.2 The Reflexive Transitive Closure

Inevitably our discussion of induction and well-foundedness will involve the notion of the reflexive transitive closure of a relation. Given spec R, say, we denote its reflexive, transitive closure by R^*.

It is a very educational exercise to rework the well-known properties of the reflexive, transitive closure operator using the fusion theorem and/or the factor operators. (See [19] for details.) This however is not the place for such an exercise, and from now on we will assume the validity of several properties without further ado. Thus we will denote $R \circ R^*$ (equally $R^* \circ R$) by R^+ and we will assume known the fact that R^+ is the transitive closure of R. We also assume known that R^* is also the least solution of the equation in X: $I \cup R \circ X \subseteq X$ as well as the least solution of the equation in X: $I \cup X \circ R \subseteq X$.

The following property, which is not difficult to prove, is mentioned explicitly because it is needed in the proof of Newman's lemma.

(14) $\quad R^* \circ S \circ T^* \;=\; R^* \circ S \cup R^* \circ R \circ S \circ T \circ T^* \cup S \circ T^* \quad .$

Here, in anticipation of some of the later discussion, we present a non-standard property illustrating the use of the fusion theorem. The theorem we want to prove is:

(15) $\quad R^* \circ \mu(X \mapsto R \backslash X) = \mu(X \mapsto R^+ \backslash X) = \mu(X \mapsto R \backslash X) \quad .$

We begin by using (11) to prove:

(16) $\quad T \circ \mu(X \mapsto R \backslash X) \subseteq \mu(X \mapsto T \backslash X) \quad \Leftarrow \quad T \circ T \subseteq T \circ R \quad .$

$$
\begin{array}{ll}
 & T \circ \mu(X \mapsto R \backslash X) \subseteq \mu(X \mapsto T \backslash X) \\
\Leftarrow & \{ \quad \text{fusion: (11)} \quad \} \\
 & \forall (X :: \; T \circ R \backslash X \subseteq T \backslash (T \circ X)) \\
\equiv & \{ \quad \text{factors} \quad \} \\
 & \forall (X :: \; T \circ T \circ R \backslash X \subseteq T \circ X) \\
\Leftarrow & \{ \quad \text{assumption: } T \circ T \subseteq T \circ R, \\
 & \quad\;\; \text{monotonicity of composition} \quad \} \\
 & \forall (X :: \; T \circ R \circ R \backslash X \subseteq T \circ X) \\
\equiv & \{ \quad \text{factor cancellation, monotonicity of composition} \quad \} \\
 & \mathit{true} \quad .
\end{array}
$$

The following simple calculation completes the proof.

$$
\begin{array}{ll}
 & R^* \circ \mu(X \mapsto R \backslash X) \\
= & \{ \quad R^* = I \cup R^+ \quad \}
\end{array}
$$

$$\begin{array}{ll} & \mu(X \mapsto R\backslash X) \cup R^{+} \circ \mu(X \mapsto R\backslash X) \\ \subseteq & \{ \quad (16) \text{ with } T := R^{+} \quad \} \\ & \mu(X \mapsto R\backslash X) \cup \mu(X \mapsto R^{+}\backslash X) \\ = & \{ \quad \text{antimonotonicity of } \backslash \text{ in its first argument} \quad \} \\ & \mu(X \mapsto R\backslash X) \\ \subseteq & \{ \quad I \subseteq R^{*} \quad \} \\ & R^{*} \circ \mu(X \mapsto R\backslash X) \quad . \end{array}$$

Dual to (16) is the following property (also included in anticipation of later requirements):

$$\nu(X \mapsto X \circ R) \,/\, T \supseteq \nu(X \mapsto X \circ T) \Leftarrow T \circ R \supseteq T \circ T \quad .$$

From this one deduces in the same way that

(17) $\quad \nu(X \mapsto X \circ R) \,/\, R^{*} = \nu(X \mapsto X \circ R^{+}) = \nu(X \mapsto X \circ R) \quad .$

4 The Monotype-Condition Isomorphism

4.1 Sets as Specs

Given a relation R, the *left domain* and *right domain* of R are defined as follows. Its left domain is the set $\{x \mid \exists(y{::}\, x[\![R]\!]y)\}$. Its right domain is the set $\{x \mid \exists(y{::}\, y[\![R]\!]x)\}$. (These are commonly called the domain and range of the relation. We prefer "left" and "right" domain in order not to introduce an artificial and unnecessary direction to relations.)

One of the beauties of relation algebra is that it is possible to represent sets as relations. Calculations with sets thus become special cases of calculations with relations. In particular, calculations with domains remain within the calculus itself and do not need to be conducted in some other formal framework. There are however several mechanisms for viewing sets as relations each of which has its own merits. Calculations are often made significantly more effective if one has a good grasp of exactly what the merits and demerits of each is.

One mechanism for representing sets as relations is via so-called "monotypes" (sometimes called "coreflexives" [15]), a second is via "left conditions" and a third via "right conditions" (sometimes called "row" and "column vectors" [24]). Axiomatically, these have the following definitions. First: we say that spec A is a *monotype* iff $A \subseteq I$. Second: we say that spec p is a *right condition* iff $p = \top\!\!\top \circ p$. Third: we say that spec p is a *left condition* iff $p = p \circ \top\!\!\top$.

It is clear that for any given universe $\mathcal{U}$ there is a one-to-one correspondence between the subsets of $\mathcal{U}$ and the monotypes. Specifically, the set A is represented by the monotype $\underline{A}$ where $x[\![\underline{A}]\!]y \equiv x{=}y \wedge x{\in}A$. Equally clear is the existence of a one-to-one correspondence between the subsets of $\mathcal{U}$ and the right conditions on $\mathcal{U}$. That is, if A

is some set then the right condition defined by A is that spec A_r such that for all x and y, $x[\![A_r]\!]y \equiv y{\in}A$. Similarly, the left condition corresponding to A is that spec A_l such that for all x and y, $x[\![A_l]\!]y \equiv x{\in}A$.

Using monotypes to represent subsets of $\mathcal{U}$ as specs a restriction on a spec is modelled by composition of the spec, either on the left or on the right, with such a monotype. Thus, if R and S are specs and A is a monotype then $A \circ R$ and $S \circ A$ are both specs, the first being interpreted as the relation R after restricting elements in its left domain to those elements in (the interpretation of) A, and the second being interpreted as the relation S after restricting elements in its right domain to those elements in A. Using conditions a restriction on the left domain of relation R is modelled by the intersection of R with a left condition, and a restriction on the right domain of R by its intersection with a right condition.

The right domain of a relation R is the smallest set such that restriction of the relation on the right to elements of that set has no effect on the relation. If we choose to represent sets by right conditions in relation algebra then it is quite obvious how to represent the right domain of R: it is $\top\!\!\top \circ R$ since

$$\forall(p\colon\ p = \top\!\!\top \circ p\colon\ p \cap R = R\ \equiv\ \top\!\!\top \circ R \subseteq p)\quad .$$

The straightforward proof of this claim makes use of only the lattice and monoid structures of a relation algebra. It is thus also valid within a regular algebra. If, on the other hand, we choose to represent sets by monotypes then the right domain of R is represented by the formula $I \cap \top\!\!\top \circ R$. This is an uglier formula than $\top\!\!\top \circ R$ because it combines two operators (meet and composition) whose behaviour relative to each other is complicated. Proof of the corresponding claim,

$$\forall(A\colon\ A \subseteq I\colon\ R \circ A = R\ \equiv\ I \cap \top\!\!\top \circ R \subseteq A)\quad ,$$

demands use of the modular identity, and thus all four substructures in a non-complemented relation algebra. It is thus not generally valid in a regular algebra.

These, and other, considerations seem to suggest that right conditions are the best way to represent right domains, and, dually, left conditions are the best way to represent left domains. The prominent role of composition in relation algebra, however, argues for the other choice. The point is that by choosing to represent sets by *monotypes* one can exploit to the full the enormous calculational benefit of the associativity of composition. Thus, if A is a monotype and R and S are specs, the composition $R \circ A \circ S$ can either be read as $(R \circ A) \circ S$ — a restriction on the right domain of R — or as $R \circ (A \circ S)$ — a restriction on the left domain of S. If one chooses to represent sets by left and/or right conditions then one must invent calculational rules that allow one to transform one type of restriction into the other.

The most effective calculations in relation algebra (as opposed to, for example, regular algebra) recognise and exploit the individual merits of conditions and monotypes, and thus involve a continual interplay between the two representations. This interplay is a major theme of calculations in this article. Roughly speaking, general properties of domains are often easily *established* by using the condition representation but become most *useful* when reexpressed in terms of monotypes.

4.2 The Isomorphism Formalised

Representing sets by right conditions the right domain of a spec is constructed by applying the function $(X \mapsto \top\!\!\top \circ X)$. Let us denote this function briefly by $(\top\!\!\top \circ)$.

As remarked above, in the calculus of relations the right conditions are in one-to-one correspondence with the monotypes. One element of that correspondence is the function $(\top\!\!\top \circ)$ restricted to the monotypes. Since, however, the function $(\top\!\!\top \circ)$ is a total function on *all* specs, it is desirable to seek likewise a total function on *all* specs that has range the monotypes and when restricted to the right conditions is the function $(\top\!\!\top \circ)$'s inverse. There is a closed form for this function — mentioned above — , namely the function $(X \mapsto \top\!\!\top \circ X \cap I)$. Since this closed form is unwieldy, it is preferable to avoid its use altogether. Instead we introduce the symbol " $>$ " written as a postfix to its argument to denote the function and define it to be the *lower* Galois adjoint of the function $(\top\!\!\top \circ)$ restricted to monotypes. That is, for all specs R and all monotypes A,

$$R{>} \subseteq A \equiv R \subseteq \top\!\!\top \circ A \quad .$$

We call this operator the *right domain operator*.

The *left* domain operator is defined in a similar fashion. We have, for all specs R and all monotypes A,

$$R{<} \subseteq A \equiv R \subseteq A \circ \top\!\!\top \quad .$$

The existence of the domain operators is guaranteed by the axioms stated in section 1, in particular the modular identity. Since the calculations are not relevant to the current discussion we omit them here.

We are now in a position to express formally in relation algebra the isomorphism between conditions and monotypes. Specifically, the right domain operator maps right conditions to monotypes, the function $(\top\!\!\top \circ)$ is its inverse: for all monotypes A and all right conditions p

(18) $\quad A = (\top\!\!\top \circ A){>} \quad ,$

(19) $\quad p = \top\!\!\top \circ p{>} \quad .$

Yet more can be said. The function $(\top\!\!\top \circ)$ is in fact a lattice isomorphism between the lattice of monotypes and the lattice of right conditions. That is, for all monotypes A and B,

$$A \subseteq B \equiv \top\!\!\top \circ A \subseteq \top\!\!\top \circ B \quad .$$

The right domain operator, being inverse to $(\top\!\!\top\circ)$, is thus also such a lattice isomorphism. Moreover, the rules (18) and (19) can both be made more general. Specifically, for all specs R ,

$$(\top\!\!\top\circ R)> = R> \quad ,$$

and

$$\top\!\!\top \circ R> \;=\; \top\!\!\top\circ R \quad .$$

Of course, all of these rules have duals for left conditions and left domains.

4.3 Condition and Monotype Factors

The universal distributivity of composition over join, effectively and concisely captured by the two Galois connections (6) and (7), is a crucial algebraic property of relation algebra. An advantage of subsuming set calculus within relation calculus is economy of proof: many properties of sets are just special cases of properties of specs.

Suppose we specialise (6) by instantiating R and T to left conditions p and q . The property remains valid, of course. So, formally, we have for all p and q such that $p = p\circ\top\!\!\top$ and $q = q\circ\top\!\!\top$,

(20) $\quad p \subseteq S\backslash q \equiv S\circ p \subseteq q \quad .$

We note also that $S\circ p$ is a left condition (given that p is a left condition). Furthermore, by the simple calculation below, $S\backslash q$ is also a left condition.

$$
\begin{array}{ll}
 & S\backslash q \circ \top\!\!\top = S\backslash q \\
\equiv & \quad \{ \quad I \subseteq \top\!\!\top \;\; \text{and composition is monotonic} \quad \} \\
 & S\backslash q \circ \top\!\!\top \subseteq S\backslash q \\
\equiv & \quad \{ \quad \text{Galois connection defining factor} \quad \} \\
 & S \circ S\backslash q \circ \top\!\!\top \subseteq q \\
\Leftarrow & \quad \{ \quad \text{cancellation of factors} \quad \} \\
 & q\circ\top\!\!\top \subseteq q \\
\equiv & \quad \{ \quad I \subseteq \top\!\!\top \;\; \text{and composition is monotonic} \quad \} \\
 & q\circ\top\!\!\top = q \quad .
\end{array}
$$

Thus (20) is a Galois connection between the lattice of left conditions and itself.

Computing scientists know $S\backslash q$ as the *weakest liberal precondition* guaranteeing termination of statement S in a state satisfying q . (Execution of S is viewed here as proceeding from right to left. Thus the “left domain” of S in our terminology is its range and its “right domain” is its domain in standard terminology.) To see this we simply have to fill in the interpretation of right factors and the interpretation of right conditions. More directly:

$$
\begin{array}{ll}
 & x \in [\![S\backslash q]\!] \\
\equiv & \qquad \{ \qquad \text{set calculus} \quad \} \\
 & \{x\} \subseteq [\![S\backslash q]\!] \\
\equiv & \qquad \{ \qquad (20) \text{ with } [\![p]\!] := \{x\} \qquad \} \\
 & \forall(w \colon w[\![S]\!]x \colon w \in [\![q]\!]) \quad .
\end{array}
$$

Similarly we can instantiate R and T in (7) to *right* conditions p and q. The term S/q can also be interpreted as the weakest liberal precondition guaranteeing termination of statement S in a state satisfying q so long as we reinterpret "left domain" as domain and "right domain" as range. (This indeed is more conventional in programming texts.)

Because of the ubiquity of (relational) composition as a primitive of program composition it is better to express weakest liberal preconditions in terms of monotypes. This is straightforward to do using the isomorphism between monotypes and the two types of condition. Specifically, we define, for all specs S and all monotypes A, the (right) *monotype factor* $S\mathbin{\backslash\!\!\!\cdot}A$ by, for all monotypes A and B and all specs S,

(21) $\quad A \subseteq S\mathbin{\backslash\!\!\!\cdot}B \equiv (S\circ A){<} \subseteq B \quad .$

Its dual is:

(22) $\quad A \subseteq B\mathbin{/\!\!\!\cdot}S \equiv (A\circ S){>} \subseteq B \quad .$

Note that $S\backslash q$ for left condition q and $S\mathbin{\backslash\!\!\!\cdot}B$ for monotype B are both interpreted as weakest liberal preconditions. Specifically,

$$x \in [\![S\mathbin{\backslash\!\!\!\cdot}B]\!] \equiv \forall(y \colon y[\![S]\!]x \colon y \in [\![B]\!]) \quad .$$

The isomorphism between the two representations can be expressed formally by the identity:

$$R\backslash(A\circ\top\!\!\top) \subseteq S\backslash(B\circ\top\!\!\top) \equiv R\mathbin{\backslash\!\!\!\cdot}A \subseteq S\mathbin{\backslash\!\!\!\cdot}B \quad .$$

For our own convenience it is useful to record some elementary properties of monotype factors here. Those readers familiar with weakest liberal preconditions will recognise the interpretations of these properties as old and faithful friends. (See [4] for a more detailed discussion of the connection.) The proofs we give may be less familiar and are illustrative of the elegance of calculations with Galois connections.

From (22) and (21) we obtain the cancellation properties:

(23) $\quad (S\circ S\mathbin{\backslash\!\!\!\cdot}B){<} \subseteq B \quad$ and $\quad (B\mathbin{/\!\!\!\cdot}S\circ S){>} \subseteq B \quad .$

Often these properties are used in a different form, namely:

(24) $\quad S\circ S\mathbin{\backslash\!\!\!\cdot}B \subseteq B\circ S \quad$ and $\quad B\mathbin{/\!\!\!\cdot}S\circ S \subseteq S\circ B \quad .$

The equivalence of the leftmost conjuncts in (24) and (23) is an instance of the more general

$$(S\circ A)< \subseteq B \;\equiv\; S\circ A \subseteq B\circ S \quad .$$

The equivalence of the two other conjuncts is of course completely dual.

Two other properties that are needed further on are:

(25) $\quad R\backslash A \circ S\backslash A = (R\cup S)\backslash A \qquad \text{and} \qquad R\backslash A = A/R^{\cup} \quad .$

Both can be proved straightforwardly using the rule of indirect equality —that is, for all R and S,

$$R = S \;\equiv\; \forall(T{::}\; R\subseteq T \equiv S\subseteq T) \quad ,$$

— in combination with the Galois connections defining the various operators.

5 Well-Foundedness

Having completed these preliminaries we are now in a position to formulate the notion of well-foundedness in relation algebra. This we do in three ways which we then prove to be equivalent.

Expressed in terms of points, a relation R is said to be well-founded if there are no infinite chains x_0, x_1, ... such that $x_{i+1}\,R\,x_i$ for all i, $i\geq 0$. A relation R is thus *not* well-founded if there is a set A such that

$$A \neq \phi \wedge \forall(x{:}\, x{\in}A{:}\, \exists(y{:}\, y{\in}A{:}\, y[\![R]\!]x)) \quad .$$

Noting that $\exists(y{:}\, y{\in}A{:}\, y[\![R]\!]x) \equiv x \in (A\circ R)>$ this definition converts directly into the following point-free form.

Definition 26 (Monotype-well-founded) Spec R is said to be *monotype-well-founded* if and only if it satisfies

$$\forall(A{:}\;\; A\subseteq I{:}\;\; A\subseteq \perp\!\!\perp \;\Leftarrow\; A\subseteq (A\circ R)>) \quad .$$

□

Characteristic of definition 26 is that it is a rule for establishing when a set represented by a monotype A, $A\subseteq I$, is empty. In the next definition we represent sets by conditions.

Definition 27 (Condition-well-founded) Spec R is said to be *condition-well-founded* if and only if it satisfies

$$\forall(p{:}\;\; p = \top\!\!\top\circ p{:}\;\; p\subseteq \perp\!\!\perp \;\Leftarrow\; p\subseteq p\circ R) \quad .$$

□

In the third definition we replace sets by arbitrary relations.

Definition 28 (Spec-well-founded) Spec R is said to be *spec-well-founded* if and only if it satisfies

$$\forall(S{::}\ \ S\subseteq\bot\!\!\bot \ \Leftarrow\ S\subseteq S\circ R)\ \ .$$

□

(This definition appears elsewhere under different names: for example, "definite" [3], "progressively finite" [24] and "right founded" [9].)

Note that all three definitions can also be expressed in terms of greatest prefix points. For example, R is monotype-well-founded equivales $\nu(A\mapsto(A\circ R)>)=\bot\!\!\bot$. The form of the definitions is the one that corresponds most directly to the standard definitions; later, particularly when we wish to appeal to the fusion theorem, we use the definition in terms of greatest fixed points.

The claim is that all three definitions of well-foundedness are equivalent.

As is to be expected the equivalence between monotype- and condition-well-foundedness is a straightforward consequence of the isomorphism between monotypes and conditions.

Theorem 29 For all R, R is monotype-well-founded equivales R is condition-well-founded.

Proof With dummies p and A ranging over right conditions and monotypes, respectively, we have:

$$
\begin{array}{ll}
 & \forall(p{::}\ \ p\subseteq\bot\!\!\bot \ \Leftarrow\ p\subseteq p\circ R) \\
\equiv & \qquad\{\qquad \text{range translation: } A\mapsto\top\!\!\top\circ A \text{ is a bijection} \quad\} \\
 & \forall(A{::}\ \ \top\!\!\top\circ A\subseteq\bot\!\!\bot \ \Leftarrow\ \top\!\!\top\circ A\subseteq\top\!\!\top\circ A\circ R) \\
\equiv & \qquad\{\qquad \text{monotype-condition isomorphism} \quad\} \\
 & \forall(A{::}\ \ A\subseteq\bot\!\!\bot \ \Leftarrow\ A\subseteq(A\circ R)>)\ \ .
\end{array}
$$

□

The equivalence between condition- and spec-well-founded takes a little more work.

Theorem 30 For all R, R is condition-well-founded equivales R is spec-well-founded.

Proof Condition-well-foundedness of R is obviously implied by spec-well-foundedness of R (since every condition is also a spec). To prove the opposite implication assume that R is condition-well-founded. Then, for all S we have:

$$
\begin{array}{ll}
 & S\subseteq\bot\!\!\bot \\
\equiv & \qquad\{\qquad \top\!\!\top\circ\bot\!\!\bot=\bot\!\!\bot\ , \\
 & \qquad\qquad\ \ \text{the function } (X\mapsto\top\!\!\top\circ X) \text{ is a closure operator} \quad\}
\end{array}
$$

$$\top\!\!\top \circ S \subseteq \perp\!\!\perp$$

$$\Leftarrow \qquad \{ \qquad \top\!\!\top \circ S = \top\!\!\top \circ (\top\!\!\top \circ S) \ ,$$

$$\bullet \quad R \text{ is condition-well-founded} \quad \}$$

$$\top\!\!\top \circ S \subseteq (\top\!\!\top \circ S) \circ R$$

$$\equiv \qquad \{ \qquad \text{associativity of } \circ \quad \}$$

$$\top\!\!\top \circ S \subseteq \top\!\!\top \circ (S \circ R)$$

$$\Leftarrow \qquad \{ \qquad \text{monotonicity of } \circ \quad \}$$

$$S \subseteq S \circ R \ .$$

□

In view of theorem 30 we no longer make the distinction between "monotype", "condition" or "spec" well-founded; we say that R is *well-founded* if it satisfies any one of three definitions.

The following (well-known) theorem is now an immediate consequence of (17). We mention it in order to illustrate the advantage of using a definition like definition 28 in which there is no type distinction in the variables.

Theorem 31 For all R, that R is well-founded equivales that R^+ is well-founded.

□

The calculations in this section are all very straightforward because they deal with operators and constants that are familiar. In the next section we "pseudo-invert" all the calculations. Because of the relative unfamiliarity of the operators (in particular the use of $\backslash$ instead of $\circ$) the calculations may seem less straightforward but are not really.

This concludes this section. We have established the equivalence of the properties:

- R is condition-well-founded
- R is monotype-well-founded
- R is spec-well-founded
- R^+ is (condition-, monotype- or spec-) well-founded.

6 The Induction Principle

A relation R is said to *admit induction* if the following schema can be used to establish that property P holds everywhere: prove, for all y, that the induction hypothesis $\forall(x{:}\, x[\![R]\!]y{:}\, P.x)$ implies $P.y$. That is, expressed in terms of points, R admits induction iff

$$\forall(y{::}\, P.y) \Leftarrow \forall(y{::}\, \forall(x{:}\, x[\![R]\!]y{:}\, P.x) \Rightarrow P.y) \ .$$

In this section we formulate the notion of admitting induction in relation algebra in three different ways and then show the equivalence of all three.

6.1 The Definitions

The pointwise definition of "admits induction" given above is in terms of predicates. Because we want to arrive at a definition in terms of relations we first reformulate it in terms of sets. So we define: relation R admits induction if and only if:

$$(32) \qquad \forall(y{::}\, y{\in}A) \Leftarrow \forall(y{::}\, \forall(x{:}\, x\llbracket R\rrbracket y{:}\, x{\in}A) \Rightarrow y{\in}A) \quad .$$

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 $I \subseteq A$. Furthermore, we see that the expression in the domain of the antecedent, $\forall(x{:}\, x\llbracket R\rrbracket y{:}\, x{\in}A)$, is just $y \in R\mathbin{\backslash\!\!\cdot} A$. So (32) can be drastically simplified to

$$(33) \qquad I \subseteq A \Leftarrow R\mathbin{\backslash\!\!\cdot} A \subseteq A \quad ,$$

for all monotypes A.

To aid the intuition a bit: $R\mathbin{\backslash\!\!\cdot} A$ corresponds to what is usually called the induction hypothesis, while a proof of $R\mathbin{\backslash\!\!\cdot} A \subseteq A$ is a proof of the induction step.

This then is the first definition of "admits induction".

Definition 34 (Monotype Induction) The spec R is said to *admit induction on monotypes* if and only if it satisfies

$$\forall(A{:}\; A \subseteq I{:}\; I \subseteq A \Leftarrow R\mathbin{\backslash\!\!\cdot} A \subseteq A) \quad .$$

□

If instead of representing sets by monotypes we choose to represent them by left conditions we arrive at the following definition:

Definition 35 (Condition Induction) The spec R is said to *admit induction on (left) conditions* if and only if it satisfies

$$\forall(p{:}\; p = p{\circ}\top\!\!\top{:}\; \top\!\!\top \subseteq p \Leftarrow R\backslash p \subseteq p) \quad .$$

□

Again we propose a definition in which the type difference between the variables is removed.

Definition 36 (Spec Induction) The spec R is said to *admit spec induction* if and only if it satisfies

$$\forall(S{::}\; \top\!\!\top \subseteq S \Leftarrow R\backslash S \subseteq S) \quad .$$

□

Note that all three definitions can also be expressed in terms of least prefix points. For example, R admits spec induction equivales $\mu(S \mapsto R\backslash S) = \top\!\!\top$. The form of the definitions is the one that corresponds most directly to the standard definition; later, particularly when we wish to appeal to the fusion theorem, we use the definition in terms of least fixed points.

We prove the equivalence of all three definitions by "pseudo-inverting" the proofs of theorems 29 and 30:

Theorem 37 For all specs R, that R admits induction on monotypes equivales that R admits induction on conditions.

Proof The proof is obtained by "pseudo-inverting" the proof of theorem 29. With dummies p and A ranging over left conditions and monotypes, respectively, we have:

$$
\begin{array}{ll}
 & \forall(p{::}\ \top\!\!\top \subseteq p \ \Leftarrow\ R\backslash p \subseteq p) \\
\equiv & \quad \{ \quad \text{range translation: } A \mapsto A\circ\top\!\!\top \text{ is a bijection} \quad \} \\
 & \forall(A{::}\ \top\!\!\top \subseteq A\circ\top\!\!\top \ \Leftarrow\ R\backslash(A\circ\top\!\!\top) \subseteq A\circ\top\!\!\top) \\
\equiv & \quad \{ \quad \text{condition-monotype isomorphism} \quad \} \\
 & \forall(A{::}\ I \subseteq A \ \Leftarrow\ R\backslash A \subseteq A) \quad .
\end{array}
$$

□

Theorem 38 For all specs R, that R admits induction on conditions equivales that R admits induction on specs.

Proof It is obvious that R admits induction on conditions whenever it admits induction on specs (since every condition is also a spec). To prove the opposite implication assume that R admits induction on conditions. Then, for all S we have:

$$
\begin{array}{ll}
 & \top\!\!\top \subseteq S \\
\equiv & \quad \{ \quad /\top\!\!\top \text{ is an interior operator, } \top\!\!\top/\top\!\!\top = \top\!\!\top \quad \} \\
 & \top\!\!\top \subseteq S/\top\!\!\top \\
\Leftarrow & \quad \{ \quad S/\top\!\!\top = S/\top\!\!\top \circ \top\!\!\top \quad , \\
 & \qquad \bullet \quad R \text{ admits induction on left conditions} \quad \} \\
 & R\backslash(S/\top\!\!\top) \subseteq S/\top\!\!\top \\
\equiv & \quad \{ \quad \text{associativity of } \backslash \text{ and } / \quad \} \\
 & (R\backslash S)/\top\!\!\top \subseteq S/\top\!\!\top \\
\Leftarrow & \quad \{ \quad \text{monotonicity of } /\top\!\!\top \quad \} \\
 & R\backslash S \subseteq S \quad .
\end{array}
$$

□

Just as we did in the case of well-foundedness we will now speak only of "admitting induction" rather than "admitting set induction" or "admitting spec induction".

The theorem comparable to theorem 31 is the following:

Theorem 39 For all specs R, that R admits induction equivales that R^+ admits induction.

Proof This is immediate from property (15), in particular the equality between the second and third terms.

□

This concludes this section. We have established the equivalence of

- R admits monotype induction
- R admits condition induction
- R admits spec induction
- R^+ admits (set or spec) induction.

7 The Uep of Regular Algebra

We remarked earlier that definition 28 appeared in [3] where it was called "definiteness". Reference [3] was about applying regular algebra to path-finding problems, and a fundamental fact exploited in that paper was that the property of being a regular algebra is preserved by matrix formation. Salomaa's axiomatisation [23] of regular algebra, however, involved the use of the so-called "empty word property", the formulation of which does not extend to matrices. As a replacement for Salomaa's rule the following rule was postulated in [3] as an axiom of regular algebra:

$$R \text{ is spec-well-founded} \equiv \forall(S,T\!:: \; T = S \cup T \circ R \;\equiv\; T = S \circ R^*) \quad .$$

We call this rule the *unique extension property (uep) of regular algebra.* (In fact only an implication was postulated in [3]. As we see below the follows-from is very straightforward; it is also of lesser importance. Also, as stated earlier, the terminology "definite" was used instead of "spec-well-founded".)

In this section we show that the rule is valid for any algebra complying with the properties detailed in sections 1.1 and 1.2 (the lattice and monoid structures of a relation algebra).

To make the discussion more precise we introduce yet another definition.

Definition 40 Spec R is said to be uniquely extendable iff it satisfies

(41) $\forall(S,T\!:: \; T = S \cup T \circ R \;\equiv\; T = S \circ R^*) \quad .$

□

Our claim is that unique-extendability and well-foundedness are equivalent properties.

The first step is to rewrite (41) replacing fixed points by postfix points.

Lemma 42 That spec R is uniquely extendable is equivalent to both of the following:

(a) $\nu(T \mapsto S \cup T{\circ}R) = S \circ R^*$,

(b) $\forall(S,T{::}\ T \subseteq S \cup T{\circ}R \Rightarrow T \subseteq S \circ R^*)$.

Moreover, that spec R is well-founded is equivalent to both of the following:

(c) $\nu(T \mapsto T{\circ}R) = \perp\!\!\perp$,

(d) $\forall(T{::}\ T = T{\circ}R \equiv T = \perp\!\!\perp)$.

Proof The claimed equivalences are a consequence of a general property of fixed points. Specifically, for all monotonic endofunctions f on a complete lattice the following properties are all equivalent:

(e) f has a unique fixed point ,

(f) $\nu f = \mu f$,

(g) $\forall(x,y{:}\ f.x \subseteq x \wedge y \subseteq f.y{:}\ y \subseteq x)$,

(h) $\forall(y{:}\ y \subseteq f.y{:}\ y \subseteq \mu f)$,

(i) $\forall(x{:}\ f.x \subseteq x{:}\ \nu f \subseteq x)$.

The equivalence of (e) and (f) follows from the fact that a least prefix point of a monotonic function is also a least fixed point of the function, and, dually, a greatest postfix point is also a greatest fixed point. The equivalence of (f), (g) and (h) is established in the following calculation. The inclusion of (i) in the list follows by duality.

$\forall(y{:}\ y \subseteq f.y{:}\ y \subseteq \mu f)$

$\Rightarrow$ { range restriction, $y := \nu f$ }

$\nu f \subseteq \mu f$

$\equiv$ { Knaster-Tarski (specifically, a least prefix point is a least fixed point, and a greatest postfix point is a greatest fixed point) }

$\nu f = \mu f$

$\Rightarrow$ { $y \subseteq f.y \Rightarrow y \subseteq \nu f$, $f.x \subseteq x \Rightarrow \mu f \subseteq x$ and transitivity, }

$$\forall(x,y\colon\ f.x\subseteq x \wedge y\subseteq f.y\colon\ y\subseteq x)$$

$\Rightarrow$ { range restriction, $x := \mu f$ }

$$\forall(y\colon y\subseteq f.y\colon y\subseteq \mu f) \quad .$$

The definition of unique extendability (to be precise (41)) is an instance of (e), and (a) and (b) are instances of (f) and (h), respectively. Similarly, the definition of well-foundedness (to be precise definition 28) is an instance of (h) — noting that $\perp\!\!\!\perp$ is obviously the least prefix point of the function $S\mapsto S\circ R$ — and (c) and (d) are instances of (f) and (e), respectively.
□

From lemma 42 it is obvious that well-foundedness of R is just a special case of its unique-extendability: just instantiate S to $\perp\!\!\!\perp$ in (a) to obtain (c). In other words, if R is uniquely extendable then it is well-founded. This is the elementary part of the proof. The harder part is the reverse implication.

In words, lemma 42 states that the greatest postfix point of the function $T\mapsto S\cup T\circ R$ is $S\circ R^*$. We want to relate this to R being well-founded – i.e. the greatest fixed point of the function $T\mapsto T\circ R$ is $\perp\!\!\!\perp$. In general, $\nu(T\mapsto S\cup T\circ R)\supseteq \nu(T\mapsto T\circ R)$ since ν is a monotonic function. Let us therefore endeavour to solve the equation in X :

$$\nu(T\mapsto S\cup T\circ R) = X\cup \nu(T\mapsto T\circ R) \quad .$$

We have:

$$\nu(T\mapsto S\cup T\circ R) = X\cup \nu(T\mapsto T\circ R)$$

$\Leftarrow$ { fusion theorem: $(X\cup)$ is by assumption universally $\cap$-distributive and thus an upper adjoint }

$$\forall(T{::}\ S\cup(X\cup T)\circ R = X\cup T\circ R)$$

$\equiv$ { distributivity }

$$\forall(T{::}\ S\cup X\circ R\cup T\circ R = X\cup T\circ R)$$

$\equiv$ { calculus }

$$S\cup X\circ R = X \quad .$$

Since a least prefix point is also a fixed point we conclude:

(43) $\quad \nu(T\mapsto S\cup T\circ R) \;=\; S\circ R^*\cup \nu(T\mapsto T\circ R) \quad .$

Whence:

Lemma 44 If R is well-founded then R is uniquely extendable.

Proof

$$
\begin{array}{ll}
 & R \text{ is well-founded} \\
\equiv & \{ \quad \text{lemma 42} \quad \} \\
 & \nu(T \mapsto T \circ R) = \perp\!\!\perp \\
\Rightarrow & \{ \quad (43) \quad \} \\
 & \nu(T \mapsto S \cup T \circ R) = \ S \circ R^* \\
\equiv & \{ \quad S \circ R^* = \mu(T \mapsto S \cup T \circ R) \ \text{ and lemma 42} \quad \} \\
 & R \text{ is uniquely extendable} \ .
\end{array}
$$

$\Box$

Summarising, we have proved:

Theorem 45 That R is well-founded equivales that R is uniquely-extendable.

$\Box$

Property 42(b) is an attractive way of expressing well-foundedness. It is formally stronger than definition (28) since that definition is obtained by instantiating S to $\perp\!\!\perp$. It also illustrates clearly and succinctly why well-foundedness is a useful attribute of a spec: in comparison to the definition of R^* which gives one a mechanism for proving inclusion of $S \circ R^*$ in a spec T, well-foundedness of R gives one a mechanism for proving inclusion of a spec T in $S \circ R^*$.

8 Admits-induction Implies Well-Founded

Now that we have seen several equivalent definitions of well-founded it is time to explore its relationship to admitting induction. The following lemma is the key insight.

Lemma 46 $\nu(T \mapsto T \circ R) \circ \mu(T \mapsto R \backslash T) = \perp\!\!\perp$.

Proof We have, for all X,

$$
\begin{array}{ll}
 & X \circ \mu(T \mapsto R \backslash T) = \perp\!\!\perp \\
\equiv & \{ \quad \perp\!\!\perp = \mu(T \mapsto T) \quad \} \\
 & X \circ \mu(T \mapsto R \backslash T) \subseteq \mu(T \mapsto T) \\
\Leftarrow & \{ \quad \text{basic fusion theorem} \quad \} \\
 & \forall (T :: \ X \circ R \backslash T \subseteq X \circ T) \\
\Leftarrow & \{ \quad \text{factor cancellation} \quad \} \\
 & X \subseteq X \circ R
\end{array}
$$

$$\Leftarrow \qquad \{ \qquad \text{definition of } \nu(T \mapsto T \circ R) \qquad \}$$
$$X \subseteq \nu(T \mapsto T \circ R) \ .$$

□

Theorem 47 If R admits induction then R is well-founded.

Proof If R admits induction then, by definition, $\mu(T \mapsto R \backslash T) = \top\!\!\top$. So, by lemma 46, $\nu(T \mapsto T \circ R) \circ \top\!\!\top = \bot\!\!\bot$. But then, since $I \subseteq \top\!\!\top$, $\nu(T \mapsto T \circ R) \subseteq \bot\!\!\bot$. By definition 28 we have thus established that R is well-founded.
□
The proof might almost be described as "elementary" but that is only because of the preparatory work completed before embarking on it. Its simplicity is due in no small measure to the formulation of well-foundedness and admits induction in terms of *specs* rather than in terms of *sets*.

One might suppose that "pseudo-inverting" the above leads to a proof that well-foundedness implies admits-induction. Unfortunately this is not the case: a true inverse, viz. complementation, is needed to do that. We shall not present the proof since the equivalence between well-foundedness and admitting induction in a complemented relation algebra is well-known. To prove the theorem using the techniques developed here it suffices to know that $R \backslash S = \neg(R^{\cup} \circ \neg S)$. This fact can then be used to construct a function f such that $\nu(T \mapsto T \circ R) = f.\mu(T \mapsto R \backslash T)$. (μ-fusion should be used bearing in mind the Galois connection $\neg R \subseteq S \ \equiv \ R \supseteq \neg S$ and being particularly careful about the reversal of the ordering relation.) Having constructed f it is then straightforward to establish the equivalence between the two notions. Readers who successfully tackle this exercise will have the assurance of full understanding. Pseudo-inverting lemma 46 — investigate conditions under which $\nu(T \mapsto T \circ R) \,/\, X = \top\!\!\top$ — leads to the theorem that $\nu(T \mapsto T \circ R)$ is a right condition. We also leave this as an exercise. A final exercise is to show that $\mu(T \mapsto R \backslash T)$ is a left condition.

9 Newman's Lemma

Newman's lemma [20] is a lemma from the study of term rewriting systems. These systems play an important role in, for instance, the implementation of functional programming languages. By definition, a term rewrite system is a set, together with a set of rewrite rules. A typical, and one of the oldest, examples is the λ-calculus: a set of terms, together with a set of rewrite rules such as β-reduction. The rewrite rules induce a relation on the terms of the system, so, reduced to its bare essentials, a term rewrite system is just a relation. Now an important property of the relation associated with a term rewrite system is that of confluence, another one is local confluence (also known as the Church-Rosser and weakly Church-Rosser properties respectively). For an account of term rewrite systems in general and these properties in particular see [18].

Newman's lemma states that any relation that admits induction and is locally confluent is also confluent. First we formulate these two properties in the relational calculus. Spec R is confluent is equivalent to

(48) $\quad R^* \circ (R^{\cup})^* \subseteq (R^{\cup})^* \circ R^* \quad .$

Spec R is locally confluent is

(49) $\quad R \circ R^{\cup} \subseteq (R^{\cup})^* \circ R^* \quad .$

See [5] for how to obtain these definitions from the usual formulations. Because it turns out that it is not essential for the proof of the lemma that the specs are each others converse, we generalise (48) and (49) to

(50) $\quad R^* \circ S^* \subseteq S^* \circ R^* \quad ,$

and

(51) $\quad R \circ S \subseteq S^* \circ R^* \quad .$

This generalisation of confluence is called commutation in the literature. Thus the first, (50) is a point free formulation of the fact that R and S commute, whereas the second (51) says that R and S commute locally. Using these terms we can now formulate the following generalisation of Newman's lemma.

Lemma 52 (Newman) If R and S are specs such that $R \cup S^{\cup}$ admits induction and R and S commute locally, then R and S commute.

Proof First we remark that we have, by the properties (25) of monotype factors, and the fact that converse is its own inverse:

(53) $\quad (R \cup S^{\cup}) \backslash A = R \backslash A \circ A / S \quad .$

So the assumption that $R \cup S^{\cup}$ admits induction is equivalent to, for all monotypes A:

(54) $\quad R \backslash A \circ A / S \subseteq A \Rightarrow I \subseteq A \quad .$

We also have the assumption that R and S commute locally, i.e.

(55) $\quad R \circ S \subseteq S^* \circ R^* \quad .$

We have to show that $R^* \circ S^* \subseteq S^* \circ R^*$, so we start our proof with the following calculation:

$$
\begin{array}{ll}
 & R^* \circ S^* \subseteq S^* \circ R^* \\
\equiv & \{ \quad I \text{ is identity of composition} \quad \} \\
 & R^* \circ I \circ S^* \subseteq S^* \circ R^* \\
\equiv & \{ \quad (6) \text{ and } (7) \quad \} \\
 & I \subseteq R^* \backslash (S^* \circ R^*) / S^* \\
\equiv & \{ \quad I \subseteq I ;\ (2) \quad \} \\
 & I \subseteq R^* \backslash (S^* \circ R^*) / S^* \cap I \quad .
\end{array}
$$

Now we have reached a form where we can exploit (54); to reduce the length of the expressions we introduce the shorthand A for $R^*\backslash(S^*\circ R^*)/S^* \cap I$. The properties of factors ((6) and (7)) and meet (2) give us, for all monotypes B:

(56) $\quad B \subseteq A \;\equiv\; R^* \circ B \circ S^* \subseteq S^* \circ R^*$.

By instantiating B to A we obtain the cancellation property:

(57) $\quad R^* \circ A \circ S^* \subseteq S^* \circ R^*$.

After this investigation of A, we continue the main calculation.

$$
\begin{array}{ll}
 & I \subseteq R^*\backslash(S^*\circ R^*)/S^* \cap I \\
\equiv & \qquad \{ \qquad \text{definition of } A \qquad \} \\
 & I \subseteq A \\
\Leftarrow & \qquad \{ \qquad (54) \qquad \} \\
 & R{\setminus\!\!\!\lrcorner}\, A \circ A\,{/\!\!\!\llcorner}\, S \subseteq A \\
\equiv & \qquad \{ \qquad (56) \qquad \} \\
 & R^* \circ R{\setminus\!\!\!\lrcorner}\, A \circ A\,{/\!\!\!\llcorner}\, S \circ S^* \subseteq S^* \circ R^* \\
\equiv & \qquad \{ \qquad \text{property (14) of the refl. trans. closure} \qquad \} \\
 & \quad R^* \circ R{\setminus\!\!\!\lrcorner}\, A \circ A\,{/\!\!\!\llcorner}\, S \subseteq S^* \circ R^* \\
 & \wedge\;\; R{\setminus\!\!\!\lrcorner}\, A \circ A\,{/\!\!\!\llcorner}\, S \circ S^* \subseteq S^* \circ R^* \\
 & \wedge\;\; R^* \circ R \circ R{\setminus\!\!\!\lrcorner}\, A \circ A\,{/\!\!\!\llcorner}\, S \circ S \circ S^* \subseteq S^* \circ R^* \quad .
\end{array}
$$

Now the first two conjuncts of this last clause are true; we prove only the first one, the proof of the second proceeds similarly.

$$
\begin{array}{ll}
 & R^* \circ R{\setminus\!\!\!\lrcorner}\, A \circ A\,{/\!\!\!\llcorner}\, S \\
\subseteq & \qquad \{ \qquad I \text{ is unit of composition; } R{\setminus\!\!\!\lrcorner}\, A \circ A\,{/\!\!\!\llcorner}\, S \subseteq I\circ I \subseteq I \qquad \} \\
 & I \circ R^* \circ I \\
\subseteq & \qquad \{ \qquad S^* \text{ is reflexive: } I \subseteq S^* \qquad \} \\
 & S^* \circ R^* \quad .
\end{array}
$$

So the remaining obligation is to prove the last conjunct.

$$
\begin{array}{ll}
 & R^* \circ R \circ R{\setminus\!\!\!\lrcorner}\, A \circ A\,{/\!\!\!\llcorner}\, S \circ S \circ S^* \\
\subseteq & \qquad \{ \qquad (23) \qquad \} \\
 & R^* \circ A \circ R \circ S \circ A \circ S^* \\
\Rightarrow & \qquad \{ \qquad (55) \qquad \}
\end{array}
$$

$$
\begin{array}{ll}
& R^* \circ A \circ S^* \circ R^* \circ A \circ S^* \\
\subseteq & \quad \{ \qquad (57) \quad \} \\
& S^* \circ R^* \circ R^* \circ A \circ S^* \\
\subseteq & \quad \{ \qquad R^* \text{ is transitive} \quad \} \\
& S^* \circ R^* \circ A \circ S^* \\
\subseteq & \quad \{ \qquad (57) \quad \} \\
& S^* \circ S^* \circ R^* \\
\subseteq & \quad \{ \qquad S^* \text{ is transitive} \quad \} \\
& S^* \circ R^* \quad .
\end{array}
$$

This completes the proof.
□

We have given this proof in rather great detail to show that it is possible to prove properties like (52), using the induction principle in the form of definition 34 in a purely calculational style. Compared to the original proof in [20] the proof given here is much simpler. See [17] for a proof that, although not calculational, is comparable to the one given here. It should be remarked that the generalisation —the replacement of $R{\cup}$ by an arbitrary spec— emerged quite naturally from the proof we constructed for Newman's lemma in its original form. This generalisation is in our opinion not so easy to see in a proof like the one in [17].

10 The Union of Well-Founded Relations

Often in order to establish that a complex relation is well-founded it is desirable to split the relation into component relations, establish that the components are well-founded and, thus, that the original relation is well-founded. This process requires knowing conditions under which the union of two well-founded relations is itself well-founded. In general, this is known to be a very difficult problem. Geser [16] has observed that it is sufficient that the relation be transitive. Bachmair and Dershowitz [2] have identified a different condition that they call "quasicommutativity", namely the union of well-founded relations R and S is itself well-founded whenever $S{\circ}R \subseteq (R{\cup}S)^* \circ S$. Here we present a third sufficient condition that subsumes both Geser's and Bachmair and Dershowitz's conditions. The condition was discovered by pure formal calculation: we tried to verify Geser's result and in the process derived a more general condition. Subsequently, we learnt of the paper by Bachmair and Dershowitz and were able to verify immediately that our condition was weaker than theirs.

The spec R is well-founded if and only if $\nu(X \mapsto X{\circ}R) = \perp\!\!\perp$. Our initial goal will therefore be to try to derive conditions on R and S together with a $\perp\!\!\perp$-preserving function f such that we can state a lemma of the form

$$\nu(X \mapsto X\circ(R\cup S)) \subseteq f.(\nu(X \mapsto X\circ R)\,,\, \nu(X \mapsto X\circ S)) \quad .$$

For brevity let us denote $\nu(X \mapsto X\circ(R\cup S))$ by α. We call the process of finding Y such that, for a given X, $X \subseteq Y$ *majorising* X. Thus our goal is to determine a condition under which α is majorised by some function of $\nu(X \mapsto X\circ R)$ and $\nu(X \mapsto X\circ S)$.

Let us begin by trying to filter out $\nu(X \mapsto X\circ R)$. With the use of (43) in mind, we try to calculate β such that $\alpha \subseteq \nu(X \mapsto \beta \cup X\circ R)$. We have:

$$\begin{array}{ll}
 & \alpha \subseteq \nu(X \mapsto \beta \cup X\circ R) \\
\Leftarrow & \qquad \{ \qquad \text{induction} \quad \} \\
 & \alpha \subseteq \beta \cup \alpha\circ R \\
\equiv & \qquad \{ \qquad \alpha = \alpha\circ(R\cup S) \quad \} \\
 & \alpha\circ(R\cup S) \subseteq \beta \cup \alpha\circ R \\
\equiv & \qquad \{ \qquad \text{calculus} \quad \} \\
 & \alpha\circ S \subseteq \beta \cup \alpha\circ R \quad .
\end{array}$$

Thus it is sufficient that β satisfy the equation in X: $\alpha\circ S \subseteq X \cup \alpha\circ R$. We take for β the least solution of this equation. (That the equation has a least solution is guaranteed by the fact that the function $(\cup(\alpha\circ R))$ has a lower adjoint.) Thus define β by:

(58) $\quad \forall(X{::}\ \beta \subseteq X \equiv \alpha\circ S \subseteq X \cup \alpha\circ R) \quad .$

It is useful to note that $\beta \subseteq \alpha$, since

$$\begin{array}{ll}
 & \beta \subseteq \alpha \\
\equiv & \qquad \{ \qquad \text{definition of } \beta\text{: (58)} \quad \} \\
 & \alpha\circ S \subseteq \alpha \cup \alpha\circ R \\
\equiv & \qquad \{ \qquad \alpha = \alpha\circ(R\cup S) \supseteq \alpha\circ S \quad \} \\
 & \mathit{true} \quad .
\end{array}$$

Now we try to majorise β, this time with the goal of filtering out $\nu(X \mapsto X\circ S)$. To this end we calculate γ as follows:

$$\begin{array}{ll}
 & \beta \subseteq \nu(X \mapsto \gamma \cup X\circ S) \\
\Leftarrow & \qquad \{ \qquad \text{induction} \quad \} \\
 & \beta \subseteq \gamma \cup \beta\circ S \\
\equiv & \qquad \{ \qquad \text{definition of } \beta\text{: (58)} \quad \} \\
 & \alpha\circ S \subseteq \gamma \cup \beta\circ S \cup \alpha\circ R
\end{array}$$

$\Leftarrow$ { This is the most crucial step in the calculation.
We eliminate α on both sides of the inequality.
On the left we use $\alpha \subseteq \nu(X \mapsto \beta \cup X\circ R)$
(see the 1st calculation).
On the right we use $\alpha = \alpha \circ (R\cup S)^* \supseteq \beta \circ (R\cup S)^*$ }

$\nu(X \mapsto \beta \cup X\circ R) \circ S \subseteq \gamma \cup \beta\circ S \cup \beta\circ(R\cup S)^*\circ R$

$\equiv$ { (43) }

$(\nu(X \mapsto X\circ R) \cup \beta\circ R^*) \circ S \subseteq \gamma \cup \beta\circ S \cup \beta\circ(R\cup S)^*\circ R$

$\Leftarrow$ { calculus }

$R^*\circ S \subseteq S \cup (R\cup S)^*\circ R$

$\wedge\ \nu(X \mapsto X\circ R) \circ S \subseteq \gamma$.

To summarise what we have done so far: with β defined by (58) and γ defined to be equal to $\nu(X \mapsto X\circ R) \circ S$, we have

(59) $\alpha \subseteq \nu(X \mapsto \beta \cup X\circ R)$

and

(60) $\beta \subseteq \nu(X \mapsto \gamma \cup X\circ S) \Leftarrow R^*\circ S \subseteq S \cup (R\cup S)^*\circ R$.

Let us assume that $R^*\circ S \subseteq S \cup (R\cup S)^*\circ R$. Then,

α

$\subseteq$ { (59) }

$\nu(X \mapsto \beta \cup X\circ R)$

$=$ { (43) }

$\nu(X \mapsto X\circ R) \cup \beta\circ R^*$

$\subseteq$ { assumption and (60) }

$\nu(X \mapsto X\circ R) \cup \nu(X \mapsto \gamma \cup X\circ S) \circ R^*$

$=$ { (43) }

$\nu(X \mapsto X\circ R) \cup (\nu(X \mapsto X\circ S) \cup \gamma\circ S^*) \circ R^*$

$=$ { definition of γ }

$\nu(X \mapsto X\circ R) \cup (\nu(X \mapsto X\circ S) \cup \nu(X \mapsto X\circ R) \circ S^+) \circ R^*$.

We have achieved our goal. We have calculated that

(61) $\nu(X \mapsto X\circ(R\cup S)) \subseteq f.(\nu(X \mapsto X\circ R) , \nu(X \mapsto X\circ S))$

with $\perp\!\!\perp$-preserving function f defined by

$$f.(x,y) \;=\; x \cup (y \cup x{\circ}S^{+}) \circ R^{*}$$

and under the condition that

$$R^{*}{\circ}S \;\subseteq\; S \cup (R{\cup}S)^{*}{\circ}R \quad .$$

One final bit of tidying up: It is straightforward (using the techniques developed in this paper) to prove that the above condition is equivalent to the formally weaker:

$$R{\circ}S \;\subseteq\; S \cup (R{\cup}S)^{*}{\circ}R \quad .$$

Thus we may conclude:

Theorem 62 The spec $R{\cup}S$ is well-founded if R and S are well-founded and

$$R{\circ}S \;\subseteq\; S \cup (R{\cup}S)^{*}{\circ}R \quad .$$

□

The following corollary is an immediate consequence:

Corollary 63 The spec $R{\cup}S$ is well-founded if R and S are well-founded and one of the following holds.

(a) (Geser [16]) $R{\cup}S$ is transitive ,

(b) (Bachmair and Dershowitz [2]) R and S quasi-commute (i.e. $R{\circ}S \subseteq (R{\cup}S)^{*}{\circ}R$) ,

(c) S absorbs R (i.e. $R{\circ}S \subseteq S$).

(Condition (c) seems to be part of the folklore; it is known but we do not know to whom it should be attributed.)

□

It is worth observing that property (61) is quite independent of whether or not R or S is well-founded. Rutger M. Dijkstra has suggested increasing its right side making the property easier to remember and apply. In the form suggested by Dijkstra, the general result we have proved is the following.

$$\begin{array}{ll} & \nu(X \mapsto X{\circ}(R{\cup}S)) \;\subseteq\; (\nu(X \mapsto X{\circ}R) \cup \nu(X \mapsto X{\circ}S)) \circ (R{\cup}S)^{*} \\ \Leftarrow & R{\circ}S \subseteq S \cup (R{\cup}S)^{*}{\circ}R \quad . \end{array}$$

11 Conclusion

In this paper our goal has been to demonstrate the use of the calculational method in developing theories of induction. We have shown that the combination of the early recognition of Galois connections with fixed point calculus leads to concise and effective calculations. Furthermore we have shown that the method leads to novel theorems that might otherwise have not been discovered.

The work reported in this paper has been further generalised to notions of admitting induction and well-foundedness *with respect to a datatype* and applied to the proof of termination of programs involving non-trivial data structures [12, 13, 11]. We have shown that in this context the two notions are not equivalent, and not even comparable. Moreover, in this context the notion of negation makes no sense; it is this that motivated denying the use of negation in our exploration of the relationship between admitting induction and well-foundedness.

Acknowledgements

Our thanks to Dana Buhăceanu whose solution to an examination question on this topic led to the proof of lemma 44, to Han Bäumer for introducing us to the term-rewriting literature and suggesting that we try to prove Newman's lemma, and to Lex Bijlsma for detailed criticisms and suggestions for improvement of earlier drafts of this paper. Thanks also to Ronald Bulterman, Carel Scholten, Burghard von Karger and Rutger Dijkstra for reviving our interest in constructing a presentable proof of theorem 62.

References

[1] C.J. Aarts, R.C. Backhouse, P. Hoogendijk, T.S. Voermans, and J. van der Woude. A relational theory of datatypes. Available via world-wide web at `http://www.win.tue.nl/win/cs/wp/papers`, September 1992.

[2] L. Bachmair and N. Dershowitz. Commutation, transformation and termination. In *Proceedings of the 8th Conference on Automated Deduction*, volume 230 of *LNCS*, pages 5–20, 1986.

[3] R.C. Backhouse and B.A. Carré. Regular algebra applied to path-finding problems. *Journal of the Institute of Mathematics and its Applications*, 15:161–186, 1975.

[4] R.C. Backhouse and J. van der Woude. Demonic operators and monotype factors. *Mathematical Structures in Computer Science*, 3(4):417–433, December 1993.

[5] Han Bäumer. On the use of relation algebra in the theory of reduction systems. In J.L.G. Dietz, editor, *CSN 92*, pages 54–64, Amsterdam, 1992. Centrum voor Wiskunde en Informatica.

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

[7] J.H. Conway. *Regular Algebra and Finite Machines*. Chapman and Hall, London, 1971.

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

[9] R.M. Dijkstra. Relational calculus and relational program semantics. Technical Report CS-R9408, Department of Computing Science, University of Groningen, 1994. (Originally written as a Masters thesis in Mathematics at the Universität zu Köln).

[10] R.P. Dilworth. Non-commutative residuated lattices. *Transactions of the American Mathematical Society*, 46:426–444, 1939.

[11] H. Doornbos. *Reductivity arguments and program construction*. PhD thesis, Eindhoven University of Technology, Department of Mathematics and Computing Science, June 1996.

[12] H. Doornbos and R.C. Backhouse. Induction and recursion on datatypes. In B. Möller, editor, *Mathematics of Program Construction, 3rd International Conference*, volume 947 of *LNCS*, pages 242–256. Springer-Verlag, July 1995.

[13] Henk Doornbos and Roland Backhouse. Reductivity. *Science of Computer Programming*, 1996. To appear.

[14] W.H.J. Feijen. Exercises in formula manipulation. In E.W. Dijkstra, editor, *Formal Development of Programs and Proofs*, pages 139–158. Addison-Wesley Publ. Co., 1990.

[15] P.J. Freyd and A. Scedrov. *Categories, Allegories*. North-Holland, 1990.

[16] A. Geser. *Relative Termination*. PhD thesis, University of Passau, 1990.

[17] G. Huet. Confluent reductions: Abstract properties and applications to term rewriting systems. *J. Assoc. Comput. Mach.*, 27(4):797–821, 1980.

[18] J.W. Klop. Term rewriting systems: a tutorial. *Bulletin of the EATCS*, 32:143–182, 1987.

[19] Eindhoven University of Technology Mathematics of Program Construction Group. Fixed point calculus. *Information Processing Letters*, 53(3):131–136, February 1995.

[20] M.H.A. Newman. On theories with a combinatorial definition of "equivalence". *Annals of Math.*, 43(2):223–243, 1942.

[21] Oystein Ore. Galois connexions. *Transactions of the American Mathematical Society*, 55:493–513, 1944.

[22] J. Riguet. Relations binaires, fermetures, correspondances de Galois. *Bulletin de la Société Mathématique de France*, 76:114–155, 1948.

[23] Arto Salomaa. Two complete axiom systems for the algebra of regular events. *J. Assoc. Comp. Mach.*, 13(1):158–169, January 1966.

[24] G. Schmidt and T. Ströhlein. *Relations and Graphs, Discrete Mathematics for Computer Scientists.* EATCS Monographs on Theoretical Computer Science. Springer-Verlag, Berlin Heidelberg, 1993.

[25] Alfred Tarski and Steven Givant. *A Formalization of Set Theory without Variables*, volume 41 of *Colloquium Publications.* American Mathematical Society, Providence, Rhode Island, 1987.