Components and Acyclicity of Graphs
An Exercise in Combining Precision with Concision

Roland Backhouse[a,1,*], Henk Doornbos[b,2], Roland Glück[c,1], Jaap van der Woude[b,1]

[a] *School of Computer Science, University of Nottingham, Nottingham NG8 1BB, U.K.*
[b] *Vakgroep Informatica, Technische Universiteit Eindhoven, The Netherlands*
[c] *Deutsches Zentrum für Luft- und Raumfahrt, Augsburg, Germany*

Abstract

Central to algorithmic graph theory are the concepts of acyclicity and strongly connected components of a graph, and the related search algorithms. This article is about combining mathematical precision and concision in the presentation of these concepts. Concise formulations are given for, for example, the reflexive-transitive reduction of an acyclic graph, reachability properties of acyclic graphs and their relation to the fundamental concept of "definiteness", and the decomposition of paths in a graph via the identification of its strongly connected components and a pathwise homomorphic acyclic subgraph. The relevant properties are established by precise algebraic calculation. The combination of concision and precision is achieved by the use of point-free relation algebra capturing the algebraic properties of paths in graphs, as opposed to the use of pointwise reasoning about paths between nodes in graphs.

Keywords: regular algebra, relation algebra, acyclic graph, strongly connected component, point-free reasoning, calculational method

1. Introduction

Algorithmic graph theory —by which we mean graph theory with a focus on the design and analysis of algorithms on graphs— is a vital component of computing science with diverse practical applications. Within that theory, the twin notions of acyclicity and strongly connected components play a central role. This paper is about formulating and reasoning about these notions in a calculational style based on "point-free" relation algebra. Briefly stated, "point-free" relation algebra is the algebra of fundamental operations on relations: union, intersection, composition and converse; in contrast, "pointwise"

*Corresponding author
Email addresses: roland.backhouse@nottingham.ac.uk (Roland Backhouse), henk.doornbos@questance.com (Henk Doornbos), roland.glueck@dlr.de (Roland Glück), J.C.S.P.v.d.Woude@tue.nl (Jaap van der Woude)
[1] Declaration of interests: none.
[2] Now at Questance, Groningen, The Netherlands. Declaration of interests: none.

relation algebra is essentially boolean algebra: the algebra of whether or not a relation holds on given values.

The mathematical notion underlying the definition of a strongly connected component of a graph is that of an equivalence relation. Of course, the point-free formulation of the definition of an equivalence relation is well-known. The same cannot be said for, for example, properties of paths in a graph: although the appropriate algebra —regular algebra— has been around for more than 50 years, it is still not sufficiently well-known that it is routinely applied in relevant circumstances.

Our contribution is to systematically formulate and prove properties of strongly connected components and acyclicity of graphs in point-free relation algebra. The properties we formulate are undoubtedly well-known but the same cannot be said of the calculational techniques we demonstrate. For example, we conclude the paper with a point-free formulation of the fundamental decomposition of a graph into its strongly connected components and a pathwise-homomorphic acyclic graph; our formulation captures the idea of coalescing the nodes in each strongly connected component into one node in a very concise but nevertheless completely precise formula. A relatively straightforward calculation then establishes how the decomposition is exploited to facilitate the determination of the existence of paths in a given graph. Similarly, we formulate and prove properties of paths connecting a pair of nodes in the same strongly connected component of a graph: there is always such a path and any path must lie entirely within the strongly connected component.

Sections 8, 9 and 10 discuss equivalence relations and partitions, acyclicity of a graph, and components of a graph, respectively. Full details are given of all calculations in these sections.

Prior to this, a number of sections set the scene. We view a relation algebra as an algebra consisting of three substructures with interfaces between them. The three substructures are: a lattice —introduced in section 2— , a regular algebra —introduced in section 3— , and the converse structure —introduced together with the interfaces in section 4— . For brevity, lemmas and theorems are stated in these sections without proofs.

Sections 5, 6 and 7 introduce a miscellany of topics that are used later. Section 5 introduces the left and right "domain" operators on relations, whilst section 6 introduces the "all-or-nothing" axiom allowing pointwise reasoning to be mimicked in point-free relation algebra: some pointwise reasoning is unavoidable but we use it sparingly. Finally, section 7 gives definitions of notions associated with functions (functionality, injectivity, totality and surjectivity) and concludes with a brief summary of how the axiom system presented in the initial three sections is extended to include heterogeneous relations. For brevity, proofs are also omitted in these sections.

For additional explanatory information and examples, full details of proofs and the extension of the methods presented here to the verification of standard graph algorithms, including depth-first search, see [1]. The current paper is an excerpt; additional excerpts are in preparation (eg. [2]).

An Apology It is common to include up-to-date citations in scientific publications. With a small number of exceptions, we do not do so here for a number of reasons. First, the graph algorithms and properties of graphs discussed in this paper are now common knowledge having found their way into undergraduate curricula at least forty years ago — so long ago that we have forgotten where we ourselves learned about them. (See, for

example, the classic textbook by Aho, Hopcroft and Ullman [3] first published in 1982.) Second, the foundations for the calculations presented in the paper were first laid more than forty years ago [4, 5] and completed more than twenty years ago (eg. [6, 7, 8, 9]). That writing the paper would make a worthwhile contribution to current research, in particular our conviction that point-free calculations are vital to overcoming some of the challenges faced by modern theorem-proving systems, was inspired by Glück's work [10] to which we refer the reader for more recent literature. (See also the conclusions for additional comments.)
End of Apology

2. Elements of Lattice Theory

Relation algebra is a rich algebraic structure involving a large number of operators. There is a down-side as well as an up-side to its richness. On the one hand it is very expressive, on the other hand calculations within the algebra can be difficult because of the sheer abundance of calculational rules. In order to make the algebra more tractable we present it as a number of units with interfaces between the units. Each unit is a well-understood and well-documented mathematical structure of sufficiently small size to be easily comprehended.

2.1. Complete, Complemented Lattices

A (heterogeneous) binary relation between two sets $\mathcal{A}$ and $\mathcal{B}$ is a subset of the cartesian product $\mathcal{A}\times\mathcal{B}$. In other words, a relation is an element of the powerset $2^{\mathcal{A}\times\mathcal{B}}$.

In general, a powerset (the set of subsets of a set) is partially ordered by the subset relation; it is also "complete" and "completely distributive", it has "complements" and its elements (sets) themselves have elements. This section is about axiomatising such properties of partial orderings. Section 2.2 is about axiomatising properties of the element-of relation.

A *complete lattice* is a partially ordered set equipped with unrestricted supremum and infimum operators. Let us assume the set is denoted by $\mathcal{A}$ and the ordering is denoted by $\subseteq$. Of course, we assume that the ordering is reflexive, transitive and anti-symmetric.

That the ordering is *complete* means that every function f with target $\mathcal{A}$ has a supremum, denoted by $\cup f$, satisfying the property

$$\langle \forall x \ :: \ \cup f \ \subseteq \ x \ \equiv \ \langle \forall u :: f.u \subseteq x \rangle \rangle \tag{1}$$

and an infimum, denoted by $\cap f$, satisfying the property

$$\langle \forall x \ :: \ x \subseteq \cap f \ \equiv \ \langle \forall u :: x \subseteq f.u \rangle \rangle \ . \tag{2}$$

Properties (1) and (2) specialise to binary suprema and infima, which we denote in the usual way by infix operators. That is,

$$\langle \forall\, x,y,z \ :: \ y \cup z \subseteq x \ \equiv \ y \subseteq x \wedge z \subseteq x \rangle \tag{3}$$

and

$$\langle \forall\, x,y,z \ :: \ x \subseteq y \cap z \ \equiv \ x \subseteq y \wedge x \subseteq z \rangle \ . \tag{4}$$

Aside In many cases, we want to use a function without giving it a specific name. In such cases, we use the notation $\langle x :: E \rangle$, where x is a variable and E is some expression. We also write $\langle \oplus x :: E \rangle$ rather than the strictly correct $\oplus \langle x :: E \rangle$ (where $\oplus$ is some extremum operator). Typically, we omit type information in quantified expressions relying on the context to make the types clear. Occasionally we do include type information in expressions of the form $\langle \oplus x : R : E \rangle$, where R is some expression. The advantage of using a consistent notation for quantification is that it is possible to formulate calculational rules based on assumed properties of the quantifier. We assume that the reader is familiar with the calculational rules.

As the reader may already have surmised, we use an infix dot to denote function application — as in " $f.u$ ". The dot is omitted when a symbol rather than an identifier is used to denote the function.) **End of Aside**

A complete lattice has a *top* (a greatest element, the infimum of the unique function with source the empty set), which we denote by $\top\!\top$, and a *bottom* (a least element, the supremum of the unique function with source the empty set), which we denote by $\bot\!\bot$. That is,

$$\langle \forall x :: \bot\!\bot \subseteq x \subseteq \top\!\top \rangle \quad . \tag{5}$$

(We use the notation $\top\!\top$ and $\bot\!\bot$ rather than the more common $\top$ and $\bot$ because $\top$ is easily confused with T .)

A complete lattice is said to be *completely distributive* iff for all sets $\mathcal{J}$ and $\mathcal{K}$ and all functions f of type $\mathcal{A} \leftarrow \mathcal{J} \times \mathcal{K}$, the following equality and its dual hold:

$$\langle \cap j : j \in \mathcal{J} : \langle \cup k : k \in \mathcal{K} : f.(j,k) \rangle \rangle \;=\; \langle \cup g : g \in \mathcal{K} \leftarrow \mathcal{J} : \langle \cap j : j \in \mathcal{J} : f.(j\,,g.j) \rangle \rangle \quad .$$

(The dual equality is obtained by swapping the infimum and supremum operators.)

The reader may want to instantiate the above formula with $\forall$ as the infimum operator and $\exists$ as the supremum operator; the resulting formula is a statement of the axiom of choice in predicate calculus.

A powerset ordered by set inclusion is a complete, completely distributive lattice but the full power of the distributivity property is rarely used; so-called "universal distributivity" most often suffices. Formally, a complete lattice is said to be *universally distributive* if

$$\langle \forall x,f \;::\; x \cup (\cap f) \;=\; \langle \cap j :: x \cup f.j \rangle \;\;\wedge\;\; x \cap (\cup f) \;=\; \langle \cup j :: x \cap f.j \rangle \rangle \quad .$$

We frequently apply universal distributivity without specific reference to the rule. Particular examples that we use frequently are $x \cap \bot\!\bot = \bot\!\bot$ and $x \cup \top\!\top = \top\!\top$.

A powerset ordered by set inclusion is complemented but, as for complete distributivity, the existence of complements is sometimes unnecessary. The weaker notion of "pseudo-(co)complementation" is a consequence of universal distributivity.

Definition 6. Suppose $(\mathcal{A}, \subseteq)$ is a partially ordered set with bottom element $\bot\!\bot$, top element $\top\!\top$ and finite infima and suprema. A *pseudo-complement* of an element p of $\mathcal{A}$ is a solution of the equation

$$x \;::\; \langle \forall q \;::\; q \subseteq x \equiv q \cap p = \bot\!\bot \rangle \quad . \tag{7}$$

A *pseudo-cocomplement* of an element p of $\mathcal{A}$ is a solution of the equation

$$x :: \langle \forall q :: x \subseteq q \equiv q \cup p = \top\!\!\top \rangle \quad . \tag{8}$$

A *complement* of an element p of $\mathcal{A}$ is an element that is simultaneously a pseudo-complement and a pseudo-cocomplement of p. The poset is *complemented* if all of its elements have a complement.
□

Full details of the properties of pseudo-(co)complements and complements are given in [1].

The properties of complements in a complete, universally distributive, complemented lattice are familiar from set theory. First, complements are unique. We denote the unique complement of element x by $-x$. Second, complementation is an order isomorphism of $(\mathcal{A}, \subseteq)$ and $(\mathcal{A}, \supseteq)$. Specifically, for all x and y in $\mathcal{A}$,

$$-(-x) = x \quad \text{and} \tag{9}$$

$$-x \subseteq y \;\equiv\; x \supseteq -y \quad . \tag{10}$$

It follows that complementation distributes through infima and suprema: for all f,

$$-\langle \cap x :: f.x \rangle \;=\; \langle \cup x :: -(f.x) \rangle \quad \wedge \quad -\langle \cup x :: f.x \rangle \;=\; \langle \cap x :: -(f.x) \rangle \quad . \tag{11}$$

Finally, we have the *shunting rule*: for all x, y and z,

$$x \cap y \subseteq z \quad \equiv \quad x \subseteq -y \cup z \quad . \tag{12}$$

Warning: The notation used here for complementation is temporary. Later we need to distinguish between complements in different lattices, and for each we need to introduce a different symbol. **End of Warning**

2.2. Atoms, Saturation and Powersets

A powerset forms a complete, universally distributive, complemented lattice under the subset ordering. However, these properties do not characterise the properties of the *elements* of the sets in the powerset. For this, we need the notion of a "saturated", "atomic" lattice: elements of a set are modelled by so-called "atoms". We avoid the use of saturated atomicity wherever possible. However, there are some circumstances where its use is unavoidable.

Throughout this section, we assume that $\mathcal{A}$ is a complete lattice. (This means that we can use the supremum and infimum operators without caveats on their existence.) For brevity, we sometimes omit to say that $\mathcal{A}$ is complete. Variables p and q range over arbitrary elements of $\mathcal{A}$. As always, we use $\subseteq$ for the ordering relation on elements of $\mathcal{A}$.

Definition 13 (Atom and Atomicity). The element p is an *atom* iff

$$\langle \forall q :: q \subseteq p \;\equiv\; q = p \vee q = \perp\!\!\perp \rangle \quad .$$

Note that $\perp\!\!\perp$ is an atom according to this definition. If p is an atom that is different from $\perp\!\!\perp$ we say that it is a *proper* atom. A lattice is said to be *atomic* if

$$\langle \forall q :: q \neq \perp\!\!\perp \;\equiv\; \langle \exists a : \mathsf{atom}.a \wedge a \neq \perp\!\!\perp : a \subseteq q \rangle \rangle \quad .$$

In words, a lattice is atomic if every proper element includes a proper atom.
□

Definition 14 (Saturated). A complete lattice is *saturated* iff

$$\langle \forall p :: p = \langle \cup a : \mathsf{atom}.a \wedge a \subseteq p : a \rangle \rangle \ .$$

□

Elsewhere the word "full" is sometimes used instead of our "saturated". Other authors also sometimes use "atomic" to mean both atomic (according to definition 13) and saturated.

The following theorem [6, theorem 6.43] is central to the use of saturated lattices as a model of powersets.

Theorem 15. Suppose $\mathcal{A}$ is a complete, universally distributive lattice. Then the following statements are equivalent.

(a) $\mathcal{A}$ is saturated,

(b) $\mathcal{A}$ is atomic and complemented,

(c) $\mathcal{A}$ is isomorphic to the powerset of its atoms.

□

We don't use theorem 15 directly. We use it indirectly in the sense that our axiomatisation of relation algebra postulates a complete, universally distributive, saturated lattice. In this section, we consider consequences of the definitions that allow pointwise reasoning akin to conventional reasoning about sets and, in particular, membership properties. Specifically, for lattice element p and proper atom a, the assertion $a \subseteq p$ effectively means $a \in p$. For example, the booleans $\neg(a \subseteq p)$ and $a \subseteq -p$ are equal; this models the commonly used property of set membership: the boolean $\neg(a \in p)$ is equal to $a \in -p$. See lemma 16. Other lemmas, such as lemmas 20 and 21, have a similar role. Proofs of the lemmas and theorem 15 can be found in [1].

We begin by exploring the notion of saturation. First, the above-mentioned lemma expressing how we mimic the defining property of the complement of a set:

Lemma 16. Suppose $\mathcal{A}$ is a complete, complemented lattice. Then for all elements p of $\mathcal{A}$ and all proper atoms a of $\mathcal{A}$,

$$\neg(a \subseteq p) \ \equiv \ a \subseteq -p \ .$$

□

The universal quantification in the definition of saturated can be eliminated:

Lemma 17. A complete, universally distributive lattice is saturated iff its greatest element is saturated, i.e. iff

$$\top\!\!\top \ = \ \langle \cup a : \mathsf{atom}.a : a \rangle \ .$$

□

Another consequence of $\top\!\!\top$ being saturated is the existence of complements:

Lemma 18. Suppose $\mathcal{A}$ is a complete lattice, and both pseudo-complemented and pseudo-cocomplemented. Then it is complemented if its greatest element, $\top\!\!\top$, is saturated.

□

Now we turn to the notion of atomicity. The assumption of universal distributivity gives an alternative definition:

Lemma 19. Suppose $\mathcal{A}$ is universally distributive. Then $\mathcal{A}$ is atomic equivales

$$\langle \forall q :: q = \bot\!\!\!\bot \;\equiv\; \langle \cup a : \mathsf{atom}.a : a \rangle \cap q \;=\; \bot\!\!\!\bot \rangle \;\;.$$

□

Lemma 20. If $p \neq \bot\!\!\!\bot$ and b is an atom, then $p = b \equiv p \subseteq b$. Also, if a and b are both proper atoms, $a = b \;\equiv\; a \cap b \neq \bot\!\!\!\bot$.

□

Atoms are *irreducible* in the following sense.

Lemma 21. Suppose $\mathcal{A}$ is a complete, universally distributive, saturated lattice and a is a proper atom of $\mathcal{A}$. Then, for all subsets S of the proper atoms of $\mathcal{A}$,

$$a \subseteq \langle \cup b : b \in S : b \rangle \;\equiv\; \langle \exists b : b \in S : a = b \rangle \;\;.$$

□

2.3. Closure Operators

We assume familiarity with the notion of a closure operator. This section introduces the notions of "complementation-fixed" and "complementation-idempotent" closure operators and their properties.

Definition 22. An endofunction f on a partially ordered set $\mathcal{A}$ is a *closure operator* if

$$\langle \forall x,y :: x \subseteq f.y \;\equiv\; f.x \subseteq f.y \rangle \;\;.$$

In words, f is a closure operator if, for all y, the set of elements at most $f.y$ is "closed" under application of the function f.

□

Definition 23. The function f is said to be *complementation fixed* iff

$$\langle \forall x :: f.(-x) = -x \;\Leftarrow\; f.x = x \rangle \;\;.$$

The function f is said to be *complementation idempotent* iff

$$\langle \forall x :: f.(-(f.x)) \;=\; -(f.x) \rangle \;\;.$$

□

Lemma 24. Suppose f is a closure operator. Then f is complementation fixed equivales f is complementation idempotent.

□

We use the notation $\mathsf{Fix}.f$ to denote the poset of fixed points of f: the partial ordering is the ordering inherited from the set on which the function f is defined.

Lemma 25. Suppose $\mathcal{A}$ is a complete, universally distributive lattice. Suppose f is a closure operator on the lattice $\mathcal{A}$ and suppose f is complementation fixed. Then $f.a$ is an atom of $\mathsf{Fix}.f$ if a is an atom of $\mathcal{A}$.

□

Theorem 26. Suppose $\mathcal{A}$ is a complete, universally distributive, saturated lattice. Suppose f is a closure operator on the lattice $\mathcal{A}$ and suppose f is complementation fixed. Then $\mathsf{Fix}.f$ is a complete, saturated lattice. The atoms in $\mathsf{Fix}.f$ are given by $\{b{:}\,\mathsf{atom}_{\mathcal{A}}.b{:}\,f.b\}$.
□

3. Regular Algebra

As remarked earlier, the set of binary relations of a given, fixed type forms a powerset. So our first step has been to axiomatise powersets as complete, universally distributive, saturated lattices. The next step is to introduce the composition of relations.

Restricting attention to homogeneous relations, the binary relations on some fixed set form a monoid under composition. We denote composition of homogeneous relations R and S (of the same type) by $R{\circ}S$ and the identity relation by I. Being a monoid means that composition is associative

$$(R{\circ}S){\circ}T \;=\; R{\circ}(S{\circ}T) \quad , \tag{27}$$

for all relations R, S and T, and I is a left and right unit of composition

$$R{\circ}I \;=\; R \;=\; I{\circ}R \quad , \tag{28}$$

for all relations R.

Extending composition to heterogeneous relations means that relations form a category: the composition of relation R of type $A{\sim}B$ and S of type $B{\sim}C$ is the relation $R{\circ}S$ of type $A{\sim}C$. For each type ("object" in category-theory parlance) there is an identity relation I_A of type $A{\sim}A$. We assume familiarity with such elementary concepts of category theory.

Definition 29 (Regular Algebra). A *regular algebra* with carrier set $\mathcal{A}$ is the combination of a monoid $(\mathcal{A}, \circ, I)$ and a complete lattice $(\mathcal{A}, \subseteq)$ such that, for each element R of $\mathcal{A}$, the endofunctions $(R\circ)$ and $(\circ R)$ are both lower adjoints in Galois connections between $(\mathcal{A}, \subseteq)$ and itself. A regular algebra is said to be *universally distributive* if the underlying lattice is universally distributive. The elements of $\mathcal{A}$ are sometimes called *events*.
□

(We assume familiarity with Galois connections and fixed-point calculus. See [11] for a tutorial presentation.)

Although definition 29 uses the symbol "$\subseteq$" to denote the partial ordering relation in a regular algebra, it should *not* be assumed that regular algebras are invariably powersets and the ordering relation is the subset relation. Many practical applications of regular algebra involve other orderings. See [4, 5, 12] for examples. Our use here of the symbols

" $\subseteq$ " and " $\circ$ ", and the identifier " R ", is because the primary application in this paper of a regular algebra is as a vital, but often overlooked, component of relation algebra. However, the properties stated in this section have much wider applicability than just to relation algebra.

The assumption that the endofunctions $(R\circ)$ and $(\circ R)$ are both lower adjoints in Galois connections is equivalent to the existence of two binary operators $\backslash$ and $/$ satisfying the properties, for all events R, S and T,

$$R\circ S \subseteq T \;\equiv\; S \subseteq R\backslash T \quad , \tag{30}$$

and

$$R\circ S \subseteq T \;\equiv\; R \subseteq T/S \quad . \tag{31}$$

These two operators are called the *factoring*, or *division*, operators; (for all R) the events $R\backslash T$ and T/R are *right* and *left factors* of T, respectively. Although these operators are important, we don't use them directly here; we use only the fact that they exist.

Our definition of a regular algebra does not postulate the existence of a star operator. A universally distributive regular algebra is what Conway [13, p.27] calls a "standard Kleene algebra".

There are several different definitions of the star operator in a regular algebra. Possibly the best known definition is

$$R^* = \langle \cup i : 0 \leq i : R^i \rangle \quad . \tag{32}$$

Another definition[3] is

$$R^* = \langle \mu x :: I \cup R \cup x\circ x \rangle \quad . \tag{33}$$

This definition states that R^* is the reflexive, transitive closure of R.

Two other commonly used definitions are in terms of left and right iteration. Specifically, left iteration is defined by

$$R^* = \langle \mu x :: I \cup R\circ x \rangle \tag{34}$$

and right iteration by

$$R^* = \langle \mu x :: I \cup x\circ R \rangle \quad . \tag{35}$$

It is easily shown that all of these definitions are equivalent. Choosing one or other definition gives different induction rules; deciding which to use in specific circumstances requires some practice. We use all four different definitions at some stage below.

The *transitive closure* of R is denoted by R^+. Like the reflexive, transitive closure it has several equivalent definitions, the most common being:

$$R^+ = \langle \cup i : 1 \leq i : R^i \rangle \tag{36}$$

and

$$R^+ \;=\; \langle \mu x :: R \cup x\circ x \rangle \;=\; \langle \mu x :: R \cup x\circ R \rangle \;=\; \langle \mu x :: R \cup R\circ x \rangle \quad . \tag{37}$$

Important properties of the star operator are as follows:

[3]The symbol μ denotes the least-fixed-point operator.

(a) $R \circ S^* \subseteq T^* \circ R \;\Leftarrow\; R \circ S \subseteq T \circ R$

(b) $T^* \circ R \subseteq R \circ S^* \;\Leftarrow\; T \circ R \subseteq R \circ S$

(c) $R \circ (S \circ R)^* \;=\; (R \circ S)^* \circ R$

(d) $(R \cup S)^* \;=\; S^* \circ (R \circ S^*)^* \;=\; (S^* \circ R)^* \circ S^*$

Properties (a) and (b) are called *leapfrog* rules (because R "leapfrogs" from one side of a star term to the other). Both have the immediate corollary that * is monotonic. Properties (c) and (d) are called the *mirror* rule and *star-decomposition* rule, respectively. The mirror rule and star-decomposition rules were identified as vital to the derivation of so-called elimination algorithms for path-finding problems in graphs in [4, 5, 14]. They play an equally important role below.

There are many other properties of the star operator that we use without further ado.

3.1. Starth Roots

This section is a preliminary to our proof in section 9 that the so-called "reflexive, transitive reduction" of an acyclic graph is the least "starth root" of the graph. Whereas in section 9, the subject of interest is relations, and more specifically graphs (i.e. binary relations on a finite set), the results in this section are more general and applicable to, for example, labelled graphs where the labels are themselves elements of the carrier set of a regular algebra.

Definition 38 (Starth Root). Suppose U is an event of a regular algebra. A *starth root* of U is any event V that satisfies $V^* = U^*$; it is *minimal* if no smaller event has this property. It is *least* if it is at most all starth roots. Formally, V is *a minimal starth root* of U if

$$V^* = U^* \;\wedge\; \langle \forall W \,:\, W \subseteq V \wedge W^* = U^* \,:\, W = V \rangle$$

and V is *the least starth root* of U if

$$V^* = U^* \;\wedge\; \langle \forall W : W^* = U^* : V \subseteq W \rangle \quad .$$

□

Definition 39 (Reflexive and Transitive Reduction). Let A and B be events in a complemented regular algebra with unit I. Suppose the complement[4] of event U is denoted by $\neg U$. Then $A \cap \neg I$ is called the *reflexive reduction* of A and $B \cap \neg(B \circ B^+)$ is called the *transitive reduction* of B. The transitive reduction of the reflexive reduction of A is called the *reflexive-transitive reduction* of A.
□

[4] In order to comply with later usage, this is the point at which we need to introduce a different symbol for complementation. The symbol " $\neg$ " has been chosen because it fits with conventional practice. That it is the same symbol as the symbol we use for negation of booleans should not cause any confusion.

We denote the reflexive-transitive reduction of A by $\mathsf{red}.A$. That is,

$$\mathsf{red}.A \;=\; A \cap \neg I \cap \neg((A \cap \neg I) \circ (A \cap \neg I)^+) \quad . \tag{40}$$

If G represents the edges of a graph, the reflexive-transitive reduction $\mathsf{red}.G$ "reduces" G by eliminating self-loops and edges connecting distinct nodes that are subsumed by paths of edge-length two or more and not involving self-loops. (Self-loops are edges from a node to itself. The multiple occurrences of "$\cap \neg I$" in (40) serve to eliminate such edges, leaving only edges connecting distinct nodes.)

The reflexive-transitive reduction of a relation is an important concept. For example, it underlies the display of (small, finite) posets by means of a so-called Hasse diagram: the relation displayed in such a diagram is not the partial ordering but its reflexive-transitive reduction. The concept is important in other applications. For example, the basis of the Knuth-Morris-Pratt pattern matching algorithm (and its generalisations [15, 16, 17]) is the "factor graph" of a regular language defined by the pattern, and the "factor graph" is the reflexive-transitive reduction of Conway's "factor matrix" of the language [18, 19]. Definitions 38 and 39 abstract from Brzozowski's study of roots of star events [20].

A couple of lemmas on reflexive reduction prove useful later:

Lemma 41. Let X be an event in a complemented regular algebra with unit I. Then

$$X^* \;=\; (X \cap \neg I)^* \quad .$$

(In words, the reflexive reduction of X is a starth root of X.)

Proof

$$\begin{array}{ll} & X^* = (X \cap \neg I)^* \\ \Leftarrow & \quad \{ \quad X \supseteq X \cap \neg I \text{ , monotonicity of star} \quad \} \\ & X^* \subseteq (X \cap \neg I)^* \\ = & \quad \{ \quad {}^* \text{ is a closure operator} \quad \} \\ & X \subseteq (X \cap \neg I)^* \\ \Leftarrow & \quad \{ \quad I \cup Y \subseteq Y^* \text{ with } Y := X \cap \neg I \quad \} \\ & X \;\subseteq\; I \cup (X \cap \neg I) \\ = & \quad \{ \quad \text{absorption rule} \quad \} \\ & X \;\subseteq\; I \cup X \\ = & \quad \{ \quad \text{suprema} \quad \} \\ & \mathsf{true} \quad . \end{array}$$

□

Lemma 42. Let X and Y be events in a complemented regular algebra with unit I. Then

$$X^* \subseteq Y^* \;\equiv\; (X \cap \neg I)^+ \subseteq (Y \cap \neg I)^+ \quad ,$$

$$X^* = Y^* \;\equiv\; (X \cap \neg I)^+ = (Y \cap \neg I)^+ \quad .$$

Proof First,

$$
\begin{array}{ll}
 & (X \cap \neg I)^+ \subseteq (Y \cap \neg I)^+ \\
= & \quad \{ \quad {}^+ \text{ is a closure operator} \quad \} \\
 & X \cap \neg I \subseteq (Y \cap \neg I)^+ \\
= & \quad \{ \quad \text{complements} \quad \} \\
 & X \subseteq (Y \cap \neg I)^+ \cup I \\
= & \quad \{ \quad \text{for all } Z,\ Z^+ \cup I = Z^* \text{ with } Z := Y \cap \neg I, \\
 & \qquad \text{lemma 41 with } X := Y \quad \} \\
 & X \subseteq Y^* \\
= & \quad \{ \quad {}^* \text{ is a closure operator} \quad \} \\
 & X^* \subseteq Y^* \quad .
\end{array}
$$

The second property follows immediately from the anti-symmetry of set inclusion.
□

Theorem 43. Let A be an event in a complemented regular algebra with unit I. Then

$$A^* = (\mathsf{red}.A)^* \quad \Rightarrow \quad \langle \forall X : X^* = A^* : \mathsf{red}.A \subseteq X \rangle \quad .$$

That is, if the reflexive-transitive reduction of A is a starth root of A, it is the least starth root of A.

Proof Assume that $A^* = (\mathsf{red}.A)^*$ and $X^* = A^*$. We have to prove that $\mathsf{red}.A \subseteq X$.

Let $B = A \cap \neg I$, $C = B \cap \neg(B \circ B^+)$ and $Y = X \cap \neg I$. By applying lemma 41 and including the two assumptions, we have

$$A^* = B^* = C^* = X^* = Y^* \quad .$$

Next we note that

$$
\begin{array}{ll}
 & C \\
= & \quad \{ \quad \text{definition of } C \text{ and } B \quad \} \\
 & A \cap \neg I \cap \neg(B \circ B^+) \\
= & \quad \{ \quad \text{idempotency and symmetry of infimum} \quad \} \\
 & (A \cap \neg I \cap \neg(B \circ B^+)) \cap \neg I \\
= & \quad \{ \quad \text{definition of } C \text{ and } B \quad \} \\
 & C \cap \neg I \quad .
\end{array}
$$

It follows that we can apply lemma 42 with $X,Y := A,C$ and $X,Y := C,X$ to deduce that

$$B^+ = C^+ = Y^+ \quad .$$

We can now proceed with the calculation.

$$
\begin{array}{ll}
 & B \cap \neg(B \circ B^+) \subseteq X \\
= & \quad \{ \quad B \cap \neg(B \circ B^+) = C = C \cap C^+ = C \cap Y^+ \quad \} \\
 & B \cap \neg(B \circ B^+) \cap Y^+ \subseteq X \\
= & \quad \{ \quad \text{shunting rule} \quad \} \\
 & B \cap Y^+ \subseteq X \cup B \circ B^+ \\
\Leftarrow & \quad \{ \quad B \cap Y^+ \subseteq Y^+ \text{, transitivity} \quad \} \\
 & Y^+ \subseteq X \cup B \circ B^+ \\
\Leftarrow & \quad \{ \quad Y^+ = Y \cup Y \circ Y^+ \quad \} \\
 & Y \subseteq X \ \wedge \ Y \circ Y^+ \subseteq B \circ B^+ \\
= & \quad \{ \quad Y = X \cap \neg I \quad \} \\
 & Y \circ Y^+ \subseteq B \circ B^+ \\
= & \quad \{ \quad X \circ X^+ = X^+ \circ X^+ \text{ for all } X \\
 & \qquad \text{(well-known property, simple proof left to reader)} \quad \} \\
 & Y^+ \circ Y^+ \subseteq B^+ \circ B^+ \\
= & \quad \{ \quad B^+ = Y^+ \text{: see above} \quad \} \\
 & \mathsf{true} \ .
\end{array}
$$

□

Theorem 43 postulates a candidate for a least starth root. In some cases, the candidate is indeed a least starth root, but this is not always the case. For example, the reflexive-transitive reduction of the universal relation on a set with at least three elements is the empty relation, which is not a starth root of the universal relation. Fortunately, the candidate is indeed a starth root in the case relevant to the current discussion: when A is a finite acyclic graph.

The converse of theorem 43 is not valid as demonstrated by the following counterexample.

Suppose R is the relation $\{(1,2),(2,1)\}$. Then R^* is the universal relation on $\{1,2\}$ and $\mathsf{red}.R$ is the empty relation. Thus, for all X, $\mathsf{red}.R \subseteq X$; however, $R^* \neq (\mathsf{red}.R)^*$. Indeed, the least starth root of R is R itself.

4. Relation Algebra

We are now in a position to present the axioms of relation algebra. As announced earlier, the axiomatisation is *point-free* as opposed to *pointwise*. A pointwise axiomatisation defines the operators of a relation algebra in terms of *Boolean* values xRy; the variables of the axiomatisation are thus relations, R, and *points*, x and y. This is the more conventional means of defining operators on relations. A point-free axiomatisation omits the points; the variables in the axiomatisation are exclusively relations.

The advantage of a point-free axiomatisation is increased concision. This is invaluable to the goal of establishing general properties of relations. A disadvantage is that when one comes to apply such general properties to particular relations, like the at-most relation, it is particular Boolean values, like $m \leq n$, that are of interest. In addition to the axioms

we therefore give a pointwise *interpretation* of each of the operators. That is, we say, for each operator that we introduce, how the operator defines a set of pairs. Such an interpretation is often called a (set-theoretic) *model* of the axiom system. In giving the interpretation we use the notation $[\![E]\!]$ to mean "the interpretation of E". Thus we write $x[\![R]\!]y$ instead of xRy; this enhances readability and also emphasises the difference between the objects of an abstract relation algebra and the interpretation of such objects as binary relations. Note that the expression E is most often a relation, but is sometimes an ordering between relations.

The first unit in relation algebra is a lattice structure. Specifically, let $(\mathcal{A}, \subseteq)$ be a partially-ordered set. We postulate that $\mathcal{A}$ forms a complete, universally distributive lattice. The infimum and supremum operators will be denoted by $\cap$ and $\cup$, respectively. The top and bottom elements of the lattice will be denoted by $\top\!\top$ and $\bot\!\bot$, respectively. We will call elements of $\mathcal{A}$ *relations* and denote them by variables R, S and T.

As suggested by the choice of notation, the interpretation of $\subseteq$ is the subset ordering, the interpretation of $\cap$ is set intersection, and the interpretation of $\cup$ is set union. Formally,

$$[\![R \subseteq S]\!] \;\equiv\; \langle \forall x,y : x[\![R]\!]y : x[\![S]\!]y \rangle \quad ,$$

$$x\,[\![R \cap S]\!]\,y \;\equiv\; x[\![R]\!]y \wedge x[\![S]\!]y \quad \text{, and}$$

$$x\,[\![R \cup S]\!]\,y \;\equiv\; x[\![R]\!]y \vee x[\![S]\!]y \quad .$$

Universal distributivity is the familiar distributivity property of set union over set intersection and, vice-versa, set intersection over set union.

The lattice structure is the most complicated unit in the framework but one which should be familiar to the reader.

Atomicity properties will be introduced later: see section 6.

Every binary relation has a converse. At the point level the converse operator, denoted by a postfix "$^\cup$" symbol, is defined by

$$x\,[\![R^\cup]\!]\,y \;\equiv\; y[\![R]\!]x$$

for all x and y. At the point-free level we postulate the existence of a (total) unary function from relations to relations such that, for all relations R and S

$$R^\cup \subseteq S \;\equiv\; R \subseteq S^\cup \quad . \tag{44}$$

The Galois connection (44) is all that is necessary to define the converse operator and its interface with the lattice structure. Its being a Galois connection makes it so attractive.

The set of homogeneous binary relations over some universe includes the identity relation, I, defined at the point level by

$$x[\![I]\!]y \;\equiv\; x = y$$

for all x and y. Relations may also be composed via the binary composition operator, $\circ$, defined at the point level by

$$x\,[\![R \circ S]\!]\,z \;\equiv\; \langle \exists y :: x[\![R]\!]y \wedge y[\![S]\!]z \rangle \quad .$$

We capture these two notions in our algebraic framework by demanding the existence of a relation I and a binary operator, $\circ$, mapping a pair of relations to a relation, such that $(\mathcal{A}, \circ, I)$ is a monoid.

There are two interfaces to be specified. The interface with the converse operator is soon dealt with. Bearing in mind the intended relational interpretations of converse and composition we postulate

$$(R \circ S)^{\cup} = S^{\cup} \circ R^{\cup} \quad , \tag{45}$$

for all relations R and S. For the interface with the lattice structure we postulate that a relation algebra is a regular algebra. In particular, we postulate that for all relations R the functions $(R\circ)$ and $(\circ R)$ distribute universally over suprema.

4.1. Operator Precedence

We have now introduced quite a large number of operators. In order to reduce the number of parentheses in formulae we should agree on a precedence between the different operators.

A general rule we use throughout is that all prefix and postfix operators as well as subscripting and superscripting take precedence over infix operators and infix operators in turn take precedence over multifix operators. When both prefix and postfix operators are applied to an expression, we use parentheses to clarify the order of evaluation. Thus we only need to discuss the relative precedence of the infix operators.

For infix operators, the general rule is that metaoperators (operators like $\equiv$ and $\wedge$) have the lowest precedence. Next come relations like $\leq$ and $\subseteq$. The operators of relation algebra have the next highest precedence, and function application has the highest precedence of all. Among the infix operators of relation algebra the precedence is: intersection and union have the same, lowest precedence, and the highest precedence is given to composition.

4.2. Modularity Rule and Cone Rule

We have postulated that composition distributes through suprema. We have *not* postulated that composition distributes through infima. Were we to do so then the binary relations would not form a model of our algebraic framework. The lack of such a law, however, poses severe problems. We know that, for each R, the function $(R\circ)$ is monotonic and hence

$$R\circ(S \cap T) \subseteq R\circ S \cap R\circ T \quad .$$

Thus we are in a position to reason with infima of compositions so long as they appear on the bigger side of an inclusion. But we have no means of working with such a term when it appears on the smaller side of an inclusion. Something more is needed to afford the manipulative freedom we need.

The rule we now introduce to overcome this difficulty acts as an interface between all three units of the framework. We call it the *modularity rule*. (J. Riguet [21] called it "la relation de Dedekind" because of its resemblance to the modular identity, a property of normal subgroups discovered by Dedekind. Freyd and Ščedrov [22] call it the *law of modularity*, possibly for the same reason as Riguet.)

The modularity rule is that, for all relations R, S and T,

$$R \circ S \cap T \subseteq R \circ (S \cap R^{\cup} \circ T) \quad . \tag{46}$$

At first sight, this is a difficult rule to appreciate and to use. A little analysis of its structure helps. Note that the term on the smaller side of the inclusion is an infimum of two terms and the term on the larger side is a composition of two terms. None of the rules given so far cater for either of these situations. Note also that R is the only repeated variable on the larger side. Viewing composition as a multiplication operator and infimum as addition, it is as if $R^{\cup}$ is the inverse of R, it being cancelled when R is multiplied through on the righthand side in order to obtain the lefthand side.

An additional rule, sometimes called "Tarski's rule", is called the *cone rule* below: for all relations R,

$$\top\!\!\top \circ R \circ \top\!\!\top = \top\!\!\top \quad \vee \quad R = \bot\!\!\bot \quad . \tag{47}$$

The cone rule expresses the universality of the relation $\top\!\!\top$. Its significance becomes evident in section 6 where it is used in combination with the "all or nothing" rule to model reasoning about relations as sets of pairs.

Axiom systems for relation algebra often include a complementation (negation) operator and, instead of the modularity rule, the so-called Schröder rule is postulated. Our formulation of Schröder's rule is slightly different from standard accounts, as we now explain.

Suppose we consider an algebra that obeys all the axioms of relation algebra except for the modularity rule. Suppose that the algebra is complemented (i.e. every relation has a complement); we denote the complement of relation R by $\neg R$. Then the *middle-exchange rule*:

$$R \circ \neg X \circ S \subseteq \neg Y \quad \equiv \quad R^{\cup} \circ Y \circ S^{\cup} \subseteq X \tag{48}$$

is equivalent to the modularity rule.

The middle-exchange rule gets its name from the fact that the middle term in a composition is exchanged with the right side of an inclusion. It has an attractive, symmetric form, making it easy to remember in spite of having four free variables. The standard rule is the conjunction of the two equivalences obtained by instantiating R and S to the identity relation.

4.3. Summary

This concludes our discussion of the algebraic framework. In a few sentences, a relation algebra is a complete, universally distributive lattice on which is defined a monoid structure and a unary converse operator. Composition on the left and on the right both have upper adjoints, the division operators. Converse is a lattice isomorphism that preserves the unit of composition and distributes contravariantly through composition. Finally, the lattice structure, converse and the monoid structure are all interrelated via the modularity and cone rules.

5. Coreflexives and the Domain Operators

5.1. Coreflexives

In relation algebra there are several mechanisms for viewing sets as relations, each of which has its own merits. One is via "conditions" and another is via "coreflexives[5]". Axiomatically these have the following definitions. First, we say that relation R is a *coreflexive* if and only if $R \subseteq I$. Second, we say that relation R is a *right condition* if and only if $R = \top\!\!\top \circ R$. Finally, we say that R is a *left condition* if and only if $R = R \circ \top\!\!\top$.

We choose to represent sets by coreflexives, the most compelling reason for doing so being the dominant position occupied by composition among programming primitives. Introducing a guard on the left, in the middle, or on the right of a sequential composition of relations is a frequent activity that is easy to express in terms of coreflexives but clumsy to express with conditions. Moreover, coreflexives have simple and convenient properties. Specifically, for all coreflexives p and q,

$$p = I \cap p = p^{\cup} = p \circ p \quad \wedge \quad p \circ q = q \circ p = p \cap q \quad .$$

Occasionally we use the fact that the lattice of coreflexives is isomorphic to the lattice of left (or right) conditions, as expressed by the rule, for all coreflexives p and q,

$$p \subseteq q \;\equiv\; p \circ \top\!\!\top \subseteq q \circ \top\!\!\top \quad .$$

5.2. The Domain Operators

In this section, we introduce two operators mapping relations to coreflexives, the so-called *domain operators*. They play an extremely important role in the theory to follow.

We call the two operators the *left-domain operator* and the *right-domain operator*. We might have chosen to call one of them the "domain operator" and the other the "range operator", but this would have introduced an unwelcome direction in the interpretation of relations. (One of the elements in a pair satisfying a given relation would have to be designated the input and the other the output.) We prefer to make no commitment about the "direction" of a relation for as long as possible. The left- and right-domain operators are denoted by the postfix symbols " $<$ " and " $>$ ", respectively.

Definition 49 (Right Domain). The *right domain* of a relation R is the coreflexive denoted by $R>$ and defined by

$$R> = I \cap \top\!\!\top \circ R \quad .$$

Dually, the *left domain* of a relation R is the coreflexive denoted by $R<$ and defined by

$$R< = I \cap R \circ \top\!\!\top \quad .$$

□

[5] "Coreflexives" are also called "monotypes" [6, 24, 9] or "tests" [10], depending on the intended interpretation; the name "partial identity" is also used (eg. [25]). We now prefer the application-neutral terminology used by Freyd and Ščedrov [22].

We restrict our attention here to the right-domain operator. The reader is requested to dualise the results to the left-domain operator.

The intended interpretation of $R^>$ for relation R is $\{x \mid \langle \exists y :: y [\![R]\!] x \rangle\}$. Two ways we can reformulate this requirement without recourse to points are formulated in the following theorem.

Theorem 50. For all relations R and coreflexives p,

$$(R^> \subseteq p \;\equiv\; R \subseteq \top\!\top \circ p) \quad \wedge \quad (R^> \subseteq p \;\equiv\; R = R \circ p) \quad .$$

□

Theorem 50 predicts a number of useful calculational properties of the right-domain operator. We list some that we exploit later below; for brevity we omit their proofs. We also often give the hint "domains" in calculations, omitting specific mention of the rule. This includes cases where one or more of the variables is instantiated to the identity relation. (For example, an instance of theorem 51(f) is the property that, for all R, $R^> = (R^>)^>$.)

Theorem 51. For all relations R, S and T, and all coreflexives p,

(a) $\top\!\top \circ R^> = \top\!\top \circ R$,

(b) $R \cap S \circ \top\!\top \circ T \;=\; S^< \circ R \circ T^>$,

(c) $(R^\cup)^> = R^<$,

(d) $(R \cap S \circ T)^> = (S^\cup \circ R \cap T)^>$,

(e) $(R \circ \top\!\top \circ S)^> = S^> \;\Leftarrow\; R \neq \bot\!\bot$,

(f) $(R \circ S)^> = (R^> \circ S)^>$,

(g) $p^> = p$.

□

For modelling programming statements, in particular conditionals, *complemented domains* are necessary. We assume that the lattice of coreflexives is complemented and let $R^{>\bullet}$ denote the complement of $R^>$. That is,

$$R^> \cup R^{>\bullet} = I \qquad \text{and} \qquad R^> \cap R^{>\bullet} = \bot\!\bot \quad .$$

Then, for relations R and coreflexives p,

$$R^{>\bullet} \supseteq p \;\equiv\; R \circ p = \bot\!\bot \quad . \tag{52}$$

Moreover, for all R,

$$(R^>)^{>\bullet} = R^{>\bullet} = (R^{>\bullet})^> \quad . \tag{53}$$

Note that (52) is a slightly disguised Galois connection since the right side can be rewritten as $R \subseteq \bot\!\bot / p$. (See (31).) The equation defines $R^{>\bullet}$ as the largest coreflexive p such that restricting the right domain of R to p yields the empty relation. A consequence is the distributivity property

$$(R \cup S)^{>\bullet} \;=\; R^{>\bullet} \cap S^{>\bullet} \quad .$$

Just as for the non-complemented domain operator, it is difficult to simplify $(R \cap S)^{>\bullet}$.

6. All or Nothing

In this section, we add axioms that postulate that relations are sets of pairs. The two properties we assume are:

1. The poset of coreflexives is a complete, universally distributive, saturated lattice.
2. The *all-or-nothing* rule:

$$\langle \forall\, a,b,R \;:\; \mathsf{AC}.a \wedge \mathsf{AC}.b \;:\; a \circ R \circ b = \bot\!\!\!\bot \;\vee\; a \circ R \circ b = a \circ \top\!\!\!\top \circ b \rangle$$

where AC abbreviates "atomic and coreflexive".

An immediate consequence of the all-or-nothing rule is the following lemma.

Lemma 54. Suppose a is an atomic coreflexive. Then

$$a \circ \top\!\!\!\top \circ a \;=\; a \quad . \tag{55}$$

Also, if a and b are proper atomic coreflexives, then

$$a \circ \top\!\!\!\top \circ b \subseteq I \;\equiv\; a = b \quad . \tag{56}$$

□

We use lemma 54 frequently below (sometimes without specific mention).

The all-or-nothing rule is equivalent to the postulate that the lattice of relations is atomic and saturated. The proper atoms are events of the form $a \circ \top\!\!\!\top \circ b$ where a and b are proper atomic coreflexives; such an event models the pair (a, b) in conventional pointwise formulations of relation algebra [26, 25].

Theorem 57. Suppose the lattice of coreflexives is a complete, universally distributive, saturated lattice. Then, if the all-or-nothing rule is universally valid, the lattice of relations is also a saturated, atomic lattice; the atoms are elements of the form $a \circ \top\!\!\!\top \circ b$ where a and b are atoms of the lattice of coreflexives. It follows that the lattice of relations is isomorphic to the powerset of the set of elements of the form $a \circ \top\!\!\!\top \circ b$ where a and b are atoms of the lattice of coreflexives.
□

Henceforth, we assume that the lattice of coreflexives and the lattice of relations are both complete, universally distributive and saturated. In view of theorem 15, we use $\subseteq$ for the ordering relation and $\sim$ for the complement operator on coreflexives. We use $\neg$ for the complement operator on relations. Thus, for coreflexive p, $\sim p = I \cap \neg p$. The proper atomic coreflexives are variously referred to below as *points* and later, when the relations represent graphs, as *nodes*. Standard properties of powersets —the properties of set union, intersection and complementation— will be assumed, sometimes without specific mention and sometimes with the hint "set theory".

We use p and q to range over coreflexives and a and b to range over atomic coreflexives. A crucial property is, for all points a and coreflexives p,

$$\neg(a \subseteq p) \;\equiv\; a \subseteq \sim p \quad .$$

See lemma 16.

7. Functions and Heterogeneous Relations

7.1. Functionality and Totality

A subset of the relations is formed by the functions, which can be seen as deterministic relations. The characterising property of a function is that it is single-valued (also known as Leibniz's rule), i.e. if $y[\![f]\!]x$ and $z[\![f]\!]x$ then y is equal to z. This is written as:

$$\langle \forall y,z : \langle \exists x :: y[\![f]\!]x \ \wedge \ z[\![f]\!]x \rangle : y[\![I]\!]z \rangle \ .$$

After rewriting the existential quantification using relation composition and subsequently the universal quantification using the definition of relation inclusion, we obtain (the much more concise):

$$f \circ f^{\cup} \subseteq I \ . \tag{58}$$

The notion dual to functionality, viz. injectivity, is now of course easy to define: f is *injective* if and only if $f^{\cup}$ is functional.

The standard notion of a partial function is a relation that defines a unique output value for each input value in its domain. In our axiom system we have the following theorem.

Theorem 59. Suppose relation R has type $A \sim B$. Then

$$R \circ R^{\cup} \subseteq I_A \ \equiv \ \langle \forall b : b \subseteq R^{>} : \mathsf{point}.(R \circ b \circ R^{\cup}) \rangle \ .$$

Moreover, if f is a relation of type $A \sim B$ and $f \circ f^{\cup} \subseteq I_A$, the relation $f \circ b \circ f^{\cup}$ is a point of type A and

$$\langle \forall a,b \ : \ b \subseteq f^{>} \ : \ a \circ \top\!\!\top \circ b \subseteq f \ \equiv \ a \ = \ f \circ b \circ f^{\cup} \rangle \ .$$

(Recall that a point is a proper atomic coreflexive. The convention we use is that point denotes the predicate "is a point".)
□

In words, theorem 59 states that f is functional iff, for all points b in the right domain of f, the relation $f \circ b \circ f^{\cup}$ defines a unique point of type A. This is the point that we denote by $f.b$. The defining property of $f.b$ is thus

$$\langle \forall a,b \ : \ b \subseteq f^{>} \ : \ a \circ \top\!\!\top \circ b \subseteq f \ \equiv \ a = f.b \rangle \ . \tag{60}$$

A consequence of the unicity property expressed by (60) is the property that, for all functional relations f of type $C \sim A$ and g of type $C \sim B$, and all points a and b,

$$a \circ \top\!\!\top \circ b \subseteq f^{\cup} \circ g \ \equiv \ a \subseteq f^{>} \wedge f.a = g.b \wedge b \subseteq g^{>} \ . \tag{61}$$

When introducing the modularity rule in section 4.2, we emphasised the importance of distributivity properties. A distributivity property that possibly goes unnoticed in pointwise calculations but must be used explicitly in point-free calculations is the distributivity of functions over intersection: for all relations R and S and all functional relations f,

$$(R \cap S) \circ f \ = \ R \circ f \cap S \circ f \ . \tag{62}$$

Besides functionality and injectivity, there are two other dual notions which relations may enjoy: totality and surjectivity. Relation R is total means that it can accept every element of the universe as an input. Formally, relation R is *total* iff $I \subseteq R^{\cup} \circ R$. Relation R is *surjective* iff its converse $R^{\cup}$ is total.

7.2. Heterogeneous Relations

A *heterogeneous* relation R has a *type* given by two sets A and B, which we call the *target* and *source* of R. We use the notation $A \sim B$ to denote the type of a relation. Formally, a relation of type $A \sim B$ is a subset of $A \times B$. (Equivalently, it is a function with domain $A \times B$ and range Bool.) A *homogeneous* relation is a relation of type $A \sim A$ for some A.

The target and source of a relation should not be confused with its left domain and right domain. If R has type $A \sim B$ then its left domain $R^<$ has type $A \sim A$ and its right domain $R^>$ has type $B \sim B$. As always, $R^<$ and $R^>$ are coreflexives, but this property is expressed formally as $R^< \subseteq I_A$ and $R^> \subseteq I_B$, where I_A denotes the identity relation of type $A \sim A$ (and similarly for I_B).

The operators in the algebra of heterogeneous relations are typed. For example, the composition of two relations R and S, denoted as always by $R \circ S$, is only defined when the source of R equals the target of S. Moreover, the target of $R \circ S$ is the target of R and the source of $R \circ S$ is the source of S. That is, if R has type $A \sim B$ and S has type $B \sim C$ then $R \circ S$ has type $A \sim C$. We assume the reader is familiar with such rules.

As mentioned earlier, the rules of the untyped calculus are applicable in the typed calculus, with some restrictions on types. For example, the rule $R = R^< \circ R$ remains valid without restriction. Restrictions are necessary on types for, for example, the middle-exchange rule (see section 4).

Care must be taken with the overloading of notation. This is exemplified by the rule

$$R \circ \top\top \;=\; R^< \circ \top\top \quad .$$

Recall that, if R has type $A \sim B$, $R^<$ has type $A \sim A$. Thus the notation "$\top\top$" on the left side of the equation denotes the universal relation of type $B \sim C$, for some type C; on the other hand, the notation "$\top\top$" on the right side of the equation denotes the universal relation of type $A \sim C$. Rather than overload the notation in this way, we could decorate every occurrence of $\top\top$ with its type. For example, we could rephrase the rule as

$$R \circ {}_B\top\top_C \quad = \quad R^< \circ {}_A\top\top_C \quad .$$

We prefer not to do so because the type information is usually easy to infer. An exception is that we occasionally decorate the identity relation I with its type: I_A denotes the identity relation of type $A \sim A$.

Care must also be taken to distinguish between coreflexives and the sets that they represent. This is particularly relevant when defining functions since, in our formal system, a function maps a point to a point. In informal statements, less care is needed. For example, when discussing partitions of equivalence relations in section 8.2: it is necessary to introduce a so-called "cast" in order to make the type distinction between coreflexives (which are not points) and the sets that they represent (which are points).

Typed relation algebra, as briefly summarised above, extends category theory to what has been called *allegory theory*. See Freyd and Ščedrov [22] for more details.

8. Equivalence Relations and Partitions

This section recalls some general properties of equivalence relations. Section 8.1 introduces the so-called "existential image" function; the main theorem in this section

is theorem 67 which states that the existential image function defined by an equivalence relation is a complementation-fixed closure operator. Section 8.2 formulates the well-known correspondence between partitions of a set and equivalence classes.

8.1. (Left- and Right-)Existential Image

This section is about exploring the properties of the endofunction $\langle p : p \subseteq I : (R \circ p)^< \rangle$. We show that, if R is reflexive and transitive, it is a closure operator; we also show that, if R is an equivalence relation, it is complementation fixed.

To avoid clutter, we use the convention that lower case identifiers p and q range over coreflexives. So the function of interest is $\langle p :: (R \circ p)^< \rangle$. The function $\langle R :: \langle p :: (R \circ p)^< \rangle \rangle$ is essentially the same as what Bird and De Moor [27] call the *existential image functor*. Temporarily for brevity, we use the notation $\mathcal{E}R$ for the function $\langle p :: (R \circ p)^< \rangle$.

The following is easily proved.

Theorem 63. The function $\mathcal{E}$ maintains identities and distributes over composition. That is, for all A, R and S (of appropriate type),

$$\mathcal{E}(I_A) \;=\; I_{\mathsf{Cor}.A} \quad \wedge \quad \mathcal{E}(R \circ S) \;=\; \mathcal{E}R \bullet \mathcal{E}S \quad .$$

(The infix operator "$\bullet$" denotes composition of functions; $\mathsf{Cor}.A$ denotes the type of coreflexives of type $A \sim A$.) Moreover, for all relations R, $\mathcal{E}R$ is the lower adjoint in a Galois connection of the coreflexives (ordered by the subset relation) with itself. (This is because it is the composition of two lower adjoints: the function $(R \circ)$ and the left-domain operator $^<$.) Thus, for all relations R, $\mathcal{E}R$ distributes universally over unions of coreflexives; in particular, it is monotonic. Indeed, $\mathcal{E}$ is also (pointwise) monotonic. So $\mathcal{E}$ is monotonic in both its arguments. That is,

$$\mathcal{E}R.p \subseteq \mathcal{E}S.q \quad \Leftarrow \quad R \subseteq S \;\wedge\; p \subseteq q \quad .$$

□

Next we explore when the function $\mathcal{E}R$ is a closure operator.

Lemma 64. If R is reflexive and transitive, the function $\mathcal{E}R$ is a closure operator.

Proof Instantiating definition 22 of a closure operator, we have to show that, for all p and q,

$$q \;\subseteq\; \mathcal{E}R.p \quad \equiv \quad \mathcal{E}R.q \;\subseteq\; \mathcal{E}R.p \quad .$$

The equivalence is established by mutual implication. For the implication, we have:

$$\begin{array}{ll} & \mathcal{E}R.q \\ \subseteq & \quad \{ \quad \text{assume } q \subseteq \mathcal{E}R.p \text{, monotonicity of } \mathcal{E}R \quad \} \\ & \mathcal{E}R.(\mathcal{E}R.p) \\ = & \quad \{ \quad \text{distributivity (theorem 63)} \quad \} \\ & \mathcal{E}(R \circ R).p \\ \subseteq & \quad \{ \quad \text{assumption: } R \text{ is transitive; theorem 63} \quad \} \\ & \mathcal{E}R.p \end{array}$$

and, for follows-from, we have:

$$
\begin{array}{ll}
& q \subseteq \mathcal{E}R.p \\
\Leftarrow & \quad \{ \quad \text{assume } \mathcal{E}R.q \subseteq \mathcal{E}R.p \text{, transitivity of } \subseteq \quad \} \\
& q \subseteq \mathcal{E}R.q \\
\Leftarrow & \quad \{ \quad \text{assumption: } R \text{ is reflexive, i.e. } I \subseteq R \text{;} \\
& \qquad \text{monotonicity (theorem 63)} \quad \} \\
& q \subseteq \mathcal{E}I.q \\
\Leftarrow & \quad \{ \quad \mathcal{E} \text{ preserves identities (theorem 63) and reflexivity of } \subseteq \quad \} \\
& \mathsf{true} \ .
\end{array}
$$

□

Recalling definition 23, we explore conditions on R under which it is complementation-idempotent, i.e.

$$\mathcal{E}R \,.\sim(\mathcal{E}R.p) \;=\; \sim(\mathcal{E}R.p)$$

for all coreflexives p. Noting that, for all relations R, $R{\bullet\!<} = \sim(R^{<})$, we consider the more general property

$$(R \circ (R \circ S){\bullet\!<})^{<} \;=\; (R \circ S){\bullet\!<} \ ,$$

for arbitrary relations S, beginning with the inclusion.

Lemma 65. For arbitrary relations R and S,

$$(R \circ (R \circ S){\bullet\!<})^{<} \subseteq (R \circ S){\bullet\!<} \quad \Leftarrow \quad R^{\cup} \circ R \subseteq R \ .$$

Proof Note how the calculation below is used to determine simpler conditions on R for which the more complicated inclusion holds. The use of the isomorphism between conditionals and domains in the first step is driven by the fact that the negation of a condition is a condition. The use of middle-exchange then becomes obvious.

$$
\begin{array}{ll}
& (R \circ (R \circ S){\bullet\!<})^{<} \subseteq (R \circ S){\bullet\!<} \\
= & \quad \{ \quad \text{theorem 50} \quad \} \\
& R \circ (R \circ S){\bullet\!<} \circ \top\!\!\top \;\subseteq\; (R \circ S){\bullet\!<} \circ \top\!\!\top \\
= & \quad \{ \quad \text{property of negated left domain} \quad \} \\
& R \circ \neg(R \circ S \circ \top\!\!\top) \;\subseteq\; \neg(R \circ S \circ \top\!\!\top) \\
= & \quad \{ \quad \text{middle-exchange rule (48)} \\
& \qquad \text{with } R,X,S,Y := R, R \circ S \circ \top\!\!\top, I, R \circ S \circ \top\!\!\top \quad \} \\
& R^{\cup} \circ R \circ S \circ \top\!\!\top \;\subseteq\; R \circ S \circ \top\!\!\top \\
\Leftarrow & \quad \{ \quad \text{monotonicity of composition} \quad \} \\
& R^{\cup} \circ R \;\subseteq\; R \ .
\end{array}
$$

□

Corollary 66. If R is an equivalence relation then, for all S,

$$(R \circ (R \circ S)\bullet\!<)\!< \;=\; (R \circ S)\bullet\!< \quad .$$

That is, if R is an equivalence relation, $(R \circ S)\bullet\!<$ is a fixed point of the function $\mathcal{E}R$.

Proof We have:

$$\begin{array}{ll} & (R \circ (R \circ S)\bullet\!<)\!< \\ \subseteq & \quad \{ \quad R \text{ is an equivalence relation, so } R^{\cup} \circ R \subseteq R \text{, lemma 65} \quad \} \\ & (R \circ S)\bullet\!< \\ = & \quad \{ \quad I \text{ is unit of composition;} \\ & \qquad (R\bullet\!<)\!< = R\bullet\!< \text{ for all } R \text{, with } R := R \circ S \quad \} \\ & (I \circ (R \circ S)\bullet\!<)\!< \\ \subseteq & \quad \{ \quad R \text{ is an equivalence relation, so } I \subseteq R\text{,} \\ & \qquad \text{monotonicity of composition and domains} \quad \} \\ & (R \circ (R \circ S)\bullet\!<)\!< \quad . \end{array}$$

The equality thus follows by the anti-symmetry of $\subseteq$.
□

To conclude, we have:

Theorem 67. If R is an equivalence relation, the function $\mathcal{E}R$ is a complementation-fixed and complementation-idempotent closure operator.

Moreover, if R is an equivalence relation on a complete, universally distributive, saturated lattice, the set of coreflexives $\mathsf{Fix}.\mathcal{E}R$ is a complete, saturated lattice, its atoms being the set of coreflexives $(R \circ a)\!<$ where a is an atom of the lattice of all coreflexives.

Proof An equivalence relation R is reflexive ($I \subseteq R$), symmetric ($R = R^{\cup}$) and transitive ($R \circ R \subseteq R$). So the function is a closure operator by lemma 64 and, hence, complementation idempotent by corollary 66. It is thus also complementation fixed by lemma 24.

If R is an equivalence relation on a complete, universally distributive lattice, the completeness and saturation properties are given by theorem 26.
□

8.2. Partitions

As is well known, an equivalence relation *partitions* the set on which it is defined into a number of so-called *equivalence classes*. More formally, if R is an equivalence relation on a set A, there is a set C and a surjective function f of type $C \leftarrow A$, such that, for all a and b in A,

$$a [\![R]\!] b \;\equiv\; f.a = f.b \quad . \tag{68}$$

(It is common to use square brackets to denote the function f. So, instead of writing $f.a$, one writes $[a]$, or $[a]_R$ if it is thought necessary to make the equivalence relation explicit.)

Conversely, given sets A and C and a total function f of type $C \leftarrow A$, we can use equation (68) to define a homogeneous relation R on A. The relation R is then an equivalence relation.

Equation (68) is expressed more succinctly by the equation

$$R = f^{\cup} \circ f \quad . \tag{69}$$

The converse proposition is that if R is an equivalence relation on set A, the function ΛR of type $2^A \leftarrow A$ defined by

$$\Lambda R \;=\; \langle a \;::\; \mathsf{Set}\,.\,(R \circ a)^{<} \rangle$$

maps proper atoms a to equivalence classes of R (where Set "casts" a coreflexive of type $A \sim A$, for some A, to the atom of type 2^A representing the same subset of A). That is, for all equivalence relations R,

$$R \;=\; (\Lambda R)^{\cup} \circ \Lambda R \quad . \tag{70}$$

In general —i.e. for arbitrary R and not just equivalence relations— ΛR is called the *power transpose* of R [27]. If R has type $A \sim B$, ΛR has type $2^A \leftarrow B$. In order to define the power transpose, Bird and De Moor [27] postulate a number of axioms relating it to membership. (Their axiomatisation is based on the one formulated by Freyd and Ščedrov [22].) We refer the reader to [28] for an elegant account of how this axiomatisation is used to prove (70). We choose not to add further axioms but instead present our own proof.

We exploit the properties of $\mathcal{E}R$ proved in section 8.1. This we may do because an atomic coreflexive a is a special case of a coreflexive p. So the function that Bird and De Moor denote by ΛR is the restriction of $\mathcal{E}R$ to atomic coreflexives.

Lemma 71. For all relations R, all coreflexives p and all points b,

$$p \subseteq (R \circ b)^{<} \;\equiv\; p \circ R \circ b \;=\; p \circ \top\!\!\top \circ b \quad .$$

Proof The proof is by mutual implication:

$$\begin{array}{ll}
 & p \subseteq (R \circ b)^{<} \\
= & \quad \{ \quad p \text{ and } (R \circ b)^{<} \text{ are coreflexives} \quad \} \\
 & p \circ (R \circ b)^{<} \;=\; p \\
\Rightarrow & \quad \{ \quad \text{Leibniz} \quad \} \\
 & p \circ (R \circ b)^{<} \circ \top\!\!\top \circ b \;=\; p \circ \top\!\!\top \circ b \\
= & \quad \{ \quad \text{theorem 51(a)} \;;\; b \text{ is an atomic coreflexive, so } b \circ \top\!\!\top \circ b = b \quad \} \\
 & p \circ R \circ b \;=\; p \circ \top\!\!\top \circ b \\
\Rightarrow & \quad \{ \quad I \supseteq p \;;\; \text{monotonicity} \quad \} \\
 & (R \circ b)^{<} \supseteq (p \circ \top\!\!\top \circ b)^{<} \\
= & \quad \{ \quad b \text{ is proper, domains: theorem 51(e)} \quad \} \\
 & (R \circ b)^{<} \supseteq p \quad .
\end{array}$$

□

Corollary 72. If R is an equivalence relation, then for all points a and b,

$$(R \circ a)^< \;=\; (R \circ b)^< \quad \equiv \quad a \circ R \circ b \;=\; a \circ \top\!\!\top \circ b \quad .$$

Proof By lemma 71 with $R,p,b := R,a,b$,

$$a \;\subseteq\; (R \circ b)^< \quad \equiv \quad a \circ R \circ b \;=\; a \circ \top\!\!\top \circ b \quad .$$

But, by lemma 64, with $p,q := b,a$ (and instantiating the definition of $\mathcal{E}R$),

$$a \;\subseteq\; (R \circ b)^< \quad \equiv \quad (R \circ a)^< \;\subseteq\; (R \circ b)^< \quad .$$

(Note that application of lemma 64 only requires R to be reflexive and transitive.) By transitivity of equivales, we get, for all points a and b,

$$(R \circ a)^< \;\subseteq\; (R \circ b)^< \quad \equiv \quad a \circ R \circ b \;=\; a \circ \top\!\!\top \circ b \quad .$$

Swapping the roles of a and b, for all points a and b,

$$(R \circ b)^< \;\subseteq\; (R \circ a)^< \quad \equiv \quad b \circ R \circ a \;=\; b \circ \top\!\!\top \circ a \quad .$$

Now we exploit the fact that R is symmetric, i.e. $R = R^{\cup}$. We have, for all coreflexives a and b,

$$b \circ R \circ a \;=\; b \circ \top\!\!\top \circ a \quad \equiv \quad a \circ R^{\cup} \circ b \;=\; a \circ \top\!\!\top \circ b \quad .$$

Exploiting the equality $R = R^{\cup}$, the transitivity of equivales, and anti-symmetry, we conclude that

$$(R \circ a)^< \;=\; (R \circ b)^< \quad \equiv \quad a \circ R \circ b = a \circ \top\!\!\top \circ b \quad .$$

□

Theorem 73. Suppose R is an equivalence relation. Let the function f be defined to be

$$\langle a \;::\; \mathsf{Set}\,.\,(R \circ a)^< \rangle \quad .$$

(Recall that Set casts a coreflexive of type $A \sim A$, for some A, to the atom of type 2^A representing the same subset of A.) Then

$$R \;=\; f^{\cup} \circ f \quad .$$

Proof Suppose R is an equivalence relation on set A. By the definition of f, for all points a of type A and points c of type 2^A,

$$c \circ f \circ a \neq \bot\!\!\bot \quad \equiv \quad c \;=\; \mathsf{Set}.(R \circ a)^< \quad . \tag{74}$$

Thus, with dummies a and b ranging over points of type A, and dummy c ranging over points of type 2^A, we have:

$$
\begin{array}{ll}
 & R \\
= & \quad \{ \quad \text{saturation assumption: theorem 57} \\
 & \qquad \text{and all-or-nothing rule (section 6)} \quad \} \\
 & \langle \cup a,b : a \circ R \circ b = a \circ \top\!\!\top \circ b : a \circ \top\!\!\top \circ b \rangle \\
= & \quad \{ \quad \text{assumption: } R \text{ is an equivalence relation, corollary 72} \quad \} \\
 & \langle \cup a,b \ : \ (R \circ a)^< \ = \ (R \circ b)^< \ : \ a \circ \top\!\!\top \circ b \rangle \\
= & \quad \{ \quad \mathsf{Set} \text{ casts a coreflexive of type } A \sim A \text{ to a point of } 2^A \quad \} \\
 & \langle \cup a,b \ : \ \mathsf{Set}.(R \circ a)^< \ = \ \mathsf{Set}.(R \circ b)^< \ : \ a \circ \top\!\!\top \circ b \rangle \\
= & \quad \{ \quad \text{definition of total function } f : (74), \text{ and } (61) \quad \} \\
 & f^\cup \circ f \quad .
\end{array}
$$

□

The final property in this section expresses the property that every proper atom is in an equivalence class of the equivalence relation R. For this, it is inevitable that we must assume that the lattice of coreflexives is saturated.

Lemma 75. Suppose R is an equivalence relation on a saturated atomic lattice. Then

$$\langle \cup a :: (R \circ a)^< \rangle \ = \ I \quad .$$

(As always, dummy a ranges over points.)

Proof

$$
\begin{array}{ll}
 & \langle \cup a :: (R \circ a)^< \rangle \\
= & \quad \{ \quad \text{the functions } ^< \text{ and } (\, R \circ \,) \text{ are lower adjoints} \\
 & \qquad \text{and so are universally distributive} \quad \} \\
 & (R \circ \langle \cup a :: a \rangle)^< \\
= & \quad \{ \quad \text{the lattice of coreflexives is saturated, i.e. } \langle \cup a :: a \rangle \ = \ I \quad \} \\
 & (R \circ I)^< \\
= & \quad \{ \quad R^< \subseteq I \text{, for all } R \text{;} \\
 & \qquad R \text{ is reflexive, i.e. } I \subseteq R \text{; } ^< \text{ is monotonic and } I^< = I \text{.} \quad \} \\
 & I \quad .
\end{array}
$$

□

8.3. Left and Right Duals

This section has established a number of properties of the functions $\langle R :: \langle p :: (R \circ p)^< \rangle \rangle$, where p ranges over arbitrary coreflexives, and $\langle R :: \langle a :: (R \circ a)^< \rangle \rangle$, where a ranges over atomic coreflexives. As we have observed, these functions are sometimes called, respectively, the existential-image functor and the power-transpose function [27, 22].

One of the most significant beauties of relation algebra is that many operators and their properties are very easily dualised by exploiting the properties of the converse operator. The properties we have established of the existential image and power transpose are, intrinsically, properties of the *left*-domain operator; these are very easily dualised to

properties of the *right*-domain operator: we could just as easily have defined the "existential image" of relation R to be the function $\langle p :: (p \circ R)^{>} \rangle$ and the "power transpose" of R to be the function $\langle a :: (a \circ R)^{>} \rangle$. The choice we have made is arbitrary; other authors might —and sometimes do— make a different choice.

In this paper, we use both the left- and right-domain operators without bias. In particular, we use both the "left" existential-image/power-transpose functions and the "right" existential-image/power-transpose functions. See, for example, the definition of left- and right-definite, definition 76, and the subsequent discussion of well-foundedness of relations and the acyclicity of graphs.

The terminology that one chooses can often be very helpful to explain the relevance of a theory in a particular application. For example, in section 9.3 we use the terminology "reachable" for a particular instance of the (right-)existential image function in order to relate our theorems to path-finding problems in graphs. The terminology "existential image", on the other hand, emphasises a view of relations as set-valued functions, a view that is not relevant here. We hope that, by introducing the terminology, the reader is enabled to more easily recognise correspondences between our presentation and other accounts; however, from now on we no longer refer to the "existential image" or "power transpose" of a relation. We also no longer use the abbreviation $\mathcal{E}R$.

9. Acyclicity and Definiteness

This section begins our presentation of algorithmic graph theory. From now on, a *graph* G is simply a homogeneous "edge" relation of type $\mathsf{Node} \sim \mathsf{Node}$ where Node is a *finite* set. A proper atom a in the lattice of coreflexives of type Node is a *node* of the graph. Then, if a and b are both nodes, the boolean $a \circ G \circ b \neq \bot\!\!\!\bot$ represents the existence of an *edge* from a to b; if indeed $a \circ G \circ b \neq \bot\!\!\!\bot$, the edge itself is the atom $a \circ \top\!\!\!\top \circ b$ (in the poset of relations of type $\mathsf{Node} \sim \mathsf{Node}$). The existence of a *path* from a to b is represented by the boolean $a \circ G^* \circ b \neq \bot\!\!\!\bot$. (The path itself is a sequence of nodes.) In this way, relation algebra is the appropriate vehicle for a study of the algorithmic properties of the *existence* of paths in graphs. (Regular algebra is the appropriate vehicle for studying more general properties of paths in graphs.)

Acyclic graphs (graphs without cyclic paths) form an important subclass of graphs. This is not just because they naturally occur in practical problems —they correspond to partial orderings on finite sets— but also because all graphs comprise a collection of so-called "strongly connected components" that are connected by an acyclic graph. This structural property of graphs —formalised in theorem 143— is important in path-finding algorithms as well as the seemingly unrelated problem of efficiently representing the inverse of a real matrix. (See the discussion following theorem 143 for further discussion.)

Subsection 9.1 defines acyclicity in the conventional way in terms of paths. At the same time, a less well-known property, which we call "definiteness" is introduced. Whereas acyclicity is particularly appropriate to reasoning about graphs, definiteness is more general. For finite graphs, the two notions coincide, as shown in this section.

Subsection 9.2 is about showing that the reflexive-transitive reduction of a definite relation is its least starth root. Equivalently, every partial ordering on a finite set has a unique so-called "Hasse diagram".

Subsection 9.3 develops a formal proof of the following fact from graph theory: in an acyclic graph, the nodes reachable from set A coincide with the nodes reachable

from the "minimal" elements of A. The theorem is a corollary of a much more general theorem about "right-definiteness" of a relation. In more conventional terminology, it is the theorem that, given a well-founded relation on a set S, every non-empty subset of S has a minimal element (with respect to the well-founded relation).

The final subsection in this section, subsection 9.4, is about how a so-called "topological search" of an acyclic graph assigns to the nodes of the graph a "topological ordering". The definition of a topological ordering and the algorithm for topological search are formulated in point-free relation algebra.

Many properties we prove are valid for arbitrary relations and not just for graphs. That is, the assumption of finiteness is not required. Nevertheless, we often use graph terminology because this is the primary application here. In order to make the level of generality clear, we use R to denote an arbitrary relation and G to denote a graph — that is, a relation over a finite set of nodes.

9.1. Definiteness and Acyclicity

We have to define the meaning of a graph being acyclic. Obviously, a cycle gives rise to an infinite path in the graph. Conversely, an infinite path in a finite graph contains a cycle (because the number of vertices is finite). Therefore, acyclicity in finite graphs is the same as the absence of infinite paths, to which we give the name "(left or right) definite".

Definition 76 ((Right/Left) Definite). Relation R is said to be *right-definite* if and only if it satisfies

$$\langle \forall p :: p \subseteq \bot\!\!\!\bot \Leftarrow p \subseteq (p \circ R)^{>} \rangle \quad . \tag{77}$$

It is said to be *left-definite* if and only if it satisfies

$$\langle \forall p :: p \subseteq \bot\!\!\!\bot \Leftarrow p \subseteq (R \circ p)^{<} \rangle \quad . \tag{78}$$

It is said to be *definite* if it is both left- and right-definite.
□

Informally, right-definiteness means the absence of infinite "descending" paths. That is, there is not a non-empty set of atoms, represented by the coreflexive p, such that, for all atoms a in p, it is always possible to find an atom b in p such a is in the set represented by $(b \circ R)^{>}$, i.e. $b[\![R]\!]a$. Were this possible, the process can be repeated *ad infinitum*; in graphs, this means the existence of paths comprising an infinite number of edges. (See lemmas 91 and 93 for the formalisation of this argument.)

Note that R is right-definite equivales that its converse $R^{\cup}$ is left-definite. So left-definiteness means the absence of infinite "ascending" paths. A hint on how to remember which is which is that left-definiteness is defined in terms of the left-domain operator and right-definiteness in terms of the right-domain operator.

The importance of the concept of definiteness is what we have called the *unique extension property* (UEP) of relation algebra.

Theorem 79 (UEP of Relation Algebra). Suppose R is a right-definite relation. Then, for all coreflexives p and q,

$$p \;=\; (p \circ R)^{>} \cup q \quad \equiv \quad p \;=\; (q \circ R^{*})^{>} \quad .$$

Also, for all relations X and S,

$$X \;=\; X \circ R \cup S \quad\equiv\quad X \;=\; S \circ R^* \quad .$$

Dually, if R is a left-definite relation, for all coreflexives p and q,

$$p \;=\; (R \circ p)^< \cup q \quad\equiv\quad p \;=\; (R^* \circ q)^< \quad ,$$

and, for all relations X and S,

$$X \;=\; R \circ X \cup S \quad\equiv\quad X \;=\; R^* \circ S \quad .$$

□

A proof of theorem 79 can be found in [9, section 7]. Note that [9] uses the terminology "well-founded" rather than "right-definite" in order to fit with the standard terminology of the principle application considered in the paper. (In fact, [9, theorem 16] establishes an equivalence rather than just the implication stated in theorem 79. The converse implication is straightforward and of lesser importance. Also, the theorem is called the UEP of *regular* algebra in [9] because its proof depends on properties of a regular algebra rather than properties specific to relation algebra.)

The less-than relation on natural numbers is the transitive closure of the predecessor relation (the converse of the successor function, where the successor of m is $m{+}1$). And, of course, the predecessor relation is well-founded. This exemplifies a (well-known) property, namely:

Lemma 80. Relation R is right-definite equivales relation R^+ is right-definite. Similarly for left-definite and for definite. Thus R is right-definite if and only if it satisfies

$$\langle \forall p \;::\; p \subseteq \bot\!\!\!\bot \;\Leftarrow\; p \subseteq (p \circ R^+)^> \rangle \quad . \tag{81}$$

It is left-definite if and only if it satisfies

$$\langle \forall p \;::\; p \subseteq \bot\!\!\!\bot \;\Leftarrow\; p \subseteq (R^+ \circ p)^< \rangle \quad . \tag{82}$$

□

See [9] for a detailed study of properties of R and R^+ of which lemma 80 is an instance.

As mentioned earlier, in [9] the better known term "well-founded" was used instead of our "right-definite". An example of a well-founded relation is the less-than relation on the natural numbers. Expressed pointwise, (77) for this application is the property that, for all subsets p of the natural numbers,

$$p{=}\emptyset \;\Leftarrow\; \langle \forall m : m{\in}p : \langle \exists n : n{\in}p : n{<}m \rangle \rangle \quad .$$

Expressed slightly differently, this is the property, for all subsets p of the natural numbers,

$$p{=}\emptyset \;\vee\; \langle \exists m : m{\in}p : \langle \forall n : n{\in}p : n{\geq}m \rangle \rangle \quad .$$

In words, every non-empty set of natural numbers has a least element.

We mention this example because it illustrates the fact that left-definite and right-definite are *not* (in general) the same: the successor relation on the natural numbers (the converse of the predecessor relation) is not well-founded. Left- and right-definite are the same for *finite* graphs, as we shall see.

For later use, we note the following simple lemma.

Lemma 83. Suppose R is right-definite and $R \supseteq S$. Then S is right-definite. The same is true with "left" replacing "right".

Proof Immediate from the monotonicity of transitive closure, composition and the domain operators.
□

Anticipating the definition of acyclicity (definition 86), we rephrase right-definiteness in terms of atomic coreflexives.

Lemma 84. For all R and all atomic coreflexives a,

$$a \subseteq R \quad \equiv \quad a \subseteq (a \circ R)^{>} \quad .$$

Proof Suppose a is an atomic coreflexive. Then, for all R,

$$\begin{array}{ll} & a \subseteq R \\ \Rightarrow & \quad \{ \quad a \text{ is coreflexive, so } (a \circ a)^{>} = a \text{; monotonicity} \quad \} \\ & a \subseteq (a \circ R)^{>} \\ \Rightarrow & \quad \{ \quad a \circ \top\!\!\top \circ a = a \text{, monotonicity} \quad \} \\ & a \subseteq a \circ \top\!\!\top \circ (a \circ R)^{>} \\ = & \quad \{ \quad \text{domains (specifically, theorem 51(a))} \quad \} \\ & a \subseteq a \circ \top\!\!\top \circ a \circ R \\ \Rightarrow & \quad \{ \quad a \circ \top\!\!\top \circ a = a \subseteq I \text{, monotonicity and transitivity} \quad \} \\ & a \subseteq R \quad . \end{array}$$

The lemma follows by mutual implication.
□

Lemma 85. If R is right-definite, then, for all atomic coreflexives a,

$$a \subseteq \perp\!\!\!\perp \Leftarrow a \subseteq R^+ \quad .$$

Proof Assume that R is right-definite. Then,

$$\begin{array}{ll} & a \subseteq R^+ \\ = & \quad \{ \quad \text{lemma 84 with } R := R^+ \quad \} \\ & a \subseteq (a \circ R^+)^{>} \\ \Rightarrow & \quad \{ \quad \text{assumption: } R \text{ is right-definite, lemma 80} \quad \} \\ & a \subseteq \perp\!\!\!\perp \quad . \end{array}$$

□

We now define acyclicity:

Definition 86 (Acyclicity). A relation R is said to be *acyclic* if

$$I \cap R^+ \;=\; \perp\!\!\!\perp \quad .$$

A proper atomic coreflexive a is said to be *in a cycle* of R if $a \subseteq R^+$.
□

A proper atomic coreflexive a that is in a cycle of R "witnesses" the fact that R is not acyclic. Formally, by straightforward application of the assumption that the lattice of relations is atomic and definition 13, we have:

Lemma 87.

$$I \cap R^+ \neq \bot\!\!\!\bot \quad \equiv \quad \langle \exists a : \mathsf{AC}.a \wedge a \neq \bot\!\!\!\bot : a \subseteq R^+ \rangle \quad .$$

□

A straightforward calculation shows that

$$I \cap R^+ \quad = \quad I \cap (R^\cup)^+ \quad .$$

It follows that R is acyclic equivales $R^\cup$ is acyclic.

Definition 86 is meaningful for arbitrary relations but we instantiate it primarily for finite graphs. Recall that nodes are proper atomic coreflexives. So identifying a node in a cycle of graph G establishes that G is not acyclic. Formally, we have:

Lemma 88. Suppose a is an atomic coreflexive. Then $a \circ R^+ \circ a = \bot\!\!\!\bot$ if relation R is acyclic. Conversely, if $a \circ R^+ \circ a \neq \bot\!\!\!\bot$, R is not acyclic, as witnessed by a; that is, a is proper and in a cycle of R.

Proof By (55) and the all-or-nothing rule,

$$a \circ R^+ \circ a = a \quad \vee \quad a \circ R^+ \circ a = \bot\!\!\!\bot \tag{89}$$

for all atomic coreflexives a.

Assume R is acyclic. Then

$$\begin{array}{ll} & a \circ R^+ \circ a = a \\ = & \quad \{ \quad a \text{ is coreflexive, lemmas 71 (with } p,b := a,a \text{) and 84} \quad \} \\ & a \subseteq I \cap R^+ \\ \Rightarrow & \quad \{ \quad \text{assumption: } R \text{ is acyclic (definition 86)} \quad \} \\ & a = \bot\!\!\!\bot \\ \Rightarrow & \quad \{ \quad \bot\!\!\!\bot \text{ is zero of composition} \quad \} \\ & a \circ R^+ \circ a \; = \; \bot\!\!\!\bot \quad . \end{array}$$

We conclude that, if R is acyclic, $a \circ R^+ \circ a = \bot\!\!\!\bot$ for all atomic coreflexives a.

For the converse, suppose a is an atomic coreflexive and $a \circ R^+ \circ a \neq \bot\!\!\!\bot$. Then, by (89), $a \circ R^+ \circ a = a$. It follows that a is proper and, applying definition 86, a is in a cycle of R.

□

We now show that, for *finite* graphs, right (or left) definiteness equivales acyclicity. Lemma 90 shows that finiteness is not required to show that right (or left) definiteness implies acyclicity but the converse is not always true for relations on infinite sets. For example, the less-than ordering on real numbers is acyclic but it is not well-founded.

Lemma 90. A right-definite relation is acyclic. Symmetrically, a left-definite relation is acyclic.

Proof With a ranging over atomic coreflexives, we have

$$
\begin{array}{ll}
 & \mathsf{rightdefinite}.R \\
\Rightarrow & \quad \{ \quad \text{definition 76 (with } p := a \text{) and lemma 85} \quad \} \\
 & \langle \forall a \,::\, a \subseteq \bot\!\!\!\bot \Leftarrow a \subseteq R^+ \rangle \\
\Rightarrow & \quad \{ \quad \text{the lattice of coreflexives is saturated, i.e. } \langle \cup a :: a \rangle = I \quad \} \\
 & I \cap R^+ \;=\; \bot\!\!\!\bot \\
= & \quad \{ \quad \text{definition 86} \quad \} \\
 & \mathsf{acyclic}.R \quad .
\end{array}
$$

The symmetric property of left-definiteness follows straightforwardly. (See the remarks above about the relation between left-definiteness of $R^\cup$ and right-definiteness of R.) □

We turn now to the proof that definiteness follows from acyclicity. Like lemma 90, lemma 91 and corollary 92 below do not require finiteness of the relation R; however, their application in lemma 93, will force the restriction to finite graphs.

Earlier we argued informally that right-definiteness means the absence of infinite "descending" paths. Formally, we have:

Lemma 91. Suppose p is a coreflexive such that $p \neq \bot\!\!\!\bot$ and $p \subseteq (p \circ R^+)^>$. Suppose a is a proper atomic coreflexive such that $a \subseteq p$. Then, with dummy b ranging over atomic coreflexives, we have

$$\left\langle \exists b \,::\, b \neq \bot\!\!\!\bot \;\wedge\; b \subseteq p \;\wedge\; a \subseteq (b \circ R^+)^> \;\wedge\; (a \circ R^+)^> \subseteq (b \circ R^+)^> \right\rangle \quad .$$

Proof The proof of (91) is in two stages. First,

$$
\begin{array}{ll}
 & a \subseteq p \\
\Rightarrow & \quad \{ \quad \text{assumption: } p \subseteq (p \circ R^+)^>, \text{ transitivity} \quad \} \\
 & a \subseteq (p \circ R^+)^> \\
= & \quad \{ \quad \text{saturation assumption: definition 14, distributivity} \quad \} \\
 & a \;\subseteq\; \langle \cup b : b \subseteq p : (b \circ R^+)^> \rangle \\
\Rightarrow & \quad \{ \quad a \text{ is a proper atom, irreducibility: lemma 21} \quad \} \\
 & \langle \exists b : b \neq \bot\!\!\!\bot \wedge b \subseteq p : a \subseteq (b \circ R^+)^> \rangle \quad .
\end{array}
$$

Second, assuming $a \subseteq (b \circ R^+)^>$,

$$
\begin{array}{ll}
 & (a \circ R^+)^> \\
\subseteq & \quad \{ \quad \text{assumption, monotonicity} \quad \} \\
 & ((b \circ R^+)^> \circ R^+)^> \\
= & \quad \{ \quad \text{domains (specifically theorem 51(f))} \quad \} \\
 & (b \circ R^+ \circ R^+)^> \\
\subseteq & \quad \{ \quad R^+ \text{ is transitive, monotonicity} \quad \} \\
 & (b \circ R^+)^> \quad .
\end{array}
$$

□

Corollary 92. Suppose p is a coreflexive such that $p \neq \perp\!\!\!\perp$ and $p \subseteq (p \circ R^+)^>$. Then it is possible to construct an infinite sequence of proper atomic coreflexives a_i such that

$$\langle \forall i : 0 \leq i : a_i \subseteq p \rangle \ \wedge \ \langle \forall i,j : 0 \leq i < j : a_i \ \subseteq \ (a_j \circ R^+)^> \rangle \ .$$

Proof The initial term a_0 is an arbitrary element of p. That is, $a_0 \subseteq p$. (Formally, we exploit the assumption that the lattice of coreflexives is atomic: see definition 13.) Subsequent nodes are constructed by exploiting lemma 91 (with $a,b := a_i,a_{i+1}$). Because, for all i,

$$(a_i \circ R^+)^> \ \subseteq \ (a_{i+1} \circ R^+)^>$$

it follows, by transitivity, that

$$\langle \forall i,j : i < j : (a_i \circ R^+)^> \ \subseteq \ (a_j \circ R^+)^> \rangle \ .$$

Combining this with the fact that, for all i, $a_i \subseteq (a_{i+1} \circ R^+)^>$, we have:

$$\langle \forall i,j : 0 \leq i < j : a_i \ \subseteq \ (a_j \circ R^+)^> \rangle \ .$$

□

This is the point at which we are obliged to introduce the finiteness assumption.

Lemma 93. Suppose G is a finite, acyclic graph. Then G is definite.

Proof We first prove that if G is a finite graph that is not right-definite, then G is not acyclic. The contrapositive is that, if G is a finite, acyclic graph, G is right-definite.

Suppose G is not right-definite. Then there is a coreflexive p such that $p \neq \perp\!\!\!\perp$ and $p \subseteq (p \circ G^+)^>$. Applying corollary 92, construct an infinite sequence of nodes a_i such that

$$\langle \forall i,j : 0 \leq i < j : a_i \ \subseteq \ (a_j \circ G^+)^> \rangle \ .$$

There is only a finite number of nodes; so, for some m and n, $m < n$ and $a_m = a_n$. Thus

$$a_m \ \subseteq \ (a_m \circ G^+)^> \ .$$

Hence,

$$\begin{array}{ll} & \mathsf{true} \\ = & \quad \{ \quad \text{lemma 84 (with } a,R := a_m,G \text{)} \quad \} \\ & a_m \subseteq G^+ \\ \Rightarrow & \quad \{ \quad a_m = I \cap a_m \text{, monotonicity} \quad \} \\ & a_m \ \subseteq \ I \cap G^+ \\ \Rightarrow & \quad \{ \quad \perp\!\!\!\perp \neq a_m \text{, } \perp\!\!\!\perp \text{ is the least element} \quad \} \\ & \perp\!\!\!\perp \neq I \cap G^+ \ . \end{array}$$

That is, G is not acyclic.

Since acyclicity of G is equivalent to acyclicity of $G^{\cup}$, it follows straightforwardly that, if G is a finite, acyclic graph, it is also left-definite. Thus, if G is a finite, acyclic graph, it is definite.
□

To summarise, we have the following theorem.

Theorem 94. If G is a finite graph, G is acyclic equivales G is definite.

Proof Straightforward combination of corollary 90 and lemma 93.
□

9.2. Starth Root and Reflexive-Transitive Reduction

In this section, we show that the reflexive-transitive reduction of an acyclic graph is the least starth root of the graph.

Recall the definition of reflexive-transitive reduction: definition 39. The definition of the function red is quite complicated, much of the complication being due to the need to eliminate self-loops. An acyclic relation has no self-loops so the definition can be simplified:

Lemma 95. If R is acyclic, then $R = R \cap \neg I$. So

$$\mathsf{red}.R \;=\; R \cap \neg(R \circ R^+) \quad .$$

Proof

$$\begin{array}{ll} & R = R \cap \neg I \\ = & \quad \{ \quad R \supseteq R \cap \neg I \text{, anti-symmetry, } R \subseteq R \quad \} \\ & R \subseteq \neg I \\ = & \quad \{ \quad \text{shunting rule (12)} \quad \} \\ & R \cap I \subseteq \bot\!\!\!\bot \\ \Leftarrow & \quad \{ \quad R \subseteq R^+ \text{, monotonicity and transitivity} \quad \} \\ & R^+ \cap I \subseteq \bot\!\!\!\bot \\ = & \quad \{ \quad R \text{ is acyclic} \quad \} \\ & \mathsf{true} \quad . \end{array}$$

The formula for $\mathsf{red}.R$ follows by instantiating (40) and replacing R by $R \cap \neg I$.
□

Theorem 96. The least starth root of a definite relation is its reflexive-transitive reduction. That is, for all definite relations R,

$$(\mathsf{red}.R)^* = R^* \quad \wedge \quad \langle \forall X : X^* = R^* : \mathsf{red}.R \subseteq X \rangle \quad .$$

In particular, the least starth root of a finite, acyclic graph is its reflexive-transitive reduction.

Proof Assume that R is definite. By theorem 43, it suffices to prove the lefthand conjunct.

$$
\begin{array}{ll}
 & (\mathsf{red}.R)^* \;=\; R^* \\
= & \quad \{ \quad \mathsf{red}.R \subseteq R \text{ and } R \text{ is definite, so } \mathsf{red}.R \text{ is right-definite (theorem 94)} \\
 & \qquad \text{UEP of relation algebra: theorem 79} \quad \} \\
 & R^* \;=\; I \cup \mathsf{red}.R \circ R^* \\
\Leftarrow & \quad \{ \quad R^* = I \cup R^+ \text{, Leibniz} \quad \} \\
 & R^+ \;=\; \mathsf{red}.R \circ R^* \\
= & \quad \{ \quad R \text{ is left-definite,} \\
 & \qquad \text{UEP of relation algebra: theorem 79} \quad \} \\
 & R^+ \;=\; \mathsf{red}.R \cup R^+ \circ R \\
= & \quad \{ \quad \text{by lemma 90, } R \text{ is acyclic; lemma 95} \quad \} \\
 & R^+ \;=\; (R \cap \neg(R \circ R^+)) \;\cup\; R^+ \circ R \\
= & \quad \{ \quad R \circ R^+ = R^+ \circ R \text{ and absorption rule of set calculus} \quad \} \\
 & R^+ \;=\; R \cup R^+ \circ R \\
= & \quad \{ \quad \text{fixed-point definition of transitive closure} \quad \} \\
 & \mathsf{true} \quad .
\end{array}
$$

The particular case of a finite, acyclic graph follows from theorem 94.
□

Observe that the proof of theorem 96 uses both left- and right-definiteness. The lexicographic ordering on words over an alphabet of size at least two demonstrates that just one of left- or right-definiteness is not sufficient: it is right-definite (i.e. well-founded) but it is not left-definite (i.e its converse is not well-founded) and it does not have a least starth root.

A relation may have a least starth root that is not its reflexive-transitive reduction, as exemplified by the relation on $\{0,1\}$ consisting of the two pairs $(0,1)$ and $(1,0)$. It is not definite (since it is finite but not acyclic) and its reflexive-transitive reduction is the empty relation; however, the relation is equal to its least starth root.

9.3. Minimal Nodes and Reachability

This section is about formulating and proving the property that, given a right-definite relation, the set of nodes "reachable" from a given set of nodes equals the set of nodes "reachable" from a minimal subset of the given set of nodes.

Suppose G is a graph. To define reachability we observe that node x is reachable from a set of nodes A if there exists $y \in A$ such that there is a path from y to x. That there is a path from y to x can of course be expressed as $y[\![G^*]\!]x$, so reachability of x from A becomes $\langle \exists y : y \in A : y[\![G^*]\!]x \rangle$ or by definition of composition: $\langle \exists y :: y[\![A \circ G^*]\!]x \rangle$. In the last expression we recognise the pointwise definition of the domain operator: if set A is represented by the coreflexive p, the expression is equivalent to $x \in (p \circ G^*)^>$. Generalising from graph G to an arbitrary relation R, the definition of $\mathsf{reachable}.R.p$ is therefore:

$$
\mathsf{reachable}.R.p \;=\; (p \circ R^*)^> \quad . \tag{97}
$$

That a node x is a minimal element of a set of nodes A means that x is an element of A and that, furthermore, there is no edge from a node in A to x. This is more formally expressed as $x{\in}A \wedge \neg\langle \exists y : y{\in}A : y[\![R]\!]x\rangle$. Alternatively, by again introducing the domain operator and representing set A by the coreflexive p, as $x \in p \cap (p{\circ}R)^{>}\bullet$. Replacing the intersection by a composition of coreflexives, the set $\mathsf{minimal}.R.p$ of minimal elements of p is thus defined as:

$$\mathsf{minimal}.R.p \;=\; p \circ (p{\circ}R)^{>}\bullet \tag{98}$$

The formal statement of the fact that the nodes reachable from set A coincide with the nodes reachable from the minimal elements of A now becomes:

Lemma 99. Suppose relation R is right-definite. Then, for all coreflexives p,

$$\mathsf{reachable}.R.p \;=\; \mathsf{reachable}.R.(\mathsf{minimal}.R.p) \quad . \tag{100}$$

More generally, for all coreflexives p and q,

$$\mathsf{reachable}.R.p \subseteq \mathsf{reachable}.R.q \;\Leftarrow\; \mathsf{minimal}.R.p \subseteq q \quad . \tag{101}$$

Proof Assume that R is right-definite. We prove (100) by mutual inclusion. One inclusion is easy. From the definition (97) it is clear that $\mathsf{reachable}.R$ is a monotone function. Furthermore from (98) we see that p contains $\mathsf{minimal}.R.p$. Therefore

$$\mathsf{reachable}.R.p \supseteq \mathsf{reachable}.R.(\mathsf{minimal}.R.p) \quad .$$

It remains to prove the other inclusion. Somewhere we have to use the assumption of right-definiteness, but how? We have to prove that

$$\mathsf{reachable}.R.p \subseteq \mathsf{reachable}.R.(\mathsf{minimal}.R.p) \quad ,$$

whereof the *righthand* occurrence of $\mathsf{reachable}$ involves a reflexive-transitive closure. This suggests that we use the UEP of relation algebra. Furthermore, it turns out that the expression $\mathsf{minimal}.R.p$ does not play a role. Therefore, we begin by deriving a condition implying

$$\mathsf{reachable}.R.p \subseteq \mathsf{reachable}.R.q$$

for arbitrary coreflexive q. (This turns out to be the property (101).) We begin by exploiting (the dual of) lemma 64:

$$\begin{array}{ll} & \mathsf{reachable}.R.p \subseteq \mathsf{reachable}.R.q \\ = & \quad \{ \quad \text{definition } \mathsf{reachable}: (97) \quad \} \\ & (p{\circ}R^*)^{>} \subseteq (q{\circ}R^*)^{>} \\ = & \quad \{ \quad \text{the function } \langle p :: (p{\circ}R^*)^{>}\rangle \text{ is a closure operator} \\ & \qquad \text{(dual of lemma 64) and definition 22} \quad \} \\ & p \subseteq (q{\circ}R^*)^{>} \quad . \end{array}$$

Now we can invoke the right-definiteness of R. From the discussion of theorem 79 on the UEP of relation algebra it follows that, for right-definite relation R, relation $(q{\circ}R^*)^{>}$ is the greatest fixed point of the function $\langle X :: q \cup (X{\circ}R)^{>}\rangle$. Exploitation of this fact is the main step in the following calculation.

$$
\begin{array}{ll}
 & p \subseteq (q \circ R^*)^{>} \\
= & \quad \{ \quad R \text{ is right-definite: } (q \circ R^*)^{>} = \langle \nu X :: q \cup (X \circ R)^{>} \rangle \, ; \\
 & \qquad \text{fixed-point induction} \quad \} \\
 & p \subseteq (q \cup p \circ R)^{>} \\
= & \quad \{ \quad \text{domain operator is } \cup\text{-junctive} \quad \} \\
 & p \subseteq q \cup (p \circ R)^{>} \\
= & \quad \{ \quad \text{shunting (12) in the coreflexive lattice} \quad \} \\
 & p \circ (p \circ R)^{>\bullet} \subseteq q \\
= & \quad \{ \quad \text{definition (98)} \quad \} \\
 & \mathsf{minimal}.R.p \subseteq q \quad .
\end{array}
$$

With this calculation we have established the property (101). Instantiating q with $\mathsf{minimal}.R.p$ in this formula then gives the desired result:

$$\mathsf{reachable}.R.p \subseteq \mathsf{reachable}.R.(\mathsf{minimal}.R.p) \quad .$$

This completes the proof of the theorem.
□

An interesting observation can be made if we take a closer look at the antecedent of formula (101). After instantiating q to the empty relation and writing out the definition of $\mathsf{minimal}.R$ it reads: $p \circ (p \circ R)^{>\bullet} \subseteq \bot\!\!\!\bot$. Now we can apply shunting in the coreflexive lattice and we get $p \subseteq (p \circ R)^{>}$. This expression is the antecedent in (77). So, another formulation of a relation R being right-definite is: for all coreflexives p ,

$$p \subseteq \bot\!\!\!\bot \quad \Leftarrow \quad \mathsf{minimal}.R.p \subseteq \bot\!\!\!\bot \quad , \tag{102}$$

or the equivalent contrapositive (using that $\bot\!\!\!\bot$ is the bottom of the lattice): for all coreflexives p ,

$$p \neq \bot\!\!\!\bot \quad \Rightarrow \quad \mathsf{minimal}.R.p \neq \bot\!\!\!\bot \quad . \tag{103}$$

This is the familiar characterisation "every non-empty set has a minimal element" of well-foundedness.

Now we consider the converse of lemma 99. Is it true that a graph with property (100) is right-definite? This question can be answered affirmatively and the proof is simple. We show that a relation satisfying (100) also satisfies (102).

$$
\begin{array}{ll}
 & \mathsf{minimal}.R.p = \bot\!\!\!\bot \\
\Rightarrow & \quad \{ \quad \text{Leibniz} \quad \} \\
 & \mathsf{reachable}.R.(\mathsf{minimal}.R.p) = \mathsf{reachable}.R.\bot\!\!\!\bot \\
= & \quad \{ \quad \text{assumption: } \mathsf{reachable}.R.(\mathsf{minimal}.R.p) = \mathsf{reachable}.R.p \, ; \\
 & \qquad \text{definition of } \mathsf{reachable}: \text{ (97)} \quad \} \\
 & \mathsf{reachable}.R.p = (\bot\!\!\!\bot \circ R^*)^{>} \\
= & \quad \{ \quad \text{definition of } \mathsf{reachable}: \text{ (97);} \\
 & \qquad \bot\!\!\!\bot \text{ is zero of composition} \quad \}
\end{array}
$$

$$
\begin{array}{ll}
& (p \circ R^*)^{>} = \perp\!\!\!\perp \\
\Rightarrow & \quad \{ \quad I \subseteq R^* \quad \} \\
& p \subseteq \perp\!\!\!\perp \ .
\end{array}
$$

We thus conclude:

Theorem 104. Relation R is right-definite equivales for all coreflexives p,

$$\mathsf{reachable}.R.p \ = \ \mathsf{reachable}.R.(\mathsf{minimal}.R.p) \ .$$

In particular, that (finite) graph G is acyclic equivales for all coreflexives p

$$\mathsf{reachable}.G.p \ = \ \mathsf{reachable}.G.(\mathsf{minimal}.G.p) \ .$$

□

9.4. Topological Search

"Topological" search is an algorithm for visiting all the nodes in an acyclic graph in so-called "topological" order.

Definition 105 (Topological Order). A *topological ordering* of a homogeneous relation R of type A is a total, injective function ord from A to the natural numbers with the property that, for all elements a and b of A, $ord.a < ord.b$ if $a[\![R^+]\!]b$.
□

Expressed as a point-free formula, the requirement for the function ord to be a topological ordering of R is as follows:

$$ord \circ ord^{\cup} \subseteq I_{\mathbb{N}} \ \wedge \ I_A = ord^{\cup} \circ ord \ \wedge \ R^+ \subseteq ord^{\cup} \circ \mathsf{less} \circ ord \ . \tag{106}$$

Here we have used "less" to denote the less-than ordering on natural numbers rather than the symbol "$<$". A straightforward lemma is the following.

Lemma 107. Suppose ord is a total, injective function of type $\mathbb{N} \leftarrow A$ and R is a homogeneous relation of type A. Then ord is a topological ordering of R equivales

$$R \subseteq ord^{\cup} \circ \mathsf{less} \circ ord \ .$$

Proof The proof is a straightforward application of the definition of transitive closure:

$$
\begin{array}{ll}
& R^+ \subseteq ord^{\cup} \circ \mathsf{less} \circ ord \\
\Leftarrow & \quad \{ \quad R^+ = \langle \mu x :: R \cup x \circ x \rangle \text{ ; fixed-point induction} \quad \} \\
& R \cup ord^{\cup} \circ \mathsf{less} \circ ord \circ ord^{\cup} \circ \mathsf{less} \circ ord \ \subseteq \ ord^{\cup} \circ \mathsf{less} \circ ord \\
= & \quad \{ \quad \mathsf{less} \circ ord \circ ord^{\cup} \circ \mathsf{less} \\
& \quad \subseteq \quad \{ \quad ord \circ ord^{\cup} \subseteq I \text{, monotonocity} \quad \} \\
& \quad \mathsf{less} \circ \mathsf{less} \\
& \quad \subseteq \quad \{ \quad \mathsf{less} \text{ is transitive} \quad \} \\
& \quad \mathsf{less} \quad ;
\end{array}
$$

definition of set union and monotonicity of composition }

$$R \subseteq ord^{\cup} \circ \mathsf{less} \circ ord$$

$$\Leftarrow \quad \{ \quad R \subseteq R^+ \quad \}$$

$$R^+ \subseteq ord^{\cup} \circ \mathsf{less} \circ ord \quad .$$

□

Lemma 107 means that the requirement (106) for the function ord to be a topological ordering of R can be simplified to

$$I_A = ord^{\cup} \circ ord \quad \wedge \quad ord \circ ord^{\cup} \subseteq I_{\mathbb{N}} \quad \wedge \quad R \subseteq ord^{\cup} \circ \mathsf{less} \circ ord \quad . \tag{108}$$

The less-than relation on natural numbers is, of course, well-founded — that is, right-definite in the terminology used here. The function ord in the definition of a topological ordering thus acts like a so-called *bound* function for establishing termination of a loop in a program. The relevant property is the following.

Lemma 109. Suppose ord is a total function of type $\mathbb{N} \leftarrow A$ for some A. Then the homogeneous relation $ord^{\cup} \circ \mathsf{less} \circ ord$ (where less denotes the less-than relation on natural numbers) is right-definite.

Proof Omitted for brevity. See [1] for full details.

□

Lemma 109 is the basis of the use of so-called "bound functions" to establish termination of loops and recursion: the function ord "bounds" the number of iterations. The only property of the relation less that is used in the proof of lemma 109 is that it is well-founded (right-definite). So "bound functions" can be used in conjunction with other well-founded relations although in some cases it would be difficult to interpret the function ord as a "bound". For example, the relation less could be taken to be the lexicographic ordering on words; the function ord would then map a state to a word.

Corollary 110. Suppose ord is a topological ordering of the homogeneous relation R. Then R is right-definite.

Proof Immediate from lemmas 83, 107 and 109.

□

We now want to consider the converse of corollary 110. Is it the case that every right-definite relation can be topologically ordered? The answer is: no, not in general. (For example, the lexicographical ordering of words over a finite alphabet is well-founded but it is not possible to assign a number to each word that defines its position in the ordering.) The answer is, however, yes if we restrict attention to finite graphs. The proof is constructive. We assume that G is a finite graph that is acyclic and we present an algorithm that constructs a topological ordering of the nodes of G.

The development of the algorithm proceeds as follows. Given a finite graph G, the requirement is to construct a topological ordering ord of all the nodes of G: specifically, the postcondition that must be satisfied is given by (108).

The obvious strategy is to order the nodes one-by-one, beginning with the empty set of nodes and ending with all the nodes of G. In order to guarantee injectivity, an obvious choice is to assign to each node the number of nodes that have already been ordered.

(Thus, the first node to be ordered is assigned the number 0, the second 1, and so on.) Introducing the coreflexive variable $seen$ to represent the nodes that have been ordered (the nodes that have been "seen" in the search of the graph) and the integer variable k to count the number of nodes in the set represented by $seen$, we design a loop that has invariants

$$seen = ord^{\cup} \circ ord \quad \wedge \quad ord \circ ord^{\cup} = \overline{\{j \mid 0 \leq j < k\}} \ , \quad \text{and} \tag{111}$$

$$seen \circ G \circ seen \subseteq ord^{\cup} \circ \mathsf{less} \circ ord \ . \tag{112}$$

The overbar notation used in (111) denotes the mapping from a set to its representation as a coreflexive. The invariant (111) states that ord is functional with right domain $seen$ and it is injective with left domain the set of natural numbers less than k. The invariant (112) states that if there is an edge in G from a node a that has been "seen" to a node b that has also been "seen" then $ord.a < ord.b$.

The invariants (111) and (112) are clearly derived from (108) by the well-known, correct-by-construction design method of replacing a constant by a variable: in this case, several occurrences of the (sometimes invisible) identity relation are replaced.

The development thus far is summarised below. The property (113) listed as an invariant has yet to be derived, as is the additional conjunct (114) in the criterion for choosing b.

$$\begin{array}{ll}
 & \{ \quad \mathsf{acyclic}.G \quad \} \\
 & seen, ord, k \ := \ \bot\!\!\!\bot, \bot\!\!\!\bot, 0 \\
; & \{ \quad \text{Invariant: } (111) \wedge (112) \wedge (113) \quad \} \\
 & \textbf{while } I_A \neq seen \textbf{ do} \\
 & \quad \textbf{begin} \\
 & \quad \quad \text{choose arbitrary node } b \text{ such that } b \subseteq \sim seen \ \wedge \ (114) \\
 & \quad ; \ seen \ := \ seen \cup b \\
 & \quad ; \ ord,k \ := \ ord \cup \overline{\{k\}} \circ \top\!\!\!\top \circ b \ , \ k{+}1 \\
 & \quad \textbf{end} \\
 & \{ \quad I_A = seen = ord^{\cup} \circ ord \ \wedge \ ord \circ ord^{\cup} \subseteq I_{\mathbf{N}} \ \wedge \ G \subseteq ord^{\cup} \circ \mathsf{less} \circ ord \quad \}
\end{array}$$

The key element of the algorithm is how to choose the next node to be ordered. It is straightforward to verify that (111) is an invariant of the algorithm as shown. The choice of node b must guarantee that (112) is maintained. That is, we require that, for all b and $seen$,

$$\begin{array}{ll}
 & (seen \cup b) \circ G \circ (seen \cup b) \ \subseteq \ (ord \cup \overline{\{k\}} \circ \top\!\!\!\top \circ b)^{\cup} \circ \mathsf{less} \circ (ord \cup \overline{\{k\}} \circ \top\!\!\!\top \circ b) \\
\Leftarrow & seen \circ G \circ seen \ \subseteq \ ord^{\cup} \circ \mathsf{less} \circ ord \ \wedge \ (111) \ \wedge \ b \subseteq \sim seen \ \wedge \ (113)
\end{array}$$

where (113) has yet to be derived.

Using distributivity properties, the left side of the topmost subset ordering expands to

$$seen \circ G \circ (seen \cup b) \ \cup \ b \circ G \circ (seen \cup b)$$

and, omitting two terms, the right side of this ordering expands to

$$ord^{\cup} \circ \mathsf{less} \circ ord \;\; \cup \;\; ord^{\cup} \circ \mathsf{less} \circ \overline{\{k\}} \circ \top\!\!\top \circ b \;\; .$$

(The two omitted terms are, in fact, equal to $\bot\!\!\bot$ but this fact is not needed.) Taking account of domains (specifically, $seen = ord^{\cup} \circ ord$ and $b \subseteq \sim seen$), the invariant (112) is thus maintained if

$$\begin{array}{ll} & seen \circ G \circ seen \;\subseteq\; ord^{\cup} \circ \mathsf{less} \circ ord \\ \wedge & seen \circ G \circ b \;\subseteq\; ord^{\cup} \circ \mathsf{less} \circ \overline{\{k\}} \circ \top\!\!\top \circ b \\ \wedge & b \circ G \circ b \;=\; \bot\!\!\bot \\ \wedge & b \circ G \circ seen \;=\; \bot\!\!\bot \;\; . \end{array}$$

The first conjunct is identical to the first conjunct on the right side of the implication; so it can be eliminated. The second conjunct follows from (111) and properties of the less-than ordering. The third conjunct is true because G is assumed to be acyclic and hence has no self-loops. Finally, the fourth conjunct enables us to identify the as-yet-undefined invariant (113): specifically,

$$\sim seen \circ G \circ seen \;=\; \bot\!\!\bot \;\; . \tag{113}$$

Of course, the introduction of a new invariant implies a new design obligation: property (113) is clearly established by the initialisation $seen := \bot\!\!\bot$ but we must guarantee that it is maintained by the loop body. Doing so gives us the additional condition for choosing node b (labelled (114) in the algorithm): maintaining the invariant demands that, for all b, G and $seen$,

$$\sim(seen \cup b) \circ G \circ (seen \cup b) \;=\; \bot\!\!\bot \;\; \Leftarrow \;\; \sim seen \circ G \circ seen = \bot\!\!\bot \wedge \text{ choice of } b \;\; .$$

An easy calculation gives the condition for choosing b as:

$$\sim(seen \cup b) \circ G \circ b \;=\; \bot\!\!\bot \;\; .$$

This condition can be strengthened to:

$$\sim seen \circ G \circ b \;=\; \bot\!\!\bot \;\; . \tag{114}$$

In words, there are no edges in the graph G from an unseen node to node b. This completes the derivation of the algorithm.

There is one more —vital— proof obligation: we have to verify that the condition for choosing b can be satisfied. This is where the assumption that G is acyclic, and hence right-definite, is crucial. Full details of this and all the informal claims made above can be found in [1].

The conclusion of this section is the following theorem.

Theorem 115. Suppose G is a finite graph. Then that there is a topological ordering of G equivales G is acyclic.

Proof The proof is by mutual implication. The algorithm just discussed establishes constructively that there is a topological ordering of G if G is acyclic. For the converse, suppose that ord is a topological ordering of G. Then

$$
\begin{array}{ll}
 & I_A \cap G^+ \\
\subseteq & \quad \{ \quad \text{definition of topological ordering: (106), and monotonicity} \quad \} \\
 & ord^\cup \circ ord \cap ord^\cup \circ \mathsf{less} \circ ord \\
= & \quad \{ \quad \text{by definition (106), } ord \text{ is a total function; distributivity} \quad \} \\
 & ord^\cup \circ (I_{\mathbf{N}} \cap \mathsf{less}) \circ ord \\
= & \quad \{ \quad I_{\mathbf{N}} \cap \mathsf{less} = \perp\!\!\!\perp \,;\ \perp\!\!\!\perp \text{ is zero of composition} \quad \} \\
 & \perp\!\!\!\perp \ .
\end{array}
$$

That is, G is acyclic.
□

10. Components

The strongly connected components of graph G are the equivalence classes of the relation $G^* \cap (G^\cup)^*$. The algebraic properties that we present in this section are most often valid for arbitrary (homogeneous binary) relations and not just for finite graphs. However, we sometimes provide informal interpretations in terms of (paths in) graphs.

We begin by giving a definition of a "component" of a relation (definition 116) and then explore its properties, first for relations in general, then for transitive relations (section 10.1), and finally for transitive and symmetric relations (section 10.2).

"Strongly connected components" are defined in section 10.3. Properties of strongly connected components are derived in sections 10.4, 10.5, 10.6 and 10.7. Section 10.4 is about connectivity properties of nodes within and without the same strongly connected component. Section 10.5 records the well-known property that every node is an element of exactly one strongly connected component. Finally, section 10.7 formalises the structural decomposition of a graph into a collection of strongly connected components and an acyclic graph that is "pathwise homomorphic" to the given graph. The non-trivial proof of this property is enabled by a lemma on starth roots of a given graph formulated and presented in section 10.6.

Definition 116. Suppose p is a coreflexive and R is a relation. We say that p is *connected by* R iff $p \circ \top\!\!\top \circ p \subseteq R$. We say that p is a *component* of R iff p is connected by R and $\langle \forall q : q \circ \top\!\!\top \circ q \subseteq R : p \subseteq q \equiv p = q \rangle$.
□

Note that $\perp\!\!\!\perp$ is, by definition, connected by R. It is also a component of R in the case that the carrier of the lattice of coreflexives is the empty set.

An obvious corollary of definition 116 is the following:

Lemma 117.

(a) Suppose q is a coreflexive and S is a relation. Then, q is connected by S if ($q \subseteq p$ and p is connected by R and $R \subseteq S$).

(b) p is connected by $R \cap S$ equivales p is connected by both R and S.

(c) The following are all equivalent:

(i) p is connected by R

(ii) p is connected by $R^\cup$

(iii) p is connected by $R \cap R^\cup$

(d) The following are all equivalent:

(i) p is a component of R

(ii) p is a component of $R^\cup$

(iii) p is a component of $R \cap R^\cup$

Proof (a) is obvious from the monotonicity of composition.
(b) is immediate from the definition of infima, in particular:

$$p \circ \top\!\!\top \circ p \subseteq R \cap S \quad \equiv \quad p \circ \top\!\!\top \circ p \subseteq R \ \wedge \ p \circ \top\!\!\top \circ p \subseteq S \quad .$$

(c) is obvious from the fact that p and $p \circ \top\!\!\top \circ p$ are symmetric. More specifically:

$$\begin{array}{ll} & p \circ \top\!\!\top \circ p \subseteq R \\ = & \quad \{ \quad \text{converse} \quad \} \\ & (p \circ \top\!\!\top \circ p)^\cup \subseteq R^\cup \\ = & \quad \{ \quad [\ (R \circ S)^\cup \ = \ S^\cup \circ R^\cup \ ],\ p^\cup = p ,\ \top\!\!\top^\cup = \top\!\!\top \quad \} \\ & p \circ \top\!\!\top \circ p \subseteq R^\cup \quad . \end{array}$$

This establishes the equivalence of (i) and (ii). That (i) implies (iii) is then established by (b) (with S instantiated to $R^\cup$) and the converse (iii) implies (i) is established by (a).
(d) Trivial consequence of (c) and the definition of component.
□

Informally, p is connected by R means that, when restricted to p, R equals the universal relation. Formally:

Lemma 118. For all coreflexives p and relations R,

$$p \circ \top\!\!\top \circ p \subseteq R \quad \equiv \quad p \circ \top\!\!\top \circ p = p \circ R \circ p \quad .$$

Proof This is proved by mutual implication as follows.

$$\begin{array}{ll} & p \circ \top\!\!\top \circ p \subseteq R \\ \Rightarrow & \quad \{ \quad p \circ p = p \text{, monotonicity of composition} \quad \} \\ & p \circ \top\!\!\top \circ p \subseteq p \circ R \circ p \\ = & \quad \{ \quad R \subseteq \top\!\!\top \text{, monotonicity of composition, anti-symmetry} \quad \} \\ & p \circ \top\!\!\top \circ p = p \circ R \circ p \\ \Rightarrow & \quad \{ \quad p \subseteq I \text{, monotonicity of composition, transitivity of } \subseteq \quad \} \\ & p \circ \top\!\!\top \circ p \subseteq R \quad . \end{array}$$

□

10.1. Transitive Relations

Lemma 119. Distinct components of a transitive relation are disjoint. Formally, suppose T is a transitive relation and p and q are both components of T. Then

$$p \cap q = \bot\!\!\!\bot \ \vee \ p = q \ .$$

Proof For coreflexives p and q, $p \circ q = p \cap q = q \circ p$. This suggests applying the definition of a component in a way that introduces their product:

$$\begin{array}{ll}
& p \cap q = \bot\!\!\!\bot \ \vee \ p = q \\
= & \quad \{ \quad \text{idempotency of } \cup \quad \} \\
& p \cap q = \bot\!\!\!\bot \ \vee \ p = p \cup q = q \\
\Leftarrow & \quad \{ \quad p \subseteq p \cup q \text{, } p \text{ is a component of } T \text{,} \\
& \qquad\ \ q \subseteq p \cup q \text{, } q \text{ is a component of } T \quad \} \\
& p \cap q = \bot\!\!\!\bot \ \vee \ (p \cup q) \circ \top\!\!\!\top \circ (p \cup q) \subseteq T \\
= & \quad \{ \quad \text{distributivity; } p \text{ and } q \text{ are both connected by } T \quad \} \\
& p \cap q = \bot\!\!\!\bot \ \vee \ (p \circ \top\!\!\!\top \circ q \subseteq T \ \wedge \ q \circ \top\!\!\!\top \circ p \subseteq T) \\
= & \quad \{ \quad \text{distributivity, } p \circ q = p \cap q = q \circ p \quad \} \\
& (p \circ q = \bot\!\!\!\bot \vee p \circ \top\!\!\!\top \circ q \subseteq T) \ \wedge \ (q \circ p = \bot\!\!\!\bot \vee q \circ \top\!\!\!\top \circ p \subseteq T) \\
\Leftarrow & \quad \{ \quad \text{cone rule: (47) with } R := p \circ q \text{ and } R := q \circ p \text{:} \\
& \qquad\ \ \text{i.e. } p \circ q = \bot\!\!\!\bot \ \vee \ \top\!\!\!\top \circ p \circ q \circ \top\!\!\!\top = \top\!\!\!\top \text{,} \\
& \qquad\ \ \text{and } q \circ p = \bot\!\!\!\bot \ \vee \ \top\!\!\!\top \circ q \circ p \circ \top\!\!\!\top = \top\!\!\!\top \quad \} \\
& p \circ \top\!\!\!\top \circ p \circ q \circ \top\!\!\!\top \circ q \subseteq T \ \wedge \ q \circ \top\!\!\!\top \circ q \circ p \circ \top\!\!\!\top \circ p \subseteq T \\
\Leftarrow & \quad \{ \quad T \text{ is transitive, transitivity of } \subseteq \quad \} \\
& p \circ \top\!\!\!\top \circ p \circ q \circ \top\!\!\!\top \circ q \subseteq T \circ T \ \wedge \ q \circ \top\!\!\!\top \circ q \circ p \circ \top\!\!\!\top \circ p \subseteq T \circ T \\
\Leftarrow & \quad \{ \quad p \text{ and } q \text{ are connected by } T \text{, composition is monotonic} \quad \} \\
& \mathsf{true} \ .
\end{array}$$

□

Lemma 120. Suppose T is a transitive relation and p and q are both components of T. Then

$$p \circ T \circ q \neq \bot\!\!\!\bot \ \wedge \ q \circ T \circ p \neq \bot\!\!\!\bot \ \Rightarrow \ p = q \ .$$

Proof

$$\begin{array}{ll}
& p \circ T \circ q \neq \bot\!\!\!\bot \\
\Rightarrow & \quad \{ \quad \text{cone rule: (47)} \quad \} \\
& \top\!\!\!\top \circ p \circ T \circ q \circ \top\!\!\!\top = \top\!\!\!\top \\
\Rightarrow & \quad \{ \quad \text{Leibniz} \quad \} \\
& p \circ \top\!\!\!\top \circ p \circ T \circ q \circ \top\!\!\!\top \circ q = p \circ \top\!\!\!\top \circ q \\
= & \quad \{ \quad p \text{ and } q \text{ are both connected by } T \text{,}
\end{array}$$

so, by lemma 118, $p \circ \top\!\!\top \circ p = p \circ T \circ p$ and $q \circ \top\!\!\top \circ q = q \circ T \circ q$ }

$p \circ T \circ p \circ T \circ q \circ T \circ q = p \circ \top\!\!\top \circ q$

$\Rightarrow$ { p and q are coreflexives, so $I \supseteq p$ and $I \supseteq q$
monotonicity and I is unit of composition }

$p \circ T \circ T \circ T \circ q \supseteq p \circ \top\!\!\top \circ q$

$\Rightarrow$ { T is a transitive relation, transitivity of $\supseteq$ }

$p \circ T \circ q \supseteq p \circ \top\!\!\top \circ q$

$=$ { $T \subseteq \top\!\!\top$, monotonicity of composition and anti-symmetry of $\subseteq$ }

$p \circ T \circ q = p \circ \top\!\!\top \circ q$.

In summary,

$$p \circ T \circ q \neq \bot\!\!\bot \;\Rightarrow\; p \circ T \circ q = p \circ \top\!\!\top \circ q \quad .$$

Interchanging p and q, we get

$$q \circ T \circ p \neq \bot\!\!\bot \;\Rightarrow\; q \circ T \circ p = q \circ \top\!\!\top \circ p \quad .$$

So,

$p \circ T \circ q \neq \bot\!\!\bot \;\wedge\; q \circ T \circ p \neq \bot\!\!\bot$

$\Rightarrow$ { above, and p and q are both connected by T }

$p \circ T \circ q = p \circ \top\!\!\top \circ q \;\wedge\; q \circ T \circ p = q \circ \top\!\!\top \circ p$

$\wedge$ $p \circ T \circ p = p \circ \top\!\!\top \circ p \;\wedge\; q \circ T \circ q = q \circ \top\!\!\top \circ q$

$\Rightarrow$ { distributivity of composition over $\cup$, Leibniz }

$(p \cup q) \circ T \circ (p \cup q) = (p \cup q) \circ \top\!\!\top \circ (p \cup q)$

$\Rightarrow$ { definition of connected and lemma 118,
$p \subseteq p \cup q$ and $q \subseteq p \cup q$, p and q are components of T,
definition 116 }

$p = p \cup q = q$.

□

Taking the contrapositive of lemma 120, we get:

Corollary 121. Suppose T is a transitive relation and p and q are both components of T. Then

$$p \circ T \circ q = \bot\!\!\bot \;\vee\; q \circ T \circ p = \bot\!\!\bot \;\Leftarrow\; p \neq q \quad .$$

□

Corollary 121 is the basis of the construction of a directed acyclic graph from the strongly connected components of a graph.

10.2. Transitive and Symmetric Relations

Undirected graphs correspond to symmetric relations. The transitive closure of relation R, denoted by R^+, has the property that

$$(R^+)^\cup = (R^\cup)^+ \quad .$$

(The proof of this property is a nice illustration of the fusion theorem: R^+ is a least fixed point and converse is Galois connected to itself and commutes with the function mapping x to $x \circ x$.) It follows that

$$(R^+)^\cup = R^+ \quad \Leftarrow \quad R^\cup = R \quad .$$

Here we consider properties of transitive and symmetric relations. A major focus from here on will be the properties of the existential-image function introduced in section 8.1.

Lemma 122. Suppose T is a transitive and symmetric relation. Then $(T \circ p)^<$ is connected by T if p is connected by T.

Proof We have

$$\begin{array}{ll} & (T \circ p)^< \circ \top\!\!\top \circ (T \circ p)^< \\ = & \quad \{ \quad \text{theorem 51(a) and (c)} \quad \} \\ & T \circ p \circ \top\!\!\top \circ p \circ T^\cup \\ \subseteq & \quad \{ \quad \text{assume } p \text{ is connected by } T \\ & \qquad \text{definition and monotonicity of composition} \quad \} \\ & T \circ T \circ T^\cup \\ \subseteq & \quad \{ \quad T \text{ is transitive and symmetric} \quad \} \\ & T \quad . \end{array}$$

The lemma follows by definition of is-connected-by.
□

Theorem 123. Suppose T is a transitive and symmetric relation. Then $p = (T \circ p)^<$ if p is a component of T.

Proof Assume T is transitive and symmetric and p is a component of T.

$$\begin{array}{ll} & p = (T \circ p)^< \\ \Leftarrow & \quad \{ \quad \text{assumptions, lemma 122, and definition 116 of component} \quad \} \\ & p \subseteq (T \circ p)^< \\ = & \quad \{ \quad [\ p \subseteq q \ \equiv \ p \circ \top\!\!\top \subseteq q \circ \top\!\!\top\ ] \text{ with } q := (T \circ p)^< \text{ ; domains} \quad \} \\ & p \circ \top\!\!\top \subseteq T \circ p \circ \top\!\!\top \\ \Leftarrow & \quad \{ \quad p \text{ is a component of } T \text{, so } p \text{ is connected by } T \\ & \qquad \text{i.e. } p \circ \top\!\!\top \circ p \subseteq T \\ & \qquad \text{monotonicity of composition and transitivity of } \subseteq \quad \} \end{array}$$

$p \circ \top\!\!\top \subseteq p \circ \top\!\!\top \circ p \circ p \circ \top\!\!\top$

$=$ { p is a coreflexive, so $p \circ p = p$, cone rule: (47) }

$p \circ \top\!\!\top \subseteq p \circ \top\!\!\top \circ p \circ \top\!\!\top \ \wedge \ (\top\!\!\top \circ p \circ \top\!\!\top = \top\!\!\top \ \vee \ p = \bot\!\!\bot)$

$=$ { distributivity of conjunction over disjunction

Leibniz and $\bot\!\!\bot$ is zero of composition and least element }

true .

□

Corollary 124. The components of an equivalence relation T are atoms in the lattice of fixed points of the function that maps coreflexive q to $(T \circ q)^<$. That is, if T is an equivalence relation and p is a component of T,

$$(q \subseteq p \ \equiv \ q = p \ \vee \ q = \bot\!\!\bot) \ \Leftarrow \ q = (T \circ q)^< \ .$$

Proof Apply lemma 25 with f instantiated to the function that maps coreflexive q to $(T \circ q)^<$. This function is a complementation-idempotent closure operator by theorem 67.

□

Theorem 125. Suppose p is a coreflexive, T is a transitive and symmetric relation and q is a component of T. Then

$$p \circ T \circ q = \bot\!\!\bot \Leftarrow p \circ q = \bot\!\!\bot \ .$$

In particular, the property holds when p and q are both components of T.

Proof

$p \circ T \circ q$

$=$ { property of domains: [$R = R^< \circ R$] with $R := T \circ q$ }

$p \circ (T \circ q)^< \circ T \circ q$

$=$ { theorem 123 with $p := q$ }

$p \circ q \circ T \circ q$

$=$ { assume $p \circ q = \bot\!\!\bot$, $\bot\!\!\bot$ is zero of composition }

$\bot\!\!\bot$.

□

10.3. Strongly Connected Components

The notion of a "strongly connected component" of a finite graph is prominent in algorithmic graph theory. This section is about fundamental properties of strongly connected components. Since the properties do not depend on the finiteness of graphs, we present them for arbitrary relations.

Definition 126 (Strongly Connected Component). Coreflexive p is said to be a *strongly connected component* of relation R if p is a component of R^*.

□

Definition 127. The function equiv mapping arbitrary relations to equivalence relations is defined by, for all R,

$$\mathsf{equiv}.R \;=\; R^* \cap (R^*)^{\cup} \quad .$$

It is a well-known fact that $\mathsf{equiv}.R$ is an equivalence relation (i.e. it is reflexive, transitive and symmetric). The straightforward (point-free) proof is omitted.
□

Theorem 128. Suppose p is a strongly connected component of R. Then p is a component of $\mathsf{equiv}.R$. Conversely, every component of $\mathsf{equiv}.R$ is a strongly connected component of R.

Proof Immediate from the definition of strongly-connected and corollary 117(d).
□

Theorem 129. Suppose p is a strongly connected component of R. Then

$$p \;=\; (\mathsf{equiv}.R \circ p)^<$$

Moreover, p is an atom in the lattice of fixed points of the function that maps p to $(\mathsf{equiv}.R \circ p)^<$.

Proof Immediate from the definition of strongly-connected, corollary 117, theorem 123 and corollary 124.
□

10.4. Absolute Connectivity

This section is about paths in a graph connecting two nodes in one and the same strongly connected component of the graph. We show that all nodes on such paths are elements of the strongly connected component.

As in section 10.3, the finiteness of graphs is not used and the stated properties are valid for arbitrary relations; nevertheless, we interpret the properties in terms of graphs.

Recall that $\sim p$ denotes the negation of p in the lattice of coreflexives. For a finite graph, lemma 131 states that there are no paths from component p to itself that pass through nodes not in p. The lemma is a corollary of lemma 130.

Lemma 130. Suppose p is a strongly connected component of relation R. Then

$$p \;=\; (p \circ R^*)^> \;\cap\; (R^* \circ p)^< \quad .$$

Proof Let us abbreviate $(p \circ R^*)^> \cap (R^* \circ p)^<$ to q. We have to prove that $q = p$. In order to exploit the assumption that p is a a strongly connected component of R, the goal is to prove that q is connected by R^*.

$$\begin{array}{ll} & q \circ \top\!\!\top \circ q \\ \subseteq & \quad \{ \quad q = (p \circ R^*)^> \cap (R^* \circ p)^< \text{, monotonicity} \quad \} \\ & (R^* \circ p)^< \circ \top\!\!\top \circ (p \circ R^*)^> \\ = & \quad \{ \quad [\; R^< \circ \top\!\!\top = R \circ \top\!\!\top \;] \text{ with } R := R^* \circ p \text{,} \end{array}$$

$$[\ \top\!\!\top \circ R^{>} = \top\!\!\top \circ R\ ] \text{ with } R := p \circ R^* \quad \}$$

$$\begin{array}{ll}
& R^* \circ p \circ \top\!\!\top \circ p \circ R^* \\
= & \quad \{ \quad p \text{ is strongly connected by } R\,, \\
& \qquad \text{definitions 116 and 126, and lemma 118} \quad \} \\
& R^* \circ p \circ R^* \circ p \circ R^* \\
\subseteq & \quad \{ \quad p \subseteq I\,, \text{ monotonicity of composition} \quad \} \\
& R^* \circ R^* \circ R^* \\
= & \quad \{ \quad R^* = R^* \circ R^* \quad \} \\
& R^* \ .
\end{array}$$

That is, by definition 116, q is connected by R^*. Hence

$$\begin{array}{ll}
& p = q \\
\Leftarrow & \quad \{ \quad p \text{ is strongly connected by } R\,, \text{ definitions 126 and 116} \quad \} \\
& q \text{ is connected by } R^* \ \wedge \ p \subseteq q \\
= & \quad \{ \quad \text{above, definition of } q \quad \} \\
& p \subseteq (p \circ R^*)^{>} \cap (R^* \circ p)^{<} \\
= & \quad \{ \quad I \subseteq R^*\,, \text{ monotonicity and properties of coreflexives} \quad \} \\
& \mathsf{true} \ .
\end{array}$$

□

Lemma 131. Suppose R is a relation and p is a strongly connected component of R. Then

$$p \circ R^* \circ \sim p \circ R^* \circ p = \bot\!\!\bot \ .$$

Proof We have:

$$\begin{array}{ll}
& p \circ R^* \circ \sim p \circ R^* \circ p \ = \ \bot\!\!\bot \\
= & \quad \{ \quad \text{domains} \quad \} \\
& p \circ R^* \circ (p \circ R^*)^{>} \circ \sim p \circ (R^* \circ p)^{<} \circ R^* \circ p \ = \ \bot\!\!\bot \\
\Leftarrow & \quad \{ \quad \bot\!\!\bot \text{ is zero of composition} \quad \} \\
& (p \circ R^*)^{>} \circ \sim p \circ (R^* \circ p)^{<} \ = \ \bot\!\!\bot \\
\Leftarrow & \quad \{ \quad [\ p \circ q = p \cap q\ ] \text{ (for coreflexives } p \text{ and } q\text{), properities of intersection} \quad \} \\
& (p \circ R^*)^{>} \cap (R^* \circ p)^{<} \ \subseteq \ p \\
= & \quad \{ \quad \text{lemma 130} \quad \} \\
& \mathsf{true} \ .
\end{array}$$

□

Like lemma 131, lemma 132 below is valid for all relations but, for finite graphs, it formulates a property of paths between nodes in the same strongly connected component: in this case, in terms of the edges that form the paths. The first term, $p \circ \top\!\!\top \circ p$, is the relation that holds between all nodes in the same component p. The second and third

terms capture the existence of paths defined by edges from the component p. The third term is more complex than the second term; it is included because it expresses more directly that elements of strongly connected component p are connected by paths formed of edges connecting elements of p. Specifically, the term $p \circ R$ represents the edges in R from a node in p, and the term $p \circ R \circ p$ represents the edges of R that connect nodes in p. So $(p \circ R)^* \circ p$ is interpreted as the relation between two nodes of which the second is in p that are connected by edges that are from nodes in p; similarly, $p \circ (p \circ R \circ p)^*$ represents the relation between two nodes of which the first is in p and that are connected by edges that connect nodes in p. The outer occurrences of "p" are necessary because (for all R) R^* includes the identity relation.

Lemma 132. Suppose R is a relation and p is a strongly connected component of R. Then

$$p \circ \top\!\!\top \circ p \;=\; (p \circ R)^* \circ p \;=\; p \circ (p \circ R \circ p)^* \circ p \quad .$$

Proof The equality between the second and third terms is straightforward:

$$\begin{array}{ll} & p \circ (p \circ R \circ p)^* \\ = & \quad \{ \quad \text{mirror rule: } [\; R \circ (S \circ R)^* = (R \circ S)^* \circ R \;] \text{ with } R,S := p, p \circ R \quad \} \\ & (p \circ p \circ R)^* \circ p \\ = & \quad \{ \quad p \text{ is a coreflexive, so } p \circ p = p \quad \} \\ & (p \circ R)^* \circ p \quad . \end{array}$$

It is somewhat more difficult to establish the equality between the first and second terms, which we now do.

The relation R^* represents paths to and from all nodes and not just nodes in p. In order to separate out paths that are not to or not from nodes in p we begin by complifying R^*:

$$\begin{array}{ll} & R^* \\ = & \quad \{ \quad p \cup \sim p = I \quad \} \\ & ((p \cup \sim p) \circ R \circ (p \cup \sim p))^* \\ = & \quad \{ \quad \text{distributivity of composition over union,} \\ & \qquad \text{idempotency of set union and } p \cup \sim p = I \quad \} \\ & (p \circ R \circ p \;\cup\; R \circ \sim p \;\cup\; \sim p \circ R)^* \\ = & \quad \{ \quad \text{star decomposition} \quad \} \\ & (p \circ R \circ p)^* \circ ((R \circ \sim p \;\cup\; \sim p \circ R) \circ (p \circ R \circ p)^*)^* \quad . \end{array}$$

We have indeed constructed a complicated expression for R^*. It is the composition of two terms; our goal is to show that the second term can be eliminated when we consider $p \circ R^* \circ p$. So that the expressions don't become too long, let us write the second term in the composition as S^*. That is,

$$S = (R \circ \sim p \;\cup\; \sim p \circ R) \circ (p \circ R \circ p)^* \quad \wedge \quad R^* = (p \circ R \circ p)^* \circ S^* \quad . \tag{133}$$

We show that

$$p \circ S^* \circ p = p \quad . \tag{134}$$

We have:

$$\begin{array}{ll} & p \circ S^* \circ p \\ = & \quad \{ \quad S^* \ = \ I \cup S \circ S^* \, , \\ & \qquad \text{distributivity of composition over union, etc.} \quad \} \\ & p \cup p \circ S \circ S^* \circ p \\ = & \quad \{ \quad \text{1st conjunct of (133), distributivity and } \ p \circ {\sim} p = \perp\!\!\!\perp \quad \} \\ & p \cup p \circ R \circ {\sim} p \circ (p \circ R \circ p)^* \circ S^* \circ p \\ = & \quad \{ \quad \text{2nd conjunct of (133)} \quad \} \\ & p \cup p \circ R \circ {\sim} p \circ R^* \circ p \\ = & \quad \{ \quad R \subseteq R^* \text{ , lemma 131} \quad \} \\ & p \quad . \end{array}$$

We can now complete the calculation.

$$\begin{array}{ll} & p \circ \top\!\!\top \circ p \\ = & \quad \{ \quad p \text{ is a strongly connected component of } R \, , \\ & \qquad \text{definition 126 and lemma 118} \quad \} \\ & p \circ R^* \circ p \\ = & \quad \{ \quad (133) \quad \} \\ & p \circ (p \circ R \circ p)^* \circ S^* \circ p \\ = & \quad \{ \quad \text{mirror rule: } [\ R \circ (S \circ R)^* = (R \circ S)^* \circ R \ ] \text{ with } R,S := p \, , p \circ R \, , \\ & \qquad p \circ p = p \quad \} \\ & (p \circ R)^* \circ p \circ S^* \circ p \\ = & \quad \{ \quad (134) \quad \} \\ & (p \circ R)^* \circ p \quad . \end{array}$$

□

10.5. Saturation

Note that atomicity has not been used anywhere above. Saturated atomicity is necessary to show that all nodes in a graph are elements of a strongly connected component of the graph. The calculations are straightforward:

Lemma 135. For all points a and relations R, $(\mathsf{equiv}.R \circ a)^<$ is a strongly connected component of R. (Recall that a point is a proper atom.)

Proof We exploit theorem 128. Accordingly, we have to show that $(\mathsf{equiv}.R \circ a)^<$ is a component of $\mathsf{equiv}.R$. That is, $(\mathsf{equiv}.R \circ a)^<$ is connected by $\mathsf{equiv}.R$ and it is maximal among such coreflexives.

First, we show that $(\mathsf{equiv}.R \circ a)^<$ is connected by $\mathsf{equiv}.R$. For all atoms a and all relations R, we have:

$(\mathsf{equiv}.R \circ a)^< \circ \top\!\!\top \circ (\mathsf{equiv}.R \circ a)^<$

$=$ { domains (specifically theorem 51(a)) }

$\mathsf{equiv}.R \circ a \circ \top\!\!\top \circ (\mathsf{equiv}.R \circ a)^\cup$

$=$ { converse }

$\mathsf{equiv}.R \circ a \circ \top\!\!\top \circ a \circ \mathsf{equiv}.R$

$=$ { $a \circ \top\!\!\top \circ a = a$ ("all or nothing axiom") }

$\mathsf{equiv}.R \circ a \circ \mathsf{equiv}.R$

$\subseteq$ { $a \subseteq I$, monotonicity }

$\mathsf{equiv}.R \circ \mathsf{equiv}.R$

$\subseteq$ { $\mathsf{equiv}.R$ is transitive }

$\mathsf{equiv}.R$.

Now we must show that, if a is a point,

$$\langle \forall q : q \circ \top\!\!\top \circ q \subseteq \mathsf{equiv}.R : (\mathsf{equiv}.R \circ a)^< \subseteq q \ \equiv \ (\mathsf{equiv}.R \circ a)^< = q \rangle \ .$$

Suppose q is a coreflexive such that $q \circ \top\!\!\top \circ q \subseteq \mathsf{equiv}.R$. Then, by lemma 118,

$$q \circ \top\!\!\top \circ q \ = \ q \circ \mathsf{equiv}.R \circ q \ .$$

So,

$(\mathsf{equiv}.R \circ a)^< \supseteq q$

$=$ { [$p \supseteq q \ \equiv \ p \circ \top\!\!\top \supseteq q \circ \top\!\!\top$] with $p := (\mathsf{equiv}.R \circ a)^<$; domains }

$\mathsf{equiv}.R \circ a \circ \top\!\!\top \ \supseteq \ q \circ \top\!\!\top$

$\Leftarrow$ { $q \circ \top\!\!\top \circ q \subseteq \mathsf{equiv}.R$ }

$q \circ \top\!\!\top \circ q \circ a \circ \top\!\!\top \supseteq q \circ \top\!\!\top$

$\Leftarrow$ { monotonicity }

$\top\!\!\top \circ q \circ a \circ \top\!\!\top \supseteq \top\!\!\top$

$=$ { assume $(\mathsf{equiv}.R \circ a)^< \subseteq q$
then, since $I \subseteq \mathsf{equiv}.R$, $(I \circ a)^< \subseteq q$
i.e. $a \subseteq q$ and $q \circ a = a$ }

$\top\!\!\top \circ a \circ \top\!\!\top \supseteq \top\!\!\top$

$=$ { a is a point, cone rule (47) }

true .

We have thus shown that, if a is a point,

$$\langle \forall q : q \circ \top\!\!\top \circ q \subseteq \mathsf{equiv}.R : (\mathsf{equiv}.R \circ a)^< \supseteq q \ \Leftarrow \ (\mathsf{equiv}.R \circ a)^< \subseteq q \rangle \ .$$

The required equivalence is a straightforward consequence of the anti-symmetry and reflexivity of the subset relation.

□

The converse of lemma 135 is the following:

Lemma 136. If p is a strongly connected component of R, and a is a point such that $a \subseteq p$, then $p = (\mathsf{equiv}.R \circ a)^<$.

Proof Assume p is a strongly connected component of R, and a is a point such that $a \subseteq p$. Then,

$$\begin{array}{ll} & \mathsf{true} \\ = & \quad \{ \quad \text{theorem 129} \quad \} \\ & p \;=\; (\mathsf{equiv}.R \circ p)^< \\ \Rightarrow & \quad \{ \quad a \subseteq p\text{, monotonicity of composition and domains} \quad \} \\ & p \;\supseteq\; (\mathsf{equiv}.R \circ a)^< \\ \Rightarrow & \quad \{ \quad \text{lemma 135, theorem 128 and definition 116} \quad \} \\ & p \;=\; (\mathsf{equiv}.R \circ a)^< \quad . \end{array}$$

□

Summarising, we have:

Theorem 137. Suppose R is a homogeneous relation. Then the strongly connected components of R are given by $\langle \cup a : \mathsf{point}.a : \{(\mathsf{equiv}.R \circ a)^<\} \rangle$. The strongly connected components partition the set of all points[6]. That is, distinct strongly connected components are disjoint and each point is an element of a strongly connected component (specifically, a is an element of $(\mathsf{equiv}.R \circ a)^<$).

Proof Lemmas 135, 136, 119 and 75 (with $R := \mathsf{equiv}.R$).
□

10.6. Starth Roots of the Equivalence Relation

We have defined $\mathsf{equiv}.R$ as $R^* \cap (R^*)^\cup$. (See definition 127.) It is useful to express it as E^* where (for graph R) E represents the edges in R that connect nodes in the same strongly connected component (i.e. nodes that are "E"quivalent under the relation $\mathsf{equiv}.R$). This is the content of theorem 139.

One application of theorem 139 is theorem 141, which states —with a minor qualification— that a graph G being acyclic is equivalent to the relation $\mathsf{equiv}.G$ being the identity relation. Application of theorem 139 is also an important step in the proof of theorem 143 below, which decomposes paths in a graph into paths in an acyclic graph connecting strongly connected components of the graph. First, a lemma:

Lemma 138. For all relations R, U, V and W,

$$R^* \;\cap\; U \circ V \circ W \;\;=\;\; R^* \;\cap\; U \circ (R^* \cap V) \circ W \quad \Leftarrow \quad U \cup W \subseteq (R^\cup)^* \quad .$$

(Note that composition has precedence over intersection. The spacing of our formulae is designed to make this clear.)

Proof We calculate the condition on U and W as follows.

[6]When applied to graphs, "points" are "nodes".

$$
\begin{array}{ll}
 & R^* \cap U \circ V \circ W \;=\; R^* \cap U \circ (R^* \cap V) \circ W \\
= & \quad \{ \quad V \supseteq R^* \cap V \text{ , monotonicity and anti-symmetry} \quad \} \\
 & R^* \cap U \circ V \circ W \;\subseteq\; R^* \cap U \circ (R^* \cap V) \circ W \\
= & \quad \{ \quad \text{properties of } \cap \quad \} \\
 & R^* \cap U \circ V \circ W \;\subseteq\; U \circ (R^* \cap V) \circ W \\
\Leftarrow & \quad \{ \quad \text{modularity rule (46) with } R,S,T := U , V \circ W , R^* , \\
 & \qquad \text{and symmetric rule with } R,S,T := W , V , U^\cup \circ R^* \quad \} \\
 & U \circ (U^\cup \circ R^* \circ W^\cup \;\cap\; V) \circ W \;\subseteq\; U \circ (R^* \cap V) \circ W \\
\Leftarrow & \quad \{ \quad \text{monotonicity} \quad \} \\
 & U^\cup \circ R^* \circ W^\cup \;\cap\; V \;\subseteq\; R^* \cap V \\
\Leftarrow & \quad \{ \quad R^* \circ R^* \circ R^* \;=\; R^* \text{, monotonicity} \quad \} \\
 & U^\cup \subseteq R^* \;\wedge\; W^\cup \subseteq R^* \\
= & \quad \{ \quad (44) \text{ and } (R^\cup)^* \;=\; (R^*)^\cup \quad \} \\
 & U \subseteq (R^\cup)^* \;\wedge\; W \subseteq (R^\cup)^* \;\; .
\end{array}
$$

(The antecedent in the statement of the lemma is, of course, equivalent to the last line of the calculation.)
□

Now, the theorem:

Theorem 139. For all relations R,

$$\mathsf{equiv}.R \;=\; (R^\cup \cap R^*)^* \;=\; (R \cap (R^\cup)^*)^* \;\; .$$

Proof We begin by proving, by induction on k, that, for all U and W,

$$R^* \cap U \circ (R^\cup)^k \circ W \;=\; R^* \cap U \circ (R^\cup \cap R^*)^k \circ W \;\Leftarrow\; U \cup W \subseteq (R^\cup)^* \;\; . \qquad (140)$$

The basis, $k = 0$ is trivial since $X^0 = I$, for all X. For the induction step, assume U and W are such that $U \cup W \subseteq (R^\cup)^*$. Then,

$$
\begin{array}{ll}
 & R^* \;\cap\; U \circ (R^\cup \cap R^*)^{k+1} \circ W \\
= & \quad \{ \quad \text{definition of } (R^\cup \cap R^*)^{k+1} \quad \} \\
 & R^* \;\cap\; U \circ (R^\cup \cap R^*)^k \circ (R^\cup \cap R^*) \circ W \\
= & \quad \{ \quad \text{by assumption, } U \subseteq (R^\cup)^* \text{; so } U \circ (R^\cup \cap R^*)^k \subseteq (R^\cup)^* , \\
 & \qquad \text{also, by assumption, } W \subseteq (R^\cup)^* \\
 & \qquad \text{lemma 138 with } U,V,W := U \circ (R^\cup \cap R^*)^k , R^\cup , W \quad \} \\
 & R^* \;\cap\; U \circ (R^\cup \cap R^*)^k \circ R^\cup \circ W \\
= & \quad \{ \quad \text{by assumption, } W \subseteq (R^\cup)^* \text{; so } R^\cup \circ W \;\subseteq\; (R^\cup)^* \\
 & \qquad \text{also, by assumption, } U \subseteq (R^\cup)^* \\
 & \qquad \text{induction hypothesis (140) with } W := R^\cup \circ W \quad \} \\
 & R^* \;\cap\; U \circ (R^\cup)^k \circ R^\cup \circ W
\end{array}
$$

$$
\begin{array}{ll}
= & \{ \quad \text{definition of } (R^{\cup})^{k+1} \quad \} \\
& R^* \ \cap \ U \circ (R^{\cup})^{k+1} \circ W \ .
\end{array}
$$

By induction, we have established (140) for all natural numbers k. Hence,

$$
\begin{array}{ll}
& \mathsf{equiv}.R \\
= & \{ \quad \text{definition 127} \quad \} \\
& R^* \cap (R^*)^{\cup} \\
= & \{ \quad (R^*)^{\cup} = (R^{\cup})^* \text{, definition of star as a sum of powers} \quad \} \\
& R^* \cap \langle \cup k : 0 \leq k : (R^{\cup})^k \rangle \\
= & \{ \quad \text{distributivity} \quad \} \\
& \langle \cup k \ : \ 0 \leq k \ : \ R^* \cap (R^{\cup})^k \rangle \\
= & \{ \quad \text{(140) with } U,W := I,I \quad \} \\
& \langle \cup k \ : \ 0 \leq k \ : \ R^* \cap (R^{\cup} \cap R^*)^k \rangle \\
= & \{ \quad \text{distributivity} \quad \} \\
& R^* \cap \langle \cup k \ : \ 0 \leq k \ : \ (R^{\cup} \cap R^*)^k \rangle \\
= & \{ \quad \text{definition of star as a sum of powers, } R^* \supseteq (R^{\cup} \cap R^*)^* \quad \} \\
& (R^{\cup} \cap R^*)^* \ .
\end{array}
$$

The final equality in the statement of the lemma follows by symmetry (formally, by replacing R by $R^{\cup}$ in the first equality and using the properties of converse).
□

Given that theorem 139 expresses a property that some might regard as obvious, the proof is surprisingly complicated: the induction hypothesis is non-trivial. It is also unfortunate that the proof uses the definition of the star operator as a sum of powers (and not as a least fixed point). A proof using fixed-point fusion would be preferable —albeit by mutual inclusion— but, so far, has eluded us.

The following theorem exploits theorem 139.

Theorem 141. If R is acyclic, $\mathsf{equiv}.R$ is the identity relation. That is,

$$I \cap R^+ = \perp\!\!\!\perp \ \Rightarrow \ \mathsf{equiv}.R = I \ .$$

Conversely, if $\mathsf{equiv}.R$ is the identity relation, $R \cap \neg I$ is acyclic. That is,

$$\mathsf{equiv}.R = I \ \Rightarrow \ I \cap (R \cap \neg I)^+ = \perp\!\!\!\perp \ .$$

(In terms of graphs, $R \cap \neg I$ is the graph R with "self-loops" removed.)

Proof Suppose $I \cap R^+ = \perp\!\!\!\perp$. Then

$$
\begin{array}{ll}
& \mathsf{equiv}.R \\
= & \{ \quad \text{theorem 139} \quad \} \\
& (R^{\cup} \cap R^*)^* \\
\subseteq & \{ \quad \text{modularity rule: (46), monotonicity} \quad \}
\end{array}
$$

$$
\begin{array}{ll}
 & (R^{\cup} \circ (I \cap R \circ R^*))^* \\
= & \quad \{ \quad R \circ R^* = R^+ \text{ , assumption: } I \cap R^+ = \perp\!\!\!\perp \quad \} \\
 & (R^{\cup} \circ \perp\!\!\!\perp)^* \\
= & \quad \{ \quad \perp\!\!\!\perp \text{ is zero of composition, } \perp\!\!\!\perp^* = I \quad \} \\
 & I \quad .
\end{array}
$$

That is, $\mathsf{equiv}.R \subseteq I$. Since, $I \subseteq \mathsf{equiv}.R$, it follows by anti-symmetry of set inclusion that $\mathsf{equiv}.R = I$.

For the converse, we have:

$$
\begin{array}{ll}
 & I \cap (R \cap \neg I)^+ \\
= & \quad \{ \quad [\ R^+ = R \circ R^*\ ] \text{ with } R := R \cap \neg I \text{ , } R^* = (R \cap \neg I)^* \quad \} \\
 & I \cap (R \cap \neg I) \circ R^* \\
\subseteq & \quad \{ \quad \text{modularity rule: (46), } I \text{ is unit of composition} \quad \} \\
 & (R \cap \neg I) \circ ((R \cap \neg I)^{\cup} \cap R^*) \\
\subseteq & \quad \{ \quad R \cap \neg I \subseteq \neg I \text{ , } (R \cap \neg I)^{\cup} \subseteq R^{\cup} \text{ , theorem 139,} \\
 & \qquad\quad [\ R \subseteq R^*\ ] \text{ with } R := R^{\cup} \cap R^* \\
 & \qquad\quad \text{monotonicity (of converse, composition and star)} \quad \} \\
 & \neg I \circ \mathsf{equiv}.R \quad .
\end{array}
$$

Thus

$$
\begin{array}{ll}
 & \mathsf{equiv}.R \subseteq I \\
\Rightarrow & \quad \{ \quad \text{above, monotonicity of composition and transitivity of } \subseteq \quad \} \\
 & I \cap (R \cap \neg I)^+ \subseteq \neg I \circ I \\
= & \quad \{ \quad I \text{ is unit of composition, complements,} \\
 & \qquad\quad \text{idempotency of intersection} \quad \} \\
 & I \cap (R \cap \neg I)^+ = \perp\!\!\!\perp \quad .
\end{array}
$$

□

Note that, although theorem 141 is valid for all relations, its significance is primarily when applied to finite graphs; the more significant property of a non-finite relation is whether or not it is left- or right-definite (or both).

10.7. A Pathwise Homomorphism

A well-known property is that the strongly connected components of a graph G define an acyclic graph G' . The nodes of the graph G' are the strongly connected components of G , and the edges of G' are the edges of G that connect nodes of G in distinct strongly connected components. Moreover, there is a path in G from node u to node v equivales there is a path in G' from the strongly connected component containing u to the strongly connected component containing v . The primary purpose of this section is to formalise this theorem.

Because the nodes of G and G' are different, it is necessary to use a *typed* algebra of *heterogeneous* relations rather than the *untyped* algebra of *homogeneous* relations. As

remarked earlier, the rules that we have been using remain valid provided some caution is exercised when overloading notation.

Suppose N is a set (of "nodes") and G is a relation of type $N{\sim}N$ (the "edges" of the "graph"). As we have seen the function

$$\langle a : a{\in}N : (\mathsf{equiv}.G \circ a)^{<}\rangle$$

maps nodes to strongly connected components. Let us denote this function by sc and the set of strongly connected components of G by C. Then sc has type $C{\leftarrow}N$ and, by theorem 73,

$$\mathsf{equiv}.G \;=\; \mathsf{sc}^{\cup} \circ \mathsf{sc} \quad . \tag{142}$$

The relation

$$\mathsf{sc} \circ G \circ \mathsf{sc}^{\cup} \;\cap\; \neg I_C$$

is a homogeneous relation on the strongly connected components of G, i.e. a relation of type $C{\sim}C$. Informally, it is a graph obtained from the graph G by coalescing the nodes in a strongly connected component of G into a single node whilst retaining the edges of G that connect nodes in distinct strongly connected components[7]. Theorem 143 establishes the formal relationship between its reflexive-transitive closure and G^*.

Theorem 143. Let $\mathcal{A}$ denote $\mathsf{sc} \circ G \circ \mathsf{sc}^{\cup} \cap \neg I_C$. Then,

$$G^* \;=\; \mathsf{sc}^{\cup} \circ \mathcal{A}^* \circ \mathsf{sc} \quad . \tag{144}$$

Moreover, $\mathcal{A}$ is acyclic. That is,

$$I_C \cap \mathcal{A}^+ \;=\; \perp\!\!\!\perp \quad . \tag{145}$$

It follows that $\mathcal{A}^*$ is a partial ordering of the strongly connected components of G.

Proof With theorem 139 in mind, we split G into two relations: D and E where D is defined by

$$D \;=\; G \cap \neg((G^{\cup})^*)$$

and E is defined by

$$E \;=\; G \cap (G^{\cup})^* \quad .$$

The relation D captures the edges of G that connect "D"istinct strongly connected components. To be precise:

$$\mathsf{sc} \circ D \circ \mathsf{sc}^{\cup} \;\subseteq\; \neg I_C \quad , \tag{146}$$

since

[7] Although we don't go into details, for any function f of appropriate type, the graph $f \circ G \circ f^{\cup}$ is "pathwise homomorphic" [29] to G; hence the title of this section.

$$
\begin{array}{ll}
 & \mathsf{sc} \circ D \circ \mathsf{sc}^{\cup} \subseteq \neg I_C \\
= & \quad \{ \quad \text{definition of } D \quad \} \\
 & \mathsf{sc} \circ (G \cap \neg((G^{\cup})^*)) \circ \mathsf{sc}^{\cup} \subseteq \neg I_C \\
= & \quad \{ \quad \text{middle-exchange (48),} \\
 & \qquad I_C \text{ is unit of composition, and complements} \quad \} \\
 & \mathsf{sc}^{\cup} \circ \mathsf{sc} \subseteq \neg G \cup (G^{\cup})^* \\
\Leftarrow & \quad \{ \quad (142) \quad \} \\
 & \mathsf{equiv}.G \subseteq (G^{\cup})^* \\
= & \quad \{ \quad \mathsf{equiv}.G = G^* \cap (G^*)^{\cup} \text{ and } (G^*)^{\cup} = (G^{\cup})^* \quad \} \\
 & \mathsf{true} \ .
\end{array}
$$

Conversely, the relation E captures the edges of G that are in "E"qual strongly connected components:

$$\mathsf{sc} \circ E \circ \mathsf{sc}^{\cup} \subseteq I_C \ , \tag{147}$$

since

$$
\begin{array}{ll}
 & \mathsf{sc} \circ E \circ \mathsf{sc}^{\cup} \\
\subseteq & \quad \{ \quad E \subseteq E^* \text{ and monotonicity} \quad \} \\
 & \mathsf{sc} \circ E^* \circ \mathsf{sc}^{\cup} \\
= & \quad \{ \quad \text{by (142) and theorem 139 with } R := G \, , \\
 & \qquad E^* = \mathsf{equiv}.G = \mathsf{sc}^{\cup} \circ \mathsf{sc} \quad \} \\
 & \mathsf{sc} \circ \mathsf{sc}^{\cup} \circ \mathsf{sc} \circ \mathsf{sc}^{\cup} \\
\subseteq & \quad \{ \quad \mathsf{sc} \text{ is a function} \quad \} \\
 & I_C \ .
\end{array}
$$

In order to prove (144) and (145) we need three additional properties of D. The first,

$$D^{\cup} \cap G^* \ = \ \perp\!\!\!\perp \ , \tag{148}$$

is obvious from the definition of D and properties of converse and complement:

$$
\begin{array}{ll}
 & D^{\cup} \cap G^* \\
= & \quad \{ \quad \text{definition of } D \quad \} \\
 & (G \cap \neg((G^{\cup})^*))^{\cup} \cap G^* \\
= & \quad \{ \quad \text{distributivity properties of converse and } [\ (G^{\cup})^{\cup} = G\ ] \quad \} \\
 & G^{\cup} \cap \neg(G^*) \cap G^* \\
= & \quad \{ \quad [\ \neg S \cap S = \perp\!\!\!\perp\ ] \text{ with } S := G^* \quad \} \\
 & \perp\!\!\!\perp \ .
\end{array}
$$

The second,

$$G^* \ = \ \mathsf{equiv}.G \circ (D \circ \mathsf{equiv}.G)^* \ , \tag{149}$$

is proved as follows:

$$
\begin{array}{ll}
 & G^* \\
= & \quad \{ \quad D \cup E = G \quad \} \\
 & (D \cup E)^* \\
= & \quad \{ \quad \text{star decomposition} \quad \} \\
 & E^* \circ (D \circ E^*)^* \\
= & \quad \{ \quad \text{by theorem 139 with } \; R := G \,, \; E^* = \mathsf{equiv}.G \quad \} \\
 & \mathsf{equiv}.G \circ (D \circ \mathsf{equiv}.G)^* \quad .
\end{array}
$$

The third property,

$$
\mathcal{A} \;=\; \mathsf{sc} \circ D \circ \mathsf{sc}^{\cup} \quad , \tag{150}
$$

is a combination of (146) and (147):

$$
\begin{array}{ll}
 & \mathcal{A} \\
= & \quad \{ \quad \text{definition of } \; \mathcal{A} \,, \; D \cup E = G \quad \} \\
 & \mathsf{sc} \circ (D \cup E) \circ \mathsf{sc}^{\cup} \;\cap\; \neg I_C \\
= & \quad \{ \quad \text{distributivity} \quad \} \\
 & (\mathsf{sc} \circ D \circ \mathsf{sc}^{\cup} \cap \neg I_C) \;\cup\; (\mathsf{sc} \circ E \circ \mathsf{sc}^{\cup} \;\cap\; \neg I_C) \\
= & \quad \{ \quad (146) \text{ and } (147) \quad \} \\
 & \mathsf{sc} \circ D \circ \mathsf{sc}^{\cup} \quad .
\end{array}
$$

We now prove (144).

$$
\begin{array}{ll}
 & G^* \\
= & \quad \{ \quad (149) \quad \} \\
 & \mathsf{equiv}.G \circ (D \circ \mathsf{equiv}.G)^* \\
= & \quad \{ \quad (142) \quad \} \\
 & \mathsf{sc}^{\cup} \circ \mathsf{sc} \circ (D \circ \mathsf{sc}^{\cup} \circ \mathsf{sc})^* \\
= & \quad \{ \quad \text{mirror rule} \quad \} \\
 & \mathsf{sc}^{\cup} \circ (\mathsf{sc} \circ D \circ \mathsf{sc}^{\cup})^* \circ \mathsf{sc} \\
= & \quad \{ \quad (150) \quad \} \\
 & \mathsf{sc}^{\cup} \circ \mathcal{A}^* \circ \mathsf{sc} \quad .
\end{array}
$$

It remains to prove that $\mathcal{A}$ is acyclic. We have:

$$
\begin{array}{ll}
 & I_C \cap \mathcal{A}^+ \\
= & \quad \{ \quad \mathcal{A}^+ = \mathcal{A} \circ \mathcal{A}^* \text{ and } (150) \quad \} \\
 & I_C \;\cap\; \mathsf{sc} \circ D \circ \mathsf{sc}^{\cup} \circ (\mathsf{sc} \circ D \circ \mathsf{sc}^{\cup})^* \\
= & \quad \{ \quad \text{mirror rule and theorem 73} \quad \} \\
 & I_C \;\cap\; \mathsf{sc} \circ (D \circ \mathsf{equiv}.G)^* \circ D \circ \mathsf{sc}^{\cup} \\
\subseteq & \quad \{ \quad \text{modularity rule: (46) (applied in both forms)} \quad \}
\end{array}
$$

$$
\begin{array}{ll}
 & \mathsf{sc} \circ (\mathsf{sc}^{\cup} \circ \mathsf{sc} \circ D^{\cup} \cap (D \circ \mathsf{equiv}.G)^*) \circ D \circ \mathsf{sc}^{\cup} \\
= & \quad \{ \quad \text{theorem 73} \quad \} \\
 & \mathsf{sc} \circ (\mathsf{equiv}.G \circ D^{\cup} \cap (D \circ \mathsf{equiv}.G)^*) \circ D \circ \mathsf{sc}^{\cup} \\
\subseteq & \quad \{ \quad \text{modularity rule: (46), and } \mathsf{equiv}.G = (\mathsf{equiv}.G)^{\cup} \quad \} \\
 & \mathsf{sc} \circ \mathsf{equiv}.G \circ (D^{\cup} \cap \mathsf{equiv}.G \circ (D \circ \mathsf{equiv}.G)^*) \circ D \circ \mathsf{sc}^{\cup} \\
= & \quad \{ \quad (149) \quad \} \\
 & \mathsf{sc} \circ \mathsf{equiv}.G \circ (D^{\cup} \cap G^*) \circ D \circ \mathsf{sc}^{\cup} \\
= & \quad \{ \quad (148) \text{ and } \perp\!\!\!\perp \text{ is zero of composition} \quad \} \\
 & \perp\!\!\!\perp \ .
\end{array}
$$

Property (145) follows from the fact that $\perp\!\!\!\perp \subseteq R$, for all R, and anti-symmetry of the subset relation.
□

The importance of theorem 143 is that solving path problems can be decomposed into solving the problems for each individual strongly connected component and then combining the results using a topological search of an acyclic graph. Perhaps surprisingly, it is also used when inverting real matrices in order to preserve sparsity. As shown in [5], the standard so-called elimination techniques for inverting a matrix are algebraically identical to algorithms for constructing paths in a graph. (Essentially, $\mathbf{A}^{-1} = (\mathbf{1} - (\mathbf{1} - \mathbf{A}))^{-1} = (\mathbf{1} - \mathbf{A})^*$. The elimination algorithms exploit the star-decomposition rule to decompose the computation of $\mathbf{A}^{-1}$ into smaller components; the mirror rule is then used to evaluate $\mathbf{A}^{-1}$ for row/column matrices.) In this application, a topological search is often called "forward substitution". See also [30] for more detailed discussion of sparsity considerations.

(Of course, this does not mean that theorem 143 is valid for other interpretations of the star operator. For example, if G is a matrix of languages, it is not valid. Many steps in the calculation are valid in other interpretations but lemma 138 relies on the modularity rule, which is valid for relations but not for languages.)

11. Conclusion

The ever-growing reliance of modern society on computer software, including in life-critical situations, makes it paramount that we have effective methods of constructing and reasoning about software systems. The demands that this entails cannot be fulfilled by traditional informal techniques: the design of software must be based on techniques that allow the precise formulation and calculation of desired properties. In order to meet the challenges, it is vital that we learn how to choose and apply algebraic calculi that are tuned to the task in hand in a way that combines concision with precision. This paper demonstrates this thesis in the context of algorithmic graph theory.

Of course, it takes practice to learn how to apply point-free relation algebra to graph theory. Moreover, the learning curve can be steep because of the multiple components (lattice theory, fixed-point calculus, and regular algebra). However, we would argue that the results are worthwhile: in our view, the calculations in this paper are easier to check (both by human beings and by mechanised theorem provers) than traditional

pointwise reasoning, which invariably involves multiple levels of universal and existential quantifications. The final theorem, theorem 143, is, we believe, a convincing example of the combination of concision and precision that we strive for; the paper contains several other examples.

Although some of the calculational rules used in this paper have been well understood for many years, we continue to encounter publications (including textbooks) that appear not to be aware of them. For example, the star-decomposition and mirror rules of regular algebra were identified almost fifty years ago as central to the derivation of path-finding algorithms and have been used several times above[8]. The highly influential textbook by Aho, Hopcroft and Ullman [3, p.220], however, very briefly introduces the transitive closure of a relation (in a parenthesised sentence) but fails to give —let alone exploit— a single algebraic property.

Some readers may nevertheless conclude that we have failed in our endeavour, as evidenced by the length of this paper.

Certainly, compared to informal proofs our calculations are substantially longer. Aho, Hopcroft and Ullman [3, pp. 219–226] present depth-first search, its application to computing a topological ordering of the nodes in an acyclic graph as well as to computing the strongly connected components of an arbitrary graph, all within less than ten pages. Their discussion of the correctness of the strongly-connected-components algorithm takes less than one page. Cormen, Leiserson and Rivest [31, pp.465–497] cover the same ground in less than forty pages. Their account of the correctness of the algorithm for computing strongly connected components —which is much more thorough than that of Aho, Hopcroft and Ullman— amounts to five pages. We haven't even begun to discuss algorithms for computing strongly connnected components: we have only laid the foundations!

It has long been known that formal, axiomatic proofs are substantially longer than informal proofs in natural language. One reason is that formal proofs are necessarily more complete and are less prone to the sin of omission. More often than their formal counterparts, informal proofs tend to omit details that are considered "obvious" but nevertheless are essential to the argument. Informal proofs undergo what has been called a "social process" before they become accepted as legitimate: they rely on the agreement of sufficiently many experts that all steps are correct and have been adequately substantiated. Informal proofs achieve concision at the expense of precision.

We would argue that the formal proofs we have given *do* combine precision with concision. This combination is evident in the documentation that we provide. See, for example, section 9.4 in which properties of topological search are fully documented. An experienced, well-trained programmer will study the documentation in order to gain a full understanding of the implementation. Formal documentation of this nature can also be "executed" as a means of testing the implementation. Indeed, a well-trained programmer should be able to check for themself the veracity of the documentation, using it to design tests in cases of doubt.

Of course, mathematical formulae are less "readable" than natural language (at least to those for whom the natural language in use is the mother tongue) but natural language

[8]The rules were first used in [4, 5] but not named; the names were coined later and used specifically in, for example, [14].

can be misleading: mathematical vernacular tends to be chosen so that it mimics everyday language but its familiarity can be deceptive. Our point-free formulae will be even less readable to those unfamiliar with them but, we would argue, it is just a question of practice to gain the necessary reading and writing skills. Traditional pointwise formulae name variables that do not need to be named, and sometimes involve several layers of universal and existential quantifications.

Finally, an important advantage of the axiomatic, algebraic calculations that we have used here is the insight that it gives into correspondences between seemingly unrelated applications. We mentioned earlier that so-called "forward substitution" in linear algebra corresponds to topological search in graph theory —acyclic graphs and triangular matrices are algebraically identical— . Our axiomatic formulation of the notions of left-definite and right-definite enables recognition of their relevance in other application areas: it is relatively easy to identify, for example, seemingly unrelated applications of the unique extension property of regular algebra. In all our calculations, it is made clear which algebraic properties have been used — which is of great assistance in avoiding the re-invention of the proverbial wheel.

Acknowledgements. We are very grateful to the anonymous referees who gave very detailed comments on earlier versions of this paper.

[1] R. Backhouse, H. Doornbos, R. Glück, J. van der Woude, Algorithmic graph theory: An exercise in point-free reasoning, `http://www.cs.nott.ac.uk/~psarb2/MPC/papers`, Also available online at ResearchGate (2021).

[2] R. Backhouse, An analysis of repeated graph search, in: G.Hutton (Ed.), MPC 2019, Porto, Portugal, Vol. 11825 of LNCS, Springer Nature, pp. 298–327 (2019).

[3] A. V. Aho, J. E. Hopcroft, J. D. Ullman, Data Structures and Algorithms, Addison-Wesley, (1982).

[4] R. Backhouse, Closure algorithms and the star-height problem of regular languages, Ph.D. thesis, University of London, available at `https://spiral.imperial.ac.uk/bitstream/10044/1/22243/2/Backhouse-RC-1976-PhD-Thesis.pdf` (1975).

[5] R. Backhouse, B. Carré, Regular algebra applied to path-finding problems, Journal of the Institute of Mathematics and its Applications 15, pp. 161–186 (1975).

[6] C. Aarts, R. Backhouse, P. Hoogendijk, T. Voermans, J. v. d. Woude, A relational theory of datatypes, available via World-Wide Web at `http://www.cs.nott.ac.uk/~psarb2/papers` (September 1992).

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

[8] H. Doornbos, Reductivity arguments and program construction, Ph.D. thesis, Department of Mathematics and Computer Science (June 1996). doi:10.6100/IR461604.

[9] H. Doornbos, R. Backhouse, J. van der Woude, A calculational approach to mathematical induction, Theoretical Computer Science 179 (1–2), pp. 103–135 (1 Jun. 1997).

[10] R. Glück, Algebraic investigation of connected components, in: P. Höfner, D. Pous, G. Struth (Eds.), Relational and Algebraic Methods in Computer Science – 16th International Conference, RAMiCS 2017, Vol. 10226 of Lecture Notes in Computer Science, Springer, pp. 109–126 (May 15–18 2017).

[11] R. Backhouse, Galois connections and fixed point calculus, in: R. Backhouse, R. Crole, J. Gibbons (Eds.), Algebraic and Coalgebraic Methods in the Mathematics of Program Construction, Vol. 2297 of LNCS Tutorial, Ch. 4, pp. 89–148, international Summer School and Workshop, Oxford, UK, April 2000, Revised Lectures (2002).

[12] R. Backhouse, Regular algebra applied to language problems, Journal of Logic and Algebraic Programming 66, pp. 71–111 (2006).

[13] J. Conway, Regular Algebra and Finite Machines, Chapman and Hall, London (1971).

[14] R. C. Backhouse, J. van den Eijnde, A. van Gasteren, Calculating path algorithms, Science of Computer Programming 22 (1–2), pp. 3–19 (1994).

[15] D. Knuth, J. Morris, V. Pratt, Fast pattern matching in strings, SIAM Journal of Computing 6, pp. 325–350 (June 1977).

[16] P. Weiner, Linear pattern matching algorithms, in: Conf. Record IEEE 14th Annual Symposium on Switching and Automata, pp. 1–11 (1973).
[17] A. V. Aho, M. J. Corasick, Efficient string matching: An aid to bibliographic search, Communications of the ACM 18 (6) pp. 333–340 (1975).
[18] R. Backhouse, R. Lutz, Factor graphs, failure functions and bi-trees, in: A. Salomaa, M. Steinby (Eds.), Fourth Colloquium on Automata, Languages and Programming, Springer-Verlag, LNCS 52, pp. 61–75 (July 1977).
[19] R. Backhouse, Factor theory and the unity of opposites, J. Logical and Algebraic Methods in Programming 85 (5), pp. 824–846 (2016). doi:10.1016/j.jlamp.2016.01.003.
URL `http://dx.doi.org/10.1016/j.jlamp.2016.01.003`
[20] J. Brzozowski, Roots of star events, Journal of the ACM 14 (3), pp. 466–477 (July 1967).
[21] J. Riguet, Relations binaires, fermetures, correspondances de Galois, Bulletin de la Société Mathématique de France 76, pp.114–155 (1948).
[22] P. Freyd, A. Ščedrov, Categories, Allegories, North-Holland, (1990).
[23] G. Schmidt, T. Ströhlein, Relations and Graphs, Discrete Mathematics for Computer Scientists, EATCS Monographs on Theoretical Computer Science, Springer-Verlag, Berlin Heidelberg (1993).
[24] R. Backhouse, J. v. d. Woude, Demonic operators and monotype factors, Mathematical Structures in Computer Science 3 (4), pp. 417–433 (December 1993).
[25] T. S. Voermans, Inductive datatypes with laws and subtyping – a relational model, Ph.D. thesis, Department of Mathematics and Computer Science, Technische Universiteit Eindhoven (1999). doi:10.6100/IR519811.
[26] F. Rietman, A note on extensionality, in: J. van Leeuwen (Ed.), Proceedings Computer Science in the Netherlands 91, pp. 468–483 (1991).
[27] R. S. Bird, O. de Moor, Algebra of Programming, Prentice-Hall International, (1997).
[28] J. N. Oliveira, Programming from metaphorisms, Journal of Logical and Algebraic Programming Methods in Programming 94, pp. 15–44 (2018).
[29] R. McNaughton, The loop complexity of pure-group events, Info. and Control 11, pp. 167–176 (1967).
[30] R. Backhouse, B. Carré, A comparison of Gaussian and Gauss-Jordan elimination in regular algebra, International Journal of Computer Mathematics 10, pp. 311–325 (1982). doi:10.1080/00207168208803290.
[31] T. H. Cormen, C. E. Leiserson, R. L. Rivest, Introduction to Algorithms, MIT Electrical Engineering and Computer Science Series, MIT Press (1990).