Components and Acyclicity of Graphs
An Exercise in Point-Free Reasoning

Roland Backhouse[a,1,*], Henk Doornbos[b,2], Roland Glück[c,3], Jaap van der Woude[d,4]

[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*
[d] *Vakgroep Informatica, Technische Universiteit Eindhoven, The Netherlands*

Abstract

Central to algorithmic graph theory are the concepts of acyclicity and strongly connected components of a graph, and the related search algorithms. This document 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 the 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 acyclity and strongly connected components play a central role. This paper is about formulating and

*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.

[3] Declaration of interests: none.

[4] Declaration of interests: none.

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" 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 very sparingly. Finally, section 7 gives point-free 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 point-free 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 $\perp\!\!\perp$. That is,

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

(We use the notation $\top\!\!\top$ and $\perp\!\!\perp$ rather than the more common $\top$ and $\perp$ 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:

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

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

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

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

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

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

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,

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

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". Because this document is primarily about point-free reasoning, 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

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

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

□

We sometimes use "point" instead of "proper atom" in informal discussion. Formal statements always make clear what is meant.

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

$$\langle\forall p :: p = \langle\cup a : atom.a \wedge a \subseteq p : a\rangle\rangle \quad .$$

□

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 relation $a \subseteq p$ 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 21 and 22, 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 $\mathcal{A}$,

$$\neg(a \subseteq p) \equiv a \subseteq -p \quad . \tag{17}$$

□

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

Lemma 18. A complete, universally distributive lattice is saturated iff its greatest element is saturated, i.e. iff

$$\top\!\!\top = \langle\cup a : atom.a : a\rangle \quad .$$

□

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

Lemma 19. 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 20. Suppose $\mathcal{A}$ is universally distributive. Then $\mathcal{A}$ is atomic equivales

$$\langle \forall q :: q = \perp\!\!\perp \;\; \equiv \;\; \langle \cup a : atom.a : a \rangle \cap q \; = \; \perp\!\!\perp \rangle \quad .$$

□

Lemma 21. If $p \neq \perp\!\!\perp$ and b is an atom, then $p = b \equiv p \subseteq b$. Also, if a and b are both proper atoms, $a = b \;\equiv\; a \cap b \neq \perp\!\!\perp$.

□

Atoms are *irreducible* in the following sense.

Lemma 22. 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 $\mathcal{A}$,

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

□

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

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

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

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

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

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

□

Lemma 25. 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 26. 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 27. 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 $\{b\colon \mathsf{atom}_{\mathcal{A}}.b\colon f.b\}$.

□

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. We assume familiarity with monoids.

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 28 (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*.

□

Although definition 28 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, 11] 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.

Our definition of a regular algebra does not postulate the existence of a star operator. A universally distributive regular algebra is what Conway [12, p.27] calls a "standard Kleene algebra".

The upper adjoints of $(R\circ)$ and $(\circ R)$ are called the (left and right) *factorisation* operators. Although these operators are important, we don't use them directly here; we use only the fact that they exist.

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

$$R^* = \langle \cup i : 0 \leq i : R^i \rangle \quad . \tag{29}$$

Another definition is

$$R^* = \langle \mu x :: I \cup R \cup x \circ x \rangle \quad . \tag{30}$$

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

$$R^* = \langle \mu x :: I \cup R \circ x \rangle \tag{31}$$

and right iteration by

$$R^* = \langle \mu x :: I \cup x \circ R \rangle \quad . \tag{32}$$

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 commonly used being:

$$R^+ = \langle \cup i : 1 \leq i : R^i \rangle \tag{33}$$

and

$$R^+ = \langle \mu x :: R \cup x \circ x \rangle = \langle \mu x :: R \cup x \circ R \rangle = \langle \mu x :: R \cup R \circ x \rangle \quad . \tag{34}$$

Important properties of the star operator are as follows:

(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 a "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, 13]. 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 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 35 (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

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

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

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

□

Definition 36 (Reflexive and Transitive Reduction). Let A and B be events in a complemented regular algebra with unit I . Suppose the complement[5] 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 .
□

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

$$\mathsf{red}.A \;=\; A \cap \neg I \cap \neg((A \cap \neg I) \circ (A \cap \neg I)^+) \quad . \tag{37}$$

Theorem 38. 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 .
□

Theorem 38 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.

[5] In order to comply with later usage, this is the point at which we need to introduce a different symbol for complementation. The symbol " ¬ " 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.

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 point-free 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.

Atomicity properties will be introduced later: see section 6.

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,

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

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

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

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

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

$$R^\cup \subseteq S \;\equiv\; R \subseteq S^\cup \quad . \tag{39}$$

The Galois connection (39) 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

$$(R\circ S)^{\cup} \;=\; S^{\cup}\circ R^{\cup} \quad , \qquad (40)$$

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 $(\circ R)$ are universally distributive.

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 (since it is universally $\cup$-junctive) 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. J. Riguet [14] named the rule after the famous mathematician J.W.R. Dedekind (he called it “la relation de Dedekind”) because of its resemblance to the modular identity, a property of normal subgroups discovered by Dedekind. Schmidt and Ströhlein [15, 16] have adopted Riguet’s terminology (they refer to “die Dedekind Formel”, the Dedekind formula) whereas Freyd and Scedrov [17] call it the *law of modularity* (possibly for the same reason as Riguet). We call it the *modularity rule*.

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

$$R{\circ}S\cap T \;\subseteq\; R\circ(S \,\cap\, R^{\cup}\circ T) \quad . \tag{41}$$

An additional rule, sometimes called “Tarski’s rule”, is called the “cone rule” below: for all relations R,

$$\top\!\!\top\circ R\circ\top\!\!\top = \top\!\!\top \quad\vee\quad R = \bot\!\!\bot \quad . \tag{42}$$

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 modular identity. Suppose that the algebra is complemented (i.e. every relation has a complement); we denote the complement of relation R by $\neg R$. Consider the *middle-exchange rule*:

$$R\circ\neg X\circ S \subseteq \neg Y \quad\equiv\quad R^{\cup}\circ Y\circ S^{\cup} \subseteq X \quad . \tag{43}$$

The middle-exchange rule 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, due to Schröder, is the conjunction of the two equivalences: for all R, S and T,

$$R{\circ}S \subseteq T \quad\equiv\quad R^{\cup}\circ\neg T \subseteq \neg S \tag{44}$$

and

$$R{\circ}S \subseteq T \quad\equiv\quad \neg T\circ S^{\cup} \subseteq \neg R \quad . \tag{45}$$

We call these rules the *rotation rules* (because of the way the variables are rotated).

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 rule.

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" [16] and another is via "coreflexives[6]". 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 $R = R \circ \top\!\!\top$.

In the relational model, we assume, for example, that the universe $\mathcal{U}$ contains two unequal values true and false . The *coreflexive* representation of the set boolean is then defined to be the relation

$$\{(\mathsf{true},\mathsf{true}),(\mathsf{false},\mathsf{false})\} \quad .$$

The *right condition* representation of the set boolean is the relation

$$\{x{:}\,x{\in}\mathcal{U}{:}\,(x,\mathsf{true})\} \cup \{x{:}\,x{\in}\mathcal{U}{:}\,(x,\mathsf{false})\}$$

It is clear that for any given universe $\mathcal{U}$ there is a one-to-one correspondence between the subsets of $\mathcal{U}$ and the coreflexives. Equally clear is the existence of a one-to-one correspondence between the subsets of $\mathcal{U}$ and the right (or left) conditions on $\mathcal{U}$.

We choose to represent sets by coreflexives, there being several reasons for doing so. One is the simple fact that guarding both on the left and on the right of a relation is accomplished in one go with coreflexives whereas demanding two sorts of conditions (left and right conditions). Moreover, coreflexives have simple and convenient properties. Specifically, for all coreflexives p and q

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

The most compelling reason, however, for choosing to represent sets by coreflexives is the dominant position occupied by composition among programming primitives. Introducing a guard in the middle 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.

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 rôle 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.

[6] "Coreflexives" are also called "monotypes" [6, 18] or "tests" [10], depending on the intended interpretation. We now prefer the application-neutral terminology used by Freyd and Ščedrov [17].

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 46 (Right Domain). Define the function $>$ from relations to coreflexives by:

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

Then, 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 (46) 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.

Theorem 47. For all relations R, S and T

(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) $(R \circ \top\!\!\top \circ S){>} = S{>} \;\Leftarrow\; R \neq \perp\!\!\perp$.

□

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,

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

Then, for relations R and coreflexives p,

$$R{>\!\bullet} \supseteq p \;\;\equiv\;\; R \circ p = \perp\!\!\perp \quad . \tag{48}$$

Moreover, for all R,

$$(R{>}){>\!\bullet} = R{>\!\bullet} = (R{>\!\bullet}){>} \quad . \tag{49}$$

Note that (48) is a slightly disguised Galois connection. 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 50. Suppose a is an atomic coreflexive. Then

$$a{\circ}\top\!\!\top{\circ}a \;=\; a \quad . \tag{51}$$

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

$$a{\circ}\top\!\!\top{\circ}b \subseteq I \;\equiv\; a = b \quad . \tag{52}$$

□

We use lemma 50 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 atoms are events of the form $a{\circ}\top\!\!\top{\circ}b$ where a and b are atomic coreflexives; such an event models the pair (a,b) in conventional pointwise formulations of relation algebra.

Theorem 53. 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 as "points" and as "nodes" (when the relations represent graphs). 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:

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

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):

$$f \circ f^{\cup} \subseteq I \quad . \tag{54}$$

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. A relation that is both injective and functional is called a *bijection*.

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 $I \subseteq R^{\cup} \circ R$. R elation R is *surjective* iff its converse $R^{\cup}$ is total.

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 ,

$$(R \cap S) \circ f \ = \ R \circ f \cap S \circ f \quad . \tag{55}$$

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 the middle-exchange and rotation rules (see section 4). For example, the inclusion $R{\circ}S \subseteq \neg(T^{\cup})$ is only defined if R has type $A{\sim}B$, S has type $B{\sim}C$ and T has type $C{\sim}A$, for some sets A, B and C. (The converse $T^{\cup}$ of T then has type $A{\sim}C$, which equals the type of $\neg(T^{\cup})$ and $R{\circ}S$.) With these type restrictions, $S{\circ}T \subseteq \neg(R^{\cup})$ is also well-defined, and the two inclusions $R{\circ}S \subseteq \neg(T^{\cup})$ and $S{\circ}T \subseteq \neg(R^{\cup})$ are equal as per the rotation rule.

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 set 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 $A{\sim}A$.

Typed relation algebra, as briefly summarised above, extends category theory to what has been called *allegory theory*. See Freyd and Ščedrov [17] for more details.

8. Equivalence Relations and Partitions

This section begins our presentation of algorithmic graph theory in point-free relation algebra. 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 $a{\circ}G{\circ}b \neq \perp\!\!\perp$ represents the existence of an *edge* from a to b; if indeed $a{\circ}G{\circ}b \neq \perp\!\!\perp$, 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 $a \circ G^{*} \circ b \neq \perp\!\!\perp$. (The path itself is a sequence of nodes.)

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.

We begin by recalling some familiar, general, properties of equivalence relations. Section 8.1 formulates the well-known correspondence between partitions of a set and equivalence classes in a point-free style and section 8.2 explores properties of the equivalence-class function, in particular with respect to complementation.

8.1. Partitions

An *equivalence relation* is a relation that is reflexive, transitive and symmetric. 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,

$$a[\![R]\!]b \;\equiv\; f.a = f.b \quad . \tag{56}$$

(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 (56) to define a homogeneous relation R on A. The relation R is then an equivalence relation.

Equation (56) is expressed more succinctly by the point-free equation

$$R = f^{\cup} \circ f \quad . \tag{57}$$

Point-free formulations of functionality, totality, surjectivity and injectivity then support effective calculation. Here, for example, is the proof that it is transitive (in every detail, including the use of the associativity of composition).

$$\begin{array}{ll}
 & (f^{\cup} \circ f) \circ (f^{\cup} \circ f) \\
= & \{ \quad \text{composition is associative} \quad \} \\
 & f^{\cup} \circ (f \circ f^{\cup}) \circ f \\
\subseteq & \{ \quad f \text{ is functional, i.e. } f \circ f^{\cup} \subseteq I_C \,, \\
 & \quad\; \text{monotonicity of composition} \quad \} \\
 & f^{\cup} \circ I_C \circ f \\
= & \{ \quad I_C \text{ is identity of composition} \quad \} \\
 & f^{\cup} \circ f \quad .
\end{array}$$

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

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

maps (coreflexive) atoms a to equivalence classes of R (where Set is a so-called "coercion function" that maps a coreflexive of type $A {\sim} A$, for some A, to an atomic coreflexive of type 2^A). That is, $R = f^{\cup} \circ f$. The proof is straightforward, although somewhat long. See theorem 63 below.

Lemma 58. For all relations R, all coreflexives p and all proper atomic coreflexives b,

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

Proof We begin by translating from domains to conditions.

$$\begin{array}{ll}
 & p \subseteq (R \circ b)_< \\
= & \{ \quad p \text{ and } (R \circ b)_< \text{ are coreflexives} \quad \} \\
 & p \circ (R \circ b)_< \;=\; p \\
= & \{ \quad \text{coreflexive-condition isomorphism} \quad \} \\
 & p \circ R \circ b \circ \top\!\!\top \;=\; p \circ \top\!\!\top \quad .
\end{array}$$

Now we use a ping-pong argument to complete the calculation:

$$
\begin{array}{ll}
 & p{\circ}R{\circ}b{\circ}\top\!\!\top \;=\; p{\circ}\top\!\!\top \\
\Rightarrow & \quad \{ \quad \text{Leibniz} \quad \} \\
 & p{\circ}R{\circ}b{\circ}\top\!\!\top{\circ}b \;=\; p{\circ}\top\!\!\top{\circ}b \\
= & \quad \{ \quad b \text{ is an atomic coreflexive, so } b{\circ}\top\!\!\top{\circ}b = b \quad \} \\
 & p{\circ}R{\circ}b \;=\; p{\circ}\top\!\!\top{\circ}b \\
\Rightarrow & \quad \{ \quad \text{Leibniz} \quad \} \\
 & p{\circ}R{\circ}b{\circ}\top\!\!\top \;=\; p{\circ}\top\!\!\top{\circ}b{\circ}\top\!\!\top \\
= & \quad \{ \quad \text{cone rule, } b \neq \perp\!\!\perp \quad \} \\
 & p{\circ}R{\circ}b{\circ}\top\!\!\top \;=\; p{\circ}\top\!\!\top \quad .
\end{array}
$$

□

Corollary 59. If R is an equivalence relation, then for all proper atomic coreflexives 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 58 with $R,p,b := R,a,b$,

$$a \subseteq (R{\circ}b)_< \quad\equiv\quad a{\circ}R{\circ}b \;=\; a{\circ}\top\!\!\top{\circ}b \quad . \qquad (60)$$

Second,

$$
\begin{array}{ll}
 & (R{\circ}a)_< \subseteq (R{\circ}b)_< \\
\Rightarrow & \quad \{ \quad \text{assuming } R \text{ is reflexive, } a \subseteq (R{\circ}a)_< \quad \} \\
 & a \subseteq (R{\circ}b)_< \\
\Rightarrow & \quad \{ \quad \text{monotonicity} \quad \} \\
 & (R{\circ}a)_< \subseteq (R \circ (R{\circ}b)_<)_< \\
= & \quad \{ \quad \text{domains} \quad \} \\
 & (R{\circ}a)_< \subseteq (R{\circ}R{\circ}b)_< \\
\Rightarrow & \quad \{ \quad \text{assuming } R \text{ is transitive, } R{\circ}R \subseteq R\text{; monotonicity} \quad \} \\
 & (R{\circ}a)_< \subseteq (R{\circ}b)_< \quad .
\end{array}
$$

That is, if R is reflexive and transitive,

$$a \subseteq (R{\circ}b)_< \quad\equiv\quad (R{\circ}a)_< \subseteq (R{\circ}b)_< \quad . \qquad (61)$$

Moreover, if R is symmetric and a and b are coreflexives,

$$a{\circ}R{\circ}b \;=\; a{\circ}\top\!\!\top{\circ}b \quad\equiv\quad b{\circ}R{\circ}a \;=\; b{\circ}\top\!\!\top{\circ}a \quad . \qquad (62)$$

Thus, if R is an equivalence relation,

$$(R\circ a)_< = (R\circ b)_<$$
$= \quad \{ \quad$ anti-symmetry $\quad \}$
$$(R\circ a)_< \subseteq (R\circ b)_< \quad \wedge \quad (R\circ b)_< \subseteq (R\circ a)_<$$
$= \quad \{ \quad (61) \quad \}$
$$a \subseteq (R\circ b)_< \quad \wedge \quad b \subseteq (R\circ a)_<$$
$= \quad \{ \quad (60) \quad \}$
$$a\circ R\circ b = a\circ\top\!\!\top\circ b \quad \wedge \quad b\circ R\circ a = b\circ\top\!\!\top\circ a$$
$= \quad \{ \quad (62) \quad \}$
$$a\circ R\circ b = a\circ\top\!\!\top\circ b \quad .$$
□

Theorem 63. Suppose R is an equivalence relation. Let the function f be defined to be $\langle a :: \mathsf{Set}\,.(R\circ a)_<\rangle$. Then $R = f^\cup\circ f$ and $f = f\circ R$.

Proof

$$R$$
$= \quad \{ \quad$ saturation assumption: theorem 53 $\quad \}$
$$\langle\cup a,b : a\circ R\circ b \neq \perp\!\!\perp : a\circ\top\!\!\top\circ b\rangle$$
$= \quad \{ \quad$ all-or-nothing rule (section 6) $\quad \}$
$$\langle\cup a,b \;:\; a\circ R\circ b = a\circ\top\!\!\top\circ b \;:\; a\circ\top\!\!\top\circ b\rangle$$
$= \quad \{ \quad$ corollary 59 $\quad \}$
$$\langle\cup a,b : (R\circ a)_< = (R\circ b)_< : a\circ\top\!\!\top\circ b\rangle$$
$= \quad \{ \quad$ definition of $f \quad \}$
$$\langle\cup a,b \;:\; a\circ f^\cup\circ f\circ b = a\circ\top\!\!\top\circ b \;:\; a\circ\top\!\!\top\circ b\rangle$$
$= \quad \{ \quad$ saturation assumption: theorem 53 $\quad \}$
$$f^\cup\circ f$$

and

$$f\circ R$$
$= \quad \{ \quad$ above $\quad \}$
$$f\circ f^\cup\circ f$$
$= \quad \{ \quad f$ is a function, so $f\circ f^\cup \subseteq I$ and hence $f\circ f^\cup = f_< \quad \}$
$$f_<\circ f$$
$= \quad \{ \quad$ domains $\quad \}$
$$f \quad .$$
□

8.2. Properties of the Partition Function

In section 8.1, the function $\langle a :: \mathsf{Set}\,.(R\circ a)_<\rangle$ was shown to map a proper atomic coreflexive a into the set of proper atoms equivalent to a under the (equivalence) relation

R . This section is about exploring the properties of the endofunction $\langle p : p \subseteq I : (R{\circ}p){<} \rangle$. We show that it is a complementation-fixed closure operator.

To avoid clutter, we use the convention that lower case identifiers p and q range over coreflexives. So the function of interest is $\langle p :: (R{\circ}p){<} \rangle$.

Recalling definition 24 of complementation-fixed and noting that, for all relations R , $R{\bullet\!<} = {\sim}(R{<})$, we explore conditions under which

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

beginning with the inclusion. Note how the calculation below is used to determine simpler conditions on R and p for which the more complicated inclusion holds.

Lemma 64. For arbitrary relations R and S ,

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

Proof We have

$$
\begin{array}{ll}
 & (R \circ (R{\circ}S){\bullet\!<}){<} \;\subseteq\; (R{\circ}S){\bullet\!<} \\
= & \quad \{ \quad \text{domain-conditional isomorphism} \quad \} \\
 & R \circ (R{\circ}S){\bullet\!<} \circ \top\!\!\top \;\subseteq\; (R{\circ}S){\bullet\!<} \circ \top\!\!\top \\
= & \quad \{ \quad \text{property of negated left domain} \quad \} \\
 & R \circ \neg(R{\circ}S{\circ}\top\!\!\top) \;\subseteq\; \neg(R{\circ}S{\circ}\top\!\!\top) \\
= & \quad \{ \quad \text{rotation rule, double negation and converse} \quad \} \\
 & \top\!\!\top \circ S^{\cup} \circ R^{\cup} \circ R \;\subseteq\; \top\!\!\top \circ S^{\cup} \circ R^{\cup} \\
\Leftarrow & \quad \{ \quad \text{monotonicity of composition} \quad \} \\
 & R^{\cup} \circ R \;\subseteq\; R^{\cup} \quad .
\end{array}
$$

□

Corollary 65. If R is an equivalence relation, for all S ,

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

In words, if R is an equivalence relation, $(R{\circ}S){\bullet\!<}$ is a fixed point of the function mapping coreflexive p to $(R{\circ}p){<}$.

Proof We have:

$$
\begin{array}{ll}
 & (R \circ (R{\circ}S){\bullet\!<}){<} \\
\subseteq & \quad \{ \quad R \text{ is an equivalence relation, so } R^{\cup}{\circ}R \subseteq R^{\cup} \text{ , lemma 64} \quad \} \\
 & (R{\circ}S){\bullet\!<} \\
= & \quad \{ \quad I \text{ is unit of composition; } (R{\bullet\!<}){<} = R{\bullet\!<} \text{ for all } R \text{, with } R := R{\circ}S \quad \} \\
 & (I \circ (R{\circ}S){\bullet\!<}){<} \\
\subseteq & \quad \{ \quad R \text{ is an equivalence relation, so } I \subseteq R \text{ ,} \\
 & \qquad\quad \text{monotonicity of composition and domains} \quad \} \\
 & (R \circ (R{\circ}S){\bullet\!<}){<} \quad .
\end{array}
$$

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

Lemma 66. If R is reflexive and transitive, the function $\langle p :: (R\circ p)< \rangle$ is a closure operator.

Proof The equivalence in definition 23 of a closure operator is established by mutual implication. Implication:

$$
\begin{array}{ll}
 & (R\circ q)< \\
\subseteq & \{ \quad \text{assume } q \subseteq (R\circ p)< \text{, monotonicity} \quad \} \\
 & (R \circ (R\circ p)<)< \\
= & \{ \quad \text{domains} \quad \} \\
 & (R\circ R\circ p)< \\
\subseteq & \{ \quad R \text{ is transitive} \quad \} \\
 & (R\circ p)<
\end{array}
$$

and follows-from:

$$
\begin{array}{ll}
 & q \subseteq (R\circ p)< \\
\Leftarrow & \{ \quad \text{assume } (R\circ q)< \subseteq (R\circ p)< \text{, transitivity of } \subseteq \quad \} \\
 & q \subseteq (R\circ q)< \\
\Leftarrow & \{ \quad R \text{ is reflexive, i.e. } I \subseteq R \quad \} \\
 & q \subseteq (I\circ q)< \\
= & \{ \quad \text{domains} \quad \} \\
 & \mathsf{true} \quad .
\end{array}
$$

□

Theorem 67. If R is an equivalence relation, the function $\langle p : p \subseteq I : (R\circ p)< \rangle$ 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 $\mathsf{Fix}.\langle p :: (R\circ p)< \rangle$ 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 $\langle p :: (R\circ p)< \rangle$ is a closure operator by lemma 66 and, hence, complementation-idempotent by corollary 65. It is thus also complementation-fixed by lemma 25.

If R is an equivalence relation on a complete, universally distributive lattice, the completeness and saturation properties are given by theorem 27.
□

Lemma 68. Suppose R is an equivalence relation on a saturated atomic lattice. Then

$$\langle \cup a : \mathsf{AC}.a : (R\circ a)< \rangle \;=\; I \quad .$$

(AC abbreviates atomic coreflexive.)

Proof

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

□

Note that, as already observed, the function $\langle p :: (R \circ p)_< \rangle$ is the lower adjoint in a Galois connection of the coreflexives (ordered by the subset relation) with itself. Thus, if R is an equivalence relation, the function is universally distributive, as well as being a complementation-fixed and complementation-idempotent closure operator.

9. Acyclic 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 130— is important in path-finding algorithms as well as the seemingly unrelated problem of efficiently representing the inverse of a real matrix.

This section studies algorithmic properties of acyclic graphs. (Point-free) relation algebra is the appropriate vehicle for such a study because a graph can be viewed as a relation, G say, over a finite universe (the nodes of the graph). That there exists an edge from node a to b is then expressed, using the all-or-nothing rule, as $a \circ G \circ b = a \circ \top\!\!\top \circ b$.

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 so-called "topological ordering". The definition of a topological ordering and the algorithm for topological search are formulated in point-free relation algebra.

Many of the theorems we present are valid for arbitrary relations, but some only for relations over a finite universe. In order to make the distinction, 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. But, conversely, an infinite path in a finite graph is 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 69 ((Right/Left) Definite). Relation R is said to be *right-definite* if and only if it satisfies

$$\langle \forall p :: p \subseteq \perp\!\!\perp \Leftarrow p \subseteq (p \circ R^+)_> \rangle \quad . \tag{70}$$

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

$$\langle \forall p :: p \subseteq \perp\!\!\perp \Leftarrow p \subseteq (R^+ \circ p)_< \rangle \quad . \tag{71}$$

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 77 and 79 for the formalisation of this argument.)

Note that R is right-definite equivales that its converse $R^\cup$ is left-definite (because $(R^\cup)^+ = (R^+)^\cup$ and so $(p \circ R^+)_> = ((R^\cup)^+ \circ p)_<$). 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 72 (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 72 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.

For later use, we note the following simple lemma.

Lemma 73. Suppose R is left definite and $R \supseteq S$. Then S is left definite. The same is true with "right" replacing "left".

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

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, (70) 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.

Anticipating the definition of acyclicity (definition 75), we rephrase right-definiteness in terms of atomic coreflexives.

Lemma 74. For all atomic coreflexives a,

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

It follows that, if R is right-definite, then for all atomic coreflexives a,

$$a \subseteq \bot\!\!\bot \;\Leftarrow\; a \subseteq R^+ \quad .$$

Proof Suppose a is an atomic coreflexive. Then

$$\begin{array}{ll} & a \subseteq R^+ \\ \Rightarrow & \{ \quad a \text{ is coreflexive, so } (a{\circ}a)_{>} = a \text{ ; monotonicity} \quad \} \\ & a \subseteq (a \circ R^+)_{>} \\ \Rightarrow & \{ \quad a{\circ}\top\!\!\top{\circ}a = a \text{ , monotonicity} \quad \} \end{array}$$

$$a \;\subseteq\; a\circ\top\!\!\top\circ(a\circ R^+)_>$$
$= \quad \{ \quad$ domains $\quad \}$
$$a \;\subseteq\; a\circ\top\!\!\top\circ a\circ R^+$$
$\Rightarrow \quad \{ \quad a\circ\top\!\!\top\circ a = a \subseteq I$, monotonicity and transitivity $\quad \}$
$$a \subseteq R^+ \quad .$$
□

We now define acyclicity:

Definition 75 (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 straightforward calculation shows that

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

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

Definition 75 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.

We now show that, for *finite* graphs, right (or left) definiteness equivales acyclicity. Lemma 76 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 76. A right-definite relation is acyclic. Symmetrically, a left-definite relation is acyclic.

Proof With a ranging over atomic coreflexives, we have

$$\mathsf{rightdefinite}.R$$
$\Rightarrow \quad \{ \quad$ definition 69 (with $p := a$) and lemma 74 $\quad \}$
$$\langle \forall a :: a \subseteq \perp\!\!\perp \Leftarrow a \subseteq R^+ \rangle$$
$\Rightarrow \quad \{ \quad$ the lattice of coreflexives is saturated, i.e. $\langle \cup a :: a \rangle \;=\; I \quad \}$
$$I \cap R^+ \;=\; \perp\!\!\perp$$
$= \quad \{ \quad$ definition 75 $\quad \}$
$$\mathsf{acyclic}.R \quad .$$

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

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

Lemma 77. Suppose p is a coreflexive such that $p \neq \perp\!\!\perp$ and $p \subseteq (p \circ G^+)\!>$. Suppose a is a proper atomic coreflexive such that $a \subseteq p$. Then, with AC abbreviating atomic coreflexive, we have

$$\left\langle \exists b \;:\; \mathsf{AC}.b \;:\; b \neq \perp\!\!\perp \;\wedge\; b \subseteq p \;\wedge\; a \subseteq (b \circ G^+)\!> \;\wedge\; (a \circ G^+)\!> \;\subseteq\; (b \circ G^+)\!> \right\rangle \;\; .$$

Proof The proof of (77) is in two stages. First,

$$\begin{array}{ll} & a \subseteq p \\ \Rightarrow & \{ \quad \text{assumption: } p \subseteq (p \circ G^+)\!>\text{, transitivity} \quad \} \\ & a \subseteq (p \circ G^+)\!> \\ = & \{ \quad \text{saturation assumption: definition 14, distributivity} \quad \} \\ & a \;\subseteq\; \langle \cup b : b \subseteq p : (b \circ G^+)\!> \rangle \\ \Rightarrow & \{ \quad a \text{ is a proper atom, irreducibility: lemma 22} \quad \} \\ & \langle \exists b : b \neq \perp\!\!\perp \wedge b \subseteq p : a \subseteq (b \circ G^+)\!> \rangle \;\; . \end{array}$$

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

$$\begin{array}{ll} & (a \circ G^+)\!> \\ \subseteq & \{ \quad \text{assumption, monotonicity} \quad \} \\ & ((b \circ G^+)\!> \circ\, G^+)\!> \\ = & \{ \quad \text{domains} \quad \} \\ & (b \circ G^+ \circ G^+)\!> \\ \subseteq & \{ \quad G^+ \text{ is transitive, monotonicity} \quad \} \\ & (b \circ G^+)\!> \;\; . \end{array}$$

□

Corollary 78. Suppose p is a coreflexive such that $p \neq \perp\!\!\perp$ and $p \subseteq (p \circ G^+)\!>$. Then it is possible to construct an infinite sequence of proper atomic coreflexives a_i such that

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

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 77 (with $a,b := a_i,a_{i+1}$). Because, for all i ,

$$(a_i \circ G^+)\!> \;\subseteq\; (a_{i+1} \circ G^+)\!>$$

it follows, by transitivity, that

$$\left\langle \forall i,j : i < j : (a_i \circ G^+)\!> \;\subseteq\; (a_j \circ G^+)\!> \right\rangle \;\; .$$

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

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

□

Lemma 79. Suppose G is a finite graph. Then G is right definite if G is acyclic.

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

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 78, construct an infinite sequence of nodes a_i such that

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

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

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

Hence,

$$
\begin{array}{ll}
 & \mathsf{true} \\
= & \{ \quad \text{lemma 74 (with } a,R := a_m,G \text{)} \quad \} \\
 & a_m \subseteq G^{+} \\
\Rightarrow & \{ \quad a_m = I \cap a_m \text{, monotonicity} \quad \} \\
 & a_m \subseteq I \cap G^{+} \\
\Rightarrow & \{ \quad \perp\!\!\perp \neq a_m \text{, } \perp\!\!\perp \text{ is the least element} \quad \} \\
 & \perp\!\!\perp \neq I \cap G^{+} \quad .
\end{array}
$$

That is, G is not acyclic.
□

Corollary 80. Suppose G is a finite graph. Then G is definite if G is acyclic.

Proof Straightforward combination of lemma 79 and properties of converse. First,

$$
\begin{array}{ll}
 & \mathsf{true} \\
= & \{ \quad \text{lemma 79} \quad \} \\
 & \langle \forall G : \mathsf{finite}.G : \mathsf{leftdefinite}.G \Leftarrow \mathsf{acyclic}.G \rangle \\
= & \{ \quad \text{converse is a bijection} \quad \} \\
 & \langle \forall G : \mathsf{finite}.G^{\cup} : \mathsf{leftdefinite}.G^{\cup} \Leftarrow \mathsf{acyclic}.G^{\cup} \rangle \\
= & \{ \quad \mathsf{finite}.G^{\cup} = \mathsf{finite}.G \text{, } \mathsf{leftdefinite}.G^{\cup} = \mathsf{rightdefinite}.G \text{,} \\
 & \quad\; \mathsf{acyclic}.G^{\cup} = \mathsf{acyclic}.G \quad \} \\
 & \langle \forall G : \mathsf{finite}.G : \mathsf{rightdefinite}.G \Leftarrow \mathsf{acyclic}.G \rangle \quad .
\end{array}
$$

So

$$
\begin{array}{ll}
 & \mathsf{true} \\
= & \{ \quad \text{lemma 79 and above} \quad \} \\
 & \quad \langle \forall G : \mathsf{finite}.G : \mathsf{leftdefinite}.G \Leftarrow \mathsf{acyclic}.G \rangle
\end{array}
$$

$$
\begin{array}{ll}
 & \wedge \quad \langle \forall G : \mathsf{finite}.G : \mathsf{rightdefinite}.G \Leftarrow \mathsf{acyclic}.G \rangle \\
= & \qquad \{ \quad \text{predicate caculus} \quad \} \\
 & \langle \forall G : \mathsf{finite}.G : \mathsf{leftdefinite}.G \wedge \mathsf{rightdefinite}.G \Leftarrow \mathsf{acyclic}.G \rangle \\
= & \qquad \{ \quad \mathsf{leftdefinite}.G \wedge \mathsf{rightdefinite}.G \equiv \mathsf{definite}.G \quad \} \\
 & \langle \forall G : \mathsf{finite}.G : \mathsf{definite}.G \Leftarrow \mathsf{acyclic}.G \rangle \quad .
\end{array}
$$

□

To summarise, we have the following theorem.

Theorem 81. If G is a finite graph, G is acyclic equivales G is definite.

Proof Straightforward combination of corollary 76 and corollary 80.
□

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 36. The definition of the function red is quite complicated. For an acyclic graph, it can be simplified:

Lemma 82. If G is an acyclic graph, then $G = G\cap\neg I$. So

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

Proof

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

The formula for $\mathsf{red}.G$ follows by instantiating (37) and replacing G by $G\cap\neg I$.
□

Theorem 83. The least starth root of a finite, acyclic graph is its reflexive-transitive reduction. That is, for all finite, acyclic graphs G ,

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

Proof By theorem 38, it suffices to prove the lefthand conjunct.

$$
\begin{array}{ll}
& (\mathsf{red}.G)^* \ = \ G^* \\
= & \{ \quad \mathsf{red}.G \subseteq G \text{ and } G \text{ is acyclic,} \\
& \quad \text{so } \mathsf{red}.G \text{ is right-definite (theorem 81 and lemma 73)} \\
& \quad \text{UEP of relation algebra: theorem 72} \quad \} \\
& G^* \ = \ I \cup \mathsf{red}.G \circ G^* \\
\Leftarrow & \{ \quad G^* = I \cup G^+ \text{, Leibniz} \quad \} \\
& G^+ \ = \ \mathsf{red}.G \circ G^* \\
= & \{ \quad G \text{ is acyclic and hence (theorem 81) left-definite,} \\
& \quad \text{UEP of relation algebra: theorem 72} \quad \} \\
& G^+ \ = \ \mathsf{red}.G \cup G^+ \circ G \\
= & \{ \quad \text{lemma 82} \quad \} \\
& G^+ \ = \ (G \cap \neg(G \circ G^+)) \cup G^+ \circ G \\
= & \{ \quad G \circ G^+ = G^+ \circ G \text{ and absorption rule of set calculus} \quad \} \\
& G^+ \ = \ G \cup G^+ \circ G \\
= & \{ \quad \text{fixed-point definition of reflexive-transitive closure} \quad \} \\
& \mathsf{true} \ .
\end{array}
$$

□

Observe that the proof of theorem 83 uses the fact that an acyclic graph is both left- and right-definite. 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.

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 point-free definition of $\mathsf{reachable}.R.p$ is therefore:

$$
\mathsf{reachable}.R.p \ = \ (p{\circ}R^*)\!> \quad . \tag{84}
$$

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 $x \in p \cap (p{\circ}R)\!\succ\!\bullet$. Replacing the intersection by a composition of coreflexives, the set $\mathsf{minimal}.R.p$ of minimal elements of p is thus defined as:

$$\mathsf{minimal}.R.p \;=\; p\circ(p{\circ}R){>\!\!\bullet} \tag{85}$$

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

$$\mathsf{reachable}.R.p \;=\; \mathsf{reachable}.R.(\mathsf{minimal}.R.p) \quad . \tag{87}$$

More generally, for all coreflexives p and q,

$$\mathsf{reachable}.R.p \subseteq \mathsf{reachable}.R.q \;\;\Leftarrow\;\; \mathsf{minimal}.R.p \subseteq q \quad . \tag{88}$$

Proof Assume that R is right-definite. We prove (87) by mutual inclusion. One inclusion is easy. From the definition (84) it is clear that $\mathsf{reachable}.R$ is a monotone function. Furthermore from (85) 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 have to use the assumption of right-definiteness, but how? We have to prove that

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

the *righthand* side of which contains 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 (88).)

$$\begin{array}{ll}
 & \mathsf{reachable}.R.p \subseteq \mathsf{reachable}.R.q \\
= & \quad \{ \quad \text{definition reachables: (84)} \quad \} \\
 & \mathsf{reachable}.R.p \subseteq (q{\circ}R^*){>} \\
= & \quad \{ \quad \text{coreflexive-condition isomorphism} \quad \} \\
 & \top\!\top\circ\mathsf{reachable}.R.p \subseteq \top\!\top\circ(q{\circ}R^*){>} \\
= & \quad \{ \quad \text{domains: } \top\!\top{\circ}X = \top\!\top\circ X{>} \quad \} \\
 & \top\!\top\circ\mathsf{reachable}.R.p \subseteq \top\!\top{\circ}q{\circ}R^* \quad .
\end{array}$$

Now we can invoke the right-definiteness of R. From the discussion of theorem 72 on the uep of relation algebra it follows that, for right-definite relation R, relation $\top\!\top{\circ}q{\circ}R^*$ is the greatest fixed point of the function $\langle X :: \top\!\top{\circ}q \cup X{\circ}R\rangle$. Exploitation of this fact is the main step in the following calculation. The first two steps help to make this possible. Note that only the follows-from is needed in the second step. However, the fact that it is an equality step aids understanding the heuristics of the calculation. (Equality steps of this nature are safe. Follows-from steps may lead to dead ends.)

$$
\begin{array}{ll}
 & \top\!\!\top \circ \mathsf{reachable}.R.p \;\subseteq\; \top\!\!\top\circ q\circ R^* \\
= & \{ \quad \text{definition } \mathsf{reachable}: (84); \\
 & \quad\;\; \text{domains: } \top\!\!\top\circ X = \top\!\!\top \circ X{>}\,;\; R^* = R^*\circ R^* \quad \} \\
 & \top\!\!\top\circ p\circ R^* \;\subseteq\; \top\!\!\top\circ q\circ R^*\circ R^* \\
= & \{ \quad (\Leftarrow) \text{ monotonicity; } (\Rightarrow) \text{ reflexivity and transitivity of } R^* \\
 & \quad\;\; \text{(only follows-from is needed)} \quad \} \\
 & \top\!\!\top\circ p \;\subseteq\; \top\!\!\top\circ q\circ R^* \\
\Leftarrow & \{ \quad R \text{ is right-definite: } \top\!\!\top\circ q\circ R^* = \langle \nu X :: \top\!\!\top\circ q\cup X\circ R\rangle\,; \\
 & \quad\;\; \text{fixed-point induction} \quad \} \\
 & \top\!\!\top\circ p \;\subseteq\; \top\!\!\top\circ q \cup \top\!\!\top\circ p\circ R \\
= & \{ \quad \text{distribution of composition over union;} \\
 & \quad\;\; \text{domains: } \top\!\!\top\circ X = \top\!\!\top \circ X{>} \quad \} \\
 & \top\!\!\top\circ p \;\subseteq\; \top\!\!\top\circ(q\cup p\circ R){>} \\
= & \{ \quad \text{coreflexive-condition isomorphism} \quad \} \\
 & p \;\subseteq\; (q\cup p\circ R){>} \\
= & \{ \quad \text{domain operator is } \cup\text{-junctive} \quad \} \\
 & p \;\subseteq\; q\cup(p\circ R){>} \\
= & \{ \quad \text{shunting in the coreflexive lattice} \quad \} \\
 & p\circ(p\circ R){>\!\bullet} \;\subseteq\; q \\
= & \{ \quad \text{definition (85)} \quad \} \\
 & \mathsf{minimal}.R.p \subseteq q \quad .
\end{array}
$$

With this calculation we have established the property (88). 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 (88). 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 definition 70. So, another formulation of a relation R being right-definite is: for all coreflexives p ,

$$p\subseteq \bot\!\!\bot \quad\Leftarrow\quad \mathsf{minimal}.R.p \subseteq \bot\!\!\bot \quad , \qquad (89)$$

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

$$p\neq \bot\!\!\bot \quad\Rightarrow\quad \mathsf{minimal}.R.p \neq \bot\!\!\bot \quad . \qquad (90)$$

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

Now we consider the converse of lemma 86. Is it true that a graph with property (87) is left-definite? This question can be answered affirmatively and the proof is simple. We show that a relation satisfying (87) also satisfies (89).

$$
\begin{array}{ll}
 & \mathsf{minimal}.R.p \;=\; \perp\!\!\perp \\
\Rightarrow & \quad \{ \quad \text{Leibniz} \quad \} \\
 & \mathsf{reachable}.R.(\mathsf{minimal}.R.p) = \mathsf{reachable}.R.\perp\!\!\perp \\
= & \quad \{ \quad \text{assumption: } \mathsf{reachable}.R.(\mathsf{minimal}.R.p) \;=\; \mathsf{reachable}.R.p\,; \\
 & \quad\quad\;\; \text{definition of } \mathsf{reachable}:\ (84) \quad \} \\
 & \mathsf{reachable}.R.p = (\perp\!\!\perp{\circ}R^*)> \\
= & \quad \{ \quad \text{definition of } \mathsf{reachable}:\ (84); \\
 & \quad\quad\;\; \perp\!\!\perp \text{ is zero of composition} \quad \} \\
 & (p{\circ}R^*)> = \perp\!\!\perp \\
\Rightarrow & \quad \{ \quad I \subseteq R^* \quad \} \\
 & p \subseteq \perp\!\!\perp \quad .
\end{array}
$$

We thus conclude:

Theorem 91. Relation R is right-definite equivales for all coreflexives p,

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

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

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

□

9.4. Topological Search

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

Definition 92 (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:

$$ord \circ ord^{\cup} \subseteq I_{\mathbb{N}} \;\wedge\; I_A = ord^{\cup} \circ ord \;\wedge\; R^+ \subseteq ord^{\cup} \circ \mathsf{less} \circ ord \quad . \tag{93}$$

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 94. 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

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

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

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

□

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 95. 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 Suppose p is a coreflexive of type A. Then

$$
\begin{array}{ll}
 & p \subseteq (p \circ ord^\cup \circ \mathsf{less} \circ ord)_> \\
\Rightarrow & \{ \quad \text{monotonicity} \quad \} \\
 & (p \circ ord^\cup)_> \ \subseteq \ ((p \circ ord^\cup \circ \mathsf{less} \circ ord)_> \circ ord^\cup)_> \\
= & \{ \quad \text{domains} \quad \} \\
 & (p \circ ord^\cup)_> \ \subseteq \ (p \circ ord^\cup \circ \mathsf{less} \circ ord \circ ord^\cup)_> \\
\Rightarrow & \{ \quad ord \text{ is functional, i.e. } ord \circ ord^\cup \subseteq I \text{ ,} \\
 & \quad \text{monotonicity and transitivity} \quad \} \\
 & (p \circ ord^\cup)_> \ \subseteq \ (p \circ ord^\cup \circ \mathsf{less})_> \\
\Rightarrow & \{ \quad \mathsf{less} \text{ is well-founded, i.e. right definite} \quad \} \\
 & (p \circ ord^\cup)_> \ \subseteq \ \perp\!\!\perp \\
= & \{ \quad \text{domains} \quad \} \\
 & p \circ ord^\cup \ \subseteq \ \perp\!\!\perp \\
\Rightarrow & \{ \quad ord \text{ is total (i.e. } I \subseteq ord^\cup \circ ord \text{),} \\
 & \quad \text{monotonicity and } \perp\!\!\perp \text{ is zero of composition} \quad \}
\end{array}
$$

$p \subseteq \perp\!\!\!\perp$.

Thus, by definition, $ord^{\cup} \circ \mathsf{less} \circ ord$ is right-definite.

□

Lemma 95 is the basis of the use of so-called "bound functions" to establsh 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 95 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 96. Suppose R is a homogeneous relation of type A. Suppose ord is a topological ordering of R. Then R is right-definite.

Proof Immediate from lemmas 73, 94 and 95.

□

We now want to consider the converse of corollary 96. 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 algorithm is shown below. The input to the algorithm is a finite, acyclic graph G and the output is a total, injective function ord mapping the nodes of G to the set $\mathbb{N}$ of natural numbers. During execution of the algorithm, ord is a total, injective function mapping the nodes that have been "seen" to $\mathbb{N}$. The algorithm uses four additional variables: $seen$ is a coreflexive representing the nodes of the graph that have been "seen", g is a graph representing the subgraph of G that has not been "seen", k is a natural number that counts the nodes that have been "seen", and b is a node that is chosen at each iteration as the next "seen" node. The criterion for choosing b is that it has not yet been "seen" and there are no edges to b in the graph g. After choosing b, all edges from b are removed from the graph g. The algorithm terminates when all nodes have been "seen".

The overbar notation, as in $\overline{\{k\}}$, is used to denote the mapping from a set to its representation as a coreflexive. The symbol " $\top\!\!\!\top$ " in " $\overline{\{k\}}\circ\top\!\!\!\top\circ b$ " denotes the universal relation of type $\mathbb{N}{\leftarrow}A$. The expression $\overline{\{k\}}\circ\top\!\!\!\top\circ b$ is the point-free representation of $\{(k,b)\}$. The assignment to ord thus extends its right domain to include the node b, assigning it the value of k in the topological ordering. The two occurrences of " $\perp\!\!\!\perp$ " in the two initial assignments have different types: the first has type $A{\leftarrow}A$ whilst the second has type $\mathbb{N}{\leftarrow}A$. Generally, we overload the symbol " $\perp\!\!\!\perp$ " in this way, leaving the reader to infer the type. We have, however, distinguished between I_A (the identity relation on nodes) and $I_{\mathbb{N}}$ (the identity relation on natural numbers) in order to enhance the reader's understanding of the postcondition.

$\{ \ \ \mathsf{acyclic}.G \ \ \}$

$seen{,}g \ := \ \perp\!\!\!\perp{,}G \ ; \ ord{,}k \ := \ \perp\!\!\!\perp{,}0$

$;\ \{$ Invariant: (97) $\wedge$ (98) $\wedge$ (99) $\wedge$ (100) below $\}$

while $seen \neq I_A$ **do**

begin

choose arbitrary node b such that $g \circ b = \perp\!\!\perp \wedge \sim\! seen \circ b = b$

$;\ seen, g \ := \ seen \cup b \ , \ g \cap \neg(b \circ g)$

$;\ ord, k \ := \ ord \cup \overline{\{k\}} \circ \top\!\!\top \circ b \ , \ k{+}1$

end

$\{ \quad ord \circ ord^{\cup} \subseteq I_{\mathbb{N}} \ \wedge \ I_A = ord^{\cup} \circ ord \ \wedge \ G^{+} \subseteq ord^{\cup} \circ \mathsf{less} \circ ord \quad \}$

The invariant is the conjunction of

$$g = \sim\! seen \circ G \circ \sim\! seen \quad , \tag{97}$$

$$\sim\! seen \circ G \circ seen = \perp\!\!\perp \quad , \tag{98}$$

$$ord \circ ord^{\cup} = \overline{\{j \mid 0 \leq j < k\}} \quad \wedge \quad ord^{\cup} \circ ord = seen \quad , \quad \text{and} \tag{99}$$

$$seen \circ G^{*} \circ seen \subseteq ord^{\cup} \circ \mathsf{atmost} \circ ord \quad . \tag{100}$$

The algorithm clearly terminates since the size of the set represented by $seen$ increases by one at each iteration.

In order to verify that the algorithm meets its specification, there are three tasks remaining.

1. Establish that each of (97), (98), (99) and (100) is truthified by the initialisation, and that the truth of each is invariant under execution of the loop body.
2. Prove that it is possible to choose a node b in accordance with the criterion for its choice.
3. Prove that the stated postcondition is a logical consequence of the invariant property and the condition for termination of the loop.

These tasks are relatively straightforward but lengthy. For reasons of brevity, we omit the details. Full details can be found in [1].

The conclusion of this section is the following theorem.

Theorem 101. 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

$$
\begin{array}{ll}
 & I \cap G^{+} \\
\subseteq & \{ \quad \text{definition: (93)} \quad \} \\
 & ord^{\cup} \circ ord \cap ord^{\cup} \circ \mathsf{less} \circ ord \\
= & \{ \quad \text{by definition (93), } ord \text{ is a total function; distributivity} \quad \} \\
 & ord^{\cup} \circ (I \cap \mathsf{less}) \circ ord \\
= & \{ \quad I \cap \mathsf{less} = \perp\!\!\perp \text{ ; } \perp\!\!\perp \text{ is zero of composition} \quad \} \\
 & \perp\!\!\perp \quad .
\end{array}
$$

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 102) 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 102. Suppose p is a coreflexive and R is a relation. We say that p *is i-connected by* R iff $p \circ \top\!\top \circ p \subseteq R$. We say that p is a *component* of R iff p is i-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, i-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.

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

Lemma 103. For all coreflexives p and relations R,

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

Proof This is proved by mutual implication as follows.

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

□

Obvious corollaries of lemma 103 are:

Corollary 104.

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

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

(c) The following are all equivalent:

- **(i)** p is i-connected by R
- **(ii)** p is i-connected by $R^{\cup}$
- **(iii)** p is i-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 proved by mutual implication:

$$
\begin{array}{ll}
& p{\circ}\top\!\!\top{\circ}p = p{\circ}R{\circ}p \;\;\wedge\;\; p{\circ}\top\!\!\top{\circ}p = p{\circ}S{\circ}p \\
\Rightarrow & \{ \quad \text{idempotency of intersection} \quad \} \\
& p{\circ}\top\!\!\top{\circ}p \;=\; p{\circ}R{\circ}p \cap p{\circ}S{\circ}p \\
= & \{ \quad p{\circ}(R{\cap}S) = p{\circ}R \cap p{\circ}S \;\text{ and }\; (R{\cap}S){\circ}p = R{\circ}p \cap S{\circ}p \\
& \quad\;\; \text{for all coreflexives } p \text{ and relations } R \text{ and } S \quad \} \\
& p{\circ}\top\!\!\top{\circ}p \;=\; p{\circ}(R{\cap}S){\circ}p \\
\Rightarrow & \{ \quad p \subseteq I \,,\; R{\cap}S \subseteq R \,,\; R{\cap}S \subseteq S \,,\text{ monotonicity of composition} \quad \} \\
& p{\circ}\top\!\!\top{\circ}p \subseteq R \;\wedge\; p{\circ}\top\!\!\top{\circ}p \subseteq S \\
= & \{ \quad \text{lemma 103} \quad \} \\
& p{\circ}\top\!\!\top{\circ}p = p{\circ}R{\circ}p \;\;\wedge\;\; p{\circ}\top\!\!\top{\circ}p = p{\circ}S{\circ}p \;\;.
\end{array}
$$

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

$$
\begin{array}{ll}
& p{\circ}\top\!\!\top{\circ}p \;=\; p{\circ}R{\circ}p \\
= & \{ \quad \text{Leibniz: apply converse operator to both sides,} \\
& \quad\;\; \text{converse is its own inverse} \quad \} \\
& (p{\circ}\top\!\!\top{\circ}p)^{\cup} \;=\; (p{\circ}R{\circ}p)^{\cup} \\
= & \{ \quad (R{\circ}S)^{\cup} \;=\; S^{\cup} \circ R^{\cup} \text{ for all } R \text{ and } S \,,\; p^{\cup} = p \,,\; \top\!\!\top^{\cup} = \top\!\!\top \quad \} \\
& p{\circ}\top\!\!\top{\circ}p \;=\; p \circ R^{\cup} \circ p \;\;.
\end{array}
$$

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).

Note that intersection in (iii) cannot be replaced by union. It is not the case that being i-connected by $R \cup R^{\cup}$ implies being i-connected by R.
(d) Trivial consequence of (c) and the definition of component.
□

10.1. Transitive Relations

Lemma 105. 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

$$p = q \;\;\vee\;\; p \cap q = \perp\!\!\perp \quad .$$

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:

$$\begin{array}{ll}
& \mathsf{true} \\
\Rightarrow & \{ \quad p \text{ and } q \text{ are i-connected by } T\text{, composition is monotonic} \quad \} \\
& p \circ \top\!\!\top \circ p \circ q \circ \top\!\!\top \circ q \subseteq T \circ T \;\;\wedge\;\; q \circ \top\!\!\top \circ q \circ p \circ \top\!\!\top \circ p \subseteq T \circ T \\
\Rightarrow & \{ \quad T \text{ is transitive, transitivity of } \subseteq \quad \} \\
& p \circ \top\!\!\top \circ p \circ q \circ \top\!\!\top \circ q \subseteq T \;\;\wedge\;\; q \circ \top\!\!\top \circ q \circ p \circ \top\!\!\top \circ p \subseteq T \\
\Rightarrow & \{ \quad \text{cone rule: } p \circ q = \perp\!\!\perp \vee \top\!\!\top \circ p \circ q \circ \top\!\!\top = \top\!\!\top \text{,} \\
& \quad\;\; \text{Leibniz and } \perp\!\!\perp \text{ is zero of composition} \quad \} \\
& (p \circ q = \perp\!\!\perp \vee p \circ \top\!\!\top \circ q \subseteq T) \;\;\wedge\;\; (q \circ p = \perp\!\!\perp \vee q \circ \top\!\!\top \circ p \subseteq T) \\
= & \{ \quad p \text{ and } q \text{ are i-connected by } T\text{, } p \circ q = p \cap q = q \circ p\text{,} \\
& \quad\;\; \text{distributivity, } R \cup S \subseteq T \equiv R \subseteq T \wedge S \subseteq T \quad \} \\
& p \cap q = \perp\!\!\perp \;\;\vee\;\; (p \cup q) \circ \top\!\!\top \circ (p \cup q) \subseteq T \\
\Rightarrow & \{ \quad p \subseteq p \cup q\text{, } p \text{ is a component of } T\text{,} \\
& \quad\;\; q \subseteq p \cup q\text{, } q \text{ is a component of } T \quad \} \\
& p \cap q = \perp\!\!\perp \;\;\vee\;\; p = p \cup q = q \\
= & \{ \quad \text{idempotency of } \cup \quad \} \\
& p \cap q = \perp\!\!\perp \;\;\vee\;\; p = q \quad .
\end{array}$$

□

Lemma 106. Suppose T is a transitive relation and p and q are both components of T. Then

$$p \circ T \circ q \neq \perp\!\!\perp \wedge q \circ T \circ p \neq \perp\!\!\perp \;\Rightarrow\; p = q \quad .$$

Proof

$$\begin{array}{ll}
& p \circ T \circ q \neq \perp\!\!\perp \\
\Rightarrow & \{ \quad \text{cone rule} \quad \} \\
& \top\!\!\top \circ p \circ T \circ q \circ \top\!\!\top = \top\!\!\top \\
\Rightarrow & \{ \quad \text{Leibniz} \quad \}
\end{array}$$

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

$=$ { p and q are both i-connected by T, so, by lemma 103, $p{\circ}\top\!\!\top{\circ}p = p{\circ}T{\circ}p$ 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 $\subseteq$ }

$$p{\circ}T{\circ}q = p{\circ}\top\!\!\top{\circ}q \quad .$$

In summary,

$$p{\circ}T{\circ}q \neq \perp\!\!\perp \Rightarrow p{\circ}T{\circ}q = p{\circ}\top\!\!\top{\circ}q \quad .$$

Interchanging p and q, we get

$$q{\circ}T{\circ}p \neq \perp\!\!\perp \Rightarrow q{\circ}T{\circ}p = q{\circ}\top\!\!\top{\circ}p \quad .$$

So,

$$p{\circ}T{\circ}q \neq \perp\!\!\perp \wedge q{\circ}T{\circ}p \neq \perp\!\!\perp$$

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

$$p{\circ}T{\circ}q = p{\circ}\top\!\!\top{\circ}q \wedge q{\circ}T{\circ}p = q{\circ}\top\!\!\top{\circ}p$$
$$\wedge \quad p{\circ}T{\circ}p = p{\circ}\top\!\!\top{\circ}p \wedge q{\circ}T{\circ}q = q{\circ}\top\!\!\top{\circ}q$$

$\Rightarrow$ { 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 i-connected and lemma 103, $p \subseteq p{\cup}q$ and $q \subseteq p{\cup}q$, p and q are components of T, definition 102 }

$$p = p{\cup}q = q \quad .$$

□

Taking the converse of lemma 106, we get:

Corollary 107. Suppose T is a transitive relation and p and q are both components of T. Then

$$p{\circ}T{\circ}q = \perp\!\!\perp \vee q{\circ}T{\circ}p = \perp\!\!\perp \Leftarrow p \neq q \quad .$$

□

Corollary 107 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 G, denoted by G^+, has the property that

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

It follows that

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

Here we consider properties of transitive and symmetric relations.

Lemma 108. Suppose T is a transitive and symmetric relation. Then $(T{\circ}p)_<$ is i-connected by T if p is i-connected by T.

Proof We have

$$\begin{array}{ll}
 & (T{\circ}p)_< \circ \top\!\!\top \circ (T{\circ}p)_< \\
= & \quad \{ \quad \text{domain-conditional isomorphism} \quad \} \\
 & T \circ p \circ \top\!\!\top \circ p \circ T^\cup \\
\subseteq & \quad \{ \quad \text{assume } p \text{ is i-connected by } T \\
 & \qquad \text{definition and monotonicity of composition} \quad \} \\
 & T \circ T \circ T^\cup \\
\subseteq & \quad \{ \quad T \text{ is transitive and symmetric} \quad \} \\
 & T \quad .
\end{array}$$

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

Lemma 109. Suppose T is a transitive and symmetric relation and p is i-connected by T. Suppose $q = (T{\circ}q)_<$ and $q \subseteq p$. Then q is i-connected by T.

Proof We aim to apply the definition of i-connected (definition 102).

$$\begin{array}{ll}
 & q{\circ}\top\!\!\top{\circ}q \\
= & \quad \{ \quad q = (T{\circ}q)_< \text{, coreflexive-condition isomprphism} \quad \} \\
 & T \circ q \circ \top\!\!\top \circ q \circ T^\cup \\
\subseteq & \quad \{ \quad q \subseteq p \text{, monotonicity of composition} \quad \} \\
 & T \circ p \circ \top\!\!\top \circ p \circ T^\cup \\
\subseteq & \quad \{ \quad p \text{ is i-connected by } T \text{, definition 102} \\
 & \qquad \text{monotonicity of composition} \quad \} \\
 & T \circ T \circ T^\cup \\
\subseteq & \quad \{ \quad T \text{ is transitive and symmetric} \quad \} \\
 & T \quad .
\end{array}$$

It follows by definition 102 that q is i-connected by T.
□

Theorem 110. 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.

$$
\begin{array}{ll}
 & p = (T \circ p)< \\
\Leftarrow & \{ \quad \text{assumptions, lemma 108, and definition 102 of component} \quad \} \\
 & p \subseteq (T \circ p)< \\
= & \{ \quad \text{coreflexive-condition isomorphism} \quad \} \\
 & p \circ \top\!\!\top \subseteq T \circ p \circ \top\!\!\top \\
\Leftarrow & \{ \quad p \text{ is a component of } T\text{, so } p \text{ is i-connected by } T \\
 & \quad\;\; \text{i.e. } p \circ \top\!\!\top \circ p \subseteq T \\
 & \quad\;\; \text{monotonicity of composition and transitivity of } \subseteq \quad \} \\
 & p \circ \top\!\!\top \subseteq p \circ \top\!\!\top \circ p \circ p \circ \top\!\!\top \\
= & \{ \quad p \text{ is a coreflexive, so } p \circ p = p\text{, cone rule} \quad \} \\
 & p \circ \top\!\!\top \subseteq p \circ \top\!\!\top \circ p \circ \top\!\!\top \;\wedge\; (\top\!\!\top \circ p \circ \top\!\!\top = \top\!\!\top \;\vee\; p = \perp\!\!\perp) \\
= & \{ \quad \text{distributivity of conjunction over disjunction} \\
 & \quad\;\; \text{Leibniz and } \perp\!\!\perp \text{ is zero of composition and least element} \quad \} \\
 & \mathsf{true} \;.
\end{array}
$$
□

Corollary 111. 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,

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

Proof Apply lemma 26 with f instantiated to the function that maps coreflexive q to $(T \circ q)<$. This function is complementation-idempotent closure operator by theorem 67.
□

Theorem 112. Suppose p is a coreflexive, T is a transitive and symmetric relation and q is a component of T. Then

$$p \circ T \circ q = \perp\!\!\perp \Leftarrow p \circ q = \perp\!\!\perp \;.$$

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

Proof

$$
\begin{array}{ll}
 & p \circ T \circ q \\
= & \{ \quad \text{property of domains: } R = R< \circ R \quad \} \\
 & p \circ (T \circ q)< \circ T \circ q
\end{array}
$$

$=$ { theorem 110 with $p := q$ }

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

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

$\perp\!\!\perp$.

□

10.3. Strongly Connected Components

Definition 113 (Strongly Connected Component). Coreflexive p is said to be a *strongly connected component* of graph G if p is a component of G^* .

□

Definition 114. The function equiv mapping arbitrary relations to equivalence relations is defined by, for all G ,

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

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

□

Theorem 115. Suppose p is a strongly connected component of G . Then p is a component of $\mathsf{equiv}.G$. Conversely, every component of $\mathsf{equiv}.G$ is a strongly connected component of G .

Proof Immediate from the definition of strongly-connected and corollary 104(d).

□

Theorem 116. Suppose p is a strongly connected component of G . Then

$$p \;=\; (\mathsf{equiv}.G \circ p)_<$$

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

Proof Immediate from the definition of strongly-connected, corollary 104, theorem 110 and corollary 111.

□

10.4. Absolute Connectivity

The following folklore property is included here for several reasons: it gives further insight into strong connectivity and it illustrates the use of the less-well-known middle-exchange rule. Most importantly, it is used in the proof of lemma 118 below. Recall that $\sim p$ to denotes the negation of p in the lattice of coreflexives.

Lemma 117. Suppose G is a relation and p is a strongly connected component of G . Then

$$p \circ G^* \circ \sim p \circ G^* \circ p = \perp\!\!\perp \quad .$$

For finite graph G , the lemma states that there are no paths from component p to itself that pass through nodes not in p .

Proof We have:

$p\circ G^*\circ{\sim}p\circ G^*\circ p \;=\; \perp\!\!\perp$

$=\qquad \{\quad \perp\!\!\perp\subseteq R$ for all R, anti-symmetry of $\subseteq$ $\quad\}$

$p\circ G^*\circ{\sim}p\circ G^*\circ p \;\subseteq\; \perp\!\!\perp$

$=\qquad \{\quad$ middle-exchange rule, ${\sim}p = I\cap\neg p$ $\quad\}$

$(p\circ G^*)^{\cup}\circ\top\!\!\top\circ(G^*\circ p)^{\cup} \;\subseteq\; \neg I\cup p$

$=\qquad \{\quad$ apply converse to both sides,
converse is its own inverse, $p^{\cup}=p$, $\top\!\!\top^{\cup}=\top\!\!\top$, $(\neg I)^{\cup}=\neg I$ $\quad\}$

$G^*\circ p\circ\top\!\!\top\circ p\circ G^* \;\subseteq\; \neg I\cup p$

$=\qquad \{\quad$ set calculus $\quad\}$

$(G^*\circ p\circ\top\!\!\top\circ p\circ G^*)\cap I \;\subseteq\; p$

$=\qquad \{\quad$ domains (specifically, theorem 47(b)),
I is the unit of composition $\quad\}$

$(G^*\circ p)_{<}\circ(p\circ G^*)_{>} \;\subseteq\; p$.

Let us abbreviate $(G^*\circ p)_{<}\circ(p\circ G^*)_{>}$ to q. Then we have to prove that $q\subseteq p$.

It is obvious that $p\subseteq q$ (because $I\subseteq G^*$ combined with properties of the domain operators and coreflexives). So we actually have to prove that $q=p$. Noting that no use has yet been made of the fact that p is a strongly connected component of G, the goal is clearly to prove that q is connected by G^*.

$q\circ\top\!\!\top\circ q$

$\subseteq\qquad \{\quad q = (G^*\circ p)_{<}\circ(p\circ G^*)_{>}$, domains and monotonicity $\quad\}$

$(G^*\circ p)_{<}\circ\top\!\!\top\circ(p\circ G^*)_{>}$

$=\qquad \{\quad R_{<}\circ\top\!\!\top = R\circ\top\!\!\top$, $\top\!\!\top\circ S_{>} = \top\!\!\top\circ S$ $\quad\}$

$G^*\circ p\circ\top\!\!\top\circ p\circ G^*$

$=\qquad \{\quad p$ is strongly connected by G,
definitions 113 and 102, and lemma 103 $\quad\}$

$G^*\circ p\circ G^*\circ p\circ G^*$

$\subseteq\qquad \{\quad p\subseteq I$, monotonicity of composition $\quad\}$

$G^*\circ G^*\circ G^*$

$=\qquad \{\quad G^* = G^*\circ G^*$ $\quad\}$

G^* .

We conclude that q is i-connected by G^*. But $p\subseteq q$ and p is a component of G^*. It follows from the definition of component (definition 102) that $p=q$. Referring back to the initial calculation, this completes the proof of the lemma.
□

Lemma 118. Suppose G is a relation and p is a strongly connected component of G. Then

$$p\circ G^*\circ p \;=\; (p\circ G)^*\circ p \;=\; p\circ(p{\circ}G{\circ}p)^*\circ p \quad .$$

(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.)

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

$$\begin{array}{ll}
 & p\circ(p\circ G\circ p)^* \\
= & \{ \quad \text{mirror rule: } R\circ(S{\circ}R)^* = (R{\circ}S)^*\circ R\text{, for all } R \text{ and } S \quad \} \\
 & (p\circ p\circ G)^*\circ p \\
= & \{ \quad p \text{ is a coreflexive, so } p{\circ}p = p \quad \} \\
 & (p\circ G)^*\circ p \quad .
\end{array}$$

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

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

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

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

$$R = (G\circ{\sim}p \;\cup\; {\sim}p\circ G)\circ(p\circ G\circ p)^* \quad\wedge\quad G^* = (p\circ G\circ p)^*\circ R^* \quad . \tag{119}$$

We show that

$$p\circ R^*\circ p = p \quad . \tag{120}$$

We have:

$$\begin{array}{ll}
 & p\circ R^*\circ p \\
= & \{ \quad R^* \;=\; I\cup R\circ R^*\,,
\end{array}$$

distributivity of composition over union, etc. $\}$

$p \cup p \circ R \circ R^* \circ p$

$=$ { (119), distributivity and $p \circ \sim p = \perp\!\!\perp$ }

$p \cup p \circ G \circ \sim p \circ (p \circ G \circ p)^* \circ R^* \circ p$

$\subseteq$ { $p \subseteq I$, so $(p \circ G \circ p)^* \subseteq G^*$
2nd conjunct of (119) and $I \subseteq (p \circ G \circ p)^*$, so $R^* \subseteq G^*$ }

$p \cup p \circ G \circ \sim p \circ G^* \circ G^* \circ p$

$=$ { $G \subseteq G^*$, $G^* \circ G^* = G^*$ and lemma 117 }

p

$\subseteq$ { $I \subseteq R^*$ }

$p \circ R^* \circ p$.

The equality follows by mutual inclusion. We can now complete the calculation.

$p \circ G^* \circ p$

$=$ { (119) }

$p \circ (p \circ G \circ p)^* \circ R^* \circ p$

$=$ { mirror rule, $p \circ p = p$ }

$(p \circ G)^* \circ p \circ R^* \circ p$

$=$ { (120) }

$(p \circ G)^* \circ p$.

□

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 121. For all proper atoms a and relations G , $(\mathsf{equiv}.G \circ a)<$ is a strongly connected component of G .

Proof We exploit theorem 115. Accordingly, we have to show that $(\mathsf{equiv}.G \circ a)<$ is a component of $\mathsf{equiv}.G$. That is, $(\mathsf{equiv}.G \circ a)<$ is i-connected by $\mathsf{equiv}.G$ and it is maximal among such coreflexives.

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

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

$=$ { domains }

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

$=$ { converse }

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

$$
\begin{array}{ll}
= & \{ \quad a\circ\top\!\top\circ a = a \ \text{(“all or nothing axiom”)} \quad \} \\
& \mathsf{equiv}.G\circ a\circ \mathsf{equiv}.G \\
\subseteq & \{ \quad a\subseteq I \text{, monotonicity} \quad \} \\
& \mathsf{equiv}.G\circ \mathsf{equiv}.G \\
\subseteq & \{ \quad \mathsf{equiv}.G \ \text{is transitive} \quad \} \\
& \mathsf{equiv}.G \quad .
\end{array}
$$

Now we must show that, if a is a proper atom,

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

Suppose q is a coreflexive such that $q\circ\top\!\top\circ q\subseteq\mathsf{equiv}.G$. Then, by lemma 103,

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

So,

$$
\begin{array}{ll}
& (\mathsf{equiv}.G\circ a)_< \ \supseteq \ q \\
= & \{ \quad \text{coreflexive-condition isomorphism,} \\
& \quad\ \text{converse, all terms are symmetric} \quad \} \\
& \mathsf{equiv}.G\circ a\circ\top\!\top \ \supseteq \ q\circ\top\!\top \\
\Leftarrow & \{ \quad q\circ\top\!\top\circ q\subseteq\mathsf{equiv}.G \quad \} \\
& q\circ\top\!\top\circ q\circ a\circ\top\!\top \supseteq q\circ\top\!\top \\
\Leftarrow & \{ \quad \text{monotonicity} \quad \} \\
& \top\!\top\circ q\circ a\circ\top\!\top \supseteq \top\!\top \\
= & \{ \quad \text{assume } (\mathsf{equiv}.G\circ a)_< \subseteq q \\
& \quad\ \text{then, since } I\subseteq\mathsf{equiv}.G \text{ , } (I\circ a)_< \subseteq q \\
& \quad\ \text{i.e. } a \subseteq q \text{ and } q\circ a = a \quad \} \\
& \top\!\top\circ a\circ\top\!\top \supseteq \top\!\top \\
= & \{ \quad a \ \text{is a proper atom, cone rule} \quad \} \\
& \mathsf{true} \quad .
\end{array}
$$

We have thus shown that, if a is a proper atom,

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

The required equivalence is a straightforward consequence of the anti-symmetry of the subset relation. (Informally, the key step in showing that $(\mathsf{equiv}.G\circ a)_<$ is a component is showing, from the assumptions on q , that the point represented by a is an element of the set represented by q .)
□

The converse of lemma 121 is the following:

Lemma 122. If p is a strongly connected component of G , and a is a proper atom such that $a\circ p = a$, then $p = (\mathsf{equiv}.G\circ a)_<$.

Proof Assume p is a strongly connected component of G, and a is a proper atom such that $a{\circ}p = a$. Then,

$$
\begin{array}{ll}
 & \mathsf{true} \\
= & \quad \{ \quad \text{theorem 116} \quad \} \\
 & p \;=\; (\mathsf{equiv}.G \circ p)_{<} \\
\Rightarrow & \quad \{ \quad a{\circ}p = a \text{, monotonicity of composition and domains} \quad \} \\
 & p \;\supseteq\; (\mathsf{equiv}.G \circ a)_{<} \\
\Rightarrow & \quad \{ \quad \text{lemma 121, definitions 113 and 102} \quad \} \\
 & p \;=\; (\mathsf{equiv}.G \circ a)_{<} \quad .
\end{array}
$$

□

Summarising, we have:

Theorem 123. Suppose G is a homogeneous relation. Then the strongly connected components of G are given by $\langle \cup a : \mathsf{atom}.a \wedge a \neq \perp\!\!\perp : \{(\mathsf{equiv}.G \circ a)_{<}\}\rangle$. The strongly connected components partition the set of all proper atoms. That is, distinct strongly connected components are disjoint and each proper atom is an element of a strongly connected component (specifically, a is an element of $(\mathsf{equiv}.G \circ a)_{<}$).

Proof Lemmas 121, 122, 105 and 68 (with $R := \mathsf{equiv}.G$).
□

10.6. Starth Roots of the Equivalence Relation

We have defined $\mathsf{equiv}.G$ as $G^* \cap (G^*)^{\cup}$. (See definition 114.) It is useful to express it as E^* where E represents the edges in G that connect nodes in the same strongly connected component (i.e. nodes that are "E"quivalent under the relation $\mathsf{equiv}.G$). This is the content of theorem 125. First, a lemma:

Lemma 124. For all relations R and S,

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

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

Proof We calculate the condition on R and S as follows.

$$
\begin{array}{ll}
 & G^* \;\cap\; R \circ G^{\cup} \circ S \;\;=\;\; G^* \;\cap\; R \circ (G^{\cup} \cap G^*) \circ S \\
= & \quad \{ \quad G^{\cup} \supseteq G^{\cup} \cap G^* \text{, monotonicity and anti-symmetry} \quad \} \\
 & G^* \;\cap\; R \circ G^{\cup} \circ S \;\;\subseteq\;\; G^* \;\cap\; R \circ (G^{\cup} \cap G^*) \circ S \\
= & \quad \{ \quad \text{properties of } \cap \quad \} \\
 & G^* \;\cap\; R \circ G^{\cup} \circ S \;\;\subseteq\;\; R \circ (G^{\cup} \cap G^*) \circ S \\
\Leftarrow & \quad \{ \quad \text{modularity rule (41), applied symmetrically} \quad \} \\
 & R \circ (R^{\cup} \circ G^* \circ S^{\cup} \;\;\cap\;\; G^{\cup}) \circ S \;\;\subseteq\;\; R \circ (G^{\cup} \cap G^*) \circ S \\
\Leftarrow & \quad \{ \quad \text{monotonicity} \quad \}
\end{array}
$$

$$
\begin{array}{ll}
& R^{\cup}\circ G^{*}\circ S^{\cup} \;\cap\; G^{\cup} \quad\subseteq\quad G^{\cup}\cap G^{*} \\
\Leftarrow & \{\qquad G^{*}\circ G^{*}\circ G^{*} \;=\; G^{*} \;=\; ((G^{\cup})^{\cup})^{*} \;=\; ((G^{\cup})^{*})^{\cup} \\
& \qquad\quad \text{monotonicity of composition} \quad \} \\
& R\subseteq (G^{\cup})^{*} \;\wedge\; S\subseteq (G^{\cup})^{*} \quad .
\end{array}
$$

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

□

Now, the theorem:

Theorem 125.

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

Proof We begin by proving, by induction on k, that, for all R and S,

$$
G^{*}\cap R\circ(G^{\cup})^{k}\circ S \;=\; G^{*}\cap R\circ(G^{\cup}\cap G^{*})^{k}\circ S \;\Leftarrow\; R\cup S\subseteq (G^{\cup})^{*} \quad . \tag{126}
$$

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

$$
\begin{array}{ll}
& G^{*} \;\cap\; R\circ(G^{\cup}\cap G^{*})^{k+1}\circ S \\
= & \{\qquad \text{definition of } (G^{\cup}\cap G^{*})^{k+1} \quad \} \\
& G^{*} \;\cap\; R\circ(G^{\cup}\cap G^{*})^{k}\circ(G^{\cup}\cap G^{*})\circ S \\
= & \{\qquad \text{by assumption, } R\subseteq (G^{\cup})^{*}\text{; so } R\circ(G^{\cup}\cap G^{*})^{k}\subseteq (G^{\cup})^{*}, \\
& \qquad\quad \text{also, by assumption, } S\subseteq (G^{\cup})^{*} \\
& \qquad\quad \text{lemma 124 with } R:=R\circ(G^{\cup}\cap G^{*})^{k} \quad \} \\
& G^{*} \;\cap\; R\circ(G^{\cup}\cap G^{*})^{k}\circ G^{\cup}\circ S \\
= & \{\qquad \text{by assumption, } S\subseteq (G^{\cup})^{*}\text{; so } G^{\cup}\circ S \;\subseteq\; (G^{\cup})^{*} \\
& \qquad\quad \text{also, by assumption, } R\subseteq (G^{\cup})^{*} \\
& \qquad\quad \text{induction hypothesis (126) with } S \;:=\; G^{\cup}\circ S \quad \} \\
& G^{*} \;\cap\; R\circ(G^{\cup})^{k}\circ G^{\cup}\circ S \\
= & \{\qquad \text{definition of } (G^{\cup})^{k+1} \quad \} \\
& G^{*} \;\cap\; R\circ(G^{\cup})^{k+1}\circ S \quad .
\end{array}
$$

By induction, we have established (126) for all natural numbers k. Hence,

$$
\begin{array}{ll}
& \mathsf{equiv}.G \\
= & \{\qquad \text{definition 114} \quad \} \\
& G^{*}\cap (G^{*})^{\cup} \\
= & \{\qquad (G^{*})^{\cup}=(G^{\cup})^{*}\text{, definition of star as a sum of powers} \quad \} \\
& G^{*}\cap \langle\cup k : 0\leq k : (G^{\cup})^{k}\rangle \\
= & \{\qquad \text{distributivity} \quad \} \\
& \langle\cup k \;:\; 0\leq k \;:\; G^{*}\cap (G^{\cup})^{k}\rangle
\end{array}
$$

$$
\begin{array}{ll}
= & \{ \quad (126) \text{ with } R{,}S := I{,}I \quad \} \\
& \langle \cup k : 0 \le k : G^* \cap (G^{\cup} \cap G^*)^k \rangle \\
= & \{ \quad \text{distributivity} \quad \} \\
& G^* \cap \langle \cup k : 0 \le k : (G^{\cup} \cap G^*)^k \rangle \\
= & \{ \quad \text{definition of star as a sum of powers, } G^* \supseteq (G^{\cup} \cap G^*)^* \quad \} \\
& (G^{\cup} \cap G^*)^* \quad .
\end{array}
$$

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

Given that theorem 125 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 125.

Theorem 127. If G is an acyclic graph, $\mathsf{equiv}.G$ is the identity relation on nodes of G. That is,

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

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

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

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

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

$$
\begin{array}{ll}
& \mathsf{equiv}.G \\
= & \{ \quad \text{theorem 125} \quad \} \\
& (G^{\cup} \cap G^*)^* \\
\subseteq & \{ \quad \text{modularity rule: (41), monotonicity} \quad \} \\
& (G^{\cup} \circ (I \cap G \circ G^*))^* \\
= & \{ \quad G \circ G^* = G^+ \text{ , assumption: } I \cap G^+ = \perp\!\!\perp \quad \} \\
& (G^{\cup} \circ \perp\!\!\perp)^* \\
= & \{ \quad \perp\!\!\perp \text{ is zero of composition, } \perp\!\!\perp^* = I \quad \} \\
& I \quad .
\end{array}
$$

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

For the converse, we have:

$$
\begin{array}{ll}
& I \cap (G \cap \neg I)^+ \\
= & \{ \quad [\; G^+ = G \circ G^* \;] \text{ with } G := G \cap \neg I \text{ , } G^* = (G \cap \neg I)^* \quad \}
\end{array}
$$

$$I \cap (G{\cap}\neg I)\circ G^*$$

$\subseteq$ { modularity rule: (41), I is unit of composition }

$$(G{\cap}\neg I) \circ ((G{\cap}\neg I)^{\cup} \cap G^*)$$

$\subseteq$ { $G{\cap}\neg I \subseteq \neg I$, $(G{\cap}\neg I)^{\cup} \subseteq G^{\cup}$, theorem 125,
$[\, G \subseteq G^* \,]$ with $G := G^{\cup} \cap G^*$
monotonicity (of converse, composition and star) }

$$\neg I \circ \mathsf{equiv}.G \quad .$$

Thus

$$\mathsf{equiv}.G \subseteq I$$

$\Rightarrow$ { above, monotonicity of composition and transitivity of $\subseteq$ }

$$I \cap (G{\cap}\neg I)^+ \subseteq \neg I \circ I$$

$=$ { I is unit of composition, complements, idempotency of intersection }

$$I \cap (G{\cap}\neg I)^+ = \perp\!\!\perp \quad .$$

□

Note that, although theorem 127 is stated as a property of graphs, it is valid for all relations: nowhere is the finiteness of graphs used in its proof. We have stated it in this way because the more significant property of a relation is whether or not it is left- or right-definite. For relations on an infinite set, acyclicity has little or no significance.

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

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

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 130, below, establishes the formal relationship between its reflexive-transitive closure and G^* .

Recalling theorem 125, lemma 129 is to be expected. In order to prove it and theorem 130 we need a little-known lemma:

Lemma 128. Suppose f is a surjective function of type $C{\leftarrow}A$ (for arbitrary C and A). Then

$$f \circ \neg(f^{\cup} \circ f) \circ f^{\cup} \;=\; \neg I_C \quad .$$

Proof We prove the theorem by mutual inclusion. First,

$$\begin{array}{ll} & f \circ \neg(f^{\cup} \circ f) \circ f^{\cup} \;\subseteq\; \neg I_C \\ = & \quad \{ \quad \text{middle exchange rule} \quad \} \\ & f^{\cup} \circ I_C \circ f \;\subseteq\; f^{\cup} \circ f \\ = & \quad \{ \quad I_C \text{ is unit of composition, reflexivity of } \subseteq \quad \} \\ & \mathsf{true} \quad . \end{array}$$

Note that no use has been made of the assumed properties of f . For the opposite inclusion, we do need to use them:

$$\begin{array}{ll} & \neg I_C \;\subseteq\; f \circ \neg(f^{\cup} \circ f) \circ f^{\cup} \\ = & \quad \{ \quad f \text{ is functional and surjective, i.e } f \circ f^{\cup} = I_C \text{ ,} \\ & \qquad I_C \text{ is identity of composition} \quad \} \\ & f \circ f^{\cup} \circ \neg I_C \circ f \circ f^{\cup} \;\subseteq\; f \circ \neg(f^{\cup} \circ f) \circ f^{\cup} \\ \Leftarrow & \quad \{ \quad \text{monotonicity of composition} \quad \} \\ & f^{\cup} \circ \neg I_C \circ f \;\subseteq\; \neg(f^{\cup} \circ f) \\ = & \quad \{ \quad \text{middle exchange rule} \quad \} \\ & f \circ f^{\cup} \circ f \circ f^{\cup} \;\subseteq\; I_C \\ = & \quad \{ \quad f \text{ is functional and surjective, i.e } f \circ f^{\cup} = I_C \quad \} \\ & \mathsf{true} \quad . \end{array}$$

□

Lemma 129.

$$\mathsf{sc} \circ G \circ \mathsf{sc}^{\cup} \;\cap\; \neg I_C \;=\; \mathsf{sc} \circ (G \cap \neg((G^{\cup})^*)) \circ \mathsf{sc}^{\cup} \quad .$$

Proof

$$\begin{array}{ll} & \mathsf{sc} \circ G \circ \mathsf{sc}^{\cup} \;\cap\; \neg I_C \\ = & \quad \{ \quad \text{lemma 128,} \\ & \qquad \text{by theorem 63, } \mathsf{sc}^{\cup} \circ \mathsf{sc} = \mathsf{equiv}.G \quad \} \end{array}$$

[7]Although we don't go into details, for any function f with source N , the graph $f \circ G \circ f^{\cup}$ is "pathwise homomorphic" [19] to G ; hence the title of this section.

$\mathsf{sc}\circ G\circ \mathsf{sc}^{\cup} \;\;\cap\;\; \mathsf{sc}\circ\neg(\mathsf{equiv}.G)\circ \mathsf{sc}^{\cup}$

$= \qquad \{ \qquad \text{definition of } \mathsf{equiv}.G \text{, distributivity} \qquad \}$

$\mathsf{sc}\circ G\circ \mathsf{sc}^{\cup} \;\;\cap\;\; \mathsf{sc}\circ(\neg(G^*)\cup\neg((G^{\cup})^*))\circ \mathsf{sc}^{\cup}$

$= \qquad \{ \qquad \mathsf{sc} \text{ is a total function, distributivity} \qquad \}$

$\mathsf{sc}\circ(G\cap\neg(G^*))\circ \mathsf{sc}^{\cup} \;\;\cup\;\; \mathsf{sc}\circ(G\cap\neg((G^{\cup})^*))\circ \mathsf{sc}^{\cup}$

$= \qquad \{ \qquad G\subseteq G^* \text{, so } G\cap\neg(G^*) = \perp\!\!\perp \qquad \}$

$\mathsf{sc}\circ(G\cap\neg((G^{\cup})^*))\circ \mathsf{sc}^{\cup} \quad .$

□

Theorem 130. Let $\mathcal{A}$ denote $\mathsf{sc}\circ G\circ \mathsf{sc}^{\cup} \cap \neg I_C$. Then,

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

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

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

Proof With theorem 125 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. Conversely, the relation E captures the edges of G that are in "E"qual strongly connected components.

Clearly $D\cup E = G$ and $D\cap E = \perp\!\!\perp$. Moreover, by theorem 125, $E^* = \mathsf{equiv}.G$. Thus

G^*

$= \qquad \{ \qquad D\cup E = G \qquad \}$

$(D\cup E)^*$

$= \qquad \{ \qquad \text{star decomposition} \qquad \}$

$E^*\circ(D\circ E^*)^*$

$= \qquad \{ \qquad \text{theorem 125: } E^* = \mathsf{equiv}.G \qquad \}$

$\mathsf{equiv}.G\circ(D\circ\mathsf{equiv}.G)^*$

$= \qquad \{ \qquad \text{equivalence relations and partitions: theorem 63} \qquad \}$

$\mathsf{sc}^{\cup}\circ\mathsf{sc}\circ(D\circ\mathsf{sc}^{\cup}\circ\mathsf{sc})^*$

$= \qquad \{ \qquad \text{mirror rule} \qquad \}$

$\mathsf{sc}^{\cup}\circ(\mathsf{sc}\circ D\circ\mathsf{sc}^{\cup})^*\circ\mathsf{sc}$

$= \qquad \{ \qquad \text{definition of } D \text{, lemma 129} \qquad \}$

$\mathsf{sc}^{\cup}\circ\mathcal{A}^*\circ\mathsf{sc} \quad .$

It remains to prove that $\mathcal{A}$ is acyclic. First,

$$
\begin{array}{ll}
 & I_C \cap \mathcal{A}^+ \ = \ \perp\!\!\perp \\
= & \{ \quad \text{shunting rule} \quad \} \\
 & \mathcal{A}^+ \subseteq \neg I_C \\
= & \{ \quad \text{lemma 128} \quad \} \\
 & \mathcal{A}^+ \ \subseteq \ \mathsf{sc} \circ \neg(\mathsf{sc}^{\cup} \circ \mathsf{sc}) \circ \mathsf{sc}^{\cup} \\
= & \{ \quad \text{theorem 63} \quad \} \\
 & \mathcal{A}^+ \ \subseteq \ \mathsf{sc} \circ \neg(\mathsf{equiv}.G) \circ \mathsf{sc}^{\cup} \quad .
\end{array}
$$

The form of the last line was the motivation for lemma 129. For brevity, let us use H to denote $G \cap \neg((G^{\cup})^*)$. Then

$$
\begin{array}{ll}
 & \mathcal{A}^+ \\
= & \{ \quad \mathcal{A}^+ = \mathcal{A} \circ \mathcal{A}^* \text{ , definition of } \mathcal{A} \text{ and } H \text{ , and lemma 129} \quad \} \\
 & \mathsf{sc} \circ H \circ \mathsf{sc}^{\cup} \circ (\mathsf{sc} \circ H \circ \mathsf{sc}^{\cup})^* \\
= & \{ \quad \text{mirror rule and theorem 63} \quad \} \\
 & \mathsf{sc} \circ (H \circ \mathsf{equiv}.G)^* \circ H \circ \mathsf{sc}^{\cup} \quad .
\end{array}
$$

So

$$
\begin{array}{ll}
 & I_C \cap \mathcal{A}^+ \ = \ \perp\!\!\perp \\
\Leftarrow & \{ \quad \text{combining the two calculations and monotonicity} \quad \} \\
 & (H \circ \mathsf{equiv}.G)^* \circ H \ \subseteq \ \neg(\mathsf{equiv}.G) \\
= & \{ \quad \text{rotation rule, } \mathsf{equiv}.G = (\mathsf{equiv}.G)^{\cup} \quad \} \\
 & \mathsf{equiv}.G \circ (H \circ \mathsf{equiv}.G)^* \ \subseteq \ \neg(H^{\cup}) \quad .
\end{array}
$$

We complete the calculation by showing that

$$
\mathsf{equiv}.G \circ (H \circ \mathsf{equiv}.G)^* \ = \ G^* \quad \wedge \quad G^* \subseteq \neg(H^{\cup}) \quad .
$$

For the first conjunct, we have:

$$
\begin{array}{ll}
 & \mathsf{equiv}.G \circ (H \circ \mathsf{equiv}.G)^* \\
= & \{ \quad \text{theorem 125} \quad \} \\
 & (G \cap (G^{\cup})^*)^* \circ (H \circ (G \cap (G^{\cup})^*)^*)^* \\
= & \{ \quad \text{star decomposition} \quad \} \\
 & ((G \cap (G^{\cup})^*) \ \cup \ H)^* \\
= & \{ \quad H = G \cap \neg((G^{\cup})^*) \text{ , distributivity and complements} \quad \} \\
 & G^* \quad .
\end{array}
$$

Now, for the second conjunct:

$$\begin{array}{ll} & \neg(H^{\cup}) \\ = & \{ \quad \text{definition of } H \quad \} \\ & \neg((G \cap \neg((G^{\cup})^{*}))^{\cup}) \\ \supseteq & \{ \quad \text{anti-monotonicity of negation, double negation} \quad \} \\ & ((G^{\cup})^{*})^{\cup} \\ = & \{ \quad (G^{\cup})^{*} = (G^{*})^{\cup} \ , \ (R^{\cup})^{\cup} = R \quad \} \\ & G^{*} \ . \end{array}$$

Combining the two calculations, we have indeed proved that $\mathcal{A}$ is acyclic.
□

The importance of theorem 130 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 [20] for more detailed discussion of sparsity considerations.

(Of course, this does not mean that theorem 130 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 124 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 much 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 130, 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.

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.

References

[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/~pasrb2/MPC/BasicGraphTheory.pdf`, Also available online at ResearchGate (2019).

[2] R. Backhouse, An analysis of repeated graph search, submitted for publication. Preprint available on ResearchGate (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 (1975) 161–186.

[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) (February 1995) 131–136.

[8] H. Doornbos, Reductivity arguments and program construction, Ph.D. thesis, Eindhoven University of Technology, Department of Mathematics and Computing Science (June 1996).

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

[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, 2017, pp. 109–126 (May 15–18 2017).

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

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

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

[8]The rules were first used in [4, 5] but not named; the names were coined later and used specifically in, for example, [13].

[14] J. Riguet, Relations binaires, fermetures, correspondances de Galois, Bulletin de la Société Mathématique de France 76 (1948) 114–155.

[15] G. Schmidt, T. Ströhlein, Relationen und Grafen, Springer-Verlag (1988).

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

[17] P. Freyd, A. Ščedrov, Categories, Allegories, North-Holland (1990).

[18] R. Backhouse, J. v. d. Woude, Demonic operators and monotype factors, Mathematical Structures in Computer Science 3 (4) (December 1993) 417–433.

[19] R. McNaughton, The loop complexity of pure-group events, Info. and Control 11 (1967) 167–176.

[20] R. Backhouse, B. Carré, A comparison of Gaussian and Gauss-Jordan elimination in regular algebra, International Journal of Computer Mathematics 10 (1982) 311–325. doi:10.1080/00207168208803290.