

# Relational Forests

Walter Guttmann

June 17, 2024

## Abstract

We study second-order formalisations of graph properties expressed as first-order formulas in relation algebras extended with a Kleene star. The formulas quantify over relations while still avoiding quantification over elements of the base set. We formalise the property of undirected graphs being acyclic this way. This involves a study of various kinds of orientation of graphs. We also verify basic algorithms to constructively prove several second-order properties.

## Contents

<b>1</b>	<b>Overview</b>	<b>1</b>
<b>2</b>	<b>Orientations and Undirected Forests</b>	<b>2</b>
2.1	Orientability . . . . .	2
2.2	Undirected forests . . . . .	9
2.3	Arc axiom . . . . .	17
2.4	Counterexamples . . . . .	18
<b>3</b>	<b>Axioms and Algorithmic Proofs</b>	<b>18</b>
3.1	Constructing a spanning tree . . . . .	19
3.2	Breadth-first search . . . . .	21
3.3	Extending partial orders to linear orders . . . . .	21

## 1 Overview

The theories described in this document study second-order specifications of graph properties expressed as first-order formulas in Stone-Kleene relation algebras. Of particular interest are undirected forests and their orientations, developed in Section 2. We also verify the correctness of a number of basic graph algorithms, which we use in constructive proofs of graph properties in Section 3.

The theories formally verify results in [5]; results from this paper are annotated with the corresponding theorem numbers. See the paper for further details and related work.

## 2 Orientations and Undirected Forests

In this theory we study orientations and various second-order specifications of undirected forests. The results are structured by the classes in which they can be proved, which correspond to algebraic structures. Most classes are generalisations of Kleene relation algebras. None of the classes except *kleene-relation-algebra* assumes the double-complement law  $--x = x$  available in Boolean algebras. The corresponding paper does not elaborate these fine distinctions, so some results take a different form in this theory. They usually specialise to Kleene relation algebras after simplification using  $--x = x$ .

**theory** *Forests*

**imports** *Stone-Kleene-Relation-Algebras.Kleene-Relation-Algebras*

**begin**

### 2.1 Orientability

**context** *bounded-distrib-allegory-signature*

**begin**

**abbreviation** *irreflexive-inf* :: 'a  $\Rightarrow$  bool **where** *irreflexive-inf* x  $\equiv$  x  $\sqcap$  1 = bot

**end**

**context** *bounded-distrib-allegory*

**begin**

**lemma** *irreflexive-inf-arc-asymmetric*:

*irreflexive-inf* x  $\implies$  arc x  $\implies$  asymmetric x  
<proof>

**lemma** *asymmetric-inf*:

asymmetric x  $\longleftrightarrow$  *irreflexive-inf* (x \* x)  
<proof>

**lemma** *asymmetric-irreflexive-inf*:

asymmetric x  $\implies$  *irreflexive-inf* x  
<proof>

**lemma** *transitive-asymmetric-irreflexive-inf*:

*transitive*  $x \implies$  *asymmetric*  $x \iff$  *irreflexive-inf*  $x$   
(proof)

**abbreviation** *orientation*  $x y \equiv y \sqcup y^T = x \wedge$  *asymmetric*  $y$

**abbreviation** *loop-orientation*  $x y \equiv y \sqcup y^T = x \wedge$  *antisymmetric*  $y$

**abbreviation** *super-orientation*  $x y \equiv x \leq y \sqcup y^T \wedge$  *asymmetric*  $y$

**abbreviation** *loop-super-orientation*  $x y \equiv x \leq y \sqcup y^T \wedge$  *antisymmetric*  $y$

**lemma** *orientation-symmetric*:

*orientation*  $x y \implies$  *symmetric*  $x$   
(proof)

**lemma** *orientation-irreflexive-inf*:

*orientation*  $x y \implies$  *irreflexive-inf*  $x$   
(proof)

**lemma** *loop-orientation-symmetric*:

*loop-orientation*  $x y \implies$  *symmetric*  $x$   
(proof)

**lemma** *loop-orientation-diagonal*:

*loop-orientation*  $x y \implies y \sqcap y^T = x \sqcap 1$   
(proof)

**lemma** *super-orientation-irreflexive-inf*:

*super-orientation*  $x y \implies$  *irreflexive-inf*  $x$   
(proof)

**lemma** *loop-super-orientation-diagonal*:

*loop-super-orientation*  $x y \implies x \sqcap 1 \leq y \sqcap y^T$   
(proof)

**definition** *orientable*  $x \equiv \exists y .$  *orientation*  $x y$

**definition** *loop-orientable*  $x \equiv \exists y .$  *loop-orientation*  $x y$

**definition** *super-orientable*  $x \equiv \exists y .$  *super-orientation*  $x y$

**definition** *loop-super-orientable*  $x \equiv \exists y .$  *loop-super-orientation*  $x y$

**lemma** *orientable-symmetric*:

*orientable*  $x \implies$  *symmetric*  $x$   
(proof)

**lemma** *orientable-irreflexive-inf*:

*orientable*  $x \implies$  *irreflexive-inf*  $x$   
(proof)

**lemma** *loop-orientable-symmetric*:

*loop-orientable*  $x \implies$  *symmetric*  $x$   
(proof)

**lemma** *super-orientable-irreflexive-inf*:  
*super-orientable*  $x \implies$  *irreflexive-inf*  $x$   
 ⟨*proof*⟩

**lemma** *orientable-down-closed*:  
**assumes** *symmetric*  $x$   
   **and**  $x \leq y$   
   **and** *orientable*  $y$   
**shows** *orientable*  $x$   
 ⟨*proof*⟩

**lemma** *loop-orientable-down-closed*:  
**assumes** *symmetric*  $x$   
   **and**  $x \leq y$   
   **and** *loop-orientable*  $y$   
**shows** *loop-orientable*  $x$   
 ⟨*proof*⟩

**lemma** *super-orientable-down-closed*:  
**assumes**  $x \leq y$   
   **and** *super-orientable*  $y$   
**shows** *super-orientable*  $x$   
 ⟨*proof*⟩

**lemma** *loop-super-orientable-down-closed*:  
**assumes**  $x \leq y$   
   **and** *loop-super-orientable*  $y$   
**shows** *loop-super-orientable*  $x$   
 ⟨*proof*⟩

**abbreviation** *orientable-1*  $x \equiv$  *loop-super-orientable*  $x$

**abbreviation** *orientable-2*  $x \equiv \exists y . x \leq y \sqcup y^T \wedge y \sqcap y^T \leq x \sqcap 1$

**abbreviation** *orientable-3*  $x \equiv \exists y . x \leq y \sqcup y^T \wedge y \sqcap y^T = x \sqcap 1$

**abbreviation** *orientable-4*  $x \equiv$  *irreflexive-inf*  $x \longrightarrow$  *super-orientable*  $x$

**abbreviation** *orientable-5*  $x \equiv$  *symmetric*  $x \longrightarrow$  *loop-orientable*  $x$

**abbreviation** *orientable-6*  $x \equiv$  *symmetric*  $x \longrightarrow (\exists y . y \sqcup y^T = x \wedge y \sqcap y^T \leq x \sqcap 1)$

**abbreviation** *orientable-7*  $x \equiv$  *symmetric*  $x \longrightarrow (\exists y . y \sqcup y^T = x \wedge y \sqcap y^T = x \sqcap 1)$

**abbreviation** *orientable-8*  $x \equiv$  *symmetric*  $x \wedge$  *irreflexive-inf*  $x \longrightarrow$  *orientable*  $x$

**lemma** *super-orientation-diagonal*:

$x \leq y \sqcup y^T \implies y \sqcap y^T \leq x \sqcap 1 \implies y \sqcap y^T = x \sqcap 1$

⟨*proof*⟩

**lemma** *orientable-2-implies-1*:

*orientable-2*  $x \implies$  *orientable-1*  $x$

⟨*proof*⟩

**lemma orientable-2-3:**  
*orientable-2*  $x \longleftrightarrow$  *orientable-3*  $x$   
 ⟨proof⟩

**lemma orientable-5-6:**  
*orientable-5*  $x \longleftrightarrow$  *orientable-6*  $x$   
 ⟨proof⟩

**lemma orientable-6-7:**  
*orientable-6*  $x \longleftrightarrow$  *orientable-7*  $x$   
 ⟨proof⟩

**lemma orientable-7-implies-8:**  
*orientable-7*  $x \implies$  *orientable-8*  $x$   
 ⟨proof⟩

**lemma orientable-5-implies-1:**  
*orientable-5*  $(x \sqcup x^T) \implies$  *orientable-1*  $x$   
 ⟨proof⟩

ternary predicate  $S$  called *split* here

**abbreviation** *split*  $x y z \equiv y \sqcap y^T = x \wedge y \sqcup y^T = z$

**Theorem 3.1**

**lemma orientation-split:**  
*orientation*  $x y \longleftrightarrow$  *split* *bot*  $y x$   
 ⟨proof⟩

**Theorem 3.2**

**lemma split-1-loop-orientation:**  
*split 1*  $y x \implies$  *loop-orientation*  $x y$   
 ⟨proof⟩

**Theorem 3.3**

**lemma loop-orientation-split:**  
*loop-orientation*  $x y \longleftrightarrow$  *split*  $(x \sqcap 1) y x$   
 ⟨proof⟩

**Theorem 3.4**

**lemma loop-orientation-split-inf-1:**  
*loop-orientation*  $x y \longleftrightarrow$  *split*  $(y \sqcap 1) y x$   
 ⟨proof⟩

**lemma loop-orientation-top-split:**  
*loop-orientation top*  $y \longleftrightarrow$  *split 1*  $y top$   
 ⟨proof⟩

injective and transitive orientations

**definition** *injectively-orientable*  $x \equiv \exists y . orientation x y \wedge injective y$

**lemma** *injectively-orientable-orientable*:  
*injectively-orientable*  $x \implies$  *orientable*  $x$   
*<proof>*

**lemma** *orientable-orientable-1*:  
*orientable*  $x \implies$  *orientable-1*  $x$   
*<proof>*

**lemma** *injectively-orientable-down-closed*:  
**assumes** *symmetric*  $x$   
**and**  $x \leq y$   
**and** *injectively-orientable*  $y$   
**shows** *injectively-orientable*  $x$   
*<proof>*

**definition** *transitively-orientable*  $x \equiv \exists y . \text{orientation } x y \wedge \text{transitive } y$

**lemma** *transitively-orientable-orientable*:  
*transitively-orientable*  $x \implies$  *orientable*  $x$   
*<proof>*

**lemma** *irreflexive-transitive-orientation-asymmetric*:  
**assumes** *irreflexive-inf*  $x$   
**and** *transitive*  $y$   
**and**  $y \sqcup y^T = x$   
**shows** *asymmetric*  $y$   
*<proof>*

[Theorem 12](#)

**lemma** *transitively-orientable-2*:  
*transitively-orientable*  $x \longleftrightarrow$  *irreflexive-inf*  $x \wedge (\exists y . y \sqcup y^T = x \wedge \text{transitive } y)$   
*<proof>*

**end**

**context** *relation-algebra-signature*  
**begin**

**abbreviation** *asymmetric-var* ::  $'a \Rightarrow \text{bool}$  **where** *asymmetric-var*  $x \equiv$   
*irreflexive*  $(x * x)$

**end**

**context** *pd-allegory*  
**begin**

[Theorem 1.4](#)

**lemma** *asymmetric-var*:

*asymmetric*  $x \longleftrightarrow$  *asymmetric-var*  $x$   
(proof)

### Theorem 1.3

(Theorem 1.2 is *asymmetric-irreflexive* in *Relation-Algebras*)

**lemma** *transitive-asymmetric-irreflexive*:  
*transitive*  $x \implies$  *asymmetric*  $x \longleftrightarrow$  *irreflexive*  $x$   
(proof)

**lemma** *orientable-irreflexive*:  
*orientable*  $x \implies$  *irreflexive*  $x$   
(proof)

**lemma** *super-orientable-irreflexive*:  
*super-orientable*  $x \implies$  *irreflexive*  $x$   
(proof)

**lemma** *orientation-diversity-split*:  
*orientation*  $(-1) y \longleftrightarrow$  *split bot*  $y (-1)$   
(proof)

**abbreviation** *linear-orderable-1*  $x \equiv$  *linear-order*  $x$

**abbreviation** *linear-orderable-2*  $x \equiv$  *linear-strict-order*  $x$

**abbreviation** *linear-orderable-3*  $x \equiv$  *transitive*  $x \wedge$  *asymmetric*  $x \wedge$  *strict-linear*  $x$

**abbreviation** *linear-orderable-3a*  $x \equiv$  *transitive*  $x \wedge$  *strict-linear*  $x$

**abbreviation** *orientable-11*  $x \equiv$  *split 1*  $x$  *top*

**abbreviation** *orientable-12*  $x \equiv$  *split bot*  $x (-1)$

**lemma** *linear-strict-order-split*:  
*linear-strict-order*  $x \longleftrightarrow$  *transitive*  $x \wedge$  *split bot*  $x (-1)$   
(proof)

### Theorem 1.6

**lemma** *linear-strict-order-without-irreflexive*:  
*linear-strict-order*  $x \longleftrightarrow$  *transitive*  $x \wedge$  *strict-linear*  $x$   
(proof)

**lemma** *linear-order-without-reflexive*:  
*linear-order*  $x \longleftrightarrow$  *antisymmetric*  $x \wedge$  *transitive*  $x \wedge$  *linear*  $x$   
(proof)

**lemma** *linear-orderable-1-implies-2*:  
*linear-orderable-1*  $x \implies$  *linear-orderable-2*  $(x \sqcap -1)$   
(proof)

**lemma** *linear-orderable-2-3*:  
*linear-orderable-2*  $x \longleftrightarrow$  *linear-orderable-3*  $x$   
(proof)

**lemma** *linear-orderable-3-3a*:  
*linear-orderable-3*  $x \longleftrightarrow$  *linear-orderable-3a*  $x$   
 ⟨*proof*⟩

**lemma** *linear-orderable-3-implies-orientable-12*:  
*linear-orderable-3*  $x \implies$  *orientable-12*  $x$   
 ⟨*proof*⟩

**lemma** *orientable-11-implies-12*:  
*orientable-11*  $x \implies$  *orientable-12*  $(x \sqcap -1)$   
 ⟨*proof*⟩

**end**

**context** *stone-relation-algebra*  
**begin**

**Theorem 3.5**

**lemma** *split-symmetric-asymmetric*:  
**assumes** *regular*  $x$   
**shows** *split*  $x \ y \ z \longleftrightarrow y \sqcap y^T = x \wedge (y \sqcap -y^T) \sqcup (y \sqcap -y^T)^T = z \sqcap -x \wedge x$   
 $\leq z$   
 ⟨*proof*⟩

**lemma** *orientable-1-2*:  
*orientable-1*  $x \longleftrightarrow$  *orientable-2*  $x$   
 ⟨*proof*⟩

**lemma** *orientable-8-implies-5*:  
**assumes** *orientable-8*  $(x \sqcap -1)$   
**shows** *orientable-5*  $x$   
 ⟨*proof*⟩

**lemma** *orientable-4-implies-1*:  
**assumes** *orientable-4*  $(x \sqcap -1)$   
**shows** *orientable-1*  $x$   
 ⟨*proof*⟩

**lemma** *orientable-1-implies-4*:  
**assumes** *orientable-1*  $(x \sqcup 1)$   
**shows** *orientable-4*  $x$   
 ⟨*proof*⟩

**lemma** *orientable-1-implies-5*:  
**assumes** *orientable-1*  $x$   
**shows** *orientable-5*  $x$   
 ⟨*proof*⟩

**Theorem 2**



**lemma** *all-orientable-characterisations:*

**shows**  $(\forall x . \text{orientable-1 } x) \longleftrightarrow (\forall x . \text{orientable-2 } x)$   
**and**  $(\forall x . \text{orientable-1 } x) \longleftrightarrow (\forall x . \text{orientable-3 } x)$   
**and**  $(\forall x . \text{orientable-1 } x) \longleftrightarrow (\forall x . \text{orientable-4 } x)$   
**and**  $(\forall x . \text{orientable-1 } x) \longleftrightarrow (\forall x . \text{orientable-5 } x)$   
**and**  $(\forall x . \text{orientable-1 } x) \longleftrightarrow (\forall x . \text{orientable-6 } x)$   
**and**  $(\forall x . \text{orientable-1 } x) \longleftrightarrow (\forall x . \text{orientable-7 } x)$   
**and**  $(\forall x . \text{orientable-1 } x) \longleftrightarrow (\forall x . \text{orientable-8 } x)$   
*<proof>*

**lemma** *orientable-12-implies-11:*

*orientable-12*  $x \implies \text{orientable-11 } (x \sqcup 1)$   
*<proof>*

**lemma** *linear-strict-order-order:*

*linear-strict-order*  $x \implies \text{linear-order } (x \sqcup 1)$   
*<proof>*

**lemma** *linear-orderable-2-implies-1:*

*linear-orderable-2*  $x \implies \text{linear-orderable-1 } (x \sqcup 1)$   
*<proof>*

[Theorem 4](#)

[Theorem 12](#)

[Theorem 13](#)

**lemma** *exists-split-characterisations:*

**shows**  $(\exists x . \text{linear-orderable-1 } x) \longleftrightarrow (\exists x . \text{linear-orderable-2 } x)$   
**and**  $(\exists x . \text{linear-orderable-1 } x) \longleftrightarrow (\exists x . \text{linear-orderable-3 } x)$   
**and**  $(\exists x . \text{linear-orderable-1 } x) \longleftrightarrow (\exists x . \text{linear-orderable-3a } x)$   
**and**  $(\exists x . \text{linear-orderable-1 } x) \longleftrightarrow \text{transitively-orientable } (-1)$   
**and**  $(\exists x . \text{linear-orderable-1 } x) \implies (\exists x . \text{orientable-11 } x)$   
**and**  $(\exists x . \text{orientable-11 } x) \longleftrightarrow (\exists x . \text{orientable-12 } x)$   
*<proof>*

[Theorem 4](#)

[Theorem 12](#)

**lemma** *exists-all-orientable:*

**shows**  $(\exists x . \text{orientable-11 } x) \longleftrightarrow (\forall x . \text{orientable-1 } x)$   
**and**  $\text{transitively-orientable } (-1) \implies (\forall x . \text{orientable-8 } x)$   
*<proof>*

**end**

## 2.2 Undirected forests

We start with a few general results in Kleene algebras and a few basic properties of directed acyclic graphs.

**context** *kleene-algebra*  
**begin**

[Theorem 1.9](#)

**lemma** *plus-separate-comp-bot*:  
  **assumes**  $x * y = \text{bot}$   
  **shows**  $(x \sqcup y)^+ = x^+ \sqcup y^+ \sqcup y^+ * x^+$   
   $\langle \text{proof} \rangle$   
**end**

**context** *bounded-distrib-kleene-allegory*  
**begin**

**lemma** *reflexive-inf-plus-star*:  
  **assumes** *reflexive*  $x$   
  **shows**  $x \sqcap y^+ \leq 1 \longleftrightarrow x \sqcap y^* = 1$   
   $\langle \text{proof} \rangle$   
**end**

**context** *pd-kleene-allegory*  
**begin**

**lemma** *acyclic-star-inf-conv-iff*:  
  **assumes** *irreflexive*  $w$   
  **shows** *acyclic*  $w \longleftrightarrow w^* \sqcap w^{T^*} = 1$   
   $\langle \text{proof} \rangle$

[Theorem 1.7](#)

**lemma** *acyclic-irreflexive-star-antisymmetric*:  
   $\text{acyclic } x \longleftrightarrow \text{irreflexive } x \wedge \text{antisymmetric } (x^*)$   
   $\langle \text{proof} \rangle$

[Theorem 1.8](#)

**lemma** *acyclic-plus-asymmetric*:  
   $\text{acyclic } x \longleftrightarrow \text{asymmetric } (x^+)$   
   $\langle \text{proof} \rangle$

[Theorem 1.3](#)

([Theorem 1.1](#) is *acyclic-asymmetric* in *Kleene-Relation-Algebras*)

**lemma** *transitive-acyclic-irreflexive*:  
   $\text{transitive } x \implies \text{acyclic } x \longleftrightarrow \text{irreflexive } x$   
   $\langle \text{proof} \rangle$

**lemma** *transitive-acyclic-asymmetric*:  
   $\text{transitive } x \implies \text{acyclic } x \longleftrightarrow \text{asymmetric } x$

*<proof>*

### Theorem 1.5

**lemma** *strict-order-transitive-acyclic:*

*strict-order*  $x \longleftrightarrow$  *transitive*  $x \wedge$  *acyclic*  $x$

*<proof>*

**lemma** *linear-strict-order-transitive-acyclic:*

*linear-strict-order*  $x \longleftrightarrow$  *transitive*  $x \wedge$  *acyclic*  $x \wedge$  *strict-linear*  $x$

*<proof>*

The following are various specifications of an undirected graph being acyclic.

**definition** *acyclic-1*  $x \equiv \forall y . \text{orientation } x y \longrightarrow \text{acyclic } y$

**definition** *acyclic-1b*  $x \equiv \forall y . \text{orientation } x y \longrightarrow y^* \sqcap y^{T*} = 1$

**definition** *acyclic-2*  $x \equiv \forall y . y \leq x \wedge \text{asymmetric } y \longrightarrow \text{acyclic } y$

**definition** *acyclic-2a*  $x \equiv \forall y . y \sqcup y^T \leq x \wedge \text{asymmetric } y \longrightarrow \text{acyclic } y$

**definition** *acyclic-2b*  $x \equiv \forall y . y \sqcup y^T \leq x \wedge \text{asymmetric } y \longrightarrow y^* \sqcap y^{T*} = 1$

**definition** *acyclic-3a*  $x \equiv \forall y . y \leq x \wedge x \leq y^* \longrightarrow y = x$

**definition** *acyclic-3b*  $x \equiv \forall y . y \leq x \wedge y^* = x^* \longrightarrow y = x$

**definition** *acyclic-3c*  $x \equiv \forall y . y \leq x \wedge x \leq y^+ \longrightarrow y = x$

**definition** *acyclic-3d*  $x \equiv \forall y . y \leq x \wedge y^+ = x^+ \longrightarrow y = x$

**definition** *acyclic-4*  $x \equiv \forall y . y \leq x \longrightarrow x \sqcap y^* \leq \neg\neg y$

**definition** *acyclic-4a*  $x \equiv \forall y . y \leq x \longrightarrow x \sqcap y^* \leq y$

**definition** *acyclic-4b*  $x \equiv \forall y . y \leq x \longrightarrow x \sqcap y^* = y$

**definition** *acyclic-4c*  $x \equiv \forall y . y \leq x \longrightarrow y \sqcap (x \sqcap \neg y)^* = \text{bot}$

**definition** *acyclic-5a*  $x \equiv \forall y . y \leq x \longrightarrow y^* \sqcap (x \sqcap \neg y)^* = 1$

**definition** *acyclic-5b*  $x \equiv \forall y . y \leq x \longrightarrow y^* \sqcap (x \sqcap \neg y)^+ \leq 1$

**definition** *acyclic-5c*  $x \equiv \forall y . y \leq x \longrightarrow y^+ \sqcap (x \sqcap \neg y)^* \leq 1$

**definition** *acyclic-5d*  $x \equiv \forall y . y \leq x \longrightarrow y^+ \sqcap (x \sqcap \neg y)^+ \leq 1$

**definition** *acyclic-5e*  $x \equiv \forall y z . y \leq x \wedge z \leq x \wedge y \sqcap z = \text{bot} \longrightarrow y^* \sqcap z^* = 1$

**definition** *acyclic-5f*  $x \equiv \forall y z . y \sqcup z \leq x \wedge y \sqcap z = \text{bot} \longrightarrow y^* \sqcap z^* = 1$

**definition** *acyclic-5g*  $x \equiv \forall y z . y \sqcup z = x \wedge y \sqcap z = \text{bot} \longrightarrow y^* \sqcap z^* = 1$

**definition** *acyclic-6*  $x \equiv \exists y . y \sqcup y^T = x \wedge \text{acyclic } y \wedge \text{injective } y$

### Theorem 6

**lemma** *acyclic-2-2a:*

**assumes** *symmetric*  $x$

**shows** *acyclic-2*  $x \longleftrightarrow$  *acyclic-2a*  $x$

*<proof>*

### Theorem 6

**lemma** *acyclic-2a-2b:*

**shows** *acyclic-2a*  $x \longleftrightarrow$  *acyclic-2b*  $x$

*<proof>*

### Theorem 5

**lemma** *acyclic-1-1b:*

**shows** *acyclic-1*  $x \longleftrightarrow$  *acyclic-1b*  $x$

*<proof>*

### Theorem 10

**lemma** *acyclic-6-1-injectively-orientable:*

*acyclic-6*  $x \iff \text{acyclic-1 } x \wedge \text{injectively-orientable } x$   
*<proof>*

**lemma** *acyclic-6-symmetric:*

*acyclic-6*  $x \implies \text{symmetric } x$   
*<proof>*

**lemma** *acyclic-6-irreflexive:*

*acyclic-6*  $x \implies \text{irreflexive } x$   
*<proof>*

**lemma** *acyclic-4-irreflexive:*

*acyclic-4*  $x \implies \text{irreflexive } x$   
*<proof>*

### Theorem 6.4

**lemma** *acyclic-2-implies-1:*

*acyclic-2*  $x \implies \text{acyclic-1 } x$   
*<proof>*

### Theorem 8

**lemma** *acyclic-4a-4b:*

*acyclic-4a*  $x \iff \text{acyclic-4b } x$   
*<proof>*

### Theorem 7

**lemma** *acyclic-3a-3b:*

*acyclic-3a*  $x \iff \text{acyclic-3b } x$   
*<proof>*

### Theorem 7

**lemma** *acyclic-3a-3c:*

**assumes** *irreflexive*  $x$   
**shows** *acyclic-3a*  $x \iff \text{acyclic-3c } x$   
*<proof>*

### Theorem 7

**lemma** *acyclic-3c-3d:*

**shows** *acyclic-3c*  $x \iff \text{acyclic-3d } x$   
*<proof>*

### Theorem 8

**lemma** *acyclic-4a-implies-3a:*

*acyclic-4a*  $x \implies \text{acyclic-3a } x$   
*<proof>*

**lemma** *acyclic-4a-implies-4*:  
*acyclic-4a*  $x \implies$  *acyclic-4*  $x$   
(*proof*)

**lemma** *acyclic-4b-implies-4c*:  
*acyclic-4b*  $x \implies$  *acyclic-4c*  $x$   
(*proof*)

[Theorem 8.5](#)

**lemma** *acyclic-4-implies-2*:  
**assumes** *symmetric*  $x$   
**shows** *acyclic-4*  $x \implies$  *acyclic-2*  $x$   
(*proof*)

[Theorem 10.3](#)

**lemma** *acyclic-6-implies-4a*:  
*acyclic-6*  $x \implies$  *acyclic-4a*  $x$   
(*proof*)

[Theorem 1.10](#)

**lemma** *top-injective-inf-complement*:  
**assumes** *injective*  $x$   
**shows**  $top * (x \sqcap y) \sqcap top * (x \sqcap -y) = bot$   
(*proof*)

**lemma** *top-injective-inf-complement-2*:  
**assumes** *injective*  $x$   
**shows**  $(x^T \sqcap y) * top \sqcap (x^T \sqcap -y) * top = bot$   
(*proof*)

[Theorem 10.3](#)

**lemma** *acyclic-6-implies-5a*:  
*acyclic-6*  $x \implies$  *acyclic-5a*  $x$   
(*proof*)

[Theorem 9.7](#)

**lemma** *acyclic-5b-implies-4*:  
**assumes** *irreflexive*  $x$   
**and** *acyclic-5b*  $x$   
**shows** *acyclic-4*  $x$   
(*proof*)

[Theorem 9](#)

**lemma** *acyclic-5a-5b*:  
*acyclic-5a*  $x \iff$  *acyclic-5b*  $x$   
(*proof*)

[Theorem 9](#)

**lemma** *acyclic-5a-5c*:  
*acyclic-5a*  $x \longleftrightarrow$  *acyclic-5c*  $x$   
 ⟨*proof*⟩

**Theorem 9**

**lemma** *acyclic-5b-5d*:  
*acyclic-5b*  $x \longleftrightarrow$  *acyclic-5d*  $x$   
 ⟨*proof*⟩

**lemma** *acyclic-5a-5e*:  
*acyclic-5a*  $x \longleftrightarrow$  *acyclic-5e*  $x$   
 ⟨*proof*⟩

**Theorem 9**

**lemma** *acyclic-5e-5f*:  
*acyclic-5e*  $x \longleftrightarrow$  *acyclic-5f*  $x$   
 ⟨*proof*⟩

**lemma** *acyclic-5e-down-closed*:  
**assumes**  $x \leq y$   
**and** *acyclic-5e*  $y$   
**shows** *acyclic-5e*  $x$   
 ⟨*proof*⟩

**lemma** *acyclic-5a-down-closed*:  
**assumes**  $x \leq y$   
**and** *acyclic-5a*  $y$   
**shows** *acyclic-5a*  $x$   
 ⟨*proof*⟩

**further variants of the existence of a linear order**

**abbreviation** *linear-orderable-4*  $x \equiv$  *transitive*  $x \wedge$  *acyclic*  $x \wedge$  *strict-linear*  $x$

**abbreviation** *linear-orderable-5*  $x \equiv$  *transitive*  $x \wedge$  *acyclic*  $x \wedge$  *linear*  $(x^*)$

**abbreviation** *linear-orderable-6*  $x \equiv$  *acyclic*  $x \wedge$  *linear*  $(x^*)$

**abbreviation** *linear-orderable-7*  $x \equiv$  *split 1*  $(x^*)$  *top*

**abbreviation** *linear-orderable-8*  $x \equiv$  *split bot*  $(x^+)$   $(-1)$

**lemma** *linear-orderable-3-4*:  
*linear-orderable-3*  $x \longleftrightarrow$  *linear-orderable-4*  $x$   
 ⟨*proof*⟩

**lemma** *linear-orderable-5-implies-6*:  
*linear-orderable-5*  $x \implies$  *linear-orderable-6*  $x$   
 ⟨*proof*⟩

**lemma** *linear-orderable-6-implies-3*:  
**assumes** *linear-orderable-6*  $x$   
**shows** *linear-orderable-3*  $(x^+)$   
 ⟨*proof*⟩

**lemma** *linear-orderable-7-implies-1:*  
*linear-orderable-7*  $x \implies$  *linear-orderable-1*  $(x^*)$   
(*proof*)

**lemma** *linear-orderable-6-implies-8:*  
*linear-orderable-6*  $x \implies$  *linear-orderable-8*  $x$   
(*proof*)

**abbreviation** *path-orderable*  $x \equiv$  *univalent*  $x \wedge$  *injective*  $x \wedge$  *acyclic*  $x \wedge$  *linear*  $(x^*)$

**lemma** *path-orderable-implies-linear-orderable-6:*  
*path-orderable*  $x \implies$  *linear-orderable-6*  $x$   
(*proof*)

**definition** *simple-paths*  $x \equiv \exists y . y \sqcup y^T = x \wedge$  *acyclic*  $y \wedge$  *injective*  $y \wedge$  *univalent*  $y$

#### Theorem 14.1

**lemma** *simple-paths-acyclic-6:*  
*simple-paths*  $x \implies$  *acyclic-6*  $x$   
(*proof*)

#### Theorem 14.2

**lemma** *simple-paths-transitively-orientable:*  
**assumes** *simple-paths*  $x$   
**shows** *transitively-orientable*  $(x^+ \sqcap -1)$   
(*proof*)

**abbreviation** *spanning*  $x y \equiv y \leq x \wedge x \leq (y \sqcup y^T)^* \wedge$  *acyclic*  $y \wedge$  *injective*  $y$   
**definition** *spannable*  $x \equiv \exists y .$  *spanning*  $x y$

**lemma** *acyclic-6-implies-spannable:*  
*acyclic-6*  $x \implies$  *spannable*  $x$   
(*proof*)

**lemma** *acyclic-3a-spannable-implies-6:*  
**assumes** *acyclic-3a*  $x$   
**and** *spannable*  $x$   
**and** *symmetric*  $x$   
**shows** *acyclic-6*  $x$   
(*proof*)

#### Theorem 10.3

**lemma** *acyclic-6-implies-3a:*  
*acyclic-6*  $x \implies$  *acyclic-3a*  $x$   
(*proof*)

#### Theorem 10.3

**lemma** *acyclic-6-implies-2*:  
 $acyclic-6\ x \implies acyclic-2\ x$   
(proof)

**Theorem 11**

**lemma** *acyclic-6-3a-spannable*:  
 $acyclic-6\ x \iff symmetric\ x \wedge spannable\ x \wedge acyclic-3a\ x$   
(proof)

**end**

**context** *stone-kleene-relation-algebra*  
**begin**

**Theorem 11.3**

**lemma** *point-spanning*:  
**assumes** *point*  $p$   
**shows** *spanning*  $(-1)$   $(p \sqcap -1)$   
*spannable*  $(-1)$   
(proof)

**lemma** *irreflexive-star*:  
 $(x \sqcap -1)^* = x^*$   
(proof)

**Theorem 6.5**

**lemma** *acyclic-2-1*:  
**assumes** *orientable*  $x$   
**shows**  $acyclic-2\ x \iff acyclic-1\ x$   
(proof)

**Theorem 8**

**lemma** *acyclic-4-4c*:  
 $acyclic-4\ x \iff acyclic-4c\ x$   
(proof)

**Theorem 9**

**lemma** *acyclic-5f-5g*:  
 $acyclic-5f\ x \iff acyclic-5g\ x$   
(proof)

**lemma** *linear-orderable-3-implies-5*:  
**assumes** *linear-orderable-3*  $x$   
**shows** *linear-orderable-5*  $x$   
(proof)

**lemma** *linear-orderable-8-implies-7*:  
 $linear-orderable-8\ x \implies linear-orderable-7\ x$



*<proof>*

### Theorem 13

**lemma** *exists-split-characterisations-2:*

**shows**  $(\exists x . \text{linear-orderable-1 } x) \longleftrightarrow (\exists x . \text{linear-orderable-4 } x)$

**and**  $(\exists x . \text{linear-orderable-1 } x) \longleftrightarrow (\exists x . \text{linear-orderable-5 } x)$

**and**  $(\exists x . \text{linear-orderable-1 } x) \longleftrightarrow (\exists x . \text{linear-orderable-6 } x)$

**and**  $(\exists x . \text{linear-orderable-1 } x) \longleftrightarrow (\exists x . \text{linear-orderable-7 } x)$

**and**  $(\exists x . \text{linear-orderable-1 } x) \longleftrightarrow (\exists x . \text{linear-orderable-8 } x)$

*<proof>*

**end**

## 2.3 Arc axiom

**class** *stone-kleene-relation-algebra-arc* = *stone-kleene-relation-algebra* +

**assumes** *arc-axiom*:  $x \neq \text{bot} \implies \exists y . \text{arc } y \wedge y \leq \text{--}x$

**begin**

**subclass** *stone-relation-algebra-tarski*

*<proof>*

**context**

**assumes** *orientable-path*:  $\text{arc } x \implies x \leq \text{--}y^* \implies \exists z . z \leq y \wedge \text{asymmetric } z \wedge x \leq \text{--}z^*$

**begin**

### Theorem 8.6

**lemma** *acyclic-2-4:*

**assumes** *irreflexive*  $x$

**and** *symmetric*  $x$

**shows**  $\text{acyclic-2 } x \longleftrightarrow \text{acyclic-4 } x$

*<proof>*

**end**

**end**

**context** *kleene-relation-algebra*

**begin**

### Theorem 8

**lemma** *acyclic-3a-implies-4b:*

**assumes** *acyclic-3a*  $x$

**shows** *acyclic-4b*  $x$

*<proof>*

**lemma** *acyclic-3a-4b:*

$\text{acyclic-3a } x \longleftrightarrow \text{acyclic-4b } x$

*<proof>*

**lemma** *acyclic-4-4a:*

*acyclic-4 x  $\longleftrightarrow$  acyclic-4a x*

*<proof>*

## 2.4 Counterexamples

Calls to nitpick have been put into comments to save processing time.

independence of (0)

**lemma** *symmetric x  $\implies$  irreflexive-inf x  $\implies$  orientable x*

*nitpick[expect=genuine,card=4,timeout=600]*

*<proof>*

**lemma** *linear-orderable-6 x  $\implies$  path-orderable x*

*nitpick[expect=genuine,card=8,timeout=600]*

*<proof>*

(5) does not imply (6)

**lemma** *symmetric x  $\implies$  irreflexive x  $\implies$  acyclic-5a x  $\implies$  acyclic-6 x*

*nitpick[expect=genuine,card=4,timeout=600]*

*<proof>*

(2) does not imply (4)

**lemma** *symmetric x  $\implies$  irreflexive x  $\implies$  acyclic-2 x  $\implies$  acyclic-4 x*

*nitpick[expect=genuine,card=8,timeout=600]*

*<proof>*

**end**

**end**

## 3 Axioms and Algorithmic Proofs

In this theory we verify the correctness of three basic graph algorithms. We use them to constructively prove a number of graph properties.

**theory** *Algorithms*

**imports** *HOL-Hoare.Hoare-Logic Forests*

**begin**

**context** *stone-kleene-relation-algebra-arc*

**begin**

Assuming the arc axiom we can define the function *choose-arc* that selects an arc in a non-empty graph.

**definition** *choose-arc*  $x \equiv$  if  $x = \text{bot}$  then  $\text{bot}$  else  $\text{SOME } y . \text{arc } y \wedge y \leq --x$

**lemma** *choose-arc-below*:

*choose-arc*  $x \leq --x$   
(proof)

**lemma** *choose-arc-arc*:

**assumes**  $x \neq \text{bot}$   
**shows** *arc* (*choose-arc*  $x$ )  
(proof)

**lemma** *choose-arc-bot*:

*choose-arc*  $\text{bot} = \text{bot}$   
(proof)

**lemma** *choose-arc-bot-iff*:

*choose-arc*  $x = \text{bot} \longleftrightarrow x = \text{bot}$   
(proof)

**lemma** *choose-arc-regular*:

*regular* (*choose-arc*  $x$ )  
(proof)

### 3.1 Constructing a spanning tree

**definition** *spanning-forest*  $f g \equiv$  *forest*  $f \wedge f \leq --g \wedge$  *components*  $g \leq$   
*forest-components*  $f \wedge$  *regular*  $f$

**definition** *kruskal-spanning-invariant*  $f g h \equiv$  *symmetric*  $g \wedge h = h^T \wedge g \sqcap --h$   
 $= h \wedge$  *spanning-forest*  $f (-h \sqcap g)$

**lemma** *spanning-forest-spanning*:

*spanning-forest*  $f g \implies$  *spanning* ( $--g$ )  $f$   
(proof)

**lemma** *spanning-forest-spanning-regular*:

**assumes** *regular*  $f$   
**and** *regular*  $g$   
**shows** *spanning-forest*  $f g \longleftrightarrow$  *spanning*  $g f$   
(proof)

We prove total correctness of Kruskal's spanning tree algorithm (ignoring edge weights) [6]. The algorithm and proof are adapted from the AFP theory *Relational-Minimum-Spanning-Trees.Kruskal* to work in Stone-Kleene relation algebras [3, 4].

**lemma** *kruskal-vc-1*:

**assumes** *symmetric g*  
**shows** *kruskal-spanning-invariant bot g g*  
 ⟨*proof*⟩

For the remainder of this theory we assume there are finitely many regular elements. This means that the graphs are finite and is needed for proving termination of the algorithms.

**context**

**assumes** *finite-regular: finite { x . regular x }*  
**begin**

**lemma** *kruskal-vc-2:*

**assumes** *kruskal-spanning-invariant f g h*  
**and** *h ≠ bot*  
**shows**  $(\text{choose-arc } h \leq \text{-forest-components } f \longrightarrow \text{kruskal-spanning-invariant } ((f \sqcap \text{-}(top * \text{choose-arc } h * f^{T*})) \sqcup (f \sqcap top * \text{choose-arc } h * f^{T*})^T \sqcup \text{choose-arc } h) g (h \sqcap \text{-choose-arc } h \sqcap \text{-choose-arc } h^T) \wedge \text{card } \{ x . \text{regular } x \wedge x \leq \text{-}h \wedge x \leq \text{-choose-arc } h \wedge x \leq \text{-choose-arc } h^T \} < \text{card } \{ x . \text{regular } x \wedge x \leq \text{-}h \}) \wedge (\neg \text{choose-arc } h \leq \text{-forest-components } f \longrightarrow \text{kruskal-spanning-invariant } f g (h \sqcap \text{-choose-arc } h \sqcap \text{-choose-arc } h^T) \wedge \text{card } \{ x . \text{regular } x \wedge x \leq \text{-}h \wedge x \leq \text{-choose-arc } h \wedge x \leq \text{-choose-arc } h^T \} < \text{card } \{ x . \text{regular } x \wedge x \leq \text{-}h \})$   
 ⟨*proof*⟩

**theorem** *kruskal-spanning:*

*VARs e f h*  
 [ *symmetric g* ]  
*f := bot;*  
*h := g;*  
**WHILE** *h ≠ bot*  
*INV { kruskal-spanning-invariant f g h }*  
*VAR { card { x . regular x ∧ x ≤ --h } }*  
*DO e := choose-arc h;*  
*IF e ≤ -forest-components f THEN*  
   *f := (f ⊓ -(top \* e \* f<sup>T\*</sup>)) ⊔ (f ⊓ top \* e \* f<sup>T\*</sup>)<sup>T</sup> ⊔ e*  
*ELSE*  
   *SKIP*  
*FI;*  
*h := h ⊓ -e ⊓ -e<sup>T</sup>*  
**OD**  
 [ *spanning-forest f g* ]  
 ⟨*proof*⟩

**lemma** *kruskal-exists-spanning:*

*symmetric g*  $\implies \exists f . \text{spanning-forest } f g$   
 ⟨*proof*⟩

**Theorem 16**

**lemma** *symmetric-spannable*:  
 $\text{symmetric } g \implies \text{spannable } (---g)$   
 ⟨proof⟩

### 3.2 Breadth-first search

We prove total correctness of a simple breadth-first search algorithm. It is a variant of an algorithm discussed in [1].

**theorem** *bfs-reachability*:

*VAR*  $p \ q \ t$   
 [ *regular*  $r \wedge$  *regular*  $s \wedge$  *vector*  $s$  ]  
 $t := \text{bot};$   
 $q := s;$   
 $p := -s \sqcap r^T * s;$   
*WHILE*  $p \neq \text{bot}$   
*INV* { *regular*  $r \wedge$  *regular*  $q \wedge$  *vector*  $q \wedge$  *asymmetric*  $t \wedge t \leq r \wedge t \leq q \wedge q = t^{T*} * s \wedge p = -q \sqcap r^T * q$  }  
*VAR* { *card* {  $x . \text{regular } x \wedge x \leq ---(-q \sqcap r^{T*} * s)$  } }  
*DO*  $t := t \sqcup (r \sqcap q * p^T);$   
 $q := q \sqcup p;$   
 $p := -q \sqcap r^T * p$   
*OD*  
 [ *asymmetric*  $t \wedge t \leq r \wedge q = t^{T*} * s \wedge q = r^{T*} * s$  ]  
 ⟨proof⟩

#### Theorem 18

**lemma** *bfs-reachability-exists*:

*regular*  $r \wedge$  *regular*  $s \wedge$  *vector*  $s \implies \exists t . \text{asymmetric } t \wedge t \leq r \wedge t^{T*} * s = r^{T*} * s$   
 ⟨proof⟩

#### Theorem 17

**lemma** *orientable-path*:

*arc*  $x \implies x \leq ---y^* \implies \exists z . z \leq y \wedge \text{asymmetric } z \wedge x \leq ---z^*$   
 ⟨proof⟩

### 3.3 Extending partial orders to linear orders

We prove total correctness of Szpilrajn's algorithm [7]. A partial-correctness proof using Prover9 is given in [2].

**theorem** *szpilrajn*:

*VAR*  $e \ t$   
 [ *order*  $p \wedge$  *regular*  $p$  ]  
 $t := p;$   
*WHILE*  $t \sqcup t^T \neq \text{top}$   
*INV* { *order*  $t \wedge$  *regular*  $t \wedge p \leq t$  }  
*VAR* { *card* {  $x . \text{regular } x \wedge x \leq -(t \sqcup t^T)$  } }  
*DO*  $e := \text{choose-arc } (-(t \sqcup t^T));$

$$t := t \sqcup t * e * t$$

OD  
 [ linear-order  $t \wedge p \leq t$  ]  
 ⟨proof⟩

### Theorem 15

**lemma** *szpilrajn-exists*:  
 order  $p \wedge$  regular  $p \implies \exists t .$  linear-order  $t \wedge p \leq t$   
 ⟨proof⟩

**lemma** *complement-one-transitively-orientable*:  
 transitively-orientable  $(-1)$   
 ⟨proof⟩

**end**

**end**

**end**

## References

- [1] R. Berghammer. Combining relational calculus and the Dijkstra–Gries method for deriving relational programs. *Information Sciences*, 119(3–4):155–171, 1999.
- [2] R. Berghammer and G. Struth. On automated program construction and verification. In C. Bolduc, J. Desharnais, and B. Ktari, editors, *Mathematics of Program Construction*, volume 6120 of *Lecture Notes in Computer Science*, pages 22–41. Springer, 2010.
- [3] W. Guttmann. Stone-Kleene relation algebras. *Archive of Formal Proofs*, 2017.
- [4] W. Guttmann. Verifying minimum spanning tree algorithms with Stone relation algebras. *Journal of Logical and Algebraic Methods in Programming*, 101:132–150, 2018.
- [5] W. Guttmann. Second-order properties of undirected graphs. In U. Fahrenberg, M. Gehrke, L. Santocanale, and M. Winter, editors, *Relational and Algebraic Methods in Computer Science (RAMiCS 2021)*, Lecture Notes in Computer Science. Springer, 2021. To appear.
- [6] J. B. Kruskal, Jr. On the shortest spanning subtree of a graph and the traveling salesman problem. *Proceedings of the American Mathematical Society*, 7(1):48–50, 1956.

- [7] E. Szpilrajn. Sur l'extension de l'ordre partiel. *Fundamenta Mathematicae*, 16:386–389, 1930.