Stone-Kleene Relation Algebras

Walter Guttmann

June 11, 2019

Abstract

We develop Stone-Kleene relation algebras, which expand Stone relation algebras with a Kleene star operation to describe reachability in weighted graphs. Many properties of the Kleene star arise as a special case of a more general theory of iteration based on Conway semirings extended by simulation axioms. This includes several theorems representing complex program transformations. We formally prove the correctness of Conway’s automata-based construction of the Kleene star of a matrix. We prove numerous results useful for reasoning about weighted graphs.

Contents

1 Synopsis and Motivation 2

2 Iterings 3
  2.1 Conway Semirings ................................. 3
  2.2 Iterings ........................................... 10

3 Kleene Algebras 16

4 Kleene Relation Algebras 25
  4.1 Prim’s Algorithm .................................. 29
    4.1.1 Preservation of Invariant ..................... 30
    4.1.2 Exchange gives Spanning Trees ................ 31
    4.1.3 Exchange gives Minimum Spanning Trees ....... 33
    4.1.4 Invariant implies Postcondition ............... 36
  4.2 Kruskal’s Algorithm ............................... 37
    4.2.1 Preservation of Invariant ..................... 37
    4.2.2 Exchange gives Spanning Trees ................ 38
    4.2.3 Exchange gives Minimum Spanning Trees ....... 39
  4.3 Related Structures ................................. 40

5 Subalgebras of Kleene Relation Algebras 40
6 Matrix Kleene Algebras

6.1 Matrix Restrictions . . . . . . . . . . . . . . . . . . . . . . . . 42
6.2 Matrices form a Kleene Algebra . . . . . . . . . . . . . . . . . 46
6.3 Matrices form a Stone-Kleene Relation Algebra . . . . . . . . 47

1 Synopsis and Motivation

This document describes the following five theory files:

* Iterings describes a general iteration operation that works for many different computation models. We first consider equational axioms based on variants of Conway semirings. We expand these structures by generalised simulation axioms, which hold in total and general correctness models, not just in partial correctness models like the induction axioms. Simulation axioms are still powerful enough to prove separation theorems and Back’s atomicity refinement theorem [4].

* Kleene Algebras form a particular instance of iterings in which the iteration is implemented as a least fixpoint. We implement them based on Kozen’s axioms [13], but most results are inherited from Conway semirings and iterings.

* Kleene Relation Algebras introduces Stone-Kleene relation algebras, which combine Stone relation algebras and Kleene algebras. This is similar to relation algebras with transitive closure [16] but allows us to talk about reachability in weighted graphs. Many results in this theory are useful for verifying the correctness of Prim’s and Kruskal’s minimum spanning tree algorithms.

* Subalgebras of Kleene Relation Algebras studies the regular elements of a Stone-Kleene relation algebra and shows that they form a Kleene relation subalgebra.

* Matrix Kleene Algebras lifts the Kleene star to finite square matrices using Conway’s automata-based construction. This involves an operation to restrict matrices to specific indices and a calculus for such restrictions. An implementation for the Kleene star of matrices was given in [3] without proof; this is the first formally verified correctness proof.

The development is based on a theory of Stone relation algebras [11, 12]. We apply Stone-Kleene relation algebras to verify Prim’s minimum spanning tree algorithm in Isabelle/HOL in [10].

Related libraries for Kleene algebras, regular algebras and relation algebras in the Archive of Formal Proofs are [1, 2, 8]. Kleene algebras are covered in the theory Kleene Algebra/Kleene Algebra.thy, but unlike the
present development it is not based on general algebras using simulation axioms, which are useful to describe various computation models. The theory Regular_Alg/Regular_Alg.thy compares different axiomatisations of regular algebras. The theory Kleene_Alg/Matrix.thy covers matrices over dioids, but does not implement the Kleene star of matrices. The theory Relation_Alg/Relation_Alg_RTC.thy combines Kleene algebras and relation algebras, but is very limited in scope and not applicable as we need the weaker axioms of Stone relation algebras.

2 Iterings

This theory introduces algebraic structures with an operation that describes iteration in various relational computation models. An iteration describes the repeated sequential execution of a computation. This is typically modelled by fixpoints, but different computation models use different fixpoints in the refinement order. We therefore look at equational and simulation axioms rather than induction axioms. Our development is based on [9] and the proposed algebras generalise Kleene algebras.

We first consider a variant of Conway semirings [5] based on idempotent left semirings. Conway semirings expand semirings by an iteration operation satisfying Conway’s sumstar and productstar axioms [7]. Many properties of iteration follow already from these equational axioms.

Next we introduce iterings, which use generalised versions of simulation axioms in addition to sumstar and productstar. Unlike the induction axioms of the Kleene star, which hold only in partial-correctness models, the simulation axioms are also valid in total and general correctness models. They are still powerful enough to prove the correctness of complex results such as separation theorems of [6] and Back’s atomicity refinement theorem [4, 17].

theory Iterings

imports Stone-Relation-Algs.Semirings

begin

2.1 Conway Semirings

In this section, we consider equational axioms for iteration. The algebraic structures are based on idempotent left semirings, which are expanded by a unary iteration operation. We start with an unfold property, one inequality of the sliding rule and distributivity over joins, which is similar to Conway’s sumstar.

class circ =
  fixes circ :: 'a ⇒ 'a (\^ [100] 100)
**class** `left-conway-semiring` = `idempotent-left-semiring + circ +
assumes` `circ-left-unfold: 1 ⊔ x * x° = x°
assumes` `circ-left-slide: (x * y)° * x ≤ x * (y * x)°
assumes` `circ-sup-1: (x ⊔ y)° = x° * (y * x°)°

begin

We obtain one inequality of Conway’s productstar, as well as of the other unfold rule.

**lemma** `circ-mult-sub`:

\[ 1 ⊔ x * (y * x)° * y \leq (x * y)^° \]

⟨proof⟩

**lemma** `circ-right-unfold-sub`:

\[ 1 ⊔ x° * x \leq x° \]

⟨proof⟩

**lemma** `circ-zero`:

\[ bot° = 1 \]

⟨proof⟩

**lemma** `circ-increasing`:

\[ x \leq x° \]

⟨proof⟩

**lemma** `circ-reflexive`:

\[ 1 \leq x° \]

⟨proof⟩

**lemma** `circ-mult-increasing`:

\[ x \leq x * x° \]

⟨proof⟩

**lemma** `circ-mult-increasing-2`:

\[ x \leq x° * x \]

⟨proof⟩

**lemma** `circ-transitive-equal`:

\[ x° * x° = x° \]

⟨proof⟩

While iteration is not idempotent, a fixpoint is reached after applying this operation twice. Iteration is idempotent for the unit.

**lemma** `circ-circ-circ`:

\[ x°°° = x°° \]

⟨proof⟩

**lemma** `circ-one`:

\[ 1° = 1°° \]

⟨proof⟩
lemma circ-sup-sub: 
\((x^\circ \cdot y)^\circ \cdot x^\circ \leq (x \sqcup y)^\circ\)
(proof)

lemma circ-plus-one: 
x^\circ = 1 \sqcup x^\circ
(proof)

Iteration satisfies a characteristic property of reflexive transitive closures.

lemma circ-rtc-2: 
1 \sqcup x \sqcup x^\circ \cdot x^\circ = x^\circ
(proof)

lemma mult-zero-circ: 
\((x \cdot \text{bot})^\circ = 1 \sqcup x \cdot \text{bot}\)
(proof)

lemma mult-zero-sup-circ: 
\((x \sqcup y \cdot \text{bot})^\circ = x^\circ \cdot (y \cdot \text{bot})^\circ\)
(proof)

lemma circ-plus-sub: 
x^\circ \cdot x \leq x \cdot x^\circ
(proof)

lemma circ-loop-fixpoint: 
y \cdot (y^\circ \cdot z) \sqcup z = y^\circ \cdot z
(proof)

lemma left-plus-below-circ: 
x \cdot x^\circ \leq x^\circ
(proof)

lemma right-plus-below-circ: 
x^\circ \cdot x \leq x^\circ
(proof)

lemma circ-sup-upper-bound: 
x \leq z^\circ \implies y \leq z^\circ \implies x \sqcup y \leq z^\circ
(proof)

lemma circ-mult-upper-bound: 
x \leq z^\circ \implies y \leq z^\circ \implies x \cdot y \leq z^\circ
(proof)

lemma circ-sub-dist: 
x^\circ \leq (x \sqcup y)^\circ
(proof)
lemma circ-sub-dist-1:
\[ x \leq (x \sqcup y)^o \]
(proof)

lemma circ-sub-dist-2:
\[ x \ast y \leq (x \sqcup y)^o \]
(proof)

lemma circ-sub-dist-3:
\[ x^o \ast y^o \leq (x \sqcup y)^o \]
(proof)

lemma circ-isotone:
\[ x \leq y \implies x^o \leq y^o \]
(proof)

lemma circ-sup-2:
\[ (x \sqcup y)^o \leq (x^o \ast y^o)^o \]
(proof)

lemma circ-sup-one-left-unfold:
\[ 1 \leq x \implies x \ast x^o = x^o \]
(proof)

lemma circ-sup-one-right-unfold:
\[ 1 \leq x \implies x^o \ast x = x^o \]
(proof)

lemma circ-decompose-4:
\[ (x^o \ast y^o)^o = x^o \ast (y^o \ast x^o)^o \]
(proof)

lemma circ-decompose-5:
\[ (x^o \ast y^o)^o = (y^o \ast x^o)^o \]
(proof)

lemma circ-decompose-6:
\[ x^o \ast (y \ast x^o)^o = y^o \ast (x \ast y^o)^o \]
(proof)

lemma circ-decompose-7:
\[ (x \sqcup y)^o = x^o \ast y^o \ast (x \sqcup y)^o \]
(proof)

lemma circ-decompose-8:
\[ (x \sqcup y)^o = (x \sqcup y)^o \ast x^o \ast y^o \]
(proof)
lemma circ-decompose-9:
\((x^\circ \ast y^\circ)^\circ = x^\circ \ast y^\circ \ast (x^\circ \ast y^\circ)^\circ\)
\langle proof \rangle

lemma circ-decompose-10:
\((x^\circ \ast y^\circ)^\circ = (x^\circ \ast y^\circ)^\circ \ast x^\circ \ast y^\circ\)
\langle proof \rangle

lemma circ-back-loop-prefixpoint:
\((z \ast y^\circ) \ast y \sqcup z \leq z \ast y^\circ\)
\langle proof \rangle

We obtain the fixpoint and prefixpoint properties of iteration, but not least or greatest fixpoint properties.

lemma circ-loop-is-fixpoint:
\text{is-fixpoint} (\lambda x \cdot y \ast x \sqcup z) (y^\circ \ast z)
\langle proof \rangle

lemma circ-back-loop-is-prefixpoint:
\text{is-prefixpoint} (\lambda x \cdot x \ast y \sqcup z) (z \ast y^\circ)
\langle proof \rangle

lemma circ-circ-sup:
\((1 \sqcup x)^\circ = x^{\circ\circ}\)
\langle proof \rangle

lemma circ-circ-mult-sub:
\(x^\circ \ast 1^\circ \leq x^{\circ\circ}\)
\langle proof \rangle

lemma left-plus-circ:
\((x \ast x^\circ)^\circ = x^\circ\)
\langle proof \rangle

lemma right-plus-circ:
\((x^\circ \ast x)^\circ = x^\circ\)
\langle proof \rangle

lemma circ-square:
\((x \ast x)^\circ \leq x^\circ\)
\langle proof \rangle

lemma circ-mult-sub-sup:
\((x \ast y)^\circ \leq (x \sqcup y)^\circ\)
\langle proof \rangle

lemma circ-sup-mult-zero:
\(x^\circ \ast y = (x \sqcup y \ast \text{bot})^{\circ\circ} \ast y\)
\langle proof \rangle
lemma troeger-1:
\[(x \sqcup y)^o = x^o \ast (I \sqcup y \ast (x \sqcup y)^o)\]
⟨proof⟩

lemma troeger-2:
\[(x \sqcup y)^o \ast z = x^o \ast (y \ast (x \sqcup y)^o \ast z \sqcup z)\]
⟨proof⟩

lemma troeger-3:
\[(x \sqcup y \ast \bot)^o = x^o \ast (I \sqcup y \ast \bot)\]
⟨proof⟩

lemma circ-sup-sub-sup-one-1:
\[x \sqcup y \leq x^o \ast (I \sqcup y)\]
⟨proof⟩

lemma circ-sup-sub-sup-one-2:
\[x^o \ast (x \sqcup y) \leq x^o \ast (I \sqcup y)\]
⟨proof⟩

lemma circ-sup-sub-sup-one:
\[x \ast x^o \ast (x \sqcup y) \leq x \ast x^o \ast (I \sqcup y)\]
⟨proof⟩

lemma circ-square-2:
\[(x \ast x)^o \ast (x \sqcup 1) \leq x^o\]
⟨proof⟩

lemma circ-extra-circ:
\[(y \ast x^o)^o = (y \ast y^o \ast x^o)^o\]
⟨proof⟩

lemma circ-circ-sub-mult:
\[1^o \ast x^o \leq x^{o^o}\]
⟨proof⟩

lemma circ-decompose-11:
\[(x^o \ast y^o)^o = (x^o \ast y^o)^o \ast x\]
⟨proof⟩

lemma circ-mult-below-circ-circ:
\[(x \ast y)^o \leq (x^o \ast y)^o \ast x^o\]
⟨proof⟩

end

The next class considers the interaction of iteration with a greatest ele-
class bounded-left-conway-semiring = bounded-idempotent-left-semiring + left-conway-semiring
begin

lemma circ-top:
  \( \text{top}^\circ = \text{top} \) 
\langle proof \rangle

lemma circ-right-top:
  \( x^\circ * \text{top} = \text{top} \) 
\langle proof \rangle

lemma circ-left-top:
  \( \text{top} * x^\circ = \text{top} \) 
\langle proof \rangle

lemma mult-top-circ:
  \( (x * \text{top})^\circ = 1 \sqcup x * \text{top} \) 
\langle proof \rangle
end

class left-zero-conway-semiring = idempotent-left-zero-semiring + left-conway-semiring
begin

lemma mult-zero-sup-circ-2:
  \( (x \sqcup y * \text{bot})^\circ = x^\circ \sqcup x^\circ * y * \text{bot} \) 
\langle proof \rangle

lemma circ-unfold-sum:
  \( (x \sqcup y)^\circ = x^\circ \sqcup x^\circ * y * (x \sqcup y)^\circ \) 
\langle proof \rangle
end

The next class assumes the full sliding equation.

class left-conway-semiring-1 = left-conway-semiring +
assumes circ-right-slide: \( x * (y * x)^\circ \leq (x * y)^\circ * x \)
begin

lemma circ-slide-1:
  \( x * (y * x)^\circ = (x * y)^\circ * x \) 
\langle proof \rangle

  This implies the full unfold rules and Conway’s productstar.

lemma circ-right-unfold-1:
  \( 1 \sqcup x^\circ * x = x^\circ \)
lemma circ-mult-1:
\[(x \ast y)^0 = 1 \sqcap x \ast (y \ast x)^0 \ast y\]

lemma circ-sup-9:
\[(x \sqcup y)^0 = (x^0 \ast y)^0 \ast x^0\]

lemma circ-plus-same:
\[x^0 \ast x = x \ast x^0\]

lemma circ-decompose-12:
\[x^0 \ast y^0 \leq (x^0 \ast y)^0 \ast x^0\]


class left-zero-conway-semiring-1 = left-zero-conway-semiring +
left-conway-semiring-1
begin

lemma circ-back-loop-fixpoint:
\[(z \ast y^0) \ast y \sqcap z = z \ast y^0\]

lemma circ-back-loop-is-fixpoint:
is-fixpoint \(\lambda x \ast x \ast y \sqcap z\) (z \ast y^0)\n
lemma circ-elimination:
\[x \ast y = \bot \implies x \ast y^0 \leq x\]

end

2.2 Iterings

This section adds simulation axioms to Conway semirings. We consider several classes with increasingly general simulation axioms.

class itering-1 = left-conway-semiring-1 +
assumes circ-simulate: \(z \ast x \leq y \ast z \longrightarrow z \ast x^0 \leq y^0 \ast z\)

begin

lemma circ-circ-mult:
\[1^0 \ast x^0 = x^{00}\]

end
lemma sub-mult-one-circ:
\[ x \ast 1^\circ \leq 1^\circ \ast x \]
⟨proof⟩

The left simulation axioms is enough to prove a basic import property of tests.

lemma circ-import:
assumes \( p \leq p \ast p \)
   and \( p \leq 1 \)
   and \( p \ast x \leq x \ast p \)
shows \( p \ast x^\circ = p \ast (p \ast x)^\circ \)
⟨proof⟩

end

Including generalisations of both simulation axioms allows us to prove separation rules.

class itering-2 = left-conway-semiring-1 +
assumes circ-simulate-right: \( z \ast x \leq y \ast z \sqcup w \Longrightarrow z \ast x^\circ \leq y^\circ \ast (z \sqcup w \ast x^\circ) \)
assumes circ-simulate-left: \( x \ast z \leq z \ast y \sqcup w \Longrightarrow x^\circ \ast z \leq (z \sqcup x^\circ \ast w) \ast y^\circ \)
begin
subclass itering-1
⟨proof⟩

lemma circ-simulate-left-1:
\[ x \ast z \leq z \ast y \Longrightarrow x^\circ \ast z \leq z \ast y^\circ \sqcup x^\circ \ast bot \]
⟨proof⟩

lemma circ-separate-1:
assumes \( y \ast x \leq x \ast y \)
shows \( (x \sqcup y)^\circ = x^\circ \ast y^\circ \)
⟨proof⟩

lemma circ-circ-mult-1:
\[ x^\circ \ast 1^\circ = x^\circ^\circ \]
⟨proof⟩

end

With distributivity, we also get Back’s atomicity refinement theorem.

class itering-3 = itering-2 + left-zero-conway-semiring-1
begin

lemma circ-simulate-1:
assumes \( y \ast x \leq x \ast y \)
shows \( y^\circ \ast x^\circ \leq x^\circ \ast y^\circ \)
⟨proof⟩
lemma atomicity-refinement:
  assumes $s = s \circ q$
  and $x = q \circ x$
  and $q \circ b = \bot$
  and $r \circ q \leq b \circ r$
  and $r \circ l \leq l \circ r$
  and $x \circ l \leq l \circ x$
  and $b \circ l \leq l \circ b$
  and $q \circ l \leq l \circ q$
  and $r_0 \circ q \leq q \circ r_0$
  and $q \leq 1$
  shows $s \circ (x \sqcup b \sqcup r \sqcup l)^\circ \circ q \leq s \circ (x \circ b_0 \circ q \sqcup r \sqcup l)^\circ$
⟨proof⟩
end

The following class contains the most general simulation axioms we consider. They allow us to prove further separation properties.
class iterating = idempotent-left-zero-semiring + circ +
  assumes circ-sup: $(x \sqcup y)^\circ = (x^\circ \circ y^\circ)^\circ \circ x^\circ$
  assumes circ-mult: $(x \circ y)^\circ = 1 \sqcup x \circ (y \circ x)^\circ \circ y$
  assumes circ-simulate-right-plus: $z \circ x \leq y \circ y^\circ \circ z \sqcup w \rightarrow z \circ x^\circ \leq y^\circ \circ (z \sqcup w \sqcup x^\circ)$
  assumes circ-simulate-left-plus: $x \circ z \leq z \circ y^\circ \sqcup w \rightarrow x^\circ \circ z \leq (z \sqcup x^\circ \circ w) \circ y^\circ$
begin

lemma circ-right-unfold:
  $1 \sqcup x^\circ \circ x = x^\circ$
⟨proof⟩

lemma circ-slide:
  $x \circ (y \circ x)^\circ = (x \circ y)^\circ \circ x$
⟨proof⟩

subclass iterating-3
⟨proof⟩

lemma circ-simulate-right-plus-1:
  $z \circ x \leq y \circ y^\circ \circ z \implies z \circ x^\circ \leq y^\circ \circ z$
⟨proof⟩

lemma circ-simulate-left-plus-1:
  $x \circ z \leq z \circ y^\circ \implies x^\circ \circ z \leq z \circ y^\circ \sqcup x^\circ \circ \bot$
⟨proof⟩

lemma circ-simulate-2:
  $y \circ x^\circ \leq x^\circ \circ y^\circ \iff y^\circ \circ x^\circ \leq x^\circ \circ y^\circ$
lemma circ-simulate-absorb:
\[ y \star x \leq x \implies y \circ x \leq x \sqcup y \circ \bot \]
\[
\text{proof}
\]

lemma circ-simulate-3:
\[ y \star x \circ \leq x \circ \implies y \circ x \star \leq x \circ \circ y \circ \]
\[
\text{proof}
\]

lemma circ-separate-mult-1:
\[ y \star x \leq x \star y \implies (x \star y) \circ \leq x \circ \star y \circ \]
\[
\text{proof}
\]

lemma circ-separate-unfold:
\[ (y \star x \circ) = y \circ \sqcup y \circ \circ y \star x \circ \star (y \star x \circ) \]
\[
\text{proof}
\]

lemma separation:
\[ \text{assumes } y \star x \leq x \star y \circ \]
\[ \text{shows } (x \sqcup y) \circ = x \circ \star y \circ \]
\[
\text{proof}
\]

lemma simulation:
\[ y \star x \leq x \star y \circ \implies y \circ x \circ \leq x \circ \star y \circ \]
\[
\text{proof}
\]

lemma circ-simulate-4:
\[ \text{assumes } y \star x \leq x \star y \circ \star (1 \sqcup y) \]
\[ \text{shows } y \circ x \circ \leq x \circ \star y \circ \]
\[
\text{proof}
\]

lemma circ-simulate-5:
\[ y \star x \leq x \star x \circ (x \sqcup y) \implies y \circ x \circ \leq x \circ \star y \circ \]
\[
\text{proof}
\]

lemma circ-simulate-6:
\[ y \star x \leq x \star (x \sqcup y) \implies y \circ x \circ \leq x \circ \star y \circ \]
\[
\text{proof}
\]

lemma circ-separate-4:
\[ \text{assumes } y \star x \leq x \star y \circ \star (1 \sqcup y) \]
\[ \text{shows } (x \sqcup y) \circ = x \circ \star y \circ \]
\[
\text{proof}
\]

lemma circ-separate-5:
\[ y \star x \leq x \star x \circ (x \sqcup y) \implies (x \sqcup y) \circ = x \circ \star y \circ \]
\[
\text{proof}
\]
lemma \textit{circ-separate-6}:
\[ y \ast x \leq x \ast (x \sqcup y) \implies (x \sqcup y) = x^o \ast y^o \]
\langle proof \rangle
end

class \textit{bounded-itering} = \textit{bounded-idempotent-left-zero-semiring} + \textit{itering}
begin
subclass \textit{bounded-left-conway-semiring} \langle proof \rangle
end

We finally expand Conway semirings and iterings by an element that corresponds to the endless loop.

class \textit{L} =
\begin{align*}
\text{fixes } & L :: 'a \\
\text{class } & \textit{left-conway-semiring-L} = \textit{left-conway-semiring} + \textit{L} + \\
\text{assumes } & \textit{one-circ-mult-split}: \quad 1^o \ast x = L \sqcup x \\
\text{assumes } & \textit{L-split-sup}: \quad x \ast (y \sqcup L) \leq x \ast y \sqcup L
\end{align*}
begin
lemma \textit{L-def}:
\[ L = 1^o \ast \bot \]
\langle proof \rangle

lemma \textit{one-circ-split}:
\[ 1^o = L \sqcup 1 \]
\langle proof \rangle

lemma \textit{one-circ-circ-split}:
\[ 1^{oo} = L \sqcup 1 \]
\langle proof \rangle

lemma \textit{sub-mult-one-circ}:
\[ x \ast 1^o \leq 1^o \ast x \]
\langle proof \rangle

lemma \textit{one-circ-mult-split-2}:
\[ 1^o \ast x = x \ast 1^o \sqcup L \]
\langle proof \rangle

lemma \textit{sub-mult-one-circ-split}:
\[ x \ast 1^o \leq x \sqcup L \]
\langle proof \rangle

14
lemma \textit{sub-mult-one-circ-split-2}: 
\[ x \cdot 1^\circ \leq x \sqcup 1^\circ \] 
\langle \text{proof} \rangle 

lemma \textit{L-split}: 
\[ x \cdot L \leq x \cdot \text{bot} \sqcup L \] 
\langle \text{proof} \rangle 

lemma \textit{L-left-zero}: 
\[ L \cdot x = L \] 
\langle \text{proof} \rangle 

lemma \textit{one-circ-L}: 
\[ 1^\circ \cdot L = L \] 
\langle \text{proof} \rangle 

lemma \textit{mult-L-circ}: 
\[ (x \cdot L)^\circ = 1 \sqcup x \cdot L \] 
\langle \text{proof} \rangle 

lemma \textit{mult-L-circ-mult}: 
\[ (x \cdot L)^\circ \cdot y = y \sqcup x \cdot L \] 
\langle \text{proof} \rangle 

lemma \textit{circ-L}: 
\[ L^\circ = L \sqcup 1 \] 
\langle \text{proof} \rangle 

lemma \textit{L-below-one-circ}: 
\[ L \leq 1^\circ \] 
\langle \text{proof} \rangle 

lemma \textit{circ-circ-mult-1}: 
\[ x^\circ \cdot 1^\circ = x^{\circ\circ} \] 
\langle \text{proof} \rangle 

lemma \textit{circ-circ-mult}: 
\[ 1^\circ \cdot x^\circ = x^{\circ\circ} \] 
\langle \text{proof} \rangle 

lemma \textit{circ-circ-split}: 
\[ x^{\circ\circ} = L \sqcup x^\circ \] 
\langle \text{proof} \rangle 

lemma \textit{circ-sup-6}: 
\[ L \sqcup (x \sqcup y)^\circ = (x^\circ \cdot y^\circ)^\circ \] 
\langle \text{proof} \rangle 

end
class \texttt{itering-L} = \texttt{itering} + \texttt{L} +
\texttt{assumes} \texttt{L-def}: \texttt{L} = 1^\circ \ast \texttt{bot}
\begin{verbatim}
lemma \texttt{one-circ-split}:
1^\circ \ast \texttt{L} \sqcup 1
\texttt{⟨proof⟩}

lemma \texttt{one-circ-mult-split}:
1^\circ \ast x = \texttt{L} \sqcup x
\texttt{⟨proof⟩}

lemma \texttt{sub-mult-one-circ-split}:
x \ast 1^\circ \leq x \sqcup \texttt{L}
\texttt{⟨proof⟩}

lemma \texttt{sub-mult-one-circ-split-2}:
x \ast 1^\circ \leq x \sqcup 1^\circ
\texttt{⟨proof⟩}

lemma \texttt{L-split}:
x \ast \texttt{L} \leq x \ast \texttt{bot} \sqcup \texttt{L}
\texttt{⟨proof⟩}

subclass \texttt{left-conway-semiring-L}
\texttt{⟨proof⟩}

lemma \texttt{circ-left-induct-mult-L}:
\texttt{L} \leq x \Rightarrow x \ast y \leq x \Rightarrow x \ast y^\circ \leq x
\texttt{⟨proof⟩}

lemma \texttt{circ-left-induct-mult-iff-L}:
\texttt{L} \leq x \Rightarrow x \ast y \leq x \iff x \ast y^\circ \leq x
\texttt{⟨proof⟩}

lemma \texttt{circ-left-induct-L}:
\texttt{L} \leq x \Rightarrow x \ast \texttt{L} \sqcup z \leq x \Rightarrow z \ast y^\circ \leq x
\texttt{⟨proof⟩}
\end{verbatim}
end
end

3 Kleene Algebras

Kleene algebras have been axiomatised by Kozen to describe the equational theory of regular languages \cite{13}. Binary relations are another important
model. This theory implements variants of Kleene algebras based on idempotent left semirings [15]. The weakening of some semiring axioms allows the treatment of further computation models. The presented algebras are special cases of iterings, so many results can be inherited.

theory Kleene-Algebras

imports Iterings

begin

We start with left Kleene algebras, which use the left unfold and left induction axioms of Kleene algebras.

class star =
  fixes star :: 'a ⇒ 'a (⋆ [100] 100)

class left-kleene-algebra = idempotent-left-semiring + star +
  assumes star-left-unfold : I ⊔ y * y* ≤ y*
  assumes star-left-induct : z ⊔ y * x ≤ x −→ y* * z ≤ x

begin

no-notation
  trancl (((⋯) [1000] 999))

abbreviation tc (⋯ [100] 100) where tc x ≡ x * x

lemma star-left-unfold-equal:
  1 ⊔ x * x* = x*  ⟨proof⟩

  This means that for some properties of Kleene algebras, only one inequality can be derived, as exemplified by the following sliding rule.

lemma star-left-slide:
  (x * y)* * x ≤ x * (y * x)*
  ⟨proof⟩

lemma star-isotone:
  x ≤ y ⇒ x* ≤ y*
  ⟨proof⟩

lemma star-sup-1:
  (x ⊔ y)* = x* * (y * x*)*
  ⟨proof⟩

end

We now show that left Kleene algebras form iterings. A sublocale is used instead of a subclass, because iterings use a different iteration operation.

sublocale left-kleene-algebra < star: left-conway-semiring where circ = star
context left-kleene-algebra
begin

A number of lemmas in this class are taken from Georg Struth’s Kleene algebra theory [2].

lemma star-sub-one:
\( x \leq 1 \implies x^* = 1 \)
⟨proof⟩

lemma star-one:
\( 1^* = 1 \)
⟨proof⟩

lemma star-left-induct-mult:
\( x \cdot y \leq y \implies x^* \cdot y \leq y \)
⟨proof⟩

lemma star-left-induct-mult-iff:
\( x \cdot y \leq y \iff x^* \cdot y \leq y \)
⟨proof⟩

lemma star-involutive:
\( x^* = x^{**} \)
⟨proof⟩

lemma star-sup-one:
\( (1 \sqcup x)^* = x^* \)
⟨proof⟩

lemma star-left-induct-equal:
\( z \sqcup x \cdot y = y \implies x^* \cdot z \leq y \)
⟨proof⟩

lemma star-left-induct-mult-equal:
\( x \cdot y = y \implies x^* \cdot y \leq y \)
⟨proof⟩

lemma star-star-upper-bound:
\( x^* \leq z^* \implies x^{**} \leq z^* \)
⟨proof⟩

lemma star-simulation-left:
assumes \( x \cdot z \leq z \cdot y \)
shows \( x^* \cdot z \leq z \cdot y^* \)
⟨proof⟩

lemma quasicomm-1:
\begin{proof}
y \ast x \leq x \ast (x \sqcup y)^* \iff y^* \ast x \leq x \ast (x \sqcup y)^*
\end{proof}

\textbf{lemma} star-rtc-3:
\begin{proof}
1 \sqcup x \sqcup y \ast y = y \implies x^* \leq y
\end{proof}

\textbf{lemma} star-decompose-1:
\begin{proof}
(x \sqcup y)^* = (x^* \ast y^*)^*
\end{proof}

\textbf{lemma} star-sum:
\begin{proof}
(x \sqcup y)^* = (x^* \sqcup y^*)^*
\end{proof}

\textbf{lemma} star-decompose-3:
\begin{proof}
(x^* \ast y^*)^* = x^* \ast (y \ast x^*)^*
\end{proof}

In contrast to iterings, we now obtain that the iteration operation results in least fixpoints.

\textbf{lemma} star-loop-least-fixpoint:
\begin{proof}
y \ast x \sqcup z = x \implies y^* \ast z \leq x
\end{proof}

\textbf{lemma} star-loop-is-least-fixpoint:
\begin{proof}
is-least-fixpoint (\lambda x . y \ast x \sqcup z) (y^* \ast z)
\end{proof}

\textbf{lemma} star-loop-mu:
\begin{proof}
\mu (\lambda x . y \ast x \sqcup z) = y^* \ast z
\end{proof}

\textbf{lemma} affine-has-least-fixpoint:
\begin{proof}
has-least-fixpoint (\lambda x . y \ast x \sqcup z)
\end{proof}

\textbf{lemma} star-outer-increasing:
\begin{proof}
x \leq y^* \ast x \ast y^*
\end{proof}

\textbf{end}\n
We next add the right induction rule, which allows us to strengthen many inequalities of left Kleene algebras to equalities.

\textbf{class} strong-left-kleene-algebra = left-kleene-algebra +
\textbf{assumes} star-right-induct: z \sqcup x \ast y \leq x \implies z \ast y^* \leq x
begin

lemma star-plus:
\[ y^* \cdot y = y \cdot y^* \]
⟨proof⟩

lemma star-slide:
\[ (x \cdot y)^* \cdot x = x \cdot (y \cdot x)^* \]
⟨proof⟩

lemma star-simulation-right:
assumes \( z \cdot x \leq y \cdot z \)
shows \( z \cdot x^* \leq y^* \cdot z \)
⟨proof⟩

end

Again we inherit results from the itering hierarchy.

sublocale strong-left-kleene-algebra < star: itering-1 where circ = star
⟨proof⟩

context strong-left-kleene-algebra
begin

lemma star-right-induct-mult:
\( y \cdot x \leq y \Rightarrow y \cdot x^* \leq y \)
⟨proof⟩

lemma star-right-induct-mult-iff:
\( y \cdot x \leq y \iff y \cdot x^* \leq y \)
⟨proof⟩

lemma star-simulation-right-equal:
\( z \cdot x = y \cdot z \Rightarrow z \cdot x^* = y^* \cdot z \)
⟨proof⟩

lemma star-simulation-star:
\( x \cdot y \leq y \cdot x \Rightarrow x^* \cdot y^* \leq y^* \cdot x^* \)
⟨proof⟩

lemma star-right-induct-equal:
\( z \sqcup y \cdot x = y \Rightarrow z \cdot x^* \leq y \)
⟨proof⟩

lemma star-right-induct-mult-equal:
\( y \cdot x = y \Rightarrow y \cdot x^* \leq y \)
⟨proof⟩

lemma star-back-loop-least-fixpoint:
\[ x * y \sqcup z = x \implies z * y^* \leq x \]

\textit{proof}

\textbf{lemma} \textit{star-back-loop-is-least-fixpoint}:

\textit{is-least-fixpoint} (\( \lambda x . \; x * y \sqcup z \)) (\( z * y^* \))

\textit{proof}

\textbf{lemma} \textit{star-back-loop-mu}:

\( \mu (\lambda x . \; x * y \sqcup z) = z * y^* \)

\textit{proof}

\textbf{lemma} \textit{star-square}:

\( x^* = (I \sqcup x) * (x * x)^* \)

\textit{proof}

\textbf{lemma} \textit{star-square-2}:

\( x^* = (x * x)^* * (x \sqcup 1) \)

\textit{proof}

\textbf{lemma} \textit{star-circ-simulate-right-plus}:

\textbf{assumes} \( z * x \leq y * y^* * z \sqcup w \)

\textbf{shows} \( z * x^* \leq y^* * (z \sqcup w * x^*) \)

\textit{proof}

\textbf{lemma} \textit{transitive-star}:

\( x * x \leq x \implies x^* = 1 \sqcup x \)

\textit{proof}

\textit{end}

The following class contains a generalisation of Kleene algebras, which lacks the right zero axiom.

\textbf{class} \textit{left-zero-kleene-algebra} = \textit{idempotent-left-zero-semiring} + \textit{strong-left-kleene-algebra}

\textit{begin}

\textbf{lemma} \textit{star-star-absorb}:

\( y^* * (y^* * x)^* * y^* = (y^* * x)^* * y^* \)

\textit{proof}

\textbf{lemma} \textit{star-circ-simulate-left-plus}:

\textbf{assumes} \( x * z \leq z * y^* \sqcup w \)

\textbf{shows} \( x^* * z \leq (z \sqcup x^* * w) * y^* \)

\textit{proof}

\textbf{lemma} \textit{star-one-sup-below}:

\( x * y^* * (I \sqcup z) \leq x * (y \sqcup z)^* \)
The following theorem is similar to the puzzle where persons insert themselves always in the middle between two groups of people in a line. Here, however, items in the middle annihilate each other, leaving just one group of items behind.

**Lemma cancel-separate:**

_**assumes**_ $x \ast y \leq 1$

_**shows**_ $x^* \ast y^* \leq x^* \sqcup y^*$

(\textit{proof})

**Lemma star-separate:**

_**assumes**_ $x \ast y = \bot$

_**and**_ $y \ast y = \bot$

_**shows**_ $(x \sqcup y)^* = x^* \sqcup y \ast x^*$

(\textit{proof})

\end

We can now inherit from the strongest variant of iterings.

**Sublocale** left-zero-kleene-algebra < star: itering where circ = star

(\textit{proof})

\begin

**Lemma star-absorb:**

$x \ast y = \bot \implies x \ast y^* = x$

(\textit{proof})

**Lemma star-separate-2:**

_**assumes**_ $x \ast z^+ \ast y = \bot$

_**and**_ $y \ast z^+ \ast y = \bot$

_**and**_ $z \ast x = \bot$

_**shows**_ $(x^* \sqcup y \ast x^*) \ast (z \ast (1 \sqcup y \ast x^*))^* = z^* \ast (x^* \sqcup y \ast x^*) \ast z^*$

(\textit{proof})

**Lemma cancel-separate-eq:**

$x \ast y \leq 1 \implies x^* \ast y^* = x^* \sqcup y^*$

(\textit{proof})

**Lemma cancel-separate-1:**

_**assumes**_ $x \ast y \leq 1$

_**shows**_ $(x \sqcup y)^* = y^* \ast x^*$

(\textit{proof})

**Lemma plus-sup:**

$(x \sqcup y)^+ = (x^* \ast y)^* \ast x^+ \sqcup (x^* \ast y)^+$

(\textit{proof})
lemma plus-half-bot:
\( x \cdot y \cdot x = \bot \implies (x \cdot y)^+ = x \cdot y \)  
⟨proof⟩

lemma cancel-separate-1-sup:
assumes \( x \cdot y \leq 1 \)
and \( y \cdot x \leq 1 \)
shows \((x \sqcup y)^* = x^* \sqcup y^*\)
⟨proof⟩
end

A Kleene algebra is obtained by requiring an idempotent semiring.

class kleene-algebra = left-zero-kleene-algebra + idempotent-semiring

The following classes are variants of Kleene algebras expanded by an additional iteration operation. This is useful to study the Kleene star in computation models that do not use least fixpoints in the refinement order as the semantics of recursion.

class left-kleene-conway-semiring = left-kleene-algebra + left-conway-semiring
begin

lemma star-below-circ:
\( x^* \leq x^0 \)  
⟨proof⟩

lemma star-zero-below-circ-mult:
\( x^* \cdot \bot \leq x^0 \cdot y \)  
⟨proof⟩

lemma star-mult-circ:
\( x^* \cdot x^0 = x^0 \)  
⟨proof⟩

lemma circ-mult-star:
\( x^0 \cdot x^* = x^0 \)  
⟨proof⟩

lemma circ-star:
\( x^{*0} = x^0 \)  
⟨proof⟩

lemma star-circ:
\( x^{*0} = x^{00} \)  
⟨proof⟩

lemma circ-sup-3:
\((x^0 \cdot y^0)^* \leq (x \sqcup y)^0 \)

23
The following classes add a greatest element.

class bounded-left-kleene-algebra = bounded-idempotent-left-semiring + left-kleene-algebra

subclass bounded-left-kleene-algebra < star: bounded-left-conway-semiring
where circ = star ⟨proof⟩

class bounded-left-zero-kleene-algebra = bounded-idempotent-left-semiring +
left-zero-kleene-algebra

sublocale bounded-left-zero-kleene-algebra < star: bounded-itering where circ = star ⟨proof⟩

class bounded-kleene-algebra = bounded-idempotent-semiring + kleene-algebra

sublocale bounded-kleene-algebra < star: bounded-itering where circ = star ⟨proof⟩

We conclude with an alternative axiomatisation of Kleene algebras.

class kleene-algebra-var = idempotent-semiring + star +
  assumes star-left-unfold-var : 1 ⊔ y * y^* ≤ y^*
  assumes star-left-induct-var : y * x ≤ x → y^* * x ≤ x
  assumes star-right-induct-var : x * y ≤ x → x * y^* ≤ x

begin

subclass kleene-algebra
  ⟨proof⟩

end

end

4 Kleene Relation Algebras

This theory combines Kleene algebras with Stone relation algebras. Relation algebras with transitive closure have been studied by [16]. The weakening to Stone relation algebras allows us to talk about reachability in weighted graphs, for example.

Many results in this theory are used in the correctness proof of Prim’s minimum spanning tree algorithm. In particular, they are concerned with the exchange property, preservation of parts of the invariant and with establishing parts of the postcondition.

theory Kleene-Relation-Algebras


begin

We first note that bounded distributive lattices can be expanded to Kleene algebras by reusing some of the operations.

sublocale bounded-distrib-lattice < comp-inf: bounded-kleene-algebra where star = λx . top and one = top and times = inf
  ⟨proof⟩
We add the Kleene star operation to each of bounded distributive allegories, pseudocomplemented distributive allegories and Stone relation algebras. We start with single-object bounded distributive allegories.

```
class bounded-distrib-kleene-allegory = bounded-distrib-allegory + kleene-algebra
begin

subclass bounded-kleene-algebra (proof)

lemma conv-star-conv:
  x^* ≤ x^{T*T}
  (proof)

  It follows that star and converse commute.

lemma conv-star-commute:
  x^{*T} = x^{T*}
  (proof)

lemma conv-plus-commute:
  x^{+T} = x^{T+}
  (proof)

  The following results are variants of a separation lemma of Kleene algebras.

lemma cancel-separate-2:
  assumes x * y ≤ 1
  shows ((w ∩ x) ∪ (z ∩ y))^* = (z ∩ y)^* * (w ∩ x)^*
  (proof)

lemma cancel-separate-3:
  assumes x * y ≤ 1
  shows (w ∩ x)^* * (z ∩ y)^* = (w ∩ x)^* ∪ (z ∩ y)^*
  (proof)

lemma cancel-separate-4:
  assumes z * y ≤ 1
  and w ≤ y ∪ z
  and x ≤ y ∪ z
  shows w^* * x^* = (w ∩ y)^* * ((w ∩ z)^* ∪ (x ∩ y)^*) * (x ∩ z)^*
  (proof)

lemma cancel-separate-5:
  assumes w * z^T ≤ 1
  shows w ∩ x * (y ∩ z) ≤ y
  (proof)

lemma cancel-separate-6:
  assumes z * y ≤ 1
  and w ≤ y ∪ z
  and x ≤ y ∪ z
```

26
and $v^* z^T \leq 1$
and $v \sqcap y^* = \text{bot}$
shows $v \sqcap w^* x^* \leq x \sqcup w$

(proof)

We show several results about the interaction of vectors and the Kleene star.

lemma vector-star-1:
assumes vector $x$
shows $x^T (x^* x^T)^* \leq x^T$
(proof)

lemma vector-star-2:
vector $x \Longrightarrow x^T (x^* x^T)^* \leq x^T \ast \text{bot}^*$
(proof)

lemma vector-vector-star:
vector $v \Longrightarrow (v^* v^T)^* = 1 \sqcup v^* v^T$
(proof)

The following equivalence relation characterises the component trees of a forest. This is a special case of undirected reachability in a directed graph.

abbreviation forest-components $f \equiv f^T* f^*$

lemma forest-components-equivalence:
injective $x \Longrightarrow$ equivalence (forest-components $x$)
(proof)

lemma forest-components-increasing:
$x \leq$ forest-components $x$
(proof)

lemma forest-components-isotone:
$x \leq y \Longrightarrow$ forest-components $x \leq$ forest-components $y$
(proof)

lemma forest-components-idempotent:
injective $x \Longrightarrow$ forest-components (forest-components $x$) = forest-components $x$
(proof)

lemma forest-components-star:
injective $x \Longrightarrow$ (forest-components $x$)$^* =$ forest-components $x$
(proof)

The following lemma shows that the nodes reachable in the graph can
be reached by only using edges between reachable nodes.

lemma reachable-restrict:
assumes vector $r$
shows $r^T g^* = r^T ((r^T g^*)^T \ast (r^T g^*) \sqcap g)^*$
lemma kruskal-acyclic-inv-1:
assumes injective f
and e * forest-components f * e = bot
shows (f ∩ top * e * f^T) * f^T * e = bot

lemma kruskal-forest-components-inf-1:
assumes f ≤ w ⊔ w^T
and injective w
and f ≤ forest-components g
shows f * forest-components (forest-components g ∩ w) ≤ forest-components (forest-components g ∩ w)

lemma kruskal-forest-components-inf:
assumes f ≤ w ⊔ w^T
and injective w
shows forest-components f ≤ forest-components (forest-components f ∩ w)

end

We next add the Kleene star to single-object pseudocomplemented distributive allegories.
class pd-kleene-allegory = pd-allegory + bounded-distrib-kleene-allegory
begin

The following definitions and results concern acyclic graphs and forests.
abbreviation acyclic :: 'a ⇒ bool where acyclic x ≡ x^+ ≤ −1
abbreviation forest :: 'a ⇒ bool where forest x ≡ injective x ∧ acyclic x

lemma forest-bot:
forest bot
(proof)

lemma acyclic-star-below-complement:
acyclic w ⇐ w^T * ≤ −w
(proof)

lemma acyclic-star-below-complement-1:
acyclic w ⇐ w * ∩ w^T = bot
(proof)

lemma acyclic-star-inf-conv:
assumes acyclic w
shows w^* ∩ w^T * = 1
proof

lemma acyclic-asymmetric:
acyclic \( w \implies \) asymmetric \( w \)
(proof)

lemma forest-separate:
assumes forest \( x \)
sows \( x^* \star x^T \star \cap x^T \star x \leq 1 \)
(proof)

The following definition captures the components of undirected weighted graphs.

abbreviation components \( g \equiv (-g)^* \)

lemma components-equivalence:
symmetric \( x \implies \) equivalence (components \( x \))
(proof)

lemma components-increasing:
\( x \leq \) components \( x \)
(proof)

lemma components-isotone:
\( x \leq y \implies \) components \( x \leq \) components \( y \)
(proof)

lemma cut-reachable:
assumes \( v^T = r^T \star t^* \)
and \( t \leq g \)
sows \( v \star -v^T \cap g \leq (r^T \star g^*)^T \star (r^T \star g^*) \)
(proof)

The following lemma shows that the predecessors of visited nodes in the minimum spanning tree extending the current tree have all been visited.

lemma predecessors-reachable:
assumes vector \( r \)
and injective \( r \)
and \( v^T = r^T \star t^* \)
and forest \( w \)
and \( t \leq w \)
and \( w \leq (r^T \star g^*)^T \star (r^T \star g^*) \cap g \)
and \( r^T \star g^* \leq r^T \star w^* \)
sows \( w \star v \leq v \)
(proof)

4.1 Prim’s Algorithm
The following results are used for proving the correctness of Prim’s minimum spanning tree algorithm.

### 4.1.1 Preservation of Invariant

We first treat the preservation of the invariant. The following lemma shows that the while-loop preserves that \( v \) represents the nodes of the constructed tree. The remaining lemmas in this section show that \( t \) is a spanning tree. The exchange property is treated in the following two sections.

**lemma reachable-inv:**
\[
\text{assumes vector } v \\
\text{ and } e \leq v \ast -v^T \\
\text{ and } e \ast t = \text{bot} \\
\text{ and } v^T = r^T \ast t^* \\
\text{ shows } (v \sqcup e^T \ast \text{top})^T = r^T \ast (t \sqcup e)^* \\
\langle \text{proof} \rangle
\]

The next result is used to show that the while-loop preserves acyclicity of the constructed tree.

**lemma acyclic-inv:**
\[
\text{assumes acyclic } t \\
\text{ and vector } v \\
\text{ and } e \leq v \ast -v^T \\
\text{ and } t \leq v \ast v^T \\
\text{ shows acyclic } (t \sqcup e) \\
\langle \text{proof} \rangle
\]

The following lemma shows that the extended tree is in the component reachable from the root.

**lemma mst-subgraph-inv-2:**
\[
\text{assumes regular } (v \ast v^T) \\
\text{ and } t \leq v \ast v^T \sqcap --g \\
\text{ and } v^T = r^T \ast t^* \\
\text{ and } e \leq v \ast -v^T \sqcap --g \\
\text{ and vector } v \\
\text{ and regular } ((v \sqcup e^T \ast \text{top}) \ast (v \sqcup e^T \ast \text{top})^T) \\
\text{ shows } t \sqcup e \leq (r^T \ast (v \sqcup e^T \ast \text{top}) \ast (v \sqcup e^T \ast \text{top})^T \sqcap g)^* \ast (r^T \ast (v \sqcup e^T \ast \text{top}) \ast (v \sqcup e^T \ast \text{top})^T \sqcap g))^* \\
\langle \text{proof} \rangle
\]

**lemma span-inv:**
\[
\text{assumes } e \leq v \ast -v^T \\
\text{ and vector } v \\
\text{ and arc } e \\
\text{ and } t \leq (v \ast v^T) \sqcap g \\
\text{ and } g^T = g \\
\text{ and } v^T = r^T \ast t^* \\
\text{ and injective } r
\]
and \( r^T \leq v^T \)
and \( r^T \ast ((v \ast v^T) \cap g)^* \leq r^T \ast t^* \)
shows \( r^T \ast ((v \ast e^T \ast top) \ast (v \cup e^T \ast top)^T) \cap g)^* \leq r^T \ast (t \cup e)^* \)

\( \langle \text{proof} \rangle \)

### 4.1.2 Exchange gives Spanning Trees

The following abbreviations are used in the spanning tree application using Prim’s algorithm to construct the new tree for the exchange property. It is obtained by replacing an edge with one that has minimal weight and reversing the path connecting these edges. Here, \( w \) represents a weighted graph, \( v \) represents a set of nodes and \( e \) represents an edge.

**abbreviation** \( \text{prim-E} :: 'a \Rightarrow 'a \Rightarrow 'a \Rightarrow 'a \) where \( \text{prim-E} w v e \equiv w \cap -v^T \cap top \ast e \ast w^T \)

**abbreviation** \( \text{prim-P} :: 'a \Rightarrow 'a \Rightarrow 'a \Rightarrow 'a \) where \( \text{prim-P} w v e \equiv w \cap -v^T \cap top \ast e \ast w^T \)

**abbreviation** \( \text{prim-EP} :: 'a \Rightarrow 'a \Rightarrow 'a \Rightarrow 'a \) where \( \text{prim-EP} w v e \equiv w \cap -v^T \cap top \ast e \ast w^T \)

**abbreviation** \( \text{prim-W} :: 'a \Rightarrow 'a \Rightarrow 'a \Rightarrow 'a \) where \( \text{prim-W} w v e \equiv (w \cap -\text{prim-EP w v e}) \cup (\text{prim-P w v e})^T \cup e \)

The lemmas in this section are used to show that the relation after exchange represents a spanning tree. The results in the next section are used to show that it is a minimum spanning tree.

**lemma** \( \text{exchange-injective-3}: \)

**assumes** \( e \leq v \ast -v^T \)

**and** vector \( v \)

**shows** \((w \cap -\text{prim-EP w v e}) \ast e^T = \text{bot}\)

\( \langle \text{proof} \rangle \)

**lemma** \( \text{exchange-injective-6}: \)

**assumes** \( \text{arc e} \)

**and** forest \( w \)

**shows** \((\text{prim-P w v e})^T \ast e^T = \text{bot}\)

\( \langle \text{proof} \rangle \)

The graph after exchanging is injective.

**lemma** \( \text{exchange-injective}: \)

**assumes** \( \text{arc e} \)

**and** \( e \leq v \ast -v^T \)

**and** forest \( w \)

**and** vector \( v \)

**shows** \( \text{injective} (\text{prim-W w v e}) \)

\( \langle \text{proof} \rangle \)

**lemma** \( \text{pv}: \)

**assumes** vector \( v \)

**shows** \((\text{prim-P w v e})^T \ast v = \text{bot} \)

31
proof

lemma vector-pred-inv:
  assumes arc e
  and $e \leq v * -v^T$
  and forest $w$
  and vector $v$
  and $w * v \leq v$
  shows $(\text{prim-W } w v e) * (v \sqcup e^T * \text{top}) \leq v \sqcup e^T * \text{top}$

proof

The graph after exchanging is acyclic.

lemma exchange-acyclic:
  assumes vector $v$
  and $e \leq v * -v^T$
  and $w * v \leq v$
  and acyclic $w$
  shows acyclic $(\text{prim-W } w v e)$

proof

The following lemma shows that an edge across the cut between visited nodes and unvisited nodes does not leave the component of visited nodes.

lemma mst-subgraph-inv:
  assumes $e \leq v * -v^T \sqcap g$
  and $t \leq g$
  and $v^T = r^T * t^*$
  shows $e \leq (r^T * g^*)^T * (r^T * g^*) \sqcap g$

proof

The following lemmas show that the tree after exchanging contains the currently constructed and tree and its extension by the chosen edge.

lemma mst-extends-old-tree:
  assumes $t \leq w$
  and $t \leq v * v^T$
  and vector $v$
  shows $t \leq \text{prim-W } w v e$

proof

lemma mst-extends-new-tree:
  $t \leq w \implies t \leq v * v^T \implies \text{vector } v \implies t \sqcup e \leq \text{prim-W } w v e$

proof

end

We finally add the Kleene star to Stone relation algebras. Kleene star and the relational operations are reasonably independent. The only additional axiom we need in the generalisation to Stone-Kleene relation algebras is that star distributes over double complement.
\textbf{class} stone-kleene-relation-algebra = stone-relation-algebra + pd-kleene-allegory
+ assumes pp-dist-star: \(-\neg(x^*) = (\neg x)^*\)

\textbf{begin}

\textbf{lemma} regular-closed-star:
regular \(x\) \implies regular \((x^*)\)
⟨proof⟩

\textbf{lemma} components-idempotent:
\(\text{components}(\text{components}\ x) = \text{components}\ x\)
⟨proof⟩

The following lemma shows that the nodes reachable in the tree after exchange contain the nodes reachable in the tree before exchange.

\textbf{lemma} mst-reachable-inv:
assumes regular \((\text{prim-EP}\ w\ v\ e)\)
and vector \(r\)
and \(e \leq v \ast -v^T\)
and vector \(v\)
and \(v^T = r^T \ast t^*\)
and \(t \leq w\)
and \(t \leq v \ast v^T\)
and \(w \ast v \leq v\)
shows \(r^T \ast w^* \leq r^T \ast (\text{prim-W}\ w\ v\ e)^*\)
⟨proof⟩

Some of the following lemmas already hold in pseudocomplemented distributive Kleene allegories.

4.1.3 Exchange gives Minimum Spanning Trees

The lemmas in this section are used to show that the after exchange we obtain a minimum spanning tree. The following lemmas show various interactions between the three constituents of the tree after exchange.

\textbf{lemma} epm-1:
vector \(v\) \implies prim-E \(w\ v\ e\) \uplus prim-P \(w\ v\ e\) = prim-EP \(w\ v\ e\)
⟨proof⟩

\textbf{lemma} epm-2:
assumes regular \((\text{prim-EP}\ w\ v\ e)\)
and vector \(v\)
shows \(w \cap -(\text{prim-EP}\ w\ v\ e)) \uplus \text{prim-P}\ w\ v\ e \uplus \text{prim-E}\ w\ v\ e = w\)
⟨proof⟩

\textbf{lemma} epm-4:
assumes \(e \leq w\)
and injective \(w\)
and $w \ast v \leq v$
and $e \leq v \ast -v^T$
shows $top \ast e \ast w^T \leq top \ast v^T$

(proof)

lemma epm-5:
assumes $e \leq w$
and injective $w$
and $w \ast v \leq v$
and $e \leq v \ast -v^T$
and vector $v$
shows prim-P $w \ v \ e = bot$

(proof)

lemma epm-6:
assumes $e \leq w$
and injective $w$
and $w \ast v \leq v$
and $e \leq v \ast -v^T$
and vector $v$
shows prim-E $w \ v \ e = e$

(proof)

lemma epm-7:
regular $(prim-EP \ w \ v \ e) \implies e \leq w \implies injective \ w \implies w \ast v \leq v \implies e \leq v \ast -v^T \implies vector \ v \implies prim-W \ w \ v \ e = w$

(proof)

lemma epm-8:
assumes acyclic $w$
shows $(w \ominus -(prim-EP \ w \ v \ e)) \cap (prim-P \ w \ v \ e)^T = bot$

(proof)

lemma epm-9:
assumes $e \leq v \ast -v^T$
and vector $v$
shows $(w \ominus -(prim-EP \ w \ v \ e)) \cap e = bot$

(proof)

lemma epm-10:
assumes $e \leq v \ast -v^T$
and vector $v$
shows $(prim-P \ w \ v \ e)^T \cap e = bot$

(proof)

lemma epm-11:
assumes vector $v$
shows $(w \ominus -(prim-EP \ w \ v \ e)) \cap prim-P \ w \ v \ e = bot$

(proof)
lemma epm-12:
assumes vector v
shows \((w \cap - (\text{prim-EP} \ w \ v \ e)) \cap \text{prim-E} \ w \ v \ e = \bot)\)
⟨proof⟩

lemma epm-13:
assumes vector v
shows \(\text{prim-P} \ w \ v \ e \cap \text{prim-E} \ w \ v \ e = \bot)\)
⟨proof⟩

The following lemmas show that the relation characterising the edge across the cut is an arc.

lemma arc-edge-1:
assumes \(e \leq v * -(v^T \cap g)\)
and vector v
and \(v^T = r^T * t^*\)
and \(t \leq g\)
and \(r^T * g^* \leq r^T * w^*\)
shows \(\text{top} * e \leq v^T * w^*\)
⟨proof⟩

lemma arc-edge-2:
assumes \(e \leq v * -(v^T \cap g)\)
and vector v
and \(v^T = r^T * t^*\)
and \(t \leq g\)
and \(r^T * g^* \leq r^T * w^*\)
and \(w * v \leq v\)
and injective w
shows \(\text{top} * e * w^T * s \leq v^T * w^*\)
⟨proof⟩

lemma arc-edge-3:
assumes \(e \leq v * -(v^T \cap g)\)
and vector v
and \(v^T = r^T * t^*\)
and \(t \leq g\)
and \(r^T * g^* \leq r^T * w^*\)
and \(w * v \leq v\)
and injective w
and \(\text{prim-E} \ w \ v \ e = \bot)\)
shows \(e = \bot)\)
⟨proof⟩

lemma arc-edge-4:
assumes \(e \leq v * -(v^T \cap g)\)
and vector v
and \(v^T = r^T * t^*\)
and \( t \leq g \)
and \( r_T^* g^* \leq r_T^* w^* \)
and arc e
shows top * prim-E w v e * top = top

⟨proof⟩

lemma arc-edge-5:
assumes vector v
and \( w * v \leq v \)
and injective w
and arc e
shows (prim-E w v e)_T * top * prim-E w v e \leq 1

⟨proof⟩

lemma arc-edge-6:
assumes vector v
and \( w * v \leq v \)
and injective w
and arc e
shows prim-E w v e * top * (prim-E w v e)_T \leq 1

⟨proof⟩

lemma arc-edge:
assumes \( e \leq v * v^T \cap g \)
and vector v
and \( v^T = r_T^* t^* \)
and \( t \leq g \)
and \( r_T^* g^* \leq r_T^* w^* \)
and \( w * v \leq v \)
and injective w
and arc e
shows arc (prim-E w v e)

⟨proof⟩

4.1.4 Invariant implies Postcondition

The lemmas in this section are used to show that the invariant implies the postcondition at the end of the algorithm. The following lemma shows that the nodes reachable in the graph are the same as those reachable in the constructed tree.

lemma span-post:
assumes regular v
and vector v
and \( v^T = r_T^* t^* \)
and \( v * v^T \cap g = \text{bot} \)
and \( t \leq v * v^T \cap g \)
and \( r_T^* (v * v^T \cap g)^* \leq r_T^* t^* \)
shows \( v^T = r_T^* g^* \)

⟨proof⟩
The following lemma shows that the minimum spanning tree extending a tree is the same as the tree at the end of the algorithm.

**lemma mst-post:**

**assumes**
- vector \( r \)
- injective \( r \)
- \( v^T = r^T \star t^r \)
- forest \( w \)
- \( t \leq w \)
- \( w \leq v \star v^T \)

**shows** \( w = t \)

(proof)

### 4.2 Kruskal’s Algorithm

The following results are used for proving the correctness of Kruskal’s minimum spanning tree algorithm.

#### 4.2.1 Preservation of Invariant

We first treat the preservation of the invariant. The following lemmas show conditions necessary for preserving that \( f \) is a forest.

**lemma kruskal-injective-inv-2:**

**assumes**
- arc \( e \)
- acyclic \( f \)

**shows** \( \text{top} \star e \star f^T \star f^T \leq -e \)

(proof)

**lemma kruskal-injective-inv-3:**

**assumes**
- arc \( e \)
- forest \( f \)

**shows** \((\text{top} \star e \star f^T \star f^T) \star (\text{top} \star e \star f^T) \cap f^T \star f \leq 1\)

(proof)

**lemma kruskal-acyclic-inv:**

**assumes**
- acyclic \( f \)
- covector \( q \)

**shows** \((f \cap -q) \sqcup (f \cap q)^T \sqcup e\)

(proof)

**lemma kruskal-exchange-acyclic-inv-1:**

**assumes**
- acyclic \( f \)
- covector \( q \)

**shows** \((f \cap -q) \sqcup (f \cap q)^T\)

(proof)
4.2.2 Exchange gives Spanning Trees

The lemmas in this section are used to show that the relation after exchange represents a spanning tree.

lemma inf-star-import:
assumes $x \leq z$
and univalent $z$
and reflexive $y$
and regular $z$
shows $x^* \cdot y \sqcap z^* \leq x^* \cdot (y \sqcap z^*)$
⟨proof⟩

lemma kruskal-exchange-forest-components-inv:
assumes injective $((w \sqcap -d) \sqcup e)$
and regular $d$
and $e \cdot top \cdot e = e$
and $d \leq top \cdot e^T \cdot w^T$
and $w \cdot e^T \cdot top = bot$
and injective $w$
and $d \leq w$
and $d \leq (w \sqcap -d)^T \cdot e^T \cdot top$
shows forest-components $w \leq$ forest-components $((w \sqcap -d) \sqcup e)$
⟨proof⟩

lemma kruskal-spanning-inv:
assumes injective $((f \sqcap -q) \sqcup (f \sqcap q)^T \sqcup e)$
and regular $q$
and regular $e$
and $(-h \sqcap -g)^* \leq$ forest-components $f$
shows components $(-h \cdot e \sqcap -e^T) \sqcap g \leq$ forest-components $((f \sqcap -q) \sqcup (f \sqcap q)^T \sqcup e)$
⟨proof⟩
lemma kruskal-exchange-spanning-inv-2:
assumes injective $w$
and $w^* \cdot e^T = e^T$
and $f \cup f^T \leq (w \cap -d \cap -d^T) \cup (w^T \cap -d \cap -d^T)$
and $d \leq \text{forest-components } f \cdot e^T \cdot \text{top}$
shows $d \leq (w \cap -d)^{T^*} \cdot e^T \cdot \text{top}$

(\text{proof})

lemma kruskal-spanning-inv-1:
assumes $e \leq F$
and regular $e$
and components $(-h \cap g) \leq F$
and equivalence $F$
shows components $(-(h \cap -e \cap -e^T) \cap g) \leq F$

(\text{proof})

lemma kruskal-reroot-edge:
assumes injective $(e^T \cdot \text{top})$
and acyclic $w$
shows $((w \cap -(\text{top} \cdot e \cdot w^{T^*})) \cup (w \cap \text{top} \cdot e \cdot w^{T^*} \cdot e^T) \cdot e^T = \text{bot}$

(\text{proof})

4.2.3 Exchange gives Minimum Spanning Trees

The lemmas in this section are used to show that the after exchange we obtain a minimum spanning tree. The following lemmas show that the relation characterising the edge across the cut is an arc.

lemma kruskal-edge-arc:
assumes equivalence $F$
and forest $w$
and arc $e$
and regular $F$
and $F \leq \text{forest-components } (F \cap w)$
and regular $w$
and $w \cdot e^T = \text{bot}$
and $e \cdot F \cdot e = \text{bot}$
and $e^T \leq w^*$
shows arc $(w \cap \text{top} \cdot e^T \cdot w^{T^*} \cap F \cdot e^T \cdot \text{top} \cap \text{top} \cdot e \cdot -F)$

(\text{proof})

lemma kruskal-edge-arc-1:
assumes $e \leq --h$
and $h \leq g$
and symmetric $h$
and components $g \leq \text{forest-components } w$
and $w \cdot e^T = \text{bot}$
shows $e^T \leq w^*$
lemma kruskal-edge-between-components-1:
assumes equivalence F
and mapping (top * e)
shows F ≤ -(w ∩ top * e^T * w^T * ∩ F * e^T * top ∩ top * e * -F)
end

lemma kruskal-edge-between-components-2:
assumes forest-components f ≤ -d
and injective f
and f ∪ f^T ≤ w ∪ w^T
shows f ∪ f^T ≤ (w ∩ -d ∩ -d^T) ∪ (w^T ∩ -d ∩ -d^T)
end

4.3 Related Structures

Stone algebras can be expanded to Stone-Kleene relation algebras by reusing some operations.

subclass stone-algebra < comp-inf: stone-kleene-relation-algebra where star = \(\lambda x \cdot top\) and one = top and times = inf and conv = id

(\textit{proof})

Every bounded linear order can be expanded to a Stone algebra, which can be expanded to a Stone relation algebra, which can be expanded to a Stone-Kleene relation algebra.

class linorder-stone-kleene-relation-algebra-expansion = linorder-stone-relation-algebra-expansion + star +
assumes star-def \([\text{simp}]\): x^* = top

begin

subclass kleene-algebra
(\textit{proof})

subclass stone-kleene-relation-algebra
(\textit{proof})

end

A Kleene relation algebra is based on a relation algebra.

class kleene-relation-algebra = relation-algebra + stone-kleene-relation-algebra
end

5 Subalgebras of Kleene Relation Algebras
In this theory we show that the regular elements of a Stone-Kleene relation algebra form a Kleene relation subalgebra.

theory Kleene-Relation-Subalgebras

imports Stone-Relation-Algebras Relation-Subalgebras Kleene-Relation-Algebras

begin

instantiation regular :: (stone-kleene-relation-algebra) kleene-relation-algebra
begin

lift-definition star-regular :: 'a regular ⇒ 'a regular is star
 ⟨proof⟩

instance ⟨proof⟩

end

end

6 Matrix Kleene Algebras

This theory gives a matrix model of Stone-Kleene relation algebras. The main result is that matrices over Kleene algebras form Kleene algebras. The automata-based construction is due to Conway [7]. An implementation of the construction in Isabelle/HOL that extends [2] was given in [3] without a correctness proof.

For specifying the size of matrices, Isabelle/HOL's type system requires the use of types, not sets. This creates two issues when trying to implement Conway's recursive construction directly. First, the matrix size changes for recursive calls, which requires dependent types. Second, some submatrices used in the construction are not square, which requires typed Kleene algebras [14], that is, categories of Kleene algebras.

Because these instruments are not available in Isabelle/HOL, we use square matrices with a constant size given by the argument of the Kleene star operation. Smaller, possibly rectangular submatrices are identified by two lists of indices: one for the rows to include and one for the columns to include. Lists are used to make recursive calls deterministic; otherwise sets would be sufficient.

theory Matrix-Kleene-Algebras


begin
6.1 Matrix Restrictions

In this section we develop a calculus of matrix restrictions. The restriction of a matrix to specific row and column indices is implemented by the following function, which keeps the size of the matrix and sets all unused entries to bot.

**definition** restrict-matrix :: 'a list ⇒ 'a list ⇒ bot

where restrict-matrix as f bs = (λ(i,j). if List.member as i ∧ List.member bs j then f (i,j) else bot)

The following function captures Conway’s automata-based construction of the Kleene star of a matrix. An index \( k \) is chosen and \( s \) contains all other indices. The matrix is split into four submatrices \( a, b, c, d \) including/not including row/column \( k \). Four matrices are computed containing the entries given by Conway’s construction. These four matrices are added to obtain the result. All matrices involved in the function have the same size, but matrix restriction is used to set irrelevant entries to bot.

**primrec** star-matrix :: 'a list ⇒ ('a,'b::{star,times,bounded-semilattice-sup-bot}) square ⇒ ('a,'b) square

where star-matrix f = star-matrix' Nil g | star-matrix' (k#s) g = (let r = [k] in let a = r(g)r in let b = r(g)s in let c = s(g)r in let d = s(g)s in let as = r(star o a)r in let ds = star-matrix' s d in let e = a ⊕ b ⊗ ds ⊗ c in let es = r(star o e)r in let f = d ⊕ c ⊗ as ⊗ b in let fs = star-matrix' s f in es ⊕ as ⊗ b ⊗ fs ⊕ ds ⊗ c ⊗ es ⊕ fs)

The Kleene star of the whole matrix is obtained by taking as indices all elements of the underlying type \( 'a \). This is conveniently supplied by the enum class.

**fun** star-matrix :: ('a::enum,'b::{star,times,bounded-semilattice-sup-bot}) square ⇒ ('a,'b) square (andatory [100] 100) where star-matrix f = star-matrix' (enum-class enum::'a list) f

The following lemmas deconstruct matrices with non-empty restrictions.

**lemma** restrict-empty-left:

\[ (∥f∥)ls = mbot \]

(proof)
lemma restrict-empty-right:
\[ \text{ks}(f)[\text{ls}] = \text{mbot} \]
\[ \langle \text{proof} \rangle \]

lemma restrict-nonempty-left:
\[ \text{fixes } f :: ('a, 'b::bounded-semilattice-sup-bot) \text{ square} \]
\[ \text{shows } (k\#\text{ks})(f)\text{ls} = [k](f)[\text{ls}] \oplus \text{ks}(f)\text{ls} \]
\[ \langle \text{proof} \rangle \]

lemma restrict-nonempty-right:
\[ \text{fixes } f :: ('a, 'b::bounded-semilattice-sup-bot) \text{ square} \]
\[ \text{shows } \text{ks}(f)(l\#\text{ls}) = \text{ks}(f)[l] \oplus \text{ks}(f)\text{ls} \]
\[ \langle \text{proof} \rangle \]

The following predicate captures that two index sets are disjoint. This has consequences for composition and the unit matrix.

abbreviation disjoint ks ls \equiv \neg(\exists x . \text{List.member ks } x \land \text{List.member ls } x) \]

lemma times-disjoint:
\[ \text{fixes } f g :: ('a, 'b::idempotent-semiring) \text{ square} \]
\[ \text{assumes disjoint ls ms} \]
\[ \text{shows } \text{ks}(f)\text{ls} \odot \text{ms}(g)\text{ns} = \text{mbot} \]
\[ \langle \text{proof} \rangle \]

lemma one-disjoint:
\[ \text{assumes disjoint ks ls} \]
\[ \text{shows } \text{ks}((\text{none}::('a, 'b::idempotent-semiring) \text{ square})\text{ls} = \text{mbot} \]
\[ \langle \text{proof} \rangle \]

The following predicate captures that an index set is a subset of another index set. This has consequences for repeated restrictions.

abbreviation is-sublist ks ls \equiv \forall x . \text{List.member ks } x \rightarrow \text{List.member ls } x \]

lemma restrict-sublist:
\[ \text{assumes is-sublist ls ks} \]
\[ \text{and is-sublist ms ns} \]
\[ \text{shows } \text{ls}(\text{ks}(f)\text{ms})\text{ms} = \text{ls}(f)\text{ms} \]
\[ \langle \text{proof} \rangle \]

lemma restrict-superlist:
\[ \text{assumes is-sublist ls ks} \]
\[ \text{and is-sublist ms ns} \]
\[ \text{shows } \text{ks}(\text{ls}(f)\text{ms})\text{ns} = \text{ls}(f)\text{ms} \]
\[ \langle \text{proof} \rangle \]
The following lemmas give the sizes of the results of some matrix operations.

**Lemma restrict-sup:**

**Fixes** $f \; g :: ('a,'b::bounded-semilattice-sup-bot) \; square$

**Shows** $\mu f g ls = \mu f ls \oplus \mu g ls$

**Proof**

**Lemma restrict-times:**

**Fixes** $f \; g :: ('a,'b::idempotent-semiring) \; square$

**Shows** $\mu f g ls \circ \mu g ms = \mu f ls \circ \mu g ms$

**Proof**

**Lemma restrict-star:**

**Fixes** $g :: ('a,'b::kleene-algebra) \; square$

**Shows** $t \langle \star-matrix t g \rangle t = \star-matrix t g$

**Proof**

**Lemma restrict-one:**

Assumes $\neg \text{List.member} k$

**Shows** $\mu mone k = \mu mone \oplus \mu k$

**Proof**

**Lemma restrict-one-left-unit:**

$\mu mone \circ \mu f ks = \mu f ks$

**Proof**

The following lemmas consider restrictions to singleton index sets.

**Lemma restrict-singleton:**

$\mu f g (i,j) = (\text{if } i = k \land j = l \text{ then } f (i,j) \text{ else } bot)$

**Proof**

**Lemma restrict-singleton-list:**

$\mu f g (i,j) = (\text{if } i = k \land \text{List.member } l \text{ then } f (i,j) \text{ else } bot)$

**Proof**

**Lemma restrict-list-singleton:**

$\mu f g (i,j) = (\text{if } \text{List.member } k \land j = l \text{ then } f (i,j) \text{ else } bot)$

**Proof**

**Lemma restrict-singleton-product:**

**Fixes** $f \; g :: ('a::finite,'b::kleene-algebra) \; square$

**Shows** $\mu f g (i,j) = (\text{if } i = k \land j = n \text{ then } f (i,l) * g (m,j) \text{ else } bot)$

**Proof**

The Kleene star unfold law holds for matrices with a single entry on the diagonal.

**Lemma restrict-star-unfold:**
lemma restrict-all:
  enum-class.enum f enum-class.enum = f
  (proof)

  The following shows the various components of a matrix product. It is
essentially a recursive implementation of the product.

lemma restrict-nonempty-product:
  fixes f g :: ('a::finite,'b::idempotent-semiring) square
  assumes ~ List.member ls l
  shows (k\#ks)(f)(l\#ls) \circ (l\#ls)(g)(m\#ms) = ([k](f)[l] \circ [l](g)[m] \oplus [k](f)ls
  \circ ls(g)[m]) \oplus ([k](f)[l] \circ [l](g)ms \oplus [k](f)ls \circ ls(g)ms) \oplus (ks(f)[l] \circ [l](g)[m]
  \oplus ks(f)ls \circ ls(g)ms) \oplus (ks(f)[l] \circ [l](g)[m]) \oplus (ks(f)ls \circ ls(g)ms)
  (proof)

  Equality of matrices is componentwise.

lemma restrict-nonempty-eq:
  (k\#ks)(f)(l\#ls) = (k\#ks)(g)(l\#ls) \iff [k](f)[l] = [k](g)[l] \land [k](f)ls = [k](g)ls \land ks(f)ls = ks(g)ls
  (proof)

  Inequality of matrices is componentwise.

lemma restrict-nonempty-less-eq:
  fixes f g :: ('a,'b::idempotent-semiring) square
  shows (k\#ks)(f)(l\#ls) \preceq (k\#ks)(g)(l\#ls) \iff [k](f)[l] \preceq [k](g)[l] \land [k](f)ls \preceq [k](g)ls
    \land ks(f)ls \preceq ks(g)ls
  (proof)

  The following lemmas treat repeated restrictions to disjoint index sets.

lemma restrict-disjoint-left:
  assumes disjoint ks ms
  shows ms(ks(f)ls) ns = mbot
  (proof)

lemma restrict-disjoint-right:
  assumes disjoint ls ns
  shows ms(ks(f)ls) ns = mbot
  (proof)

  The following lemma expresses the equality of a matrix and a product of
two matrices componentwise.

lemma restrict-nonempty-product-eq:
  fixes f g h :: ('a::finite,'b::idempotent-semiring) square
  assumes ~ List.member ks k
  and ~ List.member ls l
  and ~ List.member ms m

45
The construction. It remains to prove one unfold and two induction axioms of the Kleene algebra using Conway’s construction.

### 6.2 Matrices form a Kleene Algebra

Matrices over Kleene algebras form a Kleene algebra using Conway’s construction. It remains to prove one unfold and two induction axioms of the Kleene algebra.
Kleene star. Each proof is by induction over the size of the matrix represented by an index list.

**interpretation** matrix-kleene-algebra: kleene-algebra-var where sup = sup-matrix and less-eq = less-eq-matrix and less = less-matrix and bot = bot-matrix; ('a::enum,'b::kleene-algebra) square and one = one-matrix and times = times-matrix and star = star-matrix

(proof)

6.3 Matrices form a Stone-Kleene Relation Algebra

Matrices over Stone-Kleene relation algebras form a Stone-Kleene relation algebra. It remains to prove the axiom about the interaction of Kleene star and double complement.

**interpretation** matrix-stone-kleene-relation-algebra: stone-kleene-relation-algebra where sup = sup-matrix and inf = inf-matrix and less-eq = less-eq-matrix and less = less-matrix and bot = bot-matrix; ('a::enum,'b::stone-kleene-relation-algebra) square and top = top-matrix and uminus = uminus-matrix and one = one-matrix and times = times-matrix and conv = conv-matrix and star = star-matrix

(proof)

end

References


