

Regular Algebras

Simon Foster and Georg Struth

December 14, 2021

Abstract

Regular algebras axiomatise the equational theory of regular expressions as induced by regular language identity. We use Isabelle/HOL for a detailed systematic study of regular algebras given by Boffa, Conway, Kozen and Salomaa. We investigate the relationships between these classes, formalise a soundness proof for the smallest class (Salomaa's) and obtain completeness of the largest one (Boffa's) relative to a deep result by Krob. In addition we provide a large collection of regular identities in the general setting of Boffa's axiom.

Contents

1	Introductory Remarks	2
2	Dioids, Powers and Finite Sums	2
3	Regular Algebras	4
3.1	Conway's Classical Axioms	4
3.2	Boffa's Axioms	5
3.3	Boffa Monoid Identities	10
3.4	Conway's Conjectures	11
3.5	Kozen's Kleene Algebras	13
3.6	Salomaa's Axioms	15
4	Models of Regular Algebra	16
4.1	Language Model of Salomaa Algebra	17
4.2	Regular Language Model of Salomaa Algebra	19
5	Pratt's Counterexamples	20
6	Variants of Regular Algebra	24

1 Introductory Remarks

These Isabelle theories complement the article on *On the Fine-Structure of Regular Algebra* [5]. For an introduction to the topic, conceptual explanations and references we refer to this article. Our regular algebra hierarchy is orthogonal to the Kleene algebra hierarchy in the Archive of Formal Proofs [1]; we have not aimed at an integration for pragmatic reasons.

2 Dioids, Powers and Finite Sums

theory *Dioid-Power-Sum*

imports *Kleene-Algebra.Dioid Kleene-Algebra.Finite-Suprema*

begin

We add a few facts about powers and finite sums—in fact, finite suprema—to an existing theory field for dioids.

context *dioid-one-zero*

begin

lemma *add-iso-r*: $y \leq z \implies x + y \leq x + z$
<proof>

notation *power* ($-$ [101,50] 100)

lemma *power-subdist*: $x^n \leq (x + y)^n$
<proof>

lemma *power-inductl-var*: $x \cdot y \leq y \implies x^n \cdot y \leq y$
<proof>

lemma *power-inductr-var*: $y \cdot x \leq y \implies y \cdot x^n \leq y$
<proof>

definition *powsum* :: $'a \Rightarrow nat \Rightarrow nat \Rightarrow 'a$ ($-$ [101,50,50] 100) **where**
 $powsum\ x\ m\ n = sum\ ((\wedge)\ x)\ \{m..n + m\}$

lemmas *powsum-simps* = *powsum-def atLeastAtMostSuc-conv numerals*

lemma *powsum1* [*simp*]: $x_n^0 = x^n$
<proof>

lemma *powsum2*: $x_n^{Suc\ m} = x_n^m + x^{n+Suc\ m}$
<proof>

lemma *powsum-00* [*simp*]: $x_0^0 = 1$
<proof>

lemma *powsum-01* [*simp*]: $x_0^1 = 1 + x$
<proof>

lemma *powsum-10* [*simp*]: $x_1^0 = x$
<proof>

lemma *powsum-split*: $x_m^{i+\text{Suc } n} = x_m^i + x_{m+\text{Suc } i}^n$
<proof>

lemma *powsum-split-var1*: $x_0^{n+1} = 1 + x_1^n$
<proof>

lemma *powsum-split-var2* [*simp*]: $x^m + x_0^m = x_0^m$
<proof>

lemma *powsum-split-var3*: $x_0^{m+\text{Suc } n} = x_0^m + x_{0+\text{Suc } m}^n$
<proof>

lemma *powsum-split-var4* [*simp*]: $x_0^{m+n} + x_m^n = x_0^{m+n}$
<proof>

lemma *powsum-split-var6*: $x_0^{(\text{Suc } k)+\text{Suc } n} = x_0^{\text{Suc } k} + x_{0+\text{Suc } (\text{Suc } k)}^n$
<proof>

lemma *powsum-ext*: $x \leq x_0^{\text{Suc } n}$
<proof>

lemma *powsum-one*: $1 \leq x_0^{\text{Suc } n}$
<proof>

lemma *powsum-shift1*: $x \cdot x_m^n = x_{m+1}^n$
<proof>

lemma *powsum-shift*: $x^k \cdot x_m^n = x_{k+m}^n$
<proof>

lemma *powsum-prod-suc*: $x_0^m \cdot x_0^{\text{Suc } n} = x_0^{\text{Suc } (m+n)}$
<proof>

lemma *powsum-prod*: $x_0^m \cdot x_0^n = x_0^{m+n}$
<proof>

end

end

3 Regular Algebras

```
theory Regular-Algebras
  imports Dioid-Power-Sum Kleene-Algebra.Finite-Suprema Kleene-Algebra.Kleene-Algebra
begin
```

3.1 Conway's Classical Axioms

Conway's classical axiomatisation of Regular Algebra from [4].

```
class star-diod = dioid-one-zero + star-op + plus-ord
```

```
class conway-diod = star-diod +
  assumes C11:  $(x + y)^* = (x^* \cdot y)^* \cdot x^*$ 
  and C12:  $(x \cdot y)^* = 1 + x \cdot (y \cdot x)^* \cdot y$ 
```

```
class strong-conway-diod = conway-diod +
  assumes C13:  $(x^*)^* = x^*$ 
```

```
class C-algebra = strong-conway-diod +
  assumes C14:  $x^* = (x^{n+1})^* \cdot x_0^n$ 
```

We tried to dualise using sublocales, but this causes an infinite loop on dual.dual.dual...

```
lemma (in conway-diod) C11-var:  $(x + y)^* = x^* \cdot (y \cdot x^*)^*$ 
<proof>
```

```
lemma (in conway-diod) dual-conway-diod:
  class.conway-diod (+) ( $\odot$ ) 1 0 ( $\leq$ ) ( $<$ ) star
<proof>
```

```
lemma (in strong-conway-diod) dual-strong-conway-diod: class.strong-conway-diod
((+) ) (( $\odot$ ) ) 1 0 ( $\leq$ ) ( $<$ ) star
<proof>
```

Nitpick finds counterexamples to the following claims.

```
lemma (in conway-diod) 1* = 1
  nitpick [expect=genuine] — 3-element counterexample
<proof>
```

```
lemma (in conway-diod) (x*)* = x*
  nitpick [expect=genuine] — 3-element counterexample
<proof>
```

```
context C-algebra
begin
```

```
lemma C-unfoldl [simp]:  $1 + x \cdot x^* = x^*$ 
<proof>
```

lemma *C-slide*: $(x \cdot y)^* \cdot x = x \cdot (y \cdot x)^*$
 ⟨proof⟩

lemma *powsum-ub*: $i \leq n \implies x^i \leq x_0^n$
 ⟨proof⟩

lemma *C14-aux*: $m \leq n \implies x^m \cdot (x^n)^* = (x^n)^* \cdot x^m$
 ⟨proof⟩

end

context *diod-one-zero*
begin

lemma *opp-power-def*:
power.power 1 (\odot) $x\ n = x^n$
 ⟨proof⟩

lemma *opp-powsum-def*:
diod-one-zero.powsum (+) (\odot) 1 0 $x\ m\ n = x_m^n$
 ⟨proof⟩

end

lemma *C14-dual*:
fixes $x::'a::C\text{-algebra}$
shows $x^* = x_0^n \cdot (x^{n+1})^*$
 ⟨proof⟩

lemma *C-algebra*: *class.C-algebra* (+) (\odot) ($1::'a::C\text{-algebra}$) 0 (\leq) ($<$) *star*
 ⟨proof⟩

3.2 Boffa's Axioms

Boffa's two axiomatisations of Regular Algebra from [2, 3].

class *B1-algebra* = *conway-diod* +
assumes *R*: $x \cdot x = x \implies x^* = 1 + x$

class *B2-algebra* = *star-diod* +
assumes *B21*: $1 + x \leq x^*$
and *B22* [*simp*]: $x^* \cdot x^* = x^*$
and *B23*: $\llbracket 1 + x \leq y; y \cdot y = y \rrbracket \implies x^* \leq y$

lemma (**in** *B1-algebra*) *B1-algebra*:
class.B1-algebra (+) (\odot) 1 0 (\leq) ($<$) *star*
 ⟨proof⟩

lemma (**in** *B2-algebra*) *B2-algebra*:

class *B2-algebra* (+) (⊙) 1 0 (≤) (<) *star*
⟨*proof*⟩

instance *B1-algebra* ⊆ *B2-algebra*
⟨*proof*⟩

context *B2-algebra*
begin

lemma *star-ref*: $1 \leq x^*$
⟨*proof*⟩

lemma *star-plus-one* [*simp*]: $1 + x^* = x^*$
⟨*proof*⟩

lemma *star-trans*: $x^* \cdot x^* \leq x^*$
⟨*proof*⟩

lemma *star-trans-eq* [*simp*]: $x^* \cdot x^* = x^*$
⟨*proof*⟩

lemma *star-invol* [*simp*]: $(x^*)^* = x^*$
⟨*proof*⟩

lemma *star-1l*: $x \cdot x^* \leq x^*$
⟨*proof*⟩

lemma *star-one* [*simp*]: $1^* = 1$
⟨*proof*⟩

lemma *star-subdist*: $x^* \leq (x + y)^*$
⟨*proof*⟩

lemma *star-iso*: $x \leq y \implies x^* \leq y^*$
⟨*proof*⟩

lemma *star2*: $(1 + x)^* = x^*$
⟨*proof*⟩

lemma *star-unfoldl*: $1 + x \cdot x^* \leq x^*$
⟨*proof*⟩

lemma *star-unfoldr*: $1 + x^* \cdot x \leq x^*$
⟨*proof*⟩

lemma *star-ext*: $x \leq x^*$
⟨*proof*⟩

lemma *star-1r*: $x^* \cdot x \leq x^*$

<proof>

lemma *star-unfoldl-eq* [*simp*]: $1 + x \cdot x^* = x^*$
<proof>

lemma *star-unfoldr-eq* [*simp*]: $1 + x^* \cdot x = x^*$
<proof>

lemma *star-prod-unfold-le*: $(x \cdot y)^* \leq 1 + x \cdot (y \cdot x)^* \cdot y$
<proof>

lemma *star-prod-unfold* [*simp*]: $1 + x \cdot (y \cdot x)^* \cdot y = (x \cdot y)^*$
<proof>

lemma *star-slide1*: $(x \cdot y)^* \cdot x \leq x \cdot (y \cdot x)^*$
<proof>

lemma *star-slide-var1*: $x^* \cdot x \leq x \cdot x^*$
<proof>

lemma *star-slide*: $(x \cdot y)^* \cdot x = x \cdot (y \cdot x)^*$
<proof>

lemma *star-rtc1*: $1 + x + x^* \cdot x^* \leq x^*$
<proof>

lemma *star-rtc1-eq*: $1 + x + x^* \cdot x^* = x^*$
<proof>

lemma *star-subdist-var-1*: $x \leq (x + y)^*$
<proof>

lemma *star-subdist-var-2*: $x \cdot y \leq (x + y)^*$
<proof>

lemma *star-subdist-var-3*: $x^* \cdot y^* \leq (x + y)^*$
<proof>

lemma *R-lemma*:
 assumes $x \cdot x = x$
 shows $x^* = 1 + x$
<proof>

lemma *star-denest-var-0*: $(x + y)^* = (x^* \cdot y)^* \cdot x^*$
<proof>

lemma *star-denest*: $(x + y)^* = (x^* \cdot y^*)^*$
<proof>

lemma *star-sum-var*: $(x + y)^* = (x^* + y^*)^*$
<proof>

lemma *star-denest-var*: $(x + y)^* = x^* \cdot (y \cdot x^*)^*$
<proof>

lemma *star-denest-var-2*: $(x^* \cdot y^*)^* = x^* \cdot (y \cdot x^*)^*$
<proof>

lemma *star-denest-var-3*: $(x^* \cdot y^*)^* = x^* \cdot (y^* \cdot x^*)^*$
<proof>

lemma *star-denest-var-4*: $(x^* \cdot y^*)^* = (y^* \cdot x^*)^*$
<proof>

lemma *star-denest-var-5*: $x^* \cdot (y \cdot x^*)^* = y^* \cdot (x \cdot y^*)^*$
<proof>

lemma *star-denest-var-6*: $(x + y)^* = x^* \cdot y^* \cdot (x + y)^*$
<proof>

lemma *star-denest-var-7*: $(x + y)^* = (x + y)^* \cdot x^* \cdot y^*$
<proof>

lemma *star-denest-var-8*: $(x^* \cdot y^*)^* = x^* \cdot y^* \cdot (x^* \cdot y^*)^*$
<proof>

lemma *star-denest-var-9*: $(x^* \cdot y^*)^* = (x^* \cdot y^*)^* \cdot x^* \cdot y^*$
<proof>

lemma *star-slide-var*: $x^* \cdot x = x \cdot x^*$
<proof>

lemma *star-sum-unfold*: $(x + y)^* = x^* + x^* \cdot y \cdot (x + y)^*$
<proof>

lemma *troeger*: $x^* \cdot (y \cdot ((x + y)^* \cdot z) + z) = (x + y)^* \cdot z$
<proof>

lemma *meyer-1*: $x^* = (1 + x) \cdot (x \cdot x)^*$
<proof>

lemma *star-zero* [*simp*]: $0^* = 1$
<proof>

lemma *star-subsum* [*simp*]: $x^* + x^* \cdot x = x^*$
<proof>

lemma *prod-star-closure*: $x \leq z^* \implies y \leq z^* \implies x \cdot y \leq z^*$

<proof>

end

sublocale *B2-algebra* \subseteq *B1-algebra*

<proof>

context *B2-algebra*

begin

lemma *power-le-star*: $x^n \leq x^*$

<proof>

lemma *star-power-slide*:

assumes $k \leq n$

shows $x^k \cdot (x^n)^* = (x^n)^* \cdot x^k$

<proof>

lemma *powsum-le-star*: $x_m^n \leq x^*$

<proof>

lemma *star-sum-power-slide*:

assumes $m \leq n$

shows $x_0^m \cdot (x^n)^* = (x^n)^* \cdot x_0^m$

<proof>

lemma *aarden-aux*:

assumes $y \leq y \cdot x + z$

shows $y \leq y \cdot x^{(\text{Suc } n)} + z \cdot x^*$

<proof>

lemma *conway-powerstar1*: $(x^{n+1})^* \cdot x_0^n \cdot (x^{n+1})^* \cdot x_0^n = (x^{n+1})^* \cdot x_0^n$

<proof>

lemma *conway-powerstar2*: $1 + x \leq (x^{n+1})^* \cdot x_0^n$

<proof>

theorem *powerstar*: $x^* = (x^{n+1})^* \cdot x_0^n$

<proof>

end

sublocale *B2-algebra* \subseteq *strong-conway-diooid*

<proof>

sublocale *B2-algebra* \subseteq *C-algebra*

<proof>

The following fact could neither be verified nor falsified in Isabelle. It does

not hold for other reasons.

lemma (in *C-algebra*) $x \cdot x = x \longrightarrow x^* = 1 + x$
 ⟨proof⟩

3.3 Boffa Monoid Identities

typedef ('a , 'b) *boffa-mon* = {f :: 'a::*{finite,monoid-mult}*} ⇒ 'b::*B1-algebra*.
True }
 ⟨proof⟩

notation

Rep-boffa-mon (-)

lemma *finite* (range (*Rep-boffa-mon* M))
 ⟨proof⟩

abbreviation *boffa-pair* :: ('a, 'b) *boffa-mon* ⇒ 'a::*{finite,monoid-mult}* ⇒ 'a ⇒
 'b::*B1-algebra* **where**
boffa-pair x i j ≡ ∑ { x_k | k. i·k = j }

notation

boffa-pair (-,-)

abbreviation *conway-assms* **where**

conway-assms x ≡ (∀ i j. (x_i · x_j ≤ x_{i·j}) ∧ (x_{i,i})^{*} = x_{i,i})

lemma *pair-one*: x_{1,1} = x₁
 ⟨proof⟩

definition *conway-assm1* **where** *conway-assm1* x = (∀ i j. x_i · x_j ≤ x_{i·j})

definition *conway-assm2* **where** *conway-assm2* x = (∀ i. x_{i,i}^{*} = x_{i,i})

lemma *pair-star*:

assumes *conway-assm2* x

shows x₁^{*} = x₁

⟨proof⟩

lemma *conway-monoid-one*:

assumes *conway-assm2* x

shows x₁ = 1 + x₁

⟨proof⟩

lemma *conway-monoid-split*:

assumes *conway-assm2* x

shows ∑ {x_i | i. i ∈ UNIV} = 1 + ∑ {x_i | i. i ∈ UNIV}

⟨proof⟩

lemma *boffa-mon-aux1*: {x_{i·j} | i j. i ∈ UNIV ∧ j ∈ UNIV} = {x_i | i. i ∈ UNIV}
 ⟨proof⟩

lemma *sum-intro'* [*intro*]:

$\llbracket \text{finite } (A :: \text{'a::join-semilattice-zero set}); \text{finite } B; \forall a \in A. \exists b \in B. a \leq b \rrbracket \implies$
 $\sum A \leq \sum B$
 ⟨*proof*⟩

lemma *boffa-aux2*:

conway-assm1 $x \implies$
 $\sum \{x_i \cdot x_j \mid i \cdot j. i \in \text{UNIV} \wedge j \in \text{UNIV}\} \leq \sum \{x_{i \cdot j} \mid i \cdot j. i \in \text{UNIV} \wedge j \in \text{UNIV}\}$
 ⟨*proof*⟩

lemma *boffa-aux3*:

assumes *conway-assm1* x
shows $(\sum \{x_i \mid i. i \in \text{UNIV}\}) + (\sum \{x_i \cdot x_j \mid i \cdot j. i \in \text{UNIV} \wedge j \in \text{UNIV}\}) = (\sum \{x_i \mid i. i \in \text{UNIV}\})$
 ⟨*proof*⟩

lemma *conway-monoid-identity*:

assumes *conway-assm1* x *conway-assm2* x
shows $(\sum \{x_i \mid i. i \in \text{UNIV}\})^* = (\sum \{x_i \mid i. i \in \text{UNIV}\})$
 ⟨*proof*⟩

3.4 Conway's Conjectures

class *C0-algebra* = *strong-conway-diod* +
assumes *C0*: $x \cdot y = y \cdot z \implies x^* \cdot y = y \cdot z^*$

class *C1l-algebra* = *strong-conway-diod* +
assumes *C1l*: $x \cdot y \leq y \cdot z \implies x^* \cdot y \leq y \cdot z^*$

class *C1r-algebra* = *strong-conway-diod* +
assumes *C1r*: $y \cdot x \leq z \cdot y \implies y \cdot x^* \leq z^* \cdot y$

class *C2l-algebra* = *conway-diod* +
assumes *C2l*: $x = y \cdot x \implies x = y^* \cdot x$

class *C2r-algebra* = *conway-diod* +
assumes *C2r*: $x = x \cdot y \implies x = x \cdot y^*$

class *C3l-algebra* = *conway-diod* +
assumes *C3l*: $x \cdot y \leq y \implies x^* \cdot y \leq y$

class *C3r-algebra* = *conway-diod* +
assumes *C3r*: $y \cdot x \leq y \implies y \cdot x^* \leq y$

sublocale *C1r-algebra* \subseteq *dual*: *C1l-algebra*
 (+) (\odot) 1 0 (\leq) ($<$) *star*
 ⟨*proof*⟩

sublocale $C2r\text{-algebra} \subseteq \text{dual: } C2l\text{-algebra}$
(+) (\odot) 1 0 (\leq) ($<$) star
(proof)

sublocale $C3r\text{-algebra} \subseteq \text{dual: } C3l\text{-algebra}$
(+) (\odot) 1 0 (\leq) ($<$) star
(proof)

lemma (in $C3l\text{-algebra}$) $k2\text{-var: } z + x \cdot y \leq y \implies x^* \cdot z \leq y$
(proof)

instance $C2l\text{-algebra} \subseteq B1\text{-algebra}$
(proof)

instance $C2r\text{-algebra} \subseteq B1\text{-algebra}$
(proof)

The following claims are refuted by Nitpick

lemma (in conway-dioid)
assumes $x \cdot y = y \cdot z \implies x^* \cdot y = y \cdot z^*$
shows $1^* = 1$

(proof)

lemma (in conway-dioid)
assumes $x \cdot y \leq y \cdot z \implies x^* \cdot y \leq y \cdot z^*$
shows $1^* = 1$

(proof)

The following fact could not be refuted by Nitpick or Quickcheck; but an infinite counterexample exists.

lemma (in $B1\text{-algebra}$) $x = x \cdot y \longrightarrow x = x \cdot y^*$
(proof)

instance $C3l\text{-algebra} \subseteq C2l\text{-algebra}$
(proof)

sublocale $C2l\text{-algebra} \subseteq C3l\text{-algebra}$
(proof)

sublocale $C1l\text{-algebra} \subseteq C3l\text{-algebra}$
(proof)

sublocale $C3l\text{-algebra} \subseteq C1l\text{-algebra}$
(proof)

sublocale $C1l\text{-algebra} \subseteq C2l\text{-algebra}$
(proof)

sublocale $C3r\text{-algebra} \subseteq C2r\text{-algebra}$
 ⟨proof⟩

sublocale $C2r\text{-algebra} \subseteq C3r\text{-algebra}$
 ⟨proof⟩

sublocale $C1r\text{-algebra} \subseteq C3r\text{-algebra}$
 ⟨proof⟩

sublocale $C3r\text{-algebra} \subseteq C1r\text{-algebra}$
 ⟨proof⟩

class $C1\text{-algebra} = C1l\text{-algebra} + C1r\text{-algebra}$

class $C2\text{-algebra} = C2l\text{-algebra} + C2r\text{-algebra}$

class $C3\text{-algebra} = C3l\text{-algebra} + C3r\text{-algebra}$

sublocale $C0\text{-algebra} \subseteq C2\text{-algebra}$
 ⟨proof⟩

sublocale $C2\text{-algebra} \subseteq C0\text{-algebra}$
 ⟨proof⟩

sublocale $C2\text{-algebra} \subseteq C1\text{-algebra}$ ⟨proof⟩

sublocale $C1\text{-algebra} \subseteq C2\text{-algebra}$ ⟨proof⟩

sublocale $C2\text{-algebra} \subseteq C3\text{-algebra}$ ⟨proof⟩

sublocale $C3\text{-algebra} \subseteq C2\text{-algebra}$ ⟨proof⟩

3.5 Kozen's Kleene Algebras

Kozen's Kleene Algebras [7, 6].

class $Kl\text{-base} = \text{star-diod} +$
assumes $Kl: 1 + x \cdot x^* \leq x^*$

class $Kr\text{-base} = \text{star-diod} +$
assumes $Kr: 1 + x^* \cdot x \leq x^*$

class $K1l\text{-algebra} = Kl\text{-base} +$
assumes $\text{star-inductl}: x \cdot y \leq y \implies x^* \cdot y \leq y$

class $K1r\text{-algebra} = Kr\text{-base} +$
assumes $\text{star-inductr}: y \cdot x \leq y \implies y \cdot x^* \leq y$

class $K2l\text{-algebra} = Kl\text{-base} +$

assumes *star-inductl-var*: $z + x \cdot y \leq y \implies x^* \cdot z \leq y$

class *K2r-algebra* = *Kr-base* +
assumes *star-inductr-var*: $z + y \cdot x \leq y \implies z \cdot x^* \leq y$

class *K1-algebra* = *K1l-algebra* + *K1r-algebra*

class *K2-algebra* = *K2l-algebra* + *K2r-algebra*

sublocale *K1r-algebra* \subseteq *dual: K1l-algebra*
 (+) (\odot) 1 0 (\leq) ($<$) *star*
<proof>

sublocale *K1l-algebra* \subseteq *B2-algebra*
<proof>

sublocale *K1r-algebra* \subseteq *B2-algebra*
<proof>

sublocale *K1l-algebra* \subseteq *C2l-algebra*
<proof>

sublocale *C2l-algebra* \subseteq *K1l-algebra*
<proof>

sublocale *K1r-algebra* \subseteq *C2r-algebra*
<proof>

sublocale *C2r-algebra* \subseteq *K1r-algebra*
<proof>

sublocale *K1-algebra* \subseteq *C0-algebra*
<proof>

sublocale *C0-algebra* \subseteq *K1l-algebra* *<proof>*

sublocale *K2r-algebra* \subseteq *dual: K2l-algebra*
 (+) (\odot) 1 0 (\leq) ($<$) *star*
<proof>

sublocale *K1l-algebra* \subseteq *K2l-algebra*
<proof>

sublocale *K2l-algebra* \subseteq *K1l-algebra*
<proof>

sublocale *K1r-algebra* \subseteq *K2r-algebra*
<proof>

sublocale *K2r-algebra* \subseteq *K1r-algebra*
 ⟨*proof*⟩

sublocale *kleene-algebra* \subseteq *K1-algebra*
 ⟨*proof*⟩

sublocale *K1-algebra* \subseteq *K2-algebra* ⟨*proof*⟩

sublocale *K2-algebra* \subseteq *koz: kleene-algebra*
 ⟨*proof*⟩

3.6 Salomaa's Axioms

Salomaa's axiomatisations of Regular Algebra [9].

class *salomaa-base* = *star-dioid* +
fixes *ewp* :: 'a \Rightarrow bool
assumes *S11*: $(1 + x)^* = x^*$
and *EWP* : $ewp\ x \longleftrightarrow (\exists y. x = 1 + y \wedge \neg ewp\ y)$

class *Sr-algebra* = *salomaa-base* +
assumes *S12r*: $1 + x^* \cdot x = x^*$
and *Ar* : $\llbracket \neg ewp\ y; x = x \cdot y + z \rrbracket \Longrightarrow x = z \cdot y^*$

The following claim is ruled out by Nitpick. The unfold law cannot be weakened as in Kleene algebra.

lemma (in *salomaa-base*)
assumes *S12r'*: $1 + x^* \cdot x \leq x^*$
and *Ar'* : $\llbracket \neg ewp\ y; x = x \cdot y + z \rrbracket \Longrightarrow x = z \cdot y^*$
shows $x^* \leq 1 + x^* \cdot x$

⟨*proof*⟩

class *Sl-algebra* = *salomaa-base* +
assumes *S12l*: $1 + x \cdot x^* = x^*$
and *Al* : $\llbracket \neg ewp\ y; x = y \cdot x + z \rrbracket \Longrightarrow x = y^* \cdot z$

class *S-algebra* = *Sl-algebra* + *Sr-algebra*

sublocale *Sl-algebra* \subseteq *dual: Sr-algebra*
 (+) (\odot) 1 0 (\leq) ($<$) *star ewp*
 ⟨*proof*⟩

context *Sr-algebra*
begin

lemma *kozen-induct-r*:
assumes $y \cdot x + z \leq y$
shows $z \cdot x^* \leq y$

<proof>

end

context *Sl-algebra*

begin

lemma *kozen-induct-l*:

assumes $x \cdot y + z \leq y$

shows $x^* \cdot z \leq y$

<proof>

end

sublocale *Sr-algebra* \subseteq *K2r-algebra*

<proof>

sublocale *Sr-algebra* \subseteq *K1r-algebra* *<proof>*

sublocale *Sl-algebra* \subseteq *K2l-algebra*

<proof>

sublocale *Sl-algebra* \subseteq *K1l-algebra* *<proof>*

sublocale *S-algebra* \subseteq *K1-algebra* *<proof>*

sublocale *S-algebra* \subseteq *K2-algebra* *<proof>*

The following claim could be refuted.

lemma (in *K2-algebra*) $(\neg 1 \leq x) \longrightarrow x = x \cdot y + z \longrightarrow x = z \cdot y^*$

<proof>

class *salomaa-conj-r* = *salomaa-base* +

assumes *salomaa-small-unfold*: $1 + x^* \cdot x = x^*$

assumes *salomaa-small-r*: $\llbracket \neg \text{ewp } y ; x = x \cdot y + 1 \rrbracket \Longrightarrow x = y^*$

sublocale *Sr-algebra* \subseteq *salomaa-conj-r*

<proof>

lemma (in *salomaa-conj-r*) $(\neg \text{ewp } y) \wedge (x = x \cdot y + z) \longrightarrow x = z \cdot y^*$

<proof>

end

4 Models of Regular Algebra

theory *Regular-Algebra-Models*

imports *Regular-Algebras Kleene-Algebra.Kleene-Algebra-Models*

begin

4.1 Language Model of Salomaa Algebra

abbreviation $w\text{-length} :: 'a \text{ list} \Rightarrow \text{nat} (|-|)$
where $|x| \equiv \text{length } x$

definition $l\text{-ewp} :: 'a \text{ lan} \Rightarrow \text{bool}$ **where**
 $l\text{-ewp } X \longleftrightarrow \{\emptyset\} \subseteq X$

interpretation $lan\text{-kozen}$: $K2\text{-algebra } (+) (\cdot) 1 :: 'a \text{ lan } 0 (\subseteq) (\subset) \text{ star}$ $\langle \text{proof} \rangle$

interpretation $lan\text{-boffa}$: $B1\text{-algebra } (+) (\cdot) 1 :: 'a \text{ lan } 0 (\subseteq) (\subset) \text{ star}$ $\langle \text{proof} \rangle$

lemma $length\text{-lang-pow-lb}$:
assumes $\forall x \in X. |x| \geq k \ x \in X^{\wedge n}$
shows $|x| \geq k * n$
 $\langle \text{proof} \rangle$

lemma $l\text{-prod-elim}$: $w \in X \cdot Y \longleftrightarrow (\exists u \ v. w = u @ v \wedge u \in X \wedge v \in Y)$
 $\langle \text{proof} \rangle$

lemma $power\text{-minor-var}$:
assumes $\forall w \in X. k \leq |w|$
shows $\forall w \in X^{\text{Suc } n}. n * k \leq |w|$
 $\langle \text{proof} \rangle$

lemma $power\text{-lb}$: $(\forall w \in X. k \leq |w|) \longrightarrow (\forall w. w \in X^{\text{Suc } n} \longrightarrow n * k \leq |w|)$
 $\langle \text{proof} \rangle$

lemma $prod\text{-lb}$:
 $\llbracket (\forall w \in X. m \leq \text{length } w); (\forall w \in Y. n \leq \text{length } w) \rrbracket \Longrightarrow (\forall w \in (X \cdot Y). (m+n) \leq \text{length } w)$
 $\langle \text{proof} \rangle$

lemma $suicide\text{-aux-l}$:
 $\llbracket (\forall w \in Y. 0 \leq \text{length } w); (\forall w \in X^{\text{Suc } n}. n \leq \text{length } w) \rrbracket \Longrightarrow (\forall w \in X^{\text{Suc } n} \cdot Y. n \leq \text{length } w)$
 $\langle \text{proof} \rangle$

lemma $suicide\text{-aux-r}$:
 $\llbracket (\forall w \in Y. 0 \leq \text{length } w); (\forall w \in X^{\text{Suc } n}. n \leq \text{length } w) \rrbracket \Longrightarrow (\forall w \in Y \cdot X^{\text{Suc } n}. n \leq \text{length } w)$
 $\langle \text{proof} \rangle$

lemma $word\text{-suicide-l}$:
assumes $\neg l\text{-ewp } X \ Y \neq \{\}$
shows $(\forall w \in Y. \exists n. w \notin X^{\text{Suc } n} \cdot Y)$
 $\langle \text{proof} \rangle$

lemma *word-suicide-r*:
assumes $\neg l\text{-ewp } X \ Y \neq \{\}$
shows $(\forall w \in Y. \exists n. w \notin Y \cdot X^{\text{Suc } n})$
 $\langle \text{proof} \rangle$

lemma *word-suicide-lang-l*: $\llbracket \neg l\text{-ewp } X; Y \neq \{\} \rrbracket \implies \exists n. \neg (Y \leq X^{\text{Suc } n} \cdot Y)$
 $\langle \text{proof} \rangle$

lemma *word-suicide-lang-r*: $\llbracket \neg l\text{-ewp } X; Y \neq \{\} \rrbracket \implies \exists n. \neg (Y \leq Y \cdot X^{\text{Suc } n})$
 $\langle \text{proof} \rangle$

These duality results cannot be relocated easily

context *K1-algebra*
begin

lemma *power-dual-transfer* [*simp*]:
 $\text{power.power } (1::'a) (\odot) \ x \ n = x^n$
 $\langle \text{proof} \rangle$

lemma *aarden-aux-l*:
 $y \leq x \cdot y + z \implies y \leq x^{\text{Suc } n} \cdot y + x^* \cdot z$
 $\langle \text{proof} \rangle$

end

lemma *arden-l*:
assumes $\neg l\text{-ewp } y \ x = y \cdot x + z$
shows $x = y^* \cdot z$
 $\langle \text{proof} \rangle$

lemma *arden-r*:
assumes $\neg l\text{-ewp } y \ x = x \cdot y + z$
shows $x = z \cdot y^*$
 $\langle \text{proof} \rangle$

The following two facts provide counterexamples to Arden's rule if the empty word property is not considered.

lemma *arden-l-counter*: $\exists (x::'a \ \text{lan}) (y::'a \ \text{lan}) (z::'a \ \text{lan}). x = y \cdot x + z \wedge x \neq y^* \cdot z$
 $\langle \text{proof} \rangle$

lemma *arden-r-counter*: $\exists (x::'a \ \text{lan}) (y::'a \ \text{lan}) (z::'a \ \text{lan}). x = x \cdot y + z \wedge x \neq z \cdot y^*$
 $\langle \text{proof} \rangle$

interpretation *lan-saloomaa-l*: *Sl-algebra* $(+)$ (\cdot) $1 :: 'a \ \text{lan}$ $0 (\subseteq) (\subset)$ *star l-ewp*
 $\langle \text{proof} \rangle$

interpretation *lan-salomaa-r*: *Sr-algebra* (+) (·) 1 :: 'a *lan* 0 (\subseteq) (\subset) *star l-ewp*
 ⟨*proof*⟩

4.2 Regular Language Model of Salomaa Algebra

notation

Atom (<->) **and**
Plus (**infixl** +_r 65) **and**
Times (**infixl** ·_r 70) **and**
Star (-^{*}_r [101] 100) **and**
Zero (0_r) **and**
One (1_r)

fun *rexp-ewp* :: 'a *rexp* ⇒ *bool* **where**
rexp-ewp 0_r = *False* |
rexp-ewp 1_r = *True* |
rexp-ewp <a> = *False* |
rexp-ewp (s +_r t) = (*rexp-ewp* s ∨ *rexp-ewp* t) |
rexp-ewp (s ·_r t) = (*rexp-ewp* s ∧ *rexp-ewp* t) |
rexp-ewp (s^{*}_r) = *True*

abbreviation *ro*(s) ≡ (*if* (*rexp-ewp* s) *then* 1_r *else* 0_r)

lift-definition *r-ewp* :: 'a *reg-lan* ⇒ *bool* **is** *l-ewp* ⟨*proof*⟩

lift-definition *r-lang* :: 'a *rexp* ⇒ 'a *reg-lan* **is** *lang*
 ⟨*proof*⟩

abbreviation *r-sim* :: 'a *rexp* ⇒ 'a *rexp* ⇒ *bool* (**infix** ~ 50) **where**
p ~ *q* ≡ *r-lang* p = *r-lang* q

declare *Rep-reg-lan* [*simp*]
declare *Rep-reg-lan-inverse* [*simp*]
declare *Abs-reg-lan-inverse* [*simp*]

lemma *rexp-ewp-l-ewp*: *l-ewp* (*lang* x) = *rexp-ewp* x
 ⟨*proof*⟩

theorem *regexp-ewp*:
defines *P-def*: *P*(t) ≡ ∃ t'. t ~ *ro*(t) +_r t' ∧ *ro*(t') = 0_r
shows *P* t
 ⟨*proof*⟩

instantiation *reg-lan* :: (*type*) *Sr-algebra*
begin

lift-definition *ewp-reg-lan* :: 'a *reg-lan* ⇒ *bool* **is** *l-ewp* ⟨*proof*⟩

instance ⟨*proof*⟩

```

end

instantiation reg-lan :: (type) Sl-algebra
begin

instance ⟨proof⟩
end

instance reg-lan :: (type) S-algebra ⟨proof⟩

theorem arden-regex-l:
  assumes  $ro(y) = 0_r \ x \sim y \cdot_r x \ +_r z$ 
  shows  $x \sim y^*_r \cdot_r z$ 
  ⟨proof⟩

theorem arden-regex-r:
  assumes  $ro(y) = 0_r \ x \sim x \cdot_r y \ +_r z$ 
  shows  $x \sim z \cdot_r y^*_r$ 
  ⟨proof⟩

end

```

5 Pratt's Counterexamples

```

theory Pratts-Counterexamples
  imports Regular-Algebras
begin

```

We create two regular algebra models due to Pratt [8] which are used to distinguish K1 algebras from K1l and K1r algebras.

```

datatype pratt1 =
  P1Bot ( $\perp_1$ ) |
  P1Nat nat ( $[-]_1$ ) |
  P1Infty ( $\infty_1$ ) |
  P1Top ( $\top_1$ )

datatype pratt2 =
  P2Bot ( $\perp_2$ ) |
  P2Nat nat ( $[-]_2$ ) |
  P2Infty ( $\infty_2$ ) |
  P2Top ( $\top_2$ )

fun pratt1-max where
  pratt1-max  $[x]_1 \ [y]_1 = [max \ x \ y]_1$  |
  pratt1-max  $x \ \perp_1 = x$  |
  pratt1-max  $\perp_1 \ y = y$  |
  pratt1-max  $\infty_1 \ [y]_1 = \infty_1$  |
  pratt1-max  $[y]_1 \ \infty_1 = \infty_1$  |
  pratt1-max  $\infty_1 \ \infty_1 = \infty_1$  |

```

pratt1-max $\top_1 x = \top_1$ |
pratt1-max $x \top_1 = \top_1$

fun *pratt1-plus* :: *pratt1* \Rightarrow *pratt1* \Rightarrow *pratt1* (**infixl** $+_1$ 65) **where**

$[x]_1 +_1 [y]_1 = [x + y]_1$ |
 $\perp_1 +_1 x = \perp_1$ |
 $x +_1 \perp_1 = \perp_1$ |
 $\infty_1 +_1 [0]_1 = \infty_1$ |
 $[0]_1 +_1 \infty_1 = \infty_1$ |
 $\infty_1 +_1 \infty_1 = \top_1$ |
 $\top_1 +_1 x = \top_1$ |
 $x +_1 \top_1 = \top_1$ |
 $[x]_1 +_1 \infty_1 = \infty_1$ |
 $\infty_1 +_1 x = \top_1$

lemma *plusl-top-infty*: $\top_1 +_1 \infty_1 = \top_1$
<proof>

lemma *plusl-infty-top*: $\infty_1 +_1 \top_1 = \top_1$
<proof>

lemma *plusl-bot-infty*: $\perp_1 +_1 \infty_1 = \perp_1$
<proof>

lemma *plusl-infty-bot*: $\infty_1 +_1 \perp_1 = \perp_1$
<proof>

lemma *plusl-zero-infty*: $[0]_1 +_1 \infty_1 = \infty_1$
<proof>

lemma *plusl-infty-zero*: $\infty_1 +_1 [0]_1 = \infty_1$
<proof>

lemma *plusl-infty-num [simp]*: $x > 0 \Longrightarrow \infty_1 +_1 [x]_1 = \top_1$
<proof>

lemma *plusl-num-infty [simp]*: $x > 0 \Longrightarrow [x]_1 +_1 \infty_1 = \infty_1$
<proof>

fun *pratt2-max* **where**

pratt2-max $[x]_2 [y]_2 = [\max x y]_2$ |
pratt2-max $x \perp_2 = x$ |
pratt2-max $\perp_2 y = y$ |
pratt2-max $\infty_2 [y]_2 = \infty_2$ |
pratt2-max $[y]_2 \infty_2 = \infty_2$ |
pratt2-max $\infty_2 \infty_2 = \infty_2$ |
pratt2-max $\top_2 x = \top_2$ |
pratt2-max $x \top_2 = \top_2$

fun *pratt2-plus* :: *pratt2* \Rightarrow *pratt2* \Rightarrow *pratt2* (**infixl** +₂ 65) **where**
 $[x]_2 +_2 [y]_2 = [x + y]_2$ |
 $\perp_2 +_2 x = \perp_2$ |
 $x +_2 \perp_2 = \perp_2$ |
 $\infty_2 +_2 [0]_2 = \infty_2$ |
 $[0]_2 +_2 \infty_2 = \infty_2$ |
 $\infty_2 +_2 \infty_2 = \top_2$ |
 $\top_2 +_2 x = \top_2$ |
 $x +_2 \top_2 = \top_2$ |
 $x +_2 \infty_2 = \top_2$ |
 $\infty_2 +_2 [x]_2 = \infty_2$

instantiation *pratt1* :: *selective-semiring*
begin

definition *zero-pratt1-def*:

$$0 \equiv \perp_1$$

definition *one-pratt1-def*:

$$1 \equiv [0]_1$$

definition *plus-pratt1-def*:

$$x + y \equiv \text{pratt1-max } x \ y$$

definition *times-pratt1-def*:

$$x * y \equiv x +_1 y$$

definition *less-eq-pratt1-def*:

$$(x::\text{pratt1}) \leq y \equiv x + y = y$$

definition *less-pratt1-def*:

$$(x::\text{pratt1}) < y \equiv x \leq y \wedge x \neq y$$

instance

<proof>

end

instance *pratt1* :: *dioid-one-zero* *<proof>*

instantiation *pratt2* :: *selective-semiring*
begin

definition *zero-pratt2-def*:

$$0 \equiv \perp_2$$

definition *one-pratt2-def*:

$$1 \equiv [0]_2$$

definition *times-pratt2-def*:

$$x * y \equiv x +_2 y$$

definition *plus-pratt2* :: *pratt2* \Rightarrow *pratt2* \Rightarrow *pratt2* **where**
plus-pratt2 *x y* \equiv *pratt2-max* *x y*

definition *less-eq-pratt2-def*:
 $(x :: \text{pratt2}) \leq y \equiv x + y = y$

definition *less-pratt2-def*:
 $(x :: \text{pratt2}) < y \equiv x \leq y \wedge x \neq y$

instance
 $\langle \text{proof} \rangle$
end

lemma *top-greatest*: $x \leq \top_1$
 $\langle \text{proof} \rangle$

instantiation *pratt1* :: *star-op*
begin

definition *star-pratt1* **where**
 $x^* \equiv \text{if } (x = \perp_1 \vee x = [0]_1) \text{ then } [0]_1 \text{ else } \top_1$
instance $\langle \text{proof} \rangle$
end

instantiation *pratt2* :: *star-op*
begin

definition *star-pratt2* **where**
 $x^* \equiv \text{if } (x = \perp_2 \vee x = [0]_2) \text{ then } [0]_2 \text{ else } \top_2$
instance $\langle \text{proof} \rangle$
end

instance *pratt1* :: *K1r-algebra*
 $\langle \text{proof} \rangle$

instance *pratt2* :: *K1l-algebra*
 $\langle \text{proof} \rangle$

lemma *one-star-top*: $[1]_1^* = \top_1$
 $\langle \text{proof} \rangle$

lemma *pratt1-kozen-1l-counterexample*:
 $\exists x y :: \text{pratt1}. \neg (x \cdot y \leq y \wedge x^* \cdot y \leq y)$
 $\langle \text{proof} \rangle$

lemma *pratt2-kozen-1r-counterexample*:
 $\exists x y :: \text{pratt2}. \neg (y \cdot x \leq y \wedge y \cdot x^* \leq y)$
 $\langle \text{proof} \rangle$

end

6 Variants of Regular Algebra

theory *Regular-Algebra-Variants*
imports *Regular-Algebras* *Pratts-Counterexamples*
begin

Replacing Kozen's induction axioms by Boffa's leads to incompleteness.

lemma (in *star-doid*)
assumes $\bigwedge x. 1 + x \cdot x^* = x^*$
and $\bigwedge x. 1 + x^* \cdot x = x^*$
and $\bigwedge x. x \cdot x = x \implies x^* = 1 + x$
shows $\bigwedge x y. (x + y)^* = x^* \cdot (y \cdot x^*)^*$

<proof>

lemma (in *star-doid*)
assumes $\bigwedge x. 1 + x \cdot x^* = x^*$
and $\bigwedge x. 1 + x^* \cdot x = x^*$
and $\bigwedge x. x \cdot x = x \implies x^* = 1 + x$
shows $\bigwedge x y. x \leq y \longrightarrow x^* \leq y^*$

<proof>

lemma (in *star-doid*)
assumes $\bigwedge x. 1 + x \cdot x^* = x^*$
and $\bigwedge x. 1 + x^* \cdot x = x^*$
and $\bigwedge x y. 1 + x \leq y \wedge y \cdot y \leq y \longrightarrow x^* \leq y$
shows $\bigwedge x. 1 + x \leq x^*$

<proof>

lemma (in *star-doid*)
assumes $\bigwedge x. 1 + x \cdot x^* = x^*$
and $\bigwedge x. 1 + x^* \cdot x = x^*$
and $\bigwedge x y. 1 + x \leq y \wedge y \cdot y \leq y \longrightarrow x^* \leq y$
shows $\bigwedge x. x^* = (1 + x)^*$

<proof>

lemma (in *star-doid*)
assumes $\bigwedge x. 1 + x \cdot x^* = x^*$
and $\bigwedge x. 1 + x^* \cdot x = x^*$
and $\bigwedge x y. 1 + x + y \cdot y \leq y \implies x^* \leq y$
shows $\bigwedge x. x^* \cdot x^* \leq x^*$

<proof>

lemma (in *star-doid*)
assumes $\bigwedge x. 1 + x \cdot x^* = x^*$

and $\bigwedge x. 1 + x^* \cdot x = x^*$
and $\bigwedge x y z. x \cdot y = y \cdot z \implies x^* \cdot y = y \cdot z^*$
shows $1^* = 1$

<proof>

lemma (in star-doid)
assumes $\bigwedge x. 1 + x \cdot x^* = x^*$
and $\bigwedge x. 1 + x^* \cdot x = x^*$
and $\bigwedge x y z. x \cdot y \leq y \cdot z \implies x^* \cdot y \leq y \cdot z^*$
and $\bigwedge x y z. y \cdot x \leq z \cdot y \implies y \cdot x^* \leq z^* \cdot y$
shows $1^* = 1$

<proof>

lemma (in star-doid)
assumes $\bigwedge x. 1 + x \cdot x^* = x^*$
and $\bigwedge x. 1 + x^* \cdot x = x^*$
and $\bigwedge x y. x = y \cdot x \implies x = y^* \cdot x$
and $\bigwedge x y. x = x \cdot y \implies x = x \cdot y^*$
shows $\bigwedge x y. y \cdot x \leq y \implies y \cdot x^* \leq y$

<proof>

class C3l-var = conway-doid +
assumes *C3l-var*: $z + x \cdot y \leq y \implies x^* \cdot z \leq y$

class C3r-var = conway-doid +
assumes *C3r-var*: $z + y \cdot x \leq y \implies z \cdot x^* \leq y$

class C3-var = C3l-var + C3r-var

sublocale C3l-var \subseteq C3l-algebra
<proof>

sublocale C3l-algebra \subseteq C3l-var
<proof>

sublocale C3-var \subseteq C3-algebra
<proof>

sublocale C3-algebra \subseteq C3-var
<proof>

class Brtc-algebra = star-doid +
assumes *rtc1*: $1 + x^* \cdot x^* + x \leq x^*$
and *rtc2*: $1 + x + y \cdot y \leq y \implies x^* \leq y$

sublocale B2-algebra \subseteq Brtc-algebra
<proof>

sublocale *Brtc-algebra* \subseteq *B2-algebra*

<proof>

class *wB1-algebra* = *conway-diod* +

assumes *wR*: $x \cdot x \leq x \implies x^* = 1 + x$

sublocale *wB1-algebra* \subseteq *B1-algebra*

<proof>

lemma (in *B1-algebra*) *one-plus-star*: $x^* = (1 + x)^*$

<proof>

sublocale *B1-algebra* \subseteq *wB1-algebra*

<proof>

end

References

- [1] A. Armstrong, G. Struth, and T. Weber. Kleene algebra. *Archive of Formal Proofs*, 2013. http://isa-afp.org/entries/Kleene_Algebra.shtml, Formal proof development.
- [2] M. Boffa. Une remarque sur les systèmes complets d'identités rationnelles. *Informatique théorique et applications*, 24(4):419–423, 1990.
- [3] M. Boffa. Une condition impliquant toutes les identités rationnelles. *Informatique théorique et applications*, 29(6):515–518, 1995.
- [4] J. H. Conway. *Regular Algebra and Finite Machines*. Chapman and Hall, 1971.
- [5] S. Foster and G. Struth. On the fine-structure of regular algebra. *J. Automated Reasoning*, 54(2):165–197, 2015.
- [6] D. Kozen. On Kleene algebras and closed semirings. In B. Rován, editor, *MFCS'90*, volume 452 of *LNCS*, pages 26–47. Springer, 1990.
- [7] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390, 1994.
- [8] V. Pratt. Action logic and pure induction. Technical Report STAN-CS-90-1343, Department of Computer Science, Stanford University, 1990.
- [9] A. Salomaa. Two complete axiom systems for the algebra of regular events. *J. ACM*, 13(1):158–169, 1966.