The Equational Theory of Algebras of Languages

RAMiCS
Special session on mechanised reasoning

May 18, 2017

Paul Brunet
University College London

Introduction

$\forall\Sigma,\ \forall L, M, N \subseteq \Sigma^\star,$

$$\left(L^\smile \cap M\right) \cdot \left(1 \cap \left(N \cdot L^\smile\right)\right) = \left(1 \cap L\right) \cdot \left(L \cap M^\smile\right)^\smile$$

Introduction

$\forall \Sigma,\ \forall L, M, N \subseteq \Sigma^\star,$

$$\left(L^{\smile} \cap M\right) \cdot \left(1 \cap \left(N \cdot L^{\smile}\right)\right) = \left(1 \cap L\right) \cdot \left(L \cap M^{\smile}\right)^{\smile}$$

- Decidability

Introduction

$\forall \Sigma,\ \forall L, M, N \subseteq \Sigma^\star,$

$$\left(L^\smile \cap M\right) \cdot \left(1 \cap \left(N \cdot L^\smile\right)\right) = (1 \cap L) \cdot \left(L \cap M^\smile\right)^\smile$$

- Decidability
- Complexity

Introduction

$\forall \Sigma,\ \forall L, M, N \subseteq \Sigma^\star,$

$$\left(L^{\smile} \cap M\right) \cdot \left(1 \cap \left(N \cdot L^{\smile}\right)\right) = (1 \cap L) \cdot \left(L \cap M^{\smile}\right)^{\smile}$$

- Decidability
- Complexity
- Axiomatisation

Introduction

$\forall\Sigma,\ \forall L, M, N \subseteq \Sigma^\star,$

$$\left(L^\smile \cap M\right) \cdot \left(1 \cap \left(N \cdot L^\smile\right)\right) = (1 \cap L) \cdot \left(L \cap M^\smile\right)^\smile$$

- Decidability
- Complexity
- **Axiomatisation**

Language Algebra

Language Operators

unit language	1
empty language	0
composition	$L \cdot M$
union	$L \cup M$
intersection	$L \cap M$
mirror image	$L^{\smile}$

Language Algebra

Language Operators

unit language	1	$:= \{\epsilon\}$
empty language	0	
composition	$L \cdot M$	
union	$L \cup M$	
intersection	$L \cap M$	
mirror image	$L^{\smile}$	

Language Algebra

Language Operators

unit language	1	$:= \{\epsilon\}$
empty language	0	$:= \emptyset$
composition	$L \cdot M$	
union	$L \cup M$	
intersection	$L \cap M$	
mirror image	$L^{\smile}$	

Language Algebra

Language Operators

unit language	1	$:= \{\epsilon\}$
empty language	0	$:= \emptyset$
composition	$L \cdot M$	$:= \{uv \mid u \in L \text{ and } v \in M\}$
union	$L \cup M$	
intersection	$L \cap M$	
mirror image	$L^{\smile}$	

Language Algebra

Language Operators

unit language	1	$:= \{\epsilon\}$
empty language	0	$:= \emptyset$
composition	$L \cdot M$	$:= \{uv \mid u \in L \text{ and } v \in M\}$
union	$L \cup M$	$:= \{u \mid u \in L \text{ or } u \in M\}$
intersection	$L \cap M$	
mirror image	$L^{\smile}$	

Language Algebra

Language Operators

unit language	1	$:= \{\epsilon\}$
empty language	0	$:= \emptyset$
composition	$L \cdot M$	$:= \{uv \mid u \in L \text{ and } v \in M\}$
union	$L \cup M$	$:= \{u \mid u \in L \text{ or } u \in M\}$
intersection	$L \cap M$	$:= \{u \mid u \in L \text{ and } u \in M\}$
mirror image	$L^{\smile}$	

Language Algebra

Language Operators

unit language	1	$:= \{\epsilon\}$
empty language	0	$:= \emptyset$
composition	$L \cdot M$	$:= \{uv \mid u \in L \text{ and } v \in M\}$
union	$L \cup M$	$:= \{u \mid u \in L \text{ or } u \in M\}$
intersection	$L \cap M$	$:= \{u \mid u \in L \text{ and } u \in M\}$
mirror image	$L^{\smile}$	$:= \{x_n \dots x_1 \mid x_1 \dots x_n \in L\}$

Kleene Algebra

Where everything is nice

Let $\Sigma = \{a, b, \dots\}$ be a finite alphabet.

Regular expressions

$$e, f \in \mathrm{Reg}\langle\Sigma\rangle ::= 0 \mid 1 \mid a \mid e \cdot f \mid e \cup f \mid e^\star \mid e \cap f \mid e^\smile$$

- $\mathrm{Rel} \models e = f$: universal law of relational Kleene algebra.
- $\mathrm{Lang} \models e = f$: universal law of language Kleene algebra.
- $\mathrm{KA} \vdash e = f$: universal law of Kleene algebra.
  (i.e. logical consequence of the axioms of KA).

$$\mathrm{KA} \vdash e = f$$

$$\Updownarrow$$

$$\mathrm{Rel} \models e = f \iff \mathcal{L}(e) = \mathcal{L}(f) \iff \mathrm{Lang} \models e = f$$

decidable

Intersection & Mirror

$$e, f \in \mathsf{IMReg}\langle\Sigma\rangle ::= 0 \mid 1 \mid a \mid e \cdot f \mid e \cup f \mid e \cap f \mid e^{\smile}$$

Intersection & Mirror

Language Algebra is not Relation Algebra

$$e, f \in \mathrm{IMReg}\langle\Sigma\rangle ::= 0 \mid 1 \mid a \mid e \cdot f \mid e \cup f \mid e \cap f \mid e^{\smile}$$

$$\mathrm{Lang} \not\models a \leq a \cdot a^{\smile} \cdot a \qquad \text{but} \qquad \mathrm{Rel} \models a \leq a \cdot a^{\smile} \cdot a$$

$$\mathrm{Lang} \models (1 \cap a) \cdot b = b \cdot (1 \cap a) \qquad \text{but} \qquad \mathrm{Rel} \not\models (1 \cap a) \cdot b = b \cdot (1 \cap a)$$

Intersection & Mirror

$$e, f \in \mathsf{IMReg}\langle\Sigma\rangle ::= 0 \mid 1 \mid a \mid e \cdot f \mid e \cup f \mid e^\star \mid e \cap f \mid e^\smile$$

$$\mathrm{Lang} \models e = f \overset{?}{\Leftrightarrow} \mathcal{L}(e) = \mathcal{L}(f)$$

Intersection & Mirror

Regular languages are not enough

$$e, f \in \mathsf{IMReg}\langle\Sigma\rangle ::= 0 \mid 1 \mid a \mid e \cdot f \mid e \cup f \mid e^\star \mid e \cap f \mid e^\smile$$

$$\mathrm{Lang} \models e = f \;\not\Leftarrow\; \mathcal{L}(e) = \mathcal{L}(f) \qquad \mathrm{Lang} \models e = f \;\Rightarrow\; \mathcal{L}(e) = \mathcal{L}(f)$$

Counterexample

$$\mathcal{L}(a \cap b) = \mathcal{L}(0) \quad \Big| \quad \mathcal{L}(a) = \mathcal{L}(a^\smile)$$

$$\mathrm{Lang} \not\models a \cap b = 0 \quad \Big| \quad \mathrm{Lang} \not\models a = a^\smile$$

Outline

I. Introduction

II. Monoidal meet semilattice

III. Mirror image

IV. Sum and star

Outline

Monoidal meet-semilattice

$$e, f \in \mathbb{T}_{\Sigma} ::= 1 \mid a \mid e \cdot f \mid e \cap f$$

$$\mathrm{Lang} \models (1 \cap a) \cdot b = b \cdot (1 \cap a)$$

Monoidal meet-semilattice

$$e, f \in \mathbb{T}_{\Sigma} ::= 1 \mid a \mid e \cdot f \mid e \cap f$$

$$\mathrm{Lang} \models (1 \cap a) \cdot b = b \cdot (1 \cap a)$$

Proof. Let $\sigma : \{a, b\} \to \mathcal{P}(X^{\star})$.

Monoidal meet-semilattice

$$e, f \in \mathbb{T}_\Sigma ::= 1 \mid a \mid e \cdot f \mid e \cap f$$

$$\mathrm{Lang} \models (1 \cap a) \cdot b = b \cdot (1 \cap a)$$

Proof. Let $\sigma : \{a, b\} \to \mathcal{P}(X^\star)$.

- If $\epsilon \in \sigma(a)$:

$$\begin{aligned} \widehat{\sigma}((1 \cap a) \cdot b) &= \\ \widehat{\sigma}(b \cdot (1 \cap a)) &= \end{aligned}$$

- If $\epsilon \notin \sigma(a)$:

$$\begin{aligned} \widehat{\sigma}((1 \cap a) \cdot b) &= \\ \widehat{\sigma}(b \cdot (1 \cap a)) &= \end{aligned}$$

□

Monoidal meet-semilattice

$$e, f \in \mathbb{T}_\Sigma ::= 1 \mid a \mid e \cdot f \mid e \cap f$$

$$\mathrm{Lang} \models (1 \cap a) \cdot b = b \cdot (1 \cap a)$$

Proof. Let $\sigma : \{a, b\} \to \mathcal{P}(X^\star)$.

- If $\epsilon \in \sigma(a)$: then $\widehat{\sigma}(1 \cap a) = \{\epsilon\}$, thus:

$$\begin{aligned} \widehat{\sigma}((1 \cap a) \cdot b) &= \\ \widehat{\sigma}(b \cdot (1 \cap a)) &= \end{aligned}$$

- If $\epsilon \notin \sigma(a)$:

$$\begin{aligned} \widehat{\sigma}((1 \cap a) \cdot b) &= \\ \widehat{\sigma}(b \cdot (1 \cap a)) &= \end{aligned}$$

$\square$

Monoidal meet-semilattice

$$e, f \in \mathbb{T}_\Sigma ::= 1 \;\mid\; a \;\mid\; e \cdot f \;\mid\; e \cap f$$

$$\mathrm{Lang} \models (1 \cap a) \cdot b = b \cdot (1 \cap a)$$

Proof. Let $\sigma : \{a, b\} \to \mathcal{P}(X^\star)$.

- If $\epsilon \in \sigma(a)$: then $\widehat{\sigma}(1 \cap a) = \{\epsilon\}$, thus:

$$\begin{aligned}
\widehat{\sigma}((1 \cap a) \cdot b) &= \{\epsilon\} \cdot \sigma(b) = \sigma(b)\,. \\
\widehat{\sigma}(b \cdot (1 \cap a)) &= \sigma(b) \cdot \{\epsilon\} = \sigma(b)\,.
\end{aligned}$$

- If $\epsilon \notin \sigma(a)$:

$$\begin{aligned}
\widehat{\sigma}((1 \cap a) \cdot b) &= \\
\widehat{\sigma}(b \cdot (1 \cap a)) &=
\end{aligned}$$

□

Monoidal meet-semilattice

$$e, f \in \mathbb{T}_\Sigma ::= 1 \mid a \mid e \cdot f \mid e \cap f$$

$$\mathrm{Lang} \models (1 \cap a) \cdot b = b \cdot (1 \cap a)$$

Proof. Let $\sigma : \{a, b\} \to \mathcal{P}(X^\star)$.

- If $\epsilon \in \sigma(a)$: then $\widehat{\sigma}(1 \cap a) = \{\epsilon\}$, thus:

$$\begin{aligned} \widehat{\sigma}((1 \cap a) \cdot b) &= \{\epsilon\} \cdot \sigma(b) = \sigma(b). \\ \widehat{\sigma}(b \cdot (1 \cap a)) &= \sigma(b) \cdot \{\epsilon\} = \sigma(b). \end{aligned}$$

- If $\epsilon \notin \sigma(a)$: then $\widehat{\sigma}(1 \cap a) = \emptyset$, thus:

$$\begin{aligned} \widehat{\sigma}((1 \cap a) \cdot b) &= \\ \widehat{\sigma}(b \cdot (1 \cap a)) &= \end{aligned}$$

□

Monoidal meet-semilattice

$$e, f \in \mathbb{T}_\Sigma ::= 1 \mid a \mid e \cdot f \mid e \cap f$$

$$\mathrm{Lang} \models (1 \cap a) \cdot b = b \cdot (1 \cap a)$$

Proof. Let $\sigma : \{a, b\} \to \mathcal{P}(X^\star)$.

- If $\epsilon \in \sigma(a)$: then $\widehat{\sigma}(1 \cap a) = \{\epsilon\}$, thus:

$$\begin{aligned} \widehat{\sigma}((1 \cap a) \cdot b) &= \{\epsilon\} \cdot \sigma(b) = \sigma(b). \\ \widehat{\sigma}(b \cdot (1 \cap a)) &= \sigma(b) \cdot \{\epsilon\} = \sigma(b). \end{aligned}$$

- If $\epsilon \notin \sigma(a)$: then $\widehat{\sigma}(1 \cap a) = \emptyset$, thus:

$$\begin{aligned} \widehat{\sigma}((1 \cap a) \cdot b) &= \emptyset \cdot \sigma(b) = \emptyset. \\ \widehat{\sigma}(b \cdot (1 \cap a)) &= \sigma(b) \cdot \emptyset = \emptyset. \end{aligned}$$

□

Weak terms

$$e, f \in \mathbb{SP}_\Sigma ::= a \mid e \cdot f \mid e \cap f$$

Definition

A weak term is a pair $\langle t, A\rangle$ where $A \subseteq \Sigma$ and either $t = 1$ or $t \in \mathbb{SP}_\Sigma$. The set of weak terms is $\mathbb{W}_\Sigma$.

Weak terms

$$e, f \in \mathbb{SP}_{\Sigma} ::= a \mid e \cdot f \mid e \cap f$$

Definition

A weak term is a pair $\langle t, A \rangle$ where $A \subseteq \Sigma$ and either $t = 1$ or $t \in \mathbb{SP}_{\Sigma}$. The set of weak terms is $\mathbb{W}_{\Sigma}$.

Given a map $\sigma : \Sigma \to \mathcal{P}(X^{\star})$, we define:

$$\tilde{\sigma}\langle t, A \rangle = \begin{cases} \emptyset & \text{if } \exists a \in A : \epsilon \notin \sigma(a) \\ \widehat{\sigma}(t) & \text{otherwise} \end{cases}$$

Weak terms

$$e, f \in \mathbb{SP}_\Sigma ::= a \mid e \cdot f \mid e \cap f$$

Definition

A weak term is a pair $\langle t, A\rangle$ where $A \subseteq \Sigma$ and either $t = 1$ or $t \in \mathbb{SP}_\Sigma$. The set of weak terms is $\mathbb{W}_\Sigma$.

Given a map $\sigma : \Sigma \to \mathcal{P}(X^\star)$, we define:

$$\tilde{\sigma}\langle t, A\rangle = \begin{cases} \emptyset & \text{if } \exists a \in A : \epsilon \notin \sigma(a) \\ \widehat{\sigma}(t) & \text{otherwise} \end{cases}$$

$$\begin{aligned}
\langle 1, A\rangle \bullet \langle 1, B\rangle &\coloneqq \langle 1, A \cup B\rangle \\
\langle u, A\rangle \bullet \langle 1, B\rangle &\coloneqq \langle u, A \cup B\rangle \\
\langle 1, A\rangle \bullet \langle v, B\rangle &\coloneqq \langle v, A \cup B\rangle \\
\langle u, A\rangle \bullet \langle v, B\rangle &\coloneqq \langle u \cdot v, A \cup B\rangle
\end{aligned}$$

Weak terms

$$e, f \in \mathbb{SP}_\Sigma ::= a \mid e \cdot f \mid e \cap f$$

Definition

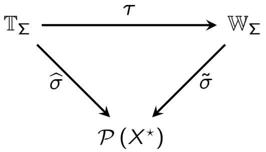
A weak term is a pair $\langle t, A\rangle$ where $A \subseteq \Sigma$ and either $t = 1$ or $t \in \mathbb{SP}_\Sigma$. The set of weak terms is $\mathbb{W}_\Sigma$.

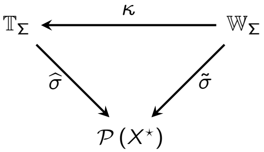
Given a map $\sigma : \Sigma \to \mathcal{P}(X^\star)$, we define:

$$\tilde{\sigma}\langle t, A\rangle = \begin{cases} \emptyset & \text{if } \exists a \in A : \epsilon \notin \sigma(a) \\ \widehat{\sigma}(t) & \text{otherwise} \end{cases}$$

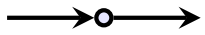
$$\begin{aligned}
\langle 1, A\rangle \bullet \langle 1, B\rangle &:= \langle 1, A \cup B\rangle & \langle 1, A\rangle \parallel \langle 1, B\rangle &:= \langle 1, A \cup B\rangle \\
\langle u, A\rangle \bullet \langle 1, B\rangle &:= \langle u, A \cup B\rangle & \langle u, A\rangle \parallel \langle 1, B\rangle &:= \langle 1, A \cup B \cup \mathit{var}(u)\rangle \\
\langle 1, A\rangle \bullet \langle v, B\rangle &:= \langle v, A \cup B\rangle & \langle 1, A\rangle \parallel \langle v, B\rangle &:= \langle 1, A \cup B \cup \mathit{var}(v)\rangle \\
\langle u, A\rangle \bullet \langle v, B\rangle &:= \langle u \cdot v, A \cup B\rangle & \langle u, A\rangle \parallel \langle v, B\rangle &:= \langle u \cap v, A \cup B\rangle.
\end{aligned}$$

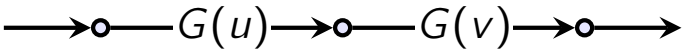
Translations to and from weak terms

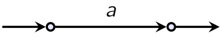


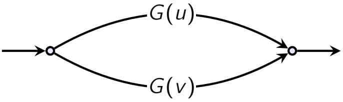


Comparing series parallel terms

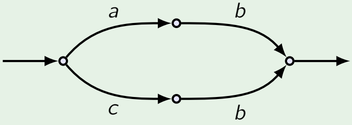
$\mathcal{G}(1) :=$ 

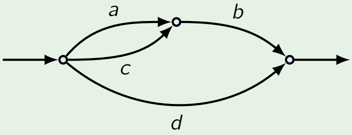
$\mathcal{G}(u \cdot v) :=$ 

$\mathcal{G}(a) :=$ 

$\mathcal{G}(u \cap v) :=$ 

Example

$\mathcal{G}\left(((a \cap c) \cdot b) \cap d\right) =$ 

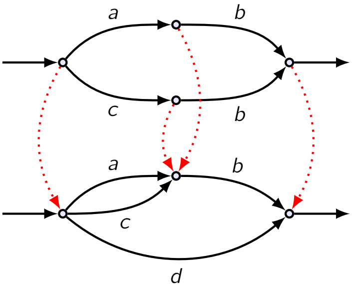
$\mathcal{G}\left((a \cdot b) \cap (c \cdot b)\right) =$ 

Preorder

Preorder on graphs

$G \blacktriangleleft H$ if there exists a graph morphism from H to G.

H :



$((a \cap c) \cdot b) \cap d$

G :

$(a \cdot b) \cap (c \cdot b)$

Characterization theorem

$$u, v \in \mathbb{SP}_\Sigma ::= a \mid u \cdot v \mid u \cap v$$

Theorem

$$\mathrm{Rel} \models u \subseteq v \Leftrightarrow \mathcal{G}(u) \blacktriangleleft \mathcal{G}(v)$$

Freyd & Scedrov, **Categories, Allegories**, *1990*

Andréka & Bredikhin, **The equational theory of union-free algebras of relations**, *1995*

Theorem

$$\forall u, v \in \mathbb{SP}_\Sigma,\ \mathrm{Rel} \models u \subseteq v \Leftrightarrow \mathrm{Lang} \models u \subseteq v.$$

Andréka, Mikulás & Németi, **The equational theory of Kleene lattices**, *TCS'11*

Preorder on weak graphs

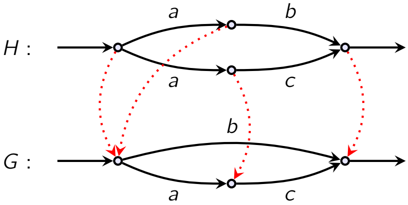
Definition

A weak graph is a pair of a graph and a set of tests.

Weak graph preorder

$\langle G, A\rangle \blacktriangleleft \langle H, B\rangle$ if $B \subseteq A$ and there is an A-weak morphism from H to G.

$A = \{a\}$



Characterisation Theorem

$\mathcal{G}\langle u, A\rangle := \langle \mathcal{G}(u), A\rangle$.

Theorem

$$(\forall \sigma,\ \tilde{\sigma}(u) \subseteq \tilde{\sigma}(v)) \Leftrightarrow \mathcal{G}(u) \blacktriangleleft \mathcal{G}(v).$$

Corollary

$\forall u, v \in \mathbb{T}_{\boldsymbol{\Sigma}}$,

$$(\forall \sigma,\ \widehat{\sigma}(u) \subseteq \widehat{\sigma}(v)) \Leftrightarrow \mathcal{G}(\tau(u)) \blacktriangleleft \mathcal{G}(\tau(v)).$$

Axiomatisation of weak graph morphism

Structural laws

$$\frac{}{A \vdash_{sp} u \leq u} \qquad \frac{A \vdash_{sp} u \leq v \qquad A \vdash_{sp} v \leq w}{A \vdash_{sp} u \leq w}$$

$$\frac{A \vdash_{sp} u \leq v \qquad A \vdash_{sp} u' \leq v'}{A \vdash_{sp} u \cdot u' \leq v \cdot v'} \qquad \frac{A \vdash_{sp} u \leq v \qquad A \vdash_{sp} u' \leq v'}{A \vdash_{sp} u \cap u' \leq v \cap v'}$$

Usual laws

$$\frac{}{A \vdash_{sp} u \cdot (v \cdot w) = (u \cdot v) \cdot w} \qquad \frac{}{A \vdash_{sp} u \cap (v \cap w) = (u \cap v) \cap w}$$

$$\frac{}{A \vdash_{sp} u \leq u \cap u} \qquad \frac{}{A \vdash_{sp} u \cap v \leq v \cap u} \qquad \frac{}{A \vdash_{sp} u \cap v \leq u}$$

Compression laws

$$\frac{var(u) \subseteq A}{A \vdash_{sp} v \leq u \cdot v} \qquad \frac{var(u) \subseteq A}{A \vdash_{sp} v \leq v \cdot u}$$

Proof.

- if $A \vdash_{sp} u \leq v$ then there exists an A-weak morphism from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: easy induction on the proof tree.

$\square$

Proof.

- if $A \vdash_{sp} u \leq v$ then there exists an A-weak morphism from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: easy induction on the proof tree.
- suppose there exists an A-weak morphism ϕ from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: we start with an induction on v.

□

Proof.

- if $A \vdash_{sp} u \leq v$ then there exists an A-weak morphism from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: easy induction on the proof tree.
- suppose there exists an A-weak morphism ϕ from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: we start with an induction on v.
  - $v = a$: simple induction on u;

□

Proof.

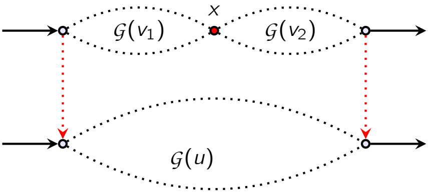
- if $A \vdash_{sp} u \leq v$ then there exists an A-weak morphism from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: easy induction on the proof tree.
- suppose there exists an A-weak morphism ϕ from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: we start with an induction on v.
  - $v = a$: simple induction on u;
  - $v = v_1 \cap v_2$: we can decompose ϕ into ϕ_1, ϕ_2, A-weak morphisms from $\mathcal{G}(v_1)$ and $\mathcal{G}(v_2)$ to $\mathcal{G}(u)$

□

Proof.

- if $A \vdash_{sp} u \leq v$ then there exists an A-weak morphism from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: easy induction on the proof tree.
- suppose there exists an A-weak morphism ϕ from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: we start with an induction on v.
  - $v = a$: simple induction on u;
  - $v = v_1 \cap v_2$: we can decompose ϕ into ϕ_1, ϕ_2, A-weak morphisms from $\mathcal{G}(v_1)$ and $\mathcal{G}(v_2)$ to $\mathcal{G}(u)$
  - $v = v_1 \cdot v_2$: we do a case analysis on $\phi(x)$:

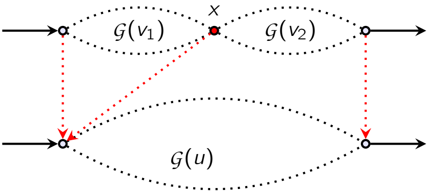
□



Proof.

- if $A \vdash_{sp} u \leq v$ then there exists an A-weak morphism from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: easy induction on the proof tree.
- suppose there exists an A-weak morphism ϕ from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: we start with an induction on v.
  - $v = a$: simple induction on u;
  - $v = v_1 \cap v_2$: we can decompose ϕ into ϕ_1, ϕ_2, A-weak morphisms from $\mathcal{G}(v_1)$ and $\mathcal{G}(v_2)$ to $\mathcal{G}(u)$
  - $v = v_1 \cdot v_2$: we do a case analysis on $\phi(x)$:
    - $\mathit{var}(v_1) \subseteq A$ and ϕ is an A-weak morphism from $\mathcal{G}(v_2)$ to $\mathcal{G}(u)$;

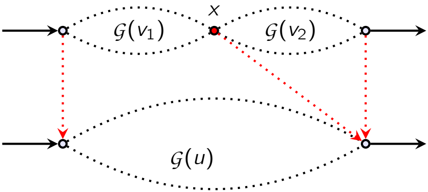
□



Proof.

- if $A \vdash_{sp} u \leq v$ then there exists an A-weak morphism from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: easy induction on the proof tree.
- suppose there exists an A-weak morphism ϕ from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: we start with an induction on v.
  - $v = a$: simple induction on u;
  - $v = v_1 \cap v_2$: we can decompose ϕ into ϕ_1, ϕ_2, A-weak morphisms from $\mathcal{G}(v_1)$ and $\mathcal{G}(v_2)$ to $\mathcal{G}(u)$
  - $v = v_1 \cdot v_2$: we do a case analysis on $\phi(x)$:
    - $\mathit{var}(v_1) \subseteq A$ and ϕ is an A-weak morphism from $\mathcal{G}(v_2)$ to $\mathcal{G}(u)$;
    - $\mathit{var}(v_2) \subseteq A$ and ϕ is an A-weak morphism from $\mathcal{G}(v_1)$ to $\mathcal{G}(u)$;

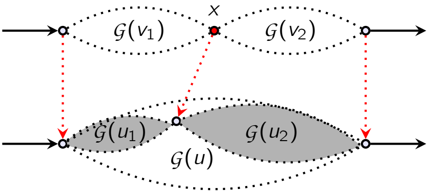
□



Proof.

- if $A \vdash_{sp} u \leq v$ then there exists an A-weak morphism from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: easy induction on the proof tree.
- suppose there exists an A-weak morphism ϕ from $\mathcal{G}(v)$ to $\mathcal{G}(u)$: we start with an induction on v.
  - $v = a$: simple induction on u;
  - $v = v_1 \cap v_2$: we can decompose ϕ into ϕ_1, ϕ_2, A-weak morphisms from $\mathcal{G}(v_1)$ and $\mathcal{G}(v_2)$ to $\mathcal{G}(u)$
  - $v = v_1 \cdot v_2$: we do a case analysis on $\phi(x)$:
    - $\mathit{var}(v_1) \subseteq A$ and ϕ is an A-weak morphism from $\mathcal{G}(v_2)$ to $\mathcal{G}(u)$;
    - $\mathit{var}(v_2) \subseteq A$ and ϕ is an A-weak morphism from $\mathcal{G}(v_1)$ to $\mathcal{G}(u)$;
    - there are two terms u_1, u_2 such that $A \vdash_{sp} u \leq u_1 \cdot u_2$ and we can decompose ϕ into ϕ_1, ϕ_2 A-weak morphisms from $\mathcal{G}(v_1)$ and $\mathcal{G}(v_2)$ to $\mathcal{G}(u_1)$ and $\mathcal{G}(u_2)$.

□



Preorder on weak terms

Completeness lemma

$A \vdash_{sp} u \leq v$ if and only if there exists an A-weak morphism from $\mathcal{G}(v)$ to $\mathcal{G}(u)$.

$\vdash_w \langle u, A\rangle \leq \langle v, B\rangle$ means that

1. $B \subseteq A$
2. and:
   - either $u = 1$ and $\mathit{var}(v) \subseteq A$
   - or $u, v \neq 1$ and $A \vdash_{sp} u \leq v$.

Lemma

$\vdash_w \langle u, A\rangle \leq \langle v, B\rangle$ if and only if $\mathcal{G}\langle u, A\rangle \blacktriangleleft \mathcal{G}\langle v, B\rangle$.

Preorder on terms

$$e, f \in \mathbb{T}_\Sigma ::= 1 \mid a \mid e \cdot f \mid e \cap f$$

$\vdash_t e = f$

$\langle \cdot, 1 \rangle$ is monoid; $\cap$ is associative, commutative and idempotent.

$$\begin{array}{lrcl}
\vdash_t & e \cap f \cdot g \cap h & = & (e \cap f \cdot g \cap h) \cap e \cdot f \\
\vdash_t & 1 \cap (e \cdot f) & = & 1 \cap (e \cap f) \\
\vdash_t & (1 \cap e) \cdot f & = & f \cdot (1 \cap e) \\
\vdash_t & ((1 \cap e) \cdot f) \cap g & = & (1 \cap e) \cdot (f \cap g)
\end{array}$$

Lemma

$$\vdash_t e = f \Leftrightarrow \vdash_w \tau(e) = \tau(f)$$

Summing up

Theorem

$$\vdash_t e = f \Leftrightarrow \vdash_w \tau(e) = \tau(f)$$

Summing up

Theorem

$$\begin{aligned} \vdash_t e = f &\Leftrightarrow \vdash_w \tau(e) = \tau(f) \\ &\Leftrightarrow \mathcal{G}(\tau(e)) \mathrel{\substack{\blacktriangleleft \\ \blacktriangleright}} \mathcal{G}(\tau(f)) \end{aligned}$$

Summing up

Theorem

$$
\begin{aligned}
\vdash_t e = f &\Leftrightarrow \vdash_w \tau(e) = \tau(f) \\
&\Leftrightarrow \mathcal{G}(\tau(e)) \blacktriangleleft\!\!\blacktriangleright \mathcal{G}(\tau(f)) \\
&\Leftrightarrow \mathrm{Lang} \models e = f
\end{aligned}
$$

Outline

Outline

Mirror image

$$e, f \in \mathbb{T}_{\Sigma}^{\smile} ::= 1 \mid a \mid e \cdot f \mid e \cap f \mid e^{\smile}$$

$$\eta : \mathbb{T}_{\Sigma}^{\smile} \to \mathbb{T}_{\Sigma \cup \Sigma'}$$

Mirror image

$$e, f \in \mathbb{T}_{\Sigma}^{\smile} ::= 1 \mid a \mid e \cdot f \mid e \cap f \mid e^{\smile}$$

$$\eta : \mathbb{T}_{\Sigma}^{\smile} \to \mathbb{T}_{\Sigma \cup \Sigma'}$$

Consider the term $(1 \cap a \cap b)^{\smile} \cdot \left(b^{\smile} \cdot c\right)^{\smile}$.

Mirror image

$$e, f \in \mathbb{T}_{\Sigma}^{\smile} ::= 1 \mid a \mid e \cdot f \mid e \cap f \mid e^{\smile}$$

$$\eta : \mathbb{T}_{\Sigma}^{\smile} \to \mathbb{T}_{\Sigma \cup \Sigma'}$$

Consider the term $(1 \cap a \cap b)^{\smile} \cdot \left(b^{\smile} \cdot c\right)^{\smile}$.

1. move $\_^{\smile}$ to variables:

$$\left(1 \cap a^{\smile} \cap b^{\smile}\right) \cdot c^{\smile} \cdot b.$$

Mirror image

$$e, f \in \mathbb{T}^{\smile}_{\Sigma} ::= 1 \mid a \mid e \cdot f \mid e \cap f \mid e^{\smile}$$

$$\eta : \mathbb{T}^{\smile}_{\Sigma} \to \mathbb{T}_{\Sigma \cup \Sigma'}$$

Consider the term $(1 \cap a \cap b)^{\smile} \cdot (b^{\smile} \cdot c)^{\smile}$.

1. move $\_^{\smile}$ to variables:

$$(1 \cap a^{\smile} \cap b^{\smile}) \cdot c^{\smile} \cdot b.$$

2. double the variables under $1 \cap \_$:

$$(1 \cap a^{\smile} \cap a \cap b^{\smile} \cap b) \cdot c^{\smile} \cdot b.$$

Mirror image

$$e, f \in \mathbb{T}_{\Sigma}^{\smile} ::= 1 \mid a \mid e \cdot f \mid e \cap f \mid e^{\smile}$$

$$\eta : \mathbb{T}_{\Sigma}^{\smile} \to \mathbb{T}_{\Sigma \cup \Sigma'}$$

Consider the term $(1 \cap a \cap b)^{\smile} \cdot (b^{\smile} \cdot c)^{\smile}$.

1. move $\_^{\smile}$ to variables:

$$\left(1 \cap a^{\smile} \cap b^{\smile}\right) \cdot c^{\smile} \cdot b.$$

2. double the variables under $1 \cap \_$:

$$\left(1 \cap a^{\smile} \cap a \cap b^{\smile} \cap b\right) \cdot c^{\smile} \cdot b.$$

3. change the alphabet to $\Sigma \cup \Sigma'$:

$$(1 \cap a' \cap a \cap b' \cap b) \cdot c' \cdot b.$$

Mirror image

$$\vdash_c (a \cdot b)^{\smile} = b^{\smile} \cdot a^{\smile} \qquad \vdash_c (a \cap b)^{\smile} = a^{\smile} \cap b^{\smile} \qquad \vdash_c a^{\smile\smile} = a$$

$$\vdash_c 1^{\smile} = 1 \qquad \vdash_c 1 \cap a^{\smile} = 1 \cap a$$

Lemma

$$\vdash_c e = f \Leftrightarrow \vdash_t \eta(e) = \eta(f).$$

Lemma

$$\mathrm{Lang} \models e = f \Leftrightarrow \mathrm{Lang} \models \eta(e) = \eta(f).$$

Outline

Outline

Adding addition

$$e, f \in \mathrm{IMReg}^{-}\langle\Sigma\rangle ::= 1 \mid a \mid e \cdot f \mid e \cap f \mid e^{\smile} \mid e + f \mid 0.$$

Term language

$$\mathcal{L}(a) = \{a\} \qquad \mathcal{L}(1) = \{1\} \qquad \mathcal{L}(0) = \emptyset \qquad \mathcal{L}(e^{\smile}) = \left\{u^{\smile} \mid u \in \mathcal{L}(e)\right\}$$

$$\mathcal{L}(e + f) = \mathcal{L}(e) \cup \mathcal{L}(f) \qquad \mathcal{L}(e \cdot f) = \{u \cdot v \mid u \in \mathcal{L}(e)\ v \in \mathcal{L}(f)\}$$

$$\mathcal{L}(e \cap f) = \{u \cap v \mid u \in \mathcal{L}(e)\ v \in \mathcal{L}(f)\}$$

$$\vdash_a e + (f + g) = (e + f) + g \qquad \vdash_a e + f = f + e \qquad \vdash_a e + e = e$$

$$\vdash_a e + 0 = e \qquad \vdash_a e \cdot 0 = 0 \qquad \vdash_a 0 \cdot e = 0 \qquad \vdash_a e \cap 0 = 0$$

$$\vdash_a (e + f)^{\smile} = e^{\smile} + f^{\smile} \qquad \vdash_a 0^{\smile} = 0$$

Adding addition - axiomatisation

Lemma

$$\vdash_a e = \sum_{u \in \mathcal{L}(e)} u$$

Lemma

$$\vdash_a e \leq f \Rightarrow \forall u \in \mathcal{L}(e), \exists v \in \mathcal{L}(f) : \vdash_c u \leq v$$

Graph language

$$\mathcal{G}(e) = \{\mathcal{G} \circ \tau \circ \eta(u) \mid u \in \mathcal{L}(e)\}.$$

$$^{\blacktriangleleft}\mathcal{G}(e) = \{G \mid \exists H \in \mathcal{G}(e) : G \blacktriangleleft H\}$$

Theorem

$$\vdash_a e = f \Leftrightarrow {}^{\blacktriangleleft}\mathcal{G}(e) = {}^{\blacktriangleleft}\mathcal{G}(f)$$

Adding addition - completeness

$$\forall \sigma,\ \widehat{\sigma}\,(e) = \bigcup_{u \in \mathcal{L}(e)} \widehat{\sigma}\,(u)\,.$$

Theorem

$$\mathrm{Lang} \models e = f \Leftrightarrow {}^{\blacktriangleleft}\mathcal{G}\,(e) = {}^{\blacktriangleleft}\mathcal{G}\,(f)$$

Theorem

$$\vdash_a e = f \Leftrightarrow \mathrm{Lang} \models e = f$$

around 9000 lines of Coq...

And now, for my next trick...

$$e, f \in \mathrm{IMReg}\langle\Sigma\rangle ::= 1 \mid a \mid e \cdot f \mid e \cap f \mid e^{\smile} \mid e + f \mid 0 \mid e^{\star}.$$

$$\mathcal{L}(e^{\star}) = \{u_1 \cdots u_n \mid n \in \mathbb{N} \text{ and } u_i \in \mathcal{L}(e)\}.$$

Theorem

$$\mathrm{Lang} \models e = f \Leftrightarrow {}^{\blacktriangleleft}\mathcal{G}(e) = {}^{\blacktriangleleft}\mathcal{G}(f)$$

And now, for my next trick...

$$e, f \in \mathrm{IMReg}\langle\Sigma\rangle ::= 1 \mid a \mid e \cdot f \mid e \cap f \mid e^{\smile} \mid e + f \mid 0 \mid e^{\star}.$$

$$\mathcal{L}(e^{\star}) = \{u_1 \cdots u_n \mid n \in \mathbb{N} \text{ and } u_i \in \mathcal{L}(e)\}.$$

Theorem

$$\mathrm{Lang} \models e = f \Leftrightarrow {}^{\blacktriangleleft}\mathcal{G}(e) = {}^{\blacktriangleleft}\mathcal{G}(f)$$

Paul Brunet, **Reversible Kleene lattices**, *<hal-01474911v2>* .
Language equivalence is EXPSPACE-complete.

That's all folks!

Thank you!

See more at:
`http://paul.brunet-zamansky.fr`

Outline

I. Introduction

II. Monoidal meet semilattice

III. Mirror image

IV. Sum and star