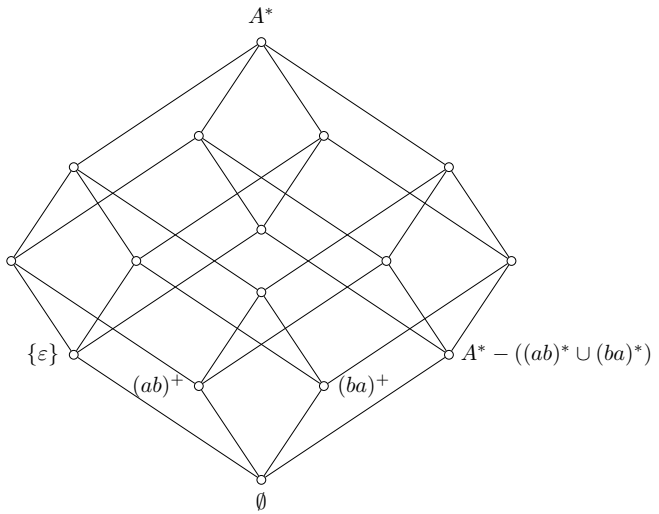
Duality in Logic

Lecture 2

Mai Gehrke

Université Paris 7 and CNRS

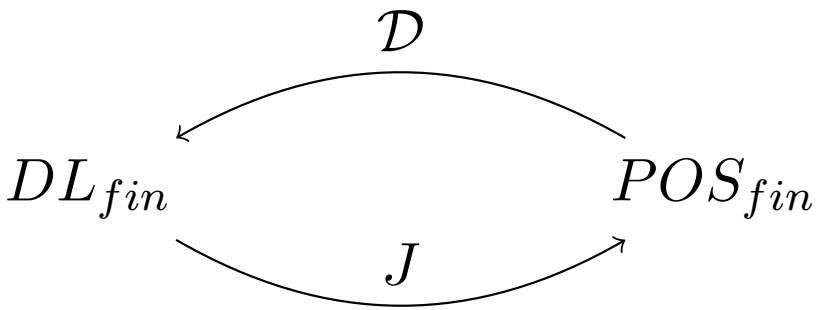


Further examples - revisited

1. Completeness of modal logic with respect to Kripke semantics was obtained via duality in the form of canonical extensions by Jónsson and Tarski in 1951. Ten years before Kripke!
2. Henkin's proof of completeness for FOL relies on building a model from an ultrafilter then adding witnesses for existential formulas. It was shown by Rasiowa and Sikorski in 1950 that this second step can be eliminated by applying Baire category theorem to the dual space of the Lindenbaum algebra.
3. In the late 1960's, Dana Scott built the first model of the lambda-calculus using an inverse limit of finite spaces (which then is a Stone space). In his 1994 paper on domains in logical form Abramsky later gave a general way of solving domain equations based on Stone duality

Duality for operators

Restrict to DL_{fin}



An operator is an operation that preserves finite joins (0 and $\vee$) in each coordinate

$$\text{operator} \quad \Diamond : D^n \to D \quad \rightsquigarrow \quad R \subseteq X \times X^n \quad \text{relation}$$

$$\Diamond \quad \mapsto \quad R_\Diamond = \{(x, \overline{x}) \mid x \leqslant \Diamond(\overline{x})\}$$

$$\left(\Diamond_R : \overline{S} \mapsto R^{-1}[S_1 \times \ldots S_n]\right) \quad \leftarrow\!\shortmid \quad R$$

Duality for operators

$$\text{operator} \quad \Diamond : D^n \to D \quad \rightsquigarrow \quad R \subseteq X \times X^n \quad \text{relation}$$

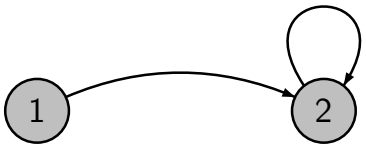
$$\Diamond \quad \mapsto \quad R_\Diamond = \{(x, \overline{x}) \mid x \leqslant \Diamond(\overline{x})\}$$

$$\left(\Diamond_R : \overline{S} \mapsto R^{-1}[S_1 \times \ldots S_n]\right) \quad \hookleftarrow \quad R$$

Some observations:

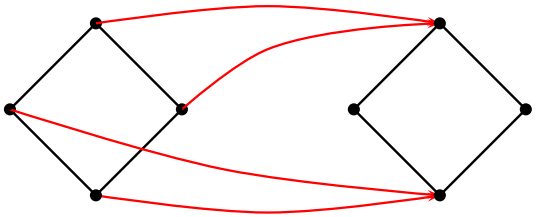
- The dual relations are those satisfying $\leqslant \circ R \circ (\leqslant)^n = R$
- R is a relational 'lower adjoint' of the corresponding operator
- xR has a minimum for each x iff $\Diamond$ is meet preserving iff $\Diamond$ is a homomorphism

Duality for operators



function

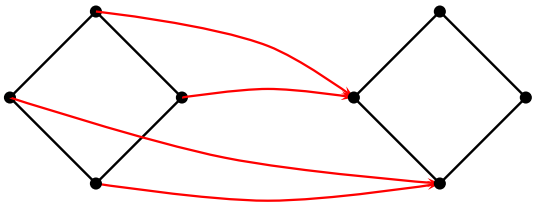
$\rightsquigarrow$



homomorphism

partial function

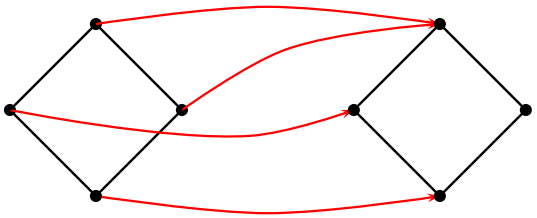
$\rightsquigarrow$



not 1-preserving

general relation

$\rightsquigarrow$



not $\wedge$-preserving

Duality for dual operators

What do we do for a $\Box$ that preserves finite meets (1 and $\wedge$) in each coordinate?

$$\text{dual operator} \quad \Box : D^n \to D \quad \rightsquigarrow \quad S \subseteq M \times M^n \quad \text{relation}$$

$$\Box \quad \mapsto \quad S_\Box = \{(m, \overline{m}) \mid m \geqslant \Box(\overline{m})\}$$

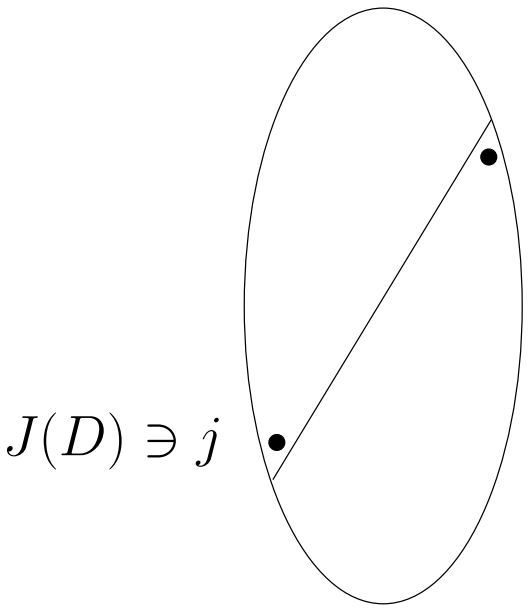
$$\left(\Box_S : \overline{u} \mapsto \bigwedge S^{-1}[{\uparrow}\overline{u} \cap M^n]\right) \quad \leftarrow\!\shortmid \quad S$$

where $M = M(D)$ and we use the duality with respect to meet-irreducibles instead of duality with respect to join-irreducibles

A neutral dual space

The posets $J(D)$ and $M(D)$ of join- and meet-irreducibles of a finite DL are order isomorphic

$$J(D) \longrightarrow M(D)$$
$$j \mapsto \bigvee \{a \in D \mid j \not\leqslant a\}$$



Choose for the dual space a set X with maps

$j : X \to J(D), x \mapsto j_x$ a bijection

$m : X \to M(D), x \mapsto m_x$ a bijection

and $\forall x \in X \ \forall a \in D \ \ (j_x \leqslant a \iff a \not\leqslant m_x)$

Duality for residuated families

Consider a binary residuated family on a finite D

$$\forall a, b, c \in D \qquad (a \cdot b \leqslant c \iff b \leqslant a \backslash c \iff a \leqslant c / b)$$

then we have, for $x, y, z \in X$

$$\begin{aligned} R.(x,y,z) &\iff j_x \leqslant j_y \cdot j_z \\ &\iff j_y \cdot j_z \not\leqslant m_x \\ &\iff j_z \not\leqslant j_y \backslash m_x \\ &\iff j_y \backslash m_x \leqslant m_z \\ &\iff S_{\backslash}(z,y,x) \end{aligned}$$

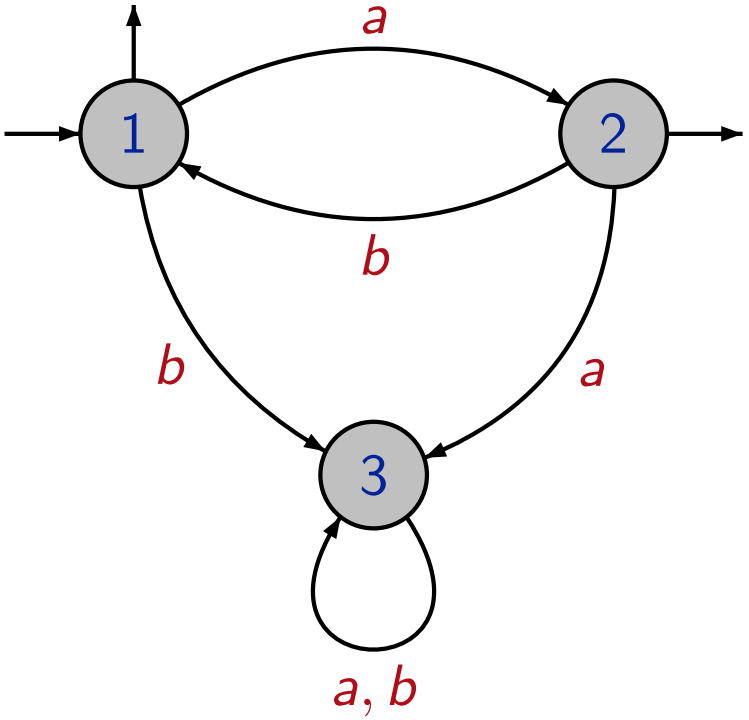
All three operations are given by one ternary relation

Duality for operations on DLs

This goes through in some form to the general setting:

- The correspondence between prime filters and ideals allows us to encode both meet and join pres/rev-ersing operations on the dual space
- If the operation is n-ary then the relation is $(n+1)$-ary and order compatible with certain topological properties
- If f is join preserving in each coordinate, then the relation is morally its lower adjoint; If f is meet preserving, then the relation is morally its upper adjoint.
- Families of operations related by residuation are all encoded by one and the same relation on the dual

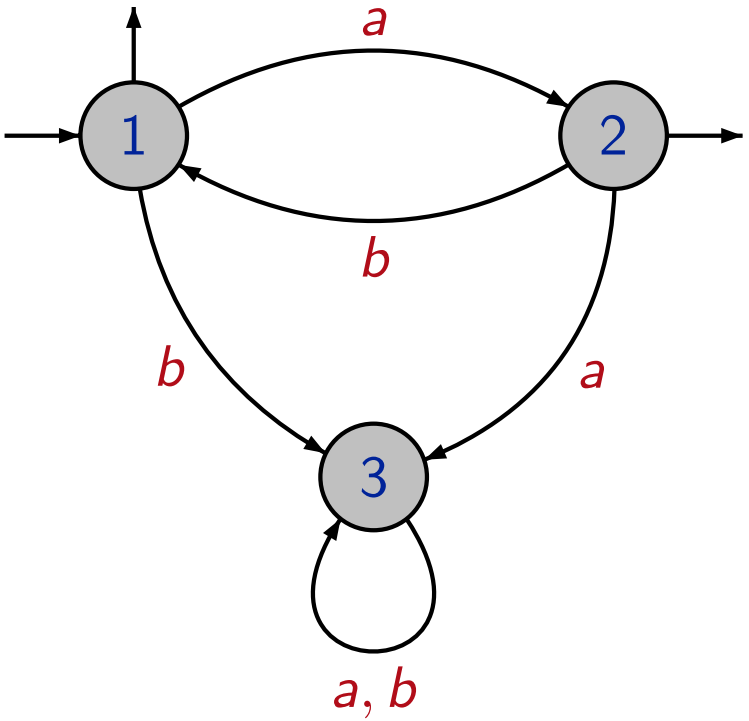
A finite automaton



The states are $\{1, 2, 3\}$.
The initial state is 1, the final states are 1 and 2.
The alphabet is $A = \{a, b\}$ The transitions are

$$1 \cdot a = 2 \qquad 2 \cdot a = 3 \qquad 3 \cdot a = 3$$
$$1 \cdot b = 3 \qquad 2 \cdot b = 1 \qquad 3 \cdot b = 3$$

Recognition by automata



Transitions extend to words: $1 \cdot aba = 2$, $1 \cdot abb = 3$.
The language recognized by the automaton is the set of words u such that $1 \cdot u$ is a final state. Here:

$$L(\mathcal{A}) = (ab)^* \cup (ab)^* a$$

where $*$ means arbitrary iteration of the product.

Rational and recognizable languages

A language is recognizable provided it is recognized by some finite automaton.

A language is rational provided it belongs to the smallest class of languages containing the finite languages which is closed under union, product and star.

Theorem: [Kleene '54] A language is rational iff it is recognizable.

Example: $L(\mathcal{A}) = (ab)^* \cup (ab)^* a$.

Corollary: The rational languages are closed under all the Boolean operations.

Logic on words

To each non-empty word u is associated a structure

$$\mathcal{M}_u = (\{1, 2, \ldots, |u|\}, <, (\mathbf{a})_{a \in A})$$

where $\mathbf{a}$ is interpreted as the set of integers i such that the i-th letter of u is an a, and $<$ as the usual order on integers.

Example:

Let $u = abbaab$ then

$$\mathcal{M}_u = (\{1, 2, 3, 4, 5, 6\}, <, (\mathbf{a}, \mathbf{b}))$$

where $\mathbf{a} = \{1, 4, 5\}$ and $\mathbf{b} = \{2, 3, 6\}$.

Some examples

The formula $\phi = \exists x\ \mathbf{a}x$ interprets as:

> *There exists a position x in u such that the letter in position x is an a.*

This defines the language $L(\phi) = A^*aA^*$.

The formula $\exists x\ \exists y\ (x < y) \wedge \mathbf{a}x \wedge \mathbf{b}y$ defines the language $A^*aA^*bA^*$.

The formula $\exists x\ \forall y\ [(x < y) \vee (x = y)] \wedge \mathbf{a}x$ defines the language aA^*.

Defining the set of words of even length

Macros:

$$(x < y) \vee (x = y) \quad \text{means } x \leqslant y$$
$$\forall y\ x \leqslant y \quad \text{means } x = 1$$
$$\forall y\ y \leqslant x \quad \text{means } x = |u|$$
$$x < y\ \wedge\ \forall z\ (x < z \to y \leqslant z) \quad \text{means } y = x + 1$$

Let $\phi\ =\ \exists X\ (1 \notin X\ \wedge\ |u| \in X\ \wedge\ \forall x\ (x \in X \leftrightarrow x + 1 \notin X))$

Then $1 \notin X$, $2 \in X$, $3 \notin X$, $4 \in X$, $\ldots$, $|u| \in X$. Thus

$$L(\phi) = \{u \mid |u| \text{ is even}\} = (A^2)^*$$

Monadic second order

Only second order quantifiers over unary predicates are allowed.

Theorem: (Büchi '60, Elgot '61)

Monadic second order captures exactly the recognizable languages.

Theorem: (McNaughton-Papert '71)

First order captures star-free languages

(star-free = the ones that can be obtained from the alphabet using the Boolean operations on languages and lifted concatenation product only).

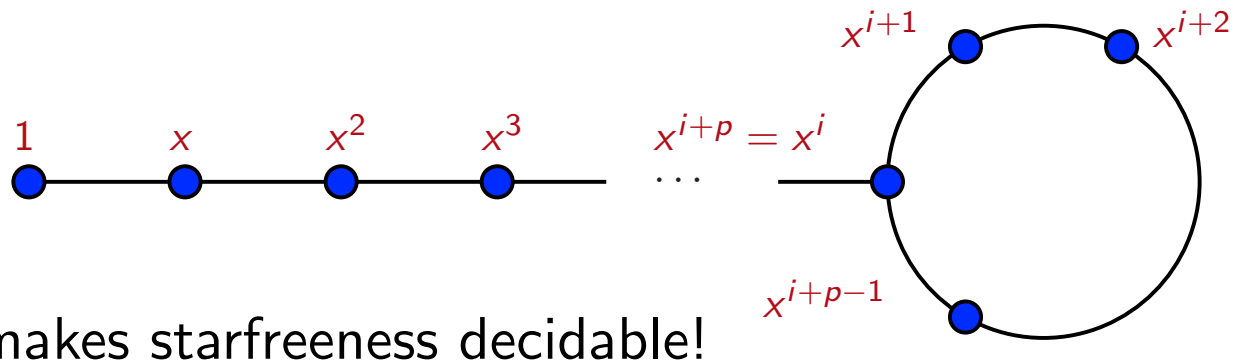
How does one decide the complexity of a given language???

Algebraic theory of automata

Theorem: [Myhill '53, Rabin-Scott '59] There is an effective way of associating with each finite automaton, $\mathcal{A}$, a finite monoid, $(M_{\mathcal{A}}, \cdot, 1)$.

Theorem: [Schützenberger '65] Starfree languages correspond to monoids M such that there exists $n > 0$ with $x^n = x^{n+1}$ for each $x \in M$.

Submonoid generated by x:



This makes starfreeness decidable!

Pseudo-varieties

The class of finite aperiodic monoids is closed under homomorphic images, subalgebras, and finite products. Such classes are called pseudo-varieties.

Eilenberg's Theorem identifies which (indexed) classes of regular languages correspond to pseudo-varieties of monoids.

Reiterman's Theorem tells us these are given by equations in pseudoterms.

The pseudo-equational specification of aperiodicity is $x^\omega \approx x^{\omega+1}$ where x^ω is a pseudoterm that evaluates to the unique idempotent in the submonoid generated by x.

Encompassing more general classes

Several generalizations of Eilenberg's and Reiterman's theorems have been obtained:

- Pin (1995) + Pin-Weil (1996)
- Pippenger (1997)
- Polák (2001)
- Esik (2002), Straubing (2002) + Kunc (2003)

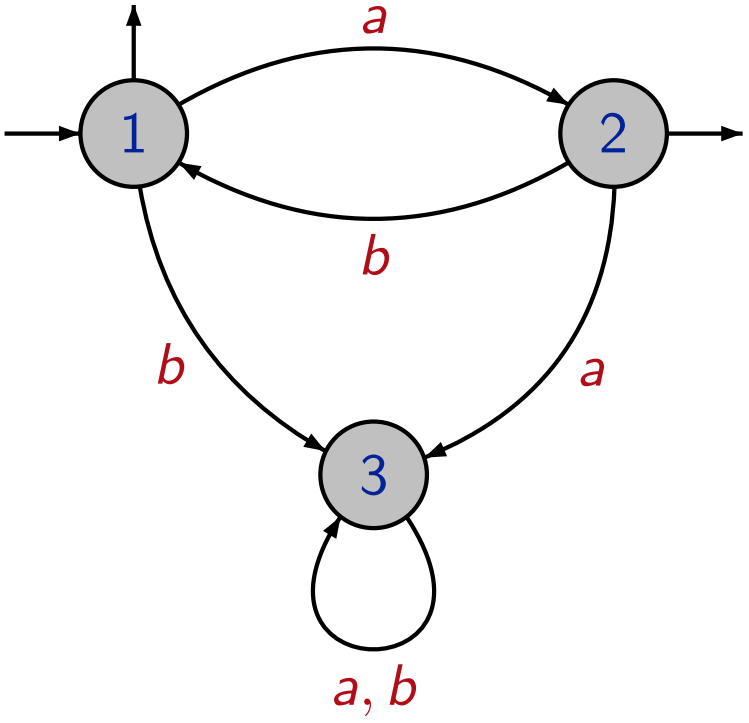
No one of these results provides a common and most general framework for these kinds of results

NOT a modular collection of results

Duality and recognizable languages

Duality applied in the setting of recognizable languages

Quotient operations



$$L(\mathcal{A}) = (ab)^* \cup (ab)^* a$$

$$a^{-1}L = \{u \in A^* \mid au \in L\} = (ba)^* b \cup (ba)^*$$

$$La^{-1} = \{u \in A^* \mid ua \in L\} = (ab)^*$$

$$b^{-1}L = \{u \in A^* \mid bu \in L\} = \emptyset$$

NB! These are recognized by the same underlying machine.

Capturing the underlying machine

Given a recognizable language L the underlying machine is captured by the Boolean algebra $\mathcal{B}(L)$ of languages generated by

$$\{ x^{-1}Ly^{-1} \mid x, y \in A^* \}$$

NB! This generating set is finite since all the languages are recognized by the same machine with varying sets of initial and final states.

NB! $\mathcal{B}(L)$ is closed under quotients since the quotient operations commute will all the Boolean operations.

The residuation ideal generated by a language

Since $\mathcal{B}(L)$ is finite it is also closed under residuation with respect to arbitrary denominators.

For any $K \in \mathcal{B}(L)$ and any $S \in A^*$

$$S\backslash K = \bigcap_{u \in S} u^{-1}K \in \mathcal{B}(L)$$

$$K/S = \bigcap_{u \in S} Ku^{-1} \in \mathcal{B}(L)$$

Theorem: [GGP2008] For a recognizable language L, the dual space of the algebra $(\mathcal{B}(L), \cap, \cup, (\ \ )^c, 0, 1, \backslash, /)$ is the syntactic monoid of L.

– *including the product operation!*

Recognition by monoids

A language $L \subseteq A^*$ is recognized by a finite monoid M provided there is a monoid morphism $\varphi : A^* \to M$ with $\varphi^{-1}(\varphi(L)) = L$.

L recognizable by a finite automaton

$\Longrightarrow$ $\mathcal{B}(L) \hookrightarrow \mathcal{P}(A^*)$ finite residuation ideal

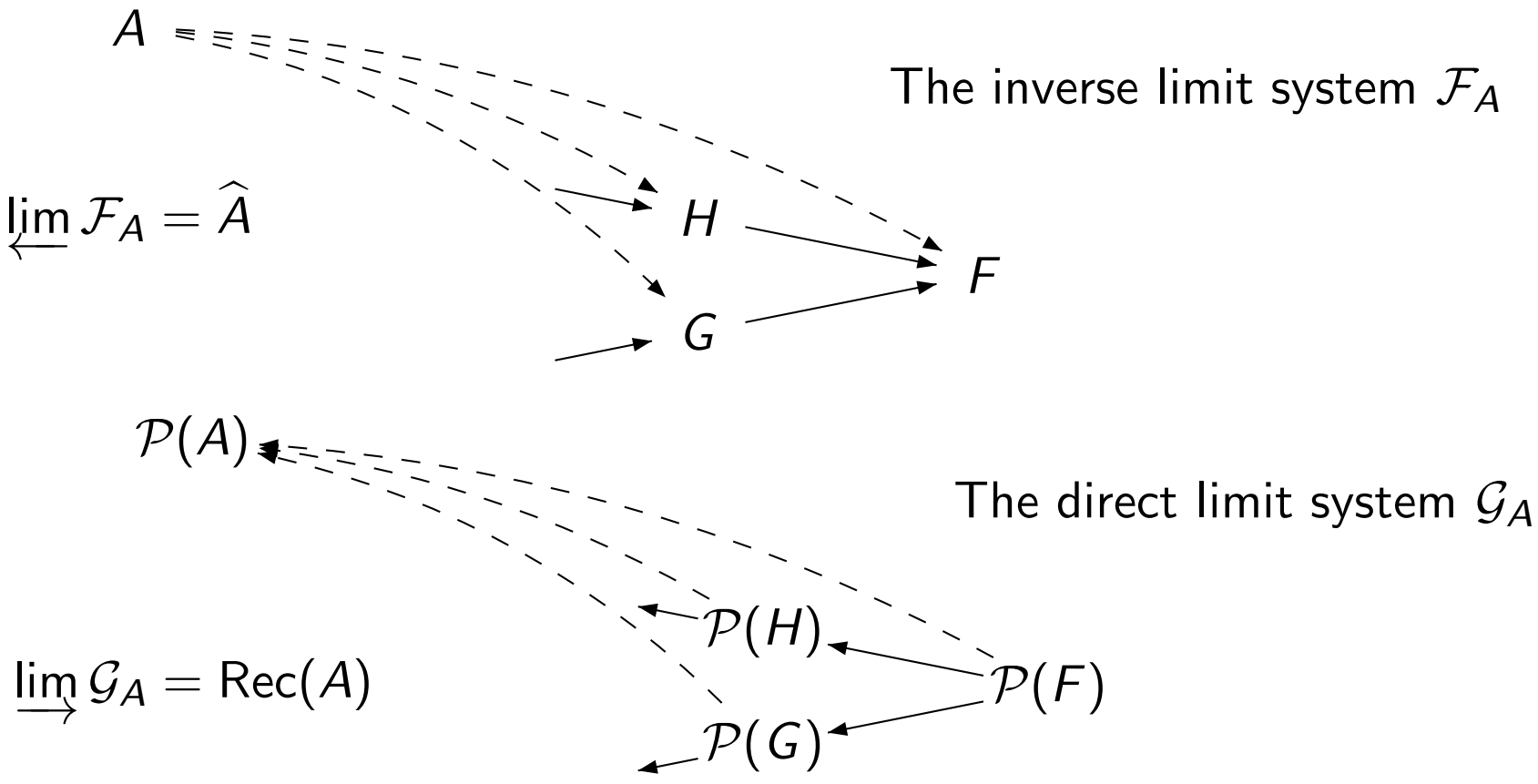
$\Longrightarrow$ $A^* \twoheadrightarrow M(L)$ finite monoid quotient

$\Longrightarrow$ L is recognizable by a finite monoid

$\Longrightarrow$ L recognizable by a finite automaton

The recognizable subsets of an abstract algebra

$$\mathrm{Rec(A)} = \{\varphi^{-1}(\mathrm{S}) \mid \varphi : \mathrm{A} \to \mathrm{F} \text{ hom, } \mathrm{F} \text{ finite, } \mathrm{S} \subseteq \mathrm{F}\}$$



The dual of $(\mathrm{Rec}(\mathrm{A}), /, \backslash)$

Theorem: [GGP2008] The dual space of

$$\mathrm{Rec}(\mathrm{A}) + \text{residuals of liftings of operations}$$

is the profinite completion $\widehat{A}$ with its operations.

In particular, the duals of the residual operations are FUNCTIONAL and CONTINUOUS.
In binary case:

$$R_{(\backslash,/)} = \cdot : \widehat{A} \times \widehat{A} \to \widehat{A}$$

Reiterman's pseudoterms

Duality yields a 1-1 correspondence between continuous monoid morphisms

$$\widehat{\varphi} : \widehat{A^*} \to F, \quad F \text{ a finite monoid}$$

and maps

$$\varphi : A \to F, \quad F \text{ a finite monoid.}$$

Theorem: [GGP2008]
The dual space $(\widehat{A^*}, \tau, \cdot)$ of the residuated Boolean algebra $(\mathrm{Rec}(\mathrm{A}^*), \cdot, /, \backslash)$ is Reiterman's space of pseudoterms over A .

Categorical dualities

subalgebras	$\longleftrightarrow$	quotient structures
quotient algebras	$\longleftrightarrow$	(generated) substructures
products	$\longleftrightarrow$	sums
sums	$\longleftrightarrow$	products

Classes of languages

$\mathcal{C}$ a class of recognizable languages closed under $\cap$ and $\cup$

$$\mathcal{C} \quad \hookrightarrow \quad Rec(A^*) \quad \hookrightarrow \quad \mathcal{P}(A^*)$$

DUALLY

$$X_{\mathcal{C}} \quad \twoheadleftarrow \quad \widehat{A^*} \quad \twoheadleftarrow \quad \beta(A^*)$$

That is, $\mathcal{C}$ is described dually by EQUATING elements of $\widehat{A^*}$.

This is Reiterman's theorem in a very general form.

The mechanism behind Reiterman's theorem

Let A be an abstract algebra.

$\mathcal{B}$ a Boolean subalgebra (sublattice) of $\mathrm{Rec(A)}$
corresponds to
$E \subseteq \widehat{A} \times \widehat{A}$ (in)equations of elements of the profinite completion of A

This correspondence is given by the following Galois connection:

$$\mathcal{P}(\mathrm{Rec(A)}) \leftrightarrows \mathcal{P}(\widehat{\mathrm{A}} \times \widehat{\mathrm{A}})$$

$$S \mapsto \approx_S = \{(x, y) \in X \mid \forall b \in S \quad (b \in y \iff b \in x)\}$$

and

$$E \mapsto B_E = \{b \in B \mid \forall (x, y) \in E \quad (b \in y \iff b \in x)\}$$

A fully modular Eilenberg-Reiterman theorem

Using the fact that sublattices of $\mathrm{Rec}(\mathrm{A}^*)$ correspond to Stone quotients of $\widehat{A^*}$ we get a vast generalization of the Eilenberg-Reiterman theory for recognizable languages

Closed under	**Equations**	**Definition**
$\cup, \cap$	$u \to v$	$\hat{\varphi}(v) \in \varphi(L) \Rightarrow \hat{\varphi}(u) \in \varphi(L)$
quotienting	$u \leqslant v$	for all $x, y,\ \ xuy \to xvy$
complement	$u \leftrightarrow v$	$u \to v$ and $v \to u$
quotienting and complement	$u = v$	for all $x, y,\ \ xuy \leftrightarrow xvy$
Closed under inverses of morphisms		**Interpretation of variables**
all morphisms		words
non-erasing morphisms		nonempty words
length multiplying morphisms		words of equal length
length preserving morphisms		letters

An example

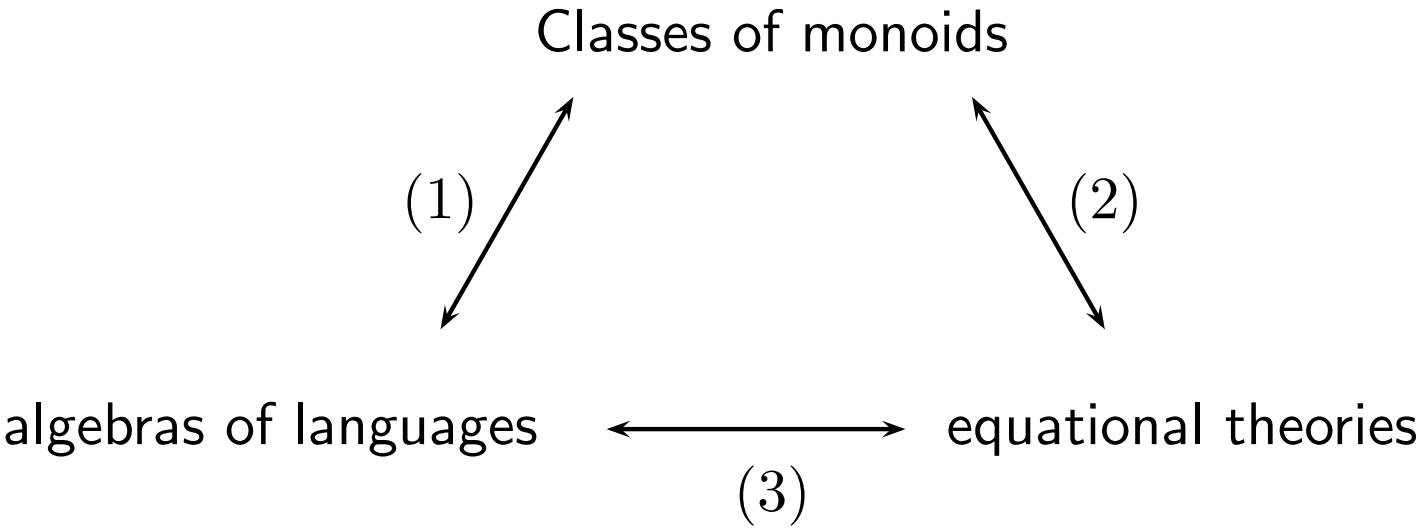
$\mathcal{C}$ = class of languages generated by finite $\cap, \cup$ from the factor languages $\langle u \rangle = A^* u A^*$, $u \in A^*$

These are called positively strongly locally testable (PSLT) languages reflecting the property of their recognizing automata.

Algebraic identities for PSLT: (making the class decidable!)

$$\begin{aligned} x^\omega y x^\omega &= x^\omega y x^\omega y x^\omega \\ x^\omega y x^\omega z x^\omega &= x^\omega z x^\omega y x^\omega \\ x^\omega y x^\omega &\leqslant x^\omega \\ x^\omega u y^\omega v x^\omega &\leftrightarrow y^\omega v x^\omega u y^\omega \\ y(xy)^\omega &\leftrightarrow (xy)^\omega \leftrightarrow (xy)^\omega x \end{aligned}$$

Eilenberg, Reiterman, and Stone

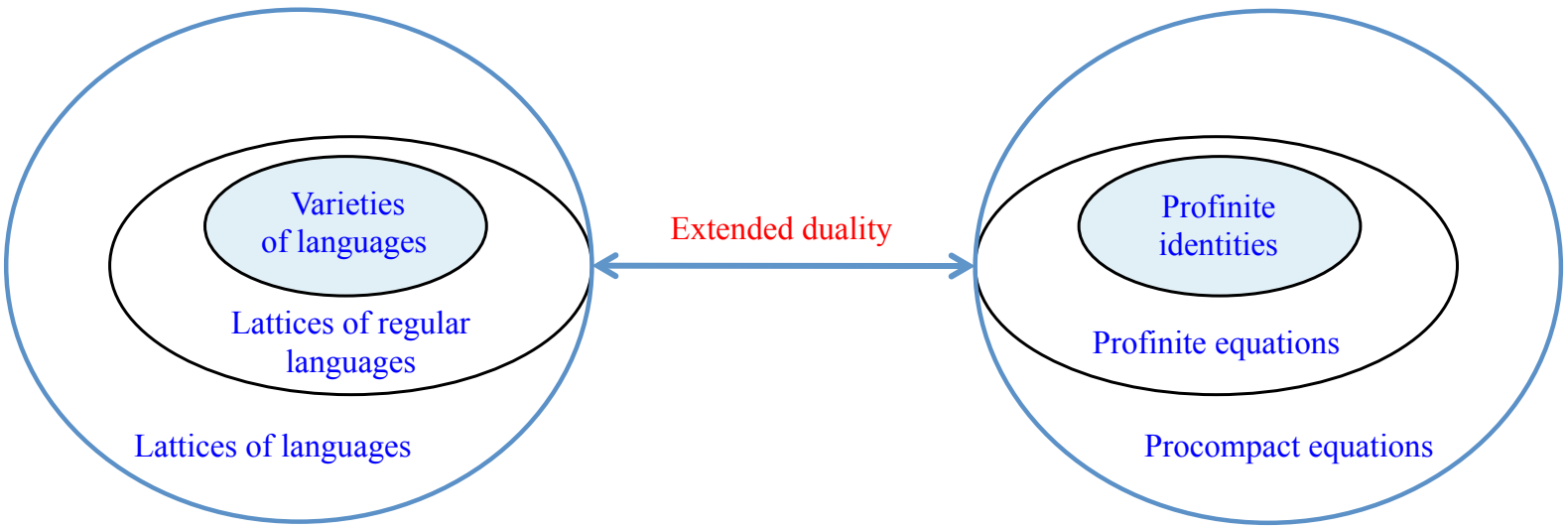


(1) Eilenberg theorems
(2) Reiterman theorems
(3) extended Stone/Priestley duality

(3) allows generalization beyond pseudo-varieties and regular languages

Equational theory of lattices of languages

[G, Grigorieff, and Pin 2008 and 2010]



The (two outer) theorems are proved using the duality between subalgebras (possibly with additional operations) and dual quotient spaces

A few References

- M. Gehrke, Duality and Recognition, Murlak and Sankowski (Eds.): *MFCS 2011*, *LNCS* **6907** (2011), 3–18.
- M. Gehrke, S. Grigorieff, J.-. Pin, A topological approach to recognition, *ICALP 2010, Part II, LNCS* **6199**, Springer Verlag, (2010), 151–162.
- M. Gehrke, Stone Duality and the Recognisable Languages over an Algebra, in Kurz et al. (Eds.): *CALCO 2009*, *LNCS* **5728** (2009), 236–250.
- M. Gehrke, S. Grigorieff, J.-. Pin, Duality and equational theory of regular languages, *ICALP 2008, Part II, LNCS* **5126**, Springer Verlag, (2008), 246–257.
- Jean-Eric Pin, Logic, semigroups and automata on words. http://www.liafa.jussieu.fr/ jep/PDF/SurveyLogic.pdf