Clones and Galois connections

Reinhard Pöschel

Institut für Algebra
Technische Universität Dresden

AAA75, Darmstadt 2007
on a "special occasion"
concerning the founder of the AAA series
November 2, 2007

Outline

Problem 1

Can one express exponentiation

$$f(x,y) := x^y$$

as composition of addition and multiplication

$$g_+(x,y) := x + y, \quad g_\cdot(x,y) := x \cdot y$$

?

$(x, y \in \mathbb{N}_+)$

Problem 2

Can one represent *every* Boolean function

$$f : \{0,1\}^n \to \{0,1\}$$

as composition of the function

$$t(x,y,z) := \textit{if } x = y \textit{ then } z \textit{ else } x$$

(where substituting constants is allowed)

?

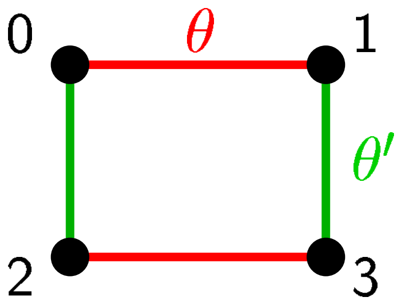
Problem 3

Let

$$A := \{0, 1, 2, 3\}$$

$$G := \{e, g\} := \{(0), (03)(12)\} \leq S_4 \text{ (permutation group)}$$

$$L := \{\theta_0, \theta, \theta', \theta_1\} \text{ (lattice of equivalence relations on } A)$$



θ_0, θ_1 trivial equivalence relations

Does there exists an algebra

$$\mathcal{A} = \langle A, F \rangle$$

such that

$$G = \operatorname{Aut} \mathcal{A} \text{ (automorphism group)}$$

$$L = \operatorname{Con} \mathcal{A} \text{ (congruence lattice)}$$

?

TECHNISCHE UNIVERSITÄT DRESDEN

Problem 4

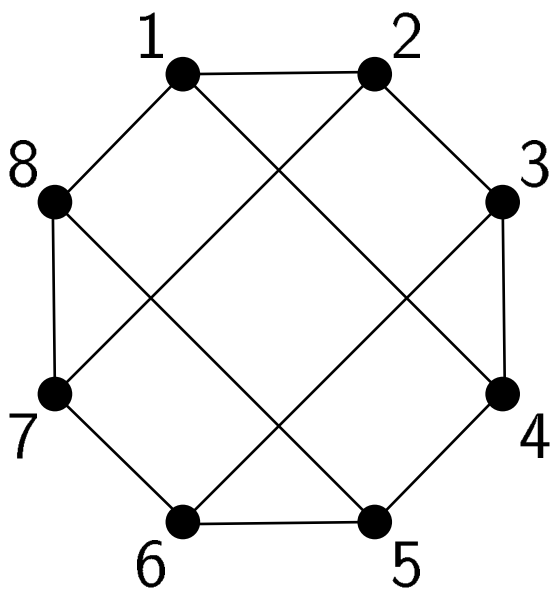
How to recognize whether

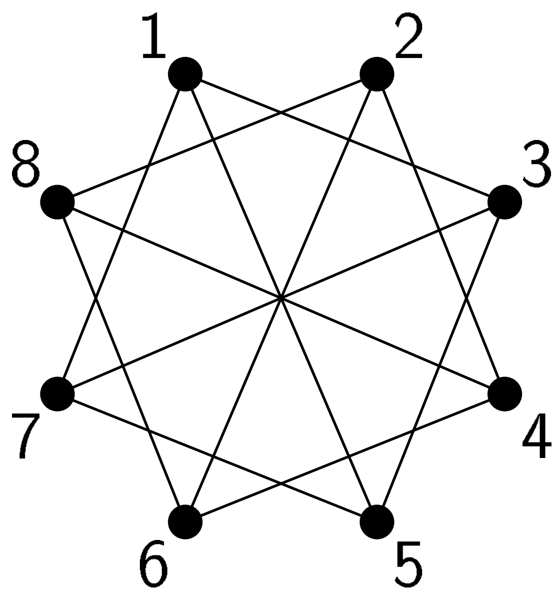
$$\operatorname{Aut}\Gamma_1 \subseteq \operatorname{Aut}\Gamma_2 \qquad (*)$$

for graphs $\Gamma_1 = (V, E_1)$, $\Gamma_2 = (V, E_2)$?

e.g.

$\Gamma_1 =$





$= \Gamma_2$

How to construct all graphs $\Gamma_2 = (V, E_2)$ satisfying $(*)$?

Problem 5

What can be said about the computational complexity of

Constraint Satisfaction Problems (CSP)

Γ set of (finitary) relations on a domain D.

General (algebraic) definition of CSP:

CSP(Γ) := set of problems of the form

Does there exist a relational homomorphism
$$(V, \Sigma) \to (D, \Sigma')$$
(between relational systems of the same type) where $\Sigma' \subseteq \Gamma$?

Special CSP:
GRAPH COLORABILITY, *GRAPH ISOMORPHISM*, *SATISFIABILITY (SAT)*

Galois connections

The *Galois connection induced by a binary relation*

$$R \subseteq G \times M$$

is given by the pair of mappings

$$\varphi : \mathfrak{P}(G) \to \mathfrak{P}(M) : X \mapsto X' := \{m \in M \mid \forall g \in X : gRm\}$$
$$\psi : \mathfrak{P}(M) \to \mathfrak{P}(G) : Y \mapsto Y' := \{g \in G \mid \forall m \in Y : gRm\}$$

A Galois connection (φ, ψ) is characterizable by the property

$$Y \subseteq \varphi(X) \iff \psi(Y) \supseteq X$$

for all $X \subseteq G$, $Y \subseteq M$.

Formal concept analysis

In Formal Concept Analysis (*Rudolf Wille* ($\sim$ 1970)),

$$(G, M, R)$$

is called *formal context*.
($g \in G$ *objects* (Gegenstände), $m \in M$ *attributes* (Merkmale))
FCA book

Concepts (X, Y) (defined by the property $Y = X'$ and $X = Y'$)
have two components (*Galois closures*) : *extent* X and *intent* Y
(dyadic view)
(each component completely determines the other)
e.g. dyadic view to sets:

$G := \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ (given "universe")

$A := \{1, 3, 5, 7, 9\}$ (definition by extent)

$A := \{n \in G \mid n \text{ is odd}\}$ (definition by properties (intent))

The "most basic Galois connection" in algebra

ALGEBRAS, LATTICES, VARIETIES VOLUME I

(1987)

Ralph N. McKenzie
University of California, Berkeley
George F. McNulty
University of South Carolina
Walter F. Taylor
University of Colorado

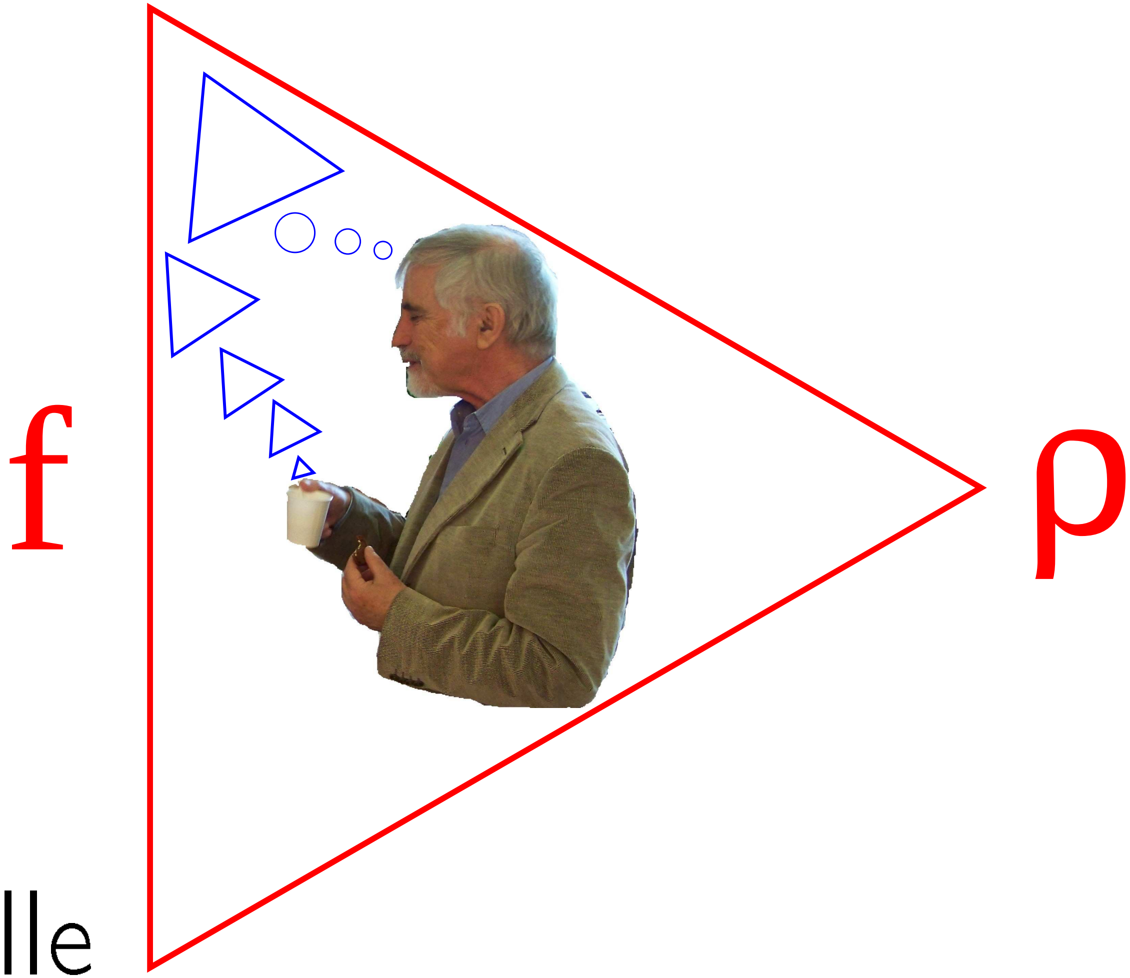
The most basic Galois connection in algebra is the one associated to the binary relation* of preservation between operations and relations. (Nearly all of the most basic concepts in algebra can be defined in terms of this relation.)

Observe that the automorphisms, endomorphisms, subuniverses, and congruences of an algebra are defined by restricting the preservation relation to special types of relations. The congruences of an algebra, for example, are the equivalence relations that are preserved by the basic operations of the algebra.

4.1 Algebras and Clones p. 147

Notation

Notation f preserves ϱ:



THE Galois connection Pol − Inv

induced by the relation $\boxed{\text{function } f \text{ preserves relation } \varrho}$: $\boxed{f \triangleright \varrho}$

$$\begin{array}{lcccccc}
f(& a_{11} & a_{12} & \dots & a_{1n} &) = & \bullet \\
f(& a_{21} & a_{22} & \dots & a_{2n} &) = & \bullet \\
 & & & & & & \\
f(& a_{m1} & a_{m2} & \dots & a_{mn} &) = & \bullet \\
 & \in \varrho & \in \varrho & \dots & \in \varrho & \Rightarrow & \in \varrho
\end{array}$$

$F \subseteq \mathrm{Op}(A)$ (set of all finitary operations $f : A^n \to A$) ("objects")

$Q \subseteq \mathrm{Rel}(A)$ (set of all finitary relations $\varrho \subseteq A^m$) ("attributes")

$\mathrm{Inv}\, F := \{\varrho \in R_A \mid \forall f \in F : f \triangleright \varrho\}$ invariant relations

$\mathrm{Pol}\, Q := \{f \in \mathrm{Op}(A) \mid \forall \varrho \in Q : f \triangleright \varrho\}$ polymorphisms

Subalgebras, Congruences, Auto-(Homo-)morphisms

Special examples for preservation property $\triangleright$:

- Subalgebras ($\varrho \subseteq A^m$):
  $\varrho \leq \langle A, F\rangle^m \iff F \triangleright \varrho$
- Congruences ($\theta \in \mathrm{Eq}(A)$ equivalence relation):
  $\theta \in \mathrm{Con}\langle A, F\rangle \iff F \triangleright \theta$
- Automorphisms ($\alpha \in S_A$ permutation):
  $\alpha \in \mathrm{Aut}\langle A, F\rangle \iff F \triangleright \alpha^\bullet \quad (\alpha^\bullet := \{(x, \alpha(x)) \mid x \in A\})$
- Homomorphisms ($h : A^n \to A$, $\mathbf{A} := \langle A, F\rangle$):
  $h \in \mathrm{Hom}(\mathbf{A}^n, \mathbf{A}) \iff F \triangleright h^\bullet \iff h \triangleright F^\bullet$

Main Theorem

Theorem (Characterization of Galois closed elements (concepts))

$\mathcal{A} = \langle A, F \rangle$ *finite algebra.*

- $\mathrm{Clo}(\mathcal{A}) = \langle F \rangle = \mathrm{Pol}\,\mathrm{Inv}\,F$ *(clone generated by F)* [1],
- $m\text{-}\mathrm{Loc}\,F = \mathrm{Pol}\,\mathrm{Inv}^{(m)}\,F$ *(m-locally closed clones, clones with m-interpolation property)*,
- $[Q] = \mathrm{Inv}\,\mathrm{Pol}\,Q$ *(relational clone generated by Q).*

$\mathcal{A} = \langle A, F \rangle$ *(arbitrary) algebra*

- $\mathrm{Loc}\,\mathrm{Clo}(\mathcal{A}) = \mathrm{Loc}\langle F \rangle = \mathrm{Pol}\,\mathrm{Inv}\,F$ *(locally closed clone generated by F)*

[1] *Lev Arkadevic Kalužnin, Лев Аркадевич Калужнин*

Definition of a clone (of operations)

A set F of finitary functions $f : A^n \to A$ (on a base set A) is called *clone*[2], if

- F contains all *projections* $(e_i^n(x_1, \dots, x_n) = x_i)$
- F is *closed under composition*[3] i.e., if $f, g_1, \dots, g_n \in F$ (f n-ary, g_i m-ary), then
$$f[g_1, \dots, g_n] \in F\ .$$

$f[g_1, \dots, g_n](x_1, \dots, x_m) := f(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m))$ clone books

For arbitrary F, $\langle F\rangle$ or $\langle F\rangle_{\mathrm{Op}(A)}$ (*clone generated by F*) is the least clone containing F.

Axiomatizing composition $\longrightarrow$ notion of *abstract clone*
T. Evans, W. Taylor, …($\sim$ 1979),
$\exists$ Cayley-like representation for abstract clones C by concrete clones: e.g.
A. Sangalli (1988): $C \cong \mathrm{Pol}\, M^{\bullet}$ for some $M \leq A^A$.

---

[2] *P.M. Cohn* (1965) attributes the notion to *Ph. Hall*
[3] *K. Menger* (1961) composition = operation par exellence

Answer to Problem 1

Can one express exponentiation

$$f(x,y) := x^y$$

as composition of addition and multiplication

$$g_+(x,y) := x+y, \quad g_\cdot(x,y) := x\cdot y$$

?

$(x, y \in \mathbb{N}_+)$

Problem: $f \in \langle g_+, g_\cdot \rangle$?
Answer: No.
Proof: Idea: Find $\varrho \in \mathrm{Rel}(A)$
such that $g_+ \rhd \varrho$, $g_\cdot \rhd \varrho$
but not $f \rhd \varrho$,
because this would contradict
to $f \in \langle g_+, g_\cdot \rangle$
$\subseteq_{Thm} \mathrm{Pol}\,\mathrm{Inv}\{g_+, g_\cdot\}$,
i.e. $f \rhd \mathrm{Inv}\{g_+, g_\cdot\}$.

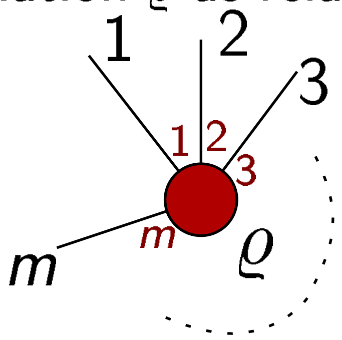
Take $\varrho := \{(x,x') \in \mathbb{N}_+^2 \mid 3 \text{ divides } x - x'\}$
ϱ is invariant for $g_+, g_\cdot$, but not for f:

$$\begin{array}{l} f(2,4) = 2^4 = 16 \\ f(2,1) = 2^1 = 2 \\ \quad\ \in \varrho \qquad\qquad \notin \varrho \end{array}$$

Definition of a relational clone

using the language of PAL
(Peircean Algebraic Logic)
C.S.Peirce 1890. . . ,
R.W. Burch 1991,
F. Dau 2000+. . .

m-ary relation ϱ as relation graph:

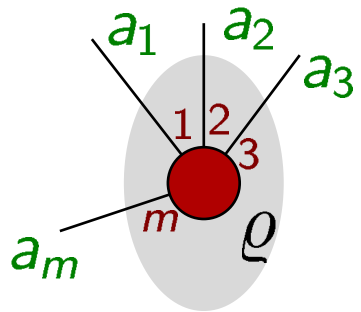


$Q \subseteq R_A$ relational algebra (clone) $:\Longleftrightarrow$ closed w.r.t.:

Definition of a relational clone

using the language of PAL
(Peircean Algebraic Logic)
C.S.Peirce 1890. . . ,
R.W. Burch 1991,
F. Dau 2000+. . .

interpretation $[\![\Gamma]\!]$ of a relation graph Γ
(evaluate edges by elements of A)



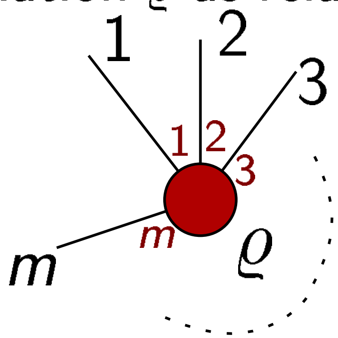
$$[\![\Gamma]\!] := \{(a_1, \ldots, a_n) \mid (a_1, \ldots, a_n) \in \varrho\}$$

$Q \subseteq R_A$ relational algebra (clone) $:\iff$ closed w.r.t.:

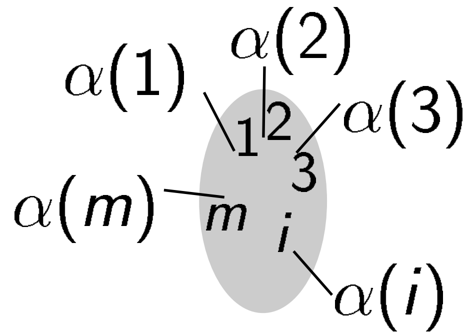
Definition of a relational clone

using the language of PAL
(Peircean Algebraic Logic)
C.S.Peirce 1890. . . ,
R.W. Burch 1991,
F. Dau 2000+. . .

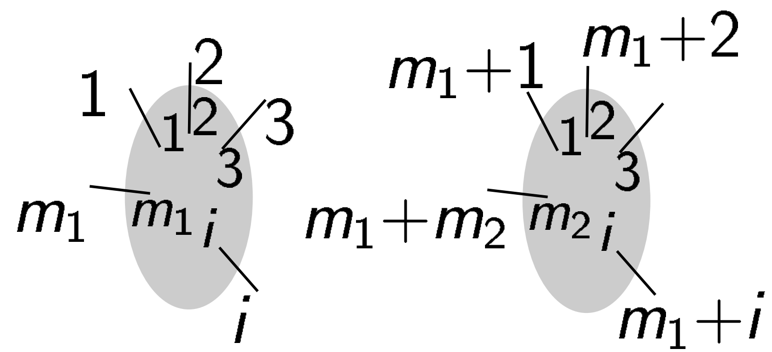
m-ary relation ϱ as relation graph:



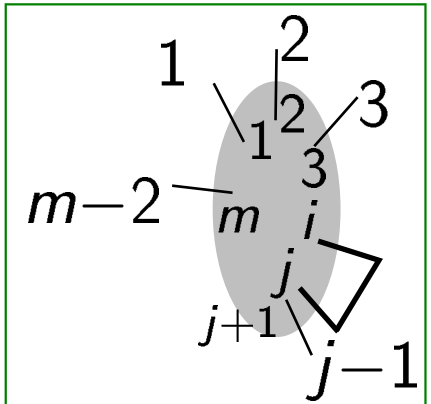
$Q \subseteq R_A$ relational algebra (clone) $:\iff$ closed w.r.t.:



permuting coordinates

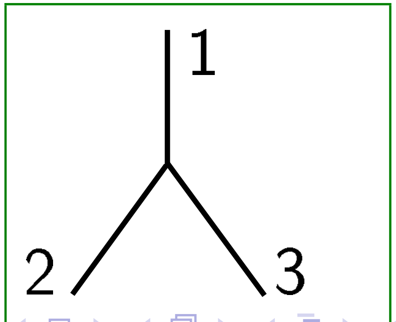


direct product



connecting with deletion

Q contains the teridentity $\mathrm{id}_3 := \{(x,x,x) \mid x \in A\}$



logical operations and relational algebras (clones)

other characterization of relational clones and Galois closures

$\varphi(x_1, \dots, x_m)$ first order formula containing quantifyers and connectives from Φ only (with relation symbols $\varrho_1, \dots, \varrho_n$ and free variables $x_1, \dots, x_m$).

Logical operation $\in \mathrm{Lop}_A(\Phi)$ on $\mathrm{Rel}(A)$:

$L_\varphi(\varrho_1, \dots, \varrho_n) := \{(a_1, \dots, a_m) \mid \models \varphi(a_1, \dots, a_m)\}$

Q *relational algebra* $\iff$ Q closed w.r.t. $\mathrm{Lop}_A(\exists, \wedge, =)\}$

Galois connection Inv – Pol

Theorem: $[Q]_{\mathrm{RA}} = \mathrm{Inv}\,\mathrm{Pol}\, Q$

Q *weak Krasner algebra* $\iff$ Q closed w.r.t. $\mathrm{Lop}_A(\exists, \wedge, \vee, =)\}$

Galois connection Inv – End

Theorem: $[Q]_{\mathrm{WKA}} = \mathrm{Inv}\,\mathrm{End}\, Q$

Q *Krasner algebra* $\iff$ Q closed w.r.t. $\mathrm{Lop}_A(\exists, \wedge, \vee, \neg, =)\}$

Galois connection Inv – Aut

Theorem: $[Q]_{\mathrm{KA}} = \mathrm{Inv}\,\mathrm{Aut}\, Q$

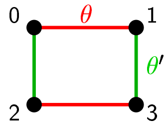
Answer to Problem 3

Answer to the problems

Problem 3

Let

$$A := \{0,1,2,3\}$$
$$G := \{e,g\} := \{(0),(03)(12)\} \le S_4 \text{ (permutation group)}$$
$$L := \{\theta_0, \theta, \theta', \theta_1\} \text{ (lattice of equivalence relations on } A)$$



θ_0, θ_1 trivial equivalence relations

Does there exists an algebra

$$\mathcal{A} = \langle A, F\rangle$$

such that

$$G = \operatorname{Aut}\mathcal{A} \text{ (automorphism group)}$$
$$L = \operatorname{Con}\mathcal{A} \text{ (congruence lattice)}$$

?

Problem:

(*) $\exists F : G = \operatorname{Aut} F,\ L = \operatorname{Con} F$?

Answer: No.

Proof:

(*) $\iff F \rhd Q := \{g^\bullet, \theta, \theta'\}$

w.l.o.g. $F = \operatorname{Pol} Q$. Then

$\operatorname{Inv} F = \operatorname{Inv}\operatorname{Pol} Q =_{Thm.} [Q]_{\mathrm{RA}}$

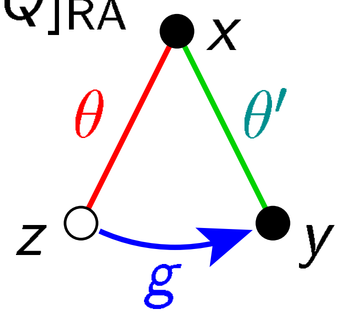
and we have:

$$G^\bullet = (\operatorname{Aut} F)^\bullet = S_A^\bullet \cap \operatorname{Inv} F = S_A^\bullet \cap [Q]_{\mathrm{RA}}$$
$$L = \operatorname{Con} F = \operatorname{Eq}(A) \cap \operatorname{Inv} F = \operatorname{Eq}(A) \cap [Q]_{\mathrm{RA}}$$

in contradiction to $\exists h^\bullet \in S_A^\bullet \cap [Q]_{\mathrm{RA}} : h \notin G$

namely $h^\bullet := L_\varphi(\theta, \theta', g^\bullet)$

$$= \{(x,y) \in A^2 \mid \underbrace{\exists z : x\theta z \wedge z g^\bullet y \wedge x\theta' y}_{\varphi}\}$$



i.e. $h = (02)(13) \notin G$

TECHNISCHE UNIVERSITÄT DRESDEN

Answer to Problem 4

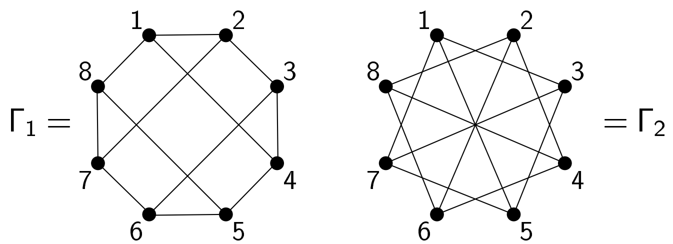
Some problems THE Galois connection Pol – Inv Clones and algebras The lattice of clones Completeness results Ans

Problem 4

How to recognize whether

$$\operatorname{Aut}\Gamma_1 \subseteq \operatorname{Aut}\Gamma_2 \qquad (*)$$

for graphs $\Gamma_1 = (V, E_1)$, $\Gamma_2 = (V, E_2)$?
e.g.



How to construct all graphs $\Gamma_2 = (V, E_2)$ satisfying $(*)$?

Concrete answer for example:
YES!

$E_2 = (E_1 \circ E_1) \setminus \Delta_V$, i.e.

$E_2 = L_\varphi(E_1) = \{(x, y) \mid \underbrace{\exists z : xE_1 z \wedge zE_1 y \wedge \neg(x{=}y)}_{\varphi}\}$

$\Longrightarrow \operatorname{Aut}\Gamma_1 \subseteq \operatorname{Aut}\Gamma_2.$

General answer:

$$\operatorname{Aut}\Gamma_1 = \operatorname{Aut} E_1 \subseteq \operatorname{Aut} E_2 = \operatorname{Aut}\Gamma_2$$

$$\iff \quad \operatorname{Inv}\operatorname{Aut} E_1 \supseteq \operatorname{Inv}\operatorname{Aut} E_2$$

$$\iff \quad [E_1]_{KA} \supseteq [E_2]_{KA} \text{ (by Theorem)}$$

$$\iff \quad \exists \text{ first order formula } \varphi \in \Phi(\exists, \wedge, \vee, \neg, =) : E_2 = L_\varphi(E_1)$$

TECHNISCHE UNIVERSITÄT DRESDEN

Specializing and generalizing the Galois connection *Pol* — *Inv*

$E \subseteq \mathrm{Op}(A)$, $R \subseteq \mathrm{Rel}(A)$ $\longrightarrow$ Galois connection given by context $(E, R, \triangleright)$:

E	R	Galois closure	References
$\mathrm{Op}(A)$	$\mathrm{Rel}(A)$	$\mathrm{Pol}\,\mathrm{Inv}\,F$	[BodKKR69a], [BodKKR69b], [Gei68], [BakP75], [Rom76], [Rom77a], [Rom77b], [PösK79], cf. 2.3, 2.5
		$\mathrm{Inv}\,\mathrm{Pol}\,Q$	[Gei68], [BodKKR69a], [BodKKR69b], [Sza78], [PösK79], [Pös79], [Pös80a], cf. 2.3, 2.5
Generalization to infinitary relations or operations			
		$\mathrm{Pol}\,\mathrm{Inv}^{\infty} F$	[Ros72], [KraP76], [Poi81]
		$\mathrm{Inv}^{\infty}\,\mathrm{Pol}\,Q$	[Ros79]
		$\mathrm{Pol}^{\infty}\,\mathrm{Inv}^{\infty} F$, $\mathrm{Inv}^{\infty}\,\mathrm{Pol}^{\infty} Q$	[Kra76b], [KraP76], [Poi81]
arity restrictions			
$\mathrm{Op}(A)$	$\mathrm{Rel}^{(m)}(A)$	$\mathrm{Pol}\,\mathrm{Inv}^{(m)} F$	[Gei68], [BakP75], [Pös80a]
		$\mathrm{Inv}^{(m)}\,\mathrm{Pol}\,Q$	[Ros78]
$\mathrm{Op}(A)$	$\mathrm{Rel}^{(1)}(A)$	$\mathrm{Pol}\,\mathrm{Sub}\,F$	[Sch82, Thm. 1.6], [Pös80a]
		$\mathrm{Sub}\,\mathrm{Pol}\,Q$	see below
$\mathrm{Op}^{(m)}(A)$	$\mathrm{Rel}(A)$	$\mathrm{Inv}\,\mathrm{Pol}^{(m)} Q$	[Sza78], [Pös80a]
$\mathrm{Tr}(A)$	$\mathrm{Rel}(A)$	$\mathrm{Inv}\,\mathrm{End}\,Q$, $\mathrm{End}\,\mathrm{Inv}\,F$	[Kra38], [Kra50], [Kra76a], [Kra86], [Gou68], [BodKKR69a], [BodKKR69b], [Pös80a], [Bör00]
$\mathrm{Sym}(A)$	$\mathrm{Rel}(A)$	$\mathrm{Inv}\,\mathrm{Aut}\,Q$ ($\mathrm{sInv}\,\mathrm{Aut}\,Q$), $\mathrm{wAut}\,\mathrm{Inv}\,F$, $\mathrm{Aut}\,\mathrm{sInv}\,F$	[Kra38], [BodKKR69a], [BodKKR69b], [Gou72a], [Pös80a], [Bör00]
$\mathrm{Sym}(A)$	$\mathrm{Rel}^{(m)}(A)$	$\mathrm{Aut}\,\mathrm{Inv}^{(m)} F$	[Wie69]
restriction to (graphs of) operations only			
$\mathrm{Op}(A)$	$\mathrm{Op}(A)^{\bullet}$	$\mathrm{Pol}\,\mathrm{Pol}\,F$	[Sza78, Thm. 13], [Faj77], [Dan77](for $\lvert A\rvert = 3$), (also Kuznecov, cf. [Val76])
$\mathrm{Op}(A)$	$\mathrm{Tr}(A)^{\bullet}$	$\mathrm{Pol}\,\mathrm{End}\,F$	[SauS82], ([Rei82] implicit operations)
		$\mathrm{End}\,\mathrm{Pol}\,Q$	see below

instead of $\mathrm{Pol}\,Q$ — $\mathrm{Inv}\,F$

now: $(E \cap \mathrm{Pol}\,Q)$ — $(R \cap \mathrm{Inv}\,F)$

concrete characterization problems

E	R	Galois closure	References
concrete characterization of $\mathrm{Aut}\,\mathcal{A}$			
$\mathrm{Op}(A)$	$\mathrm{Sym}(A)^{\bullet}$	$\mathrm{Aut}\,\mathrm{Pol}\,Q$	[Jón68] (cf. [Jón72, (2.4.3)]), [Kra50], [ArmS64], [Sza75], [Bre76]
concrete characterization of $\mathrm{Aut}\,\mathcal{A}$ *for algebras* $\mathcal{A}$ *with at most m-ary operations*			
$\mathrm{Op}^{(m)}(A)$	$\mathrm{Sym}(A)^{\bullet}$	$\mathrm{Aut}\,\mathrm{Pol}^{(m)} Q$	[Pło68], [Jón72, (2.4.1)], [Gou72a]
concrete characterization of $\mathrm{Sub}\,\mathcal{A}$			
$\mathrm{Op}(A)$	$\mathfrak{P}(A)$	$\mathrm{Sub}\,\mathrm{Pol}\,Q$	[BirF48] (cf. [Jón72, (3.6.4)]), [Gou68], [Gou72b]; for unary algebras: [Jón72, (3.6.7)], [JohS67]
concrete characterization of $\mathrm{Con}\,\mathcal{A}$			
$\mathrm{Op}(A)$	$\mathrm{Eq}(A)$	$\mathrm{Con}\,\mathrm{Pol}\,Q$	[Arm70](partial solution), [Jón72, (4.4.1)], [QuaW71], [Wer74], [Dra74]
		$\mathrm{Pol}\,\mathrm{Con}\,F$	for p-rings $\langle A; F\rangle$ [Isk72]
concrete characterization of $\mathrm{End}\,\mathcal{A}$			
$\mathrm{Op}(A)$	$\mathrm{Tr}(A)^{\bullet}$	$\mathrm{End}\,\mathrm{Pol}\,Q$	[Lam68], [GräL68], [SauS77a], [Sto69], [Sto75], [Jež72], [Sza78, Thm. 15]
concrete characterization of			
$\mathrm{Op}(A)$	$\mathrm{Sym}(A)^{\bullet} \cup \mathfrak{P}(A)$	$\mathrm{Aut}\,\mathcal{A}$ & $\mathrm{Sub}\,\mathcal{A}$	[Sto72], [Gou72b], cf. 3.5
	$\mathrm{Sym}(A)^{\bullet} \cup \mathrm{Eq}(A)$	$\mathrm{Aut}\,\mathcal{A}$ & $\mathrm{Con}\,\mathcal{A}$	[Wer74](conjecture) cf. [Pös80b], (for simple $\mathcal{A}$ [Sch64]), cf. 3.5
	$\mathrm{Op}(A)^{\bullet} \cup \mathrm{Sub}(A)$	$\mathrm{End}\,\mathcal{A}$ & $\mathrm{Sub}\,\mathcal{A}$	[SauS77b](cf. [Jón74])
	$\mathrm{Op}(A)^{\bullet} \cup \mathrm{Sub}(A) \cup \mathrm{Eq}(A)$	$\mathrm{Aut}\,\mathcal{A}$ & $\mathrm{Sub}\,\mathcal{A}$ & $\mathrm{Con}\,\mathcal{A}$	[Sza78], [Pös80a], cf. 3.5

Specializing and generalizing Pol — Inv (continued)

	Closure	Nota-tion	Galois connection	
			closed relational system	closed operational system
for finite base set A:				
(1)	$\mathrm{Lop}_A(\exists,\wedge,\vee,\neg,=)$	$[Q]_{\mathrm{KA}}$	sInv – Aut (cf. 2.3 and Tab. 1)	
			Krasner algebra (cf. 1.5, 1.6)	group of permutations
(2)	$\mathrm{Lop}_A(\exists,\wedge,\vee,=)$	$[Q]_{\mathrm{WKA}}$	Inv – End (cf. 2.3 and Tab. 1)	
			weak Krasner algebra (cf. 1.5, 1.6)	monoid of unary functions
(3)	$\mathrm{Lop}_A(\exists,\wedge,=)$	$[Q]_{\mathrm{RA}}$	Inv – Pol (cf. 2.3 and Tab. 1)	
			relational algebra (cf. 1.5, 1.6)	clone of finitary functions
(3a)	$\mathrm{Lop}_A(\forall,\exists,\wedge,=)$	$[Q]_{\forall\mathrm{RA}}$	Inv – surPol	
			$\forall$-closed relational algebra	"surjective clone"
(4)	$\mathrm{Lop}_A(\wedge,=)$		Inv – pPol	
			weak system with identity	down-closed clone of finitary partial functions
(5)	$\mathrm{Lop}_A(\wedge)$		Inv – mPol	
			weak system of relations	down-closed clone of finitary multi-functions
(6)	$\mathrm{Lop}_A(\exists,\wedge,\vee,\neg)$	$[Q]_{\mathrm{BSP}}$	sInv – sEnd (sbmEnd, resp.)	
			BSP (cf. 4.2)	Special monoid of unary functions (cf. [BörPS, 7.9])
(6')				(down-closed involuted monoid of bitotal multifunctions, resp.)
(7)	$\mathrm{Lop}_A(\wedge,\vee,\neg,=)$	$[Q]_{\mathrm{BSI}}$	sInv – spmEnd	
			BSI (cf. 4.2)	down-closed involuted monoid of pp-multifunctions (partial permutations)
(8)	$\mathrm{Lop}_A(\wedge,\vee,\neg)$	$[Q]_{\mathrm{BS}}$	sInv – smEnd	
			BS (cf. 4.2)	down-closed involuted monoid of unary multifunc-

From point of relational clones there are many further Galois connections

for arbitrary base set A:				
	Closure		Galois connection	
			closed relational system	closed operational system
Table 2, continued from previous page				
(9)	(KC) = (WKC)&($\neg$)&(sS)	$[Q]_{\mathrm{KC}}$	sInv – Aut (cf. 2.5 and Tab. 1)	
			Krasner clone (cf. 2.4)	locally closed group of permutations
(10)	(PKC) = (WKC)&(ν)&(sS)	$[Q]_{\mathrm{PKC}}$	Inv – wAut (cf. 2.5 and Tab. 1)	
			Pre-Krasner clone (cf. 2.4)	locally closed monoid of permutations
(11)	(WKC)&(sS)		Inv – sur-End	
			Inv H for sets H of surjective unary functions	locally closed monoid of surjective unary functions
(12)	(WKC)&($\neg$)		Inv – inb-End	
			Inv H for locally invertible monoids H	locally closed locally invertible monoid of unary functions
(13)	(WKC)&(ν)		Inv – inj-End	
			Inv H for monoids H of injective functions	locally closed monoid of injective unary functions
(14)	(WKC) = (RC)&(1-LOC)	$[Q]_{\mathrm{WKC}}$	Inv – End (cf. 2.5 and Tab. 1)	
			weak Krasner clone (cf. 2.4)	locally closed monoid of unary functions
(15)	(RC) = (S)&(LOC)	$[Q]_{\mathrm{RC}}$	Inv – Pol (cf. 2.5 and Tab. 1)	
			relational clone (cf. 2.4)	locally closed clone of finitary functions

clones of term operations, free algebras, varieties

Main source of clones: Take algebra $\mathbf{A} = \langle A, (f_i)_{i\in I}\rangle$

clone of term operations ($F := \{f_i \mid i \in I\}$)

$$T(\mathbf{A}) := \{t^{\mathbf{A}} \mid t \text{ term for signature } \mathbf{A}\} = \langle F\rangle_{\mathrm{Op}(A)}$$

clone of a variety V: $T(F_V(\aleph_0))$ (clone of free algebra)

Theorem

$V := \mathrm{Var}(\mathbf{A})$. *Free algebra with n generators = algebra of n-ary term operations:*

$$F_V(n) \cong T_n(\mathbf{A}) = \langle e_1^n, \dots, e_n^n\rangle_{\mathbf{A}^{A^n}} \leq \mathbf{A}^{A^n}$$

Remark: $\varrho \in \mathrm{Inv}^{(n)} F \iff \varrho \leq \mathbf{A}^n$ i.e. $\varrho \in \mathrm{Sub}(\mathbf{A}^n)$

$\mathbf{B} \in \mathrm{Var}(\mathbf{A}) \overset{\text{HSP-Thm}}{\iff} \exists \varrho \in \mathrm{Inv}^{(\infty)} F : \mathbf{B}$ is homomorphic image of ϱ

TECHNISCHE UNIVERSITÄT DRESDEN

Dyadic view to (classes of) algebras

Question: Under which conditions algebras of a class $\mathcal{K}$ (e.g. variety) are determined by their n-ary invariant relations?

$\mathbf{A_1} = \langle A, F_1 \rangle$, $\mathbf{A_2} = \langle A, F_2 \rangle \in \mathcal{K}$,
$\mathrm{Inv}^{(n)} F_1 = \mathrm{Inv}^{(n)} F_2 \implies \mathbf{A_1} = \mathbf{A_2}$? or $T(\mathbf{A_1}) = T(\mathbf{A_2})$?

Examples

- $\mathcal{K} :=$ abelian groups:
  $\mathrm{Inv}^{(3)} F_1 = \mathrm{Inv}^{(3)} F_2 \implies \mathbf{A_1} = \mathbf{A_2}$
- $\mathcal{K} :=$ groups with abelian Sylow subgroups:
  $\mathrm{Inv}^{(3)} F_1 = \mathrm{Inv}^{(3)} F_2 \implies T(\mathbf{A_1}) = T(\mathbf{A_2})$
  (*K. Kearnes, A. Szendrei* 2005)
- $\mathcal{K} :=$ entropic algebras (i.e. $F \triangleright F^{\bullet}$) with weak unit:
  $\mathrm{Inv}^{(3)} F_1 = \mathrm{Inv}^{(3)} F_2 \implies T(\mathbf{A_1}) = T(\mathbf{A_2}) = T(\text{monoid})$
  (*D. Mašulović, R. Pöschel* 2007)

Algebras with few subpowers

J. Berman, P. Idziak, P. Marković, R. McKenzie, M. Valeriote, R. Willard, Varieties with few subalgebras of powers. (2006)

$\mathcal{A} = \langle A, F \rangle$ *algebra with few subpowers* $:\iff$
$s_{\mathcal{A}}(n) := \log |\operatorname{Inv}^{(n)} F|$ can be bounded by a polynomial

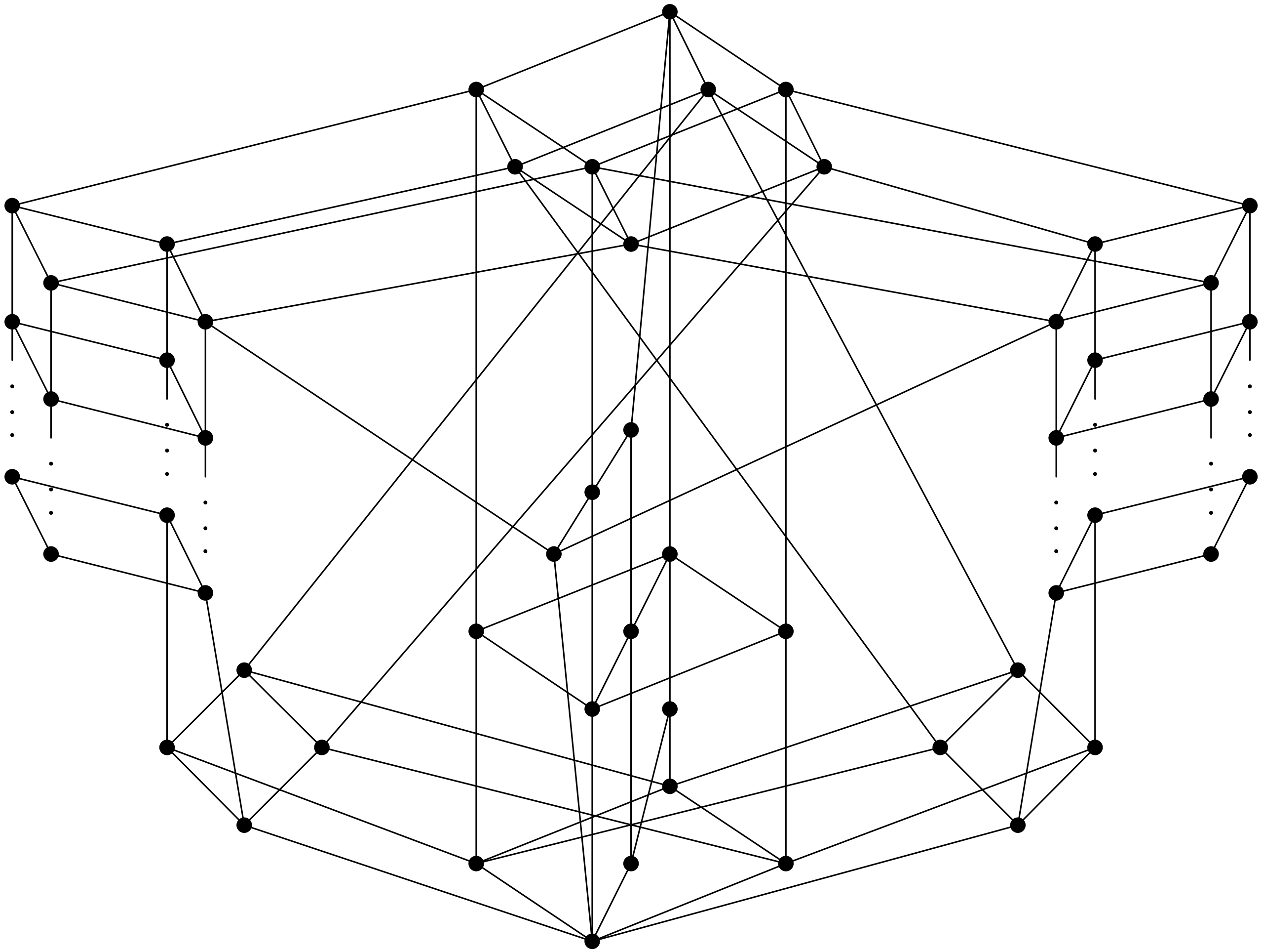
Theorem
A finite algebra $\mathcal{A}$ has few subpowers if and only if for some $k > 0$, $\mathcal{A}$ has a k-edge term (then $s_{\mathcal{A}}$ is bounded by a polynomial of degree k).

close connections to CSP (later)

Outline

The lattice $\mathcal{L}_A$ of clones on A

The lattice $\mathcal{L}_A$ of all clones on base set $A = \{0, 1\}$ is countable (*E.L.Post* 1921/41)



The lattice $\mathcal{L}_A$ of clones on A

$|A| > 2$: The lattice of all clones on base set A is uncountable
$|\mathcal{L}_A| = 2^{\aleph_0}$ for $3 \leq |A| \in \mathbb{N}$, and $|\mathcal{L}_A| = 2^{2^{|A|}}$ for infinite A

The lattice $\mathcal{L}_A$ satisfies no nontrivial lattice identities
(*A. Bulatov* 1992,...)

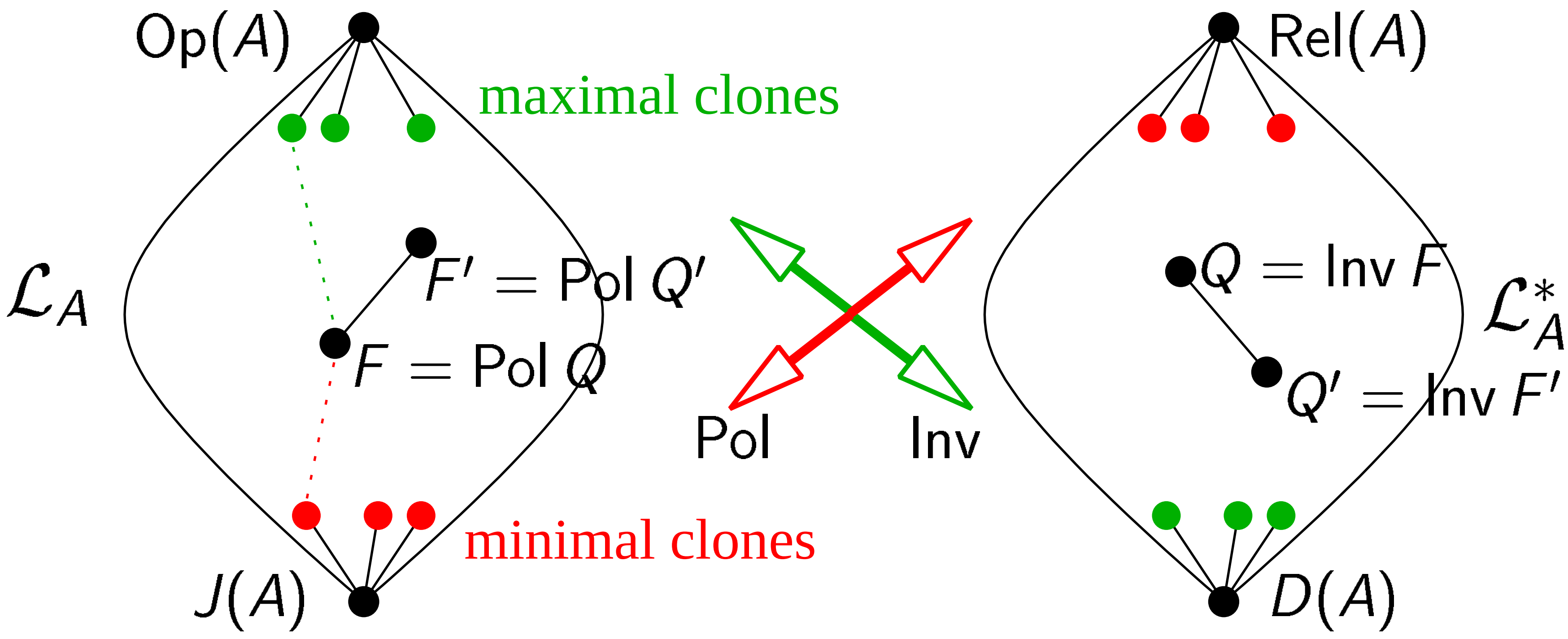
every algebraic lattice (with at most $2^{|A|}$ compact elements) is (isomorphic to) a complete sublattice of $\mathcal{L}_A$ (*M. Pinsker*)

atomic and coatomic for finite A,
but not for infinite A (*M. Goldstern, Shelah* 2002)

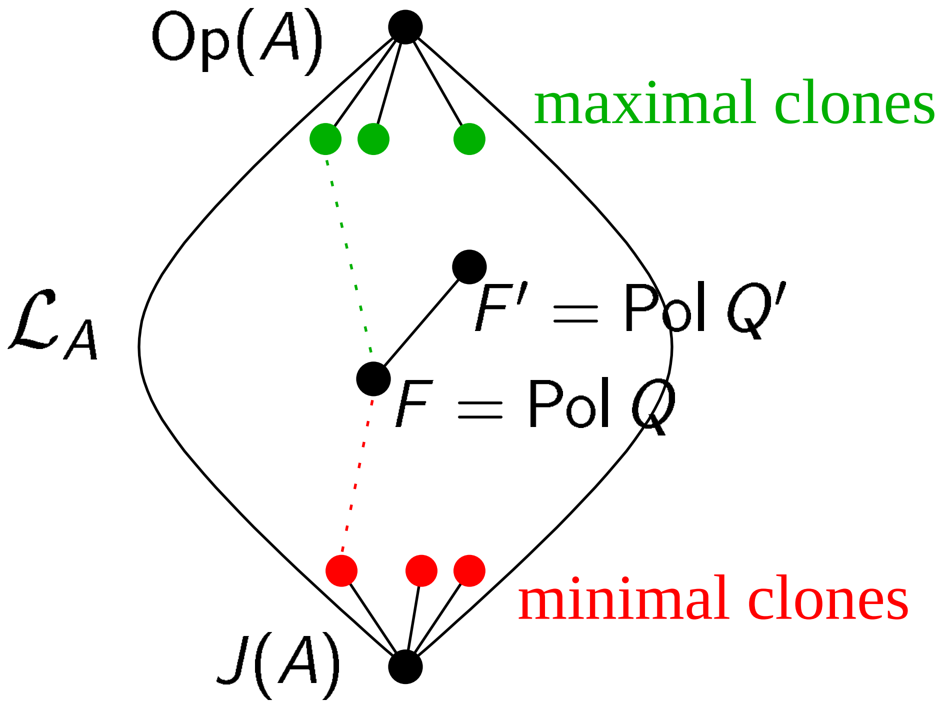
$\mathcal{L}_A$ can be partinioned in *monoidal intervals* (clones with the same unary part)

The lattice $\mathcal{L}_A$ of clones on A

dyadic view



The lattice $\mathcal{L}_A$ of clones on A



Maximal clones:

$|A| = 2$: *E.L. Post*

$|A| = 3$: *S.V. Jablonski* (1958)

$|A| = 4$: *A.I. Mal'cev* (≤ 1969)

$|A| \in \mathbb{N}$: *I.G. Rosenberg* (1970)

(of form $\mathrm{Pol}\, \varrho_i$, $i \in I$)

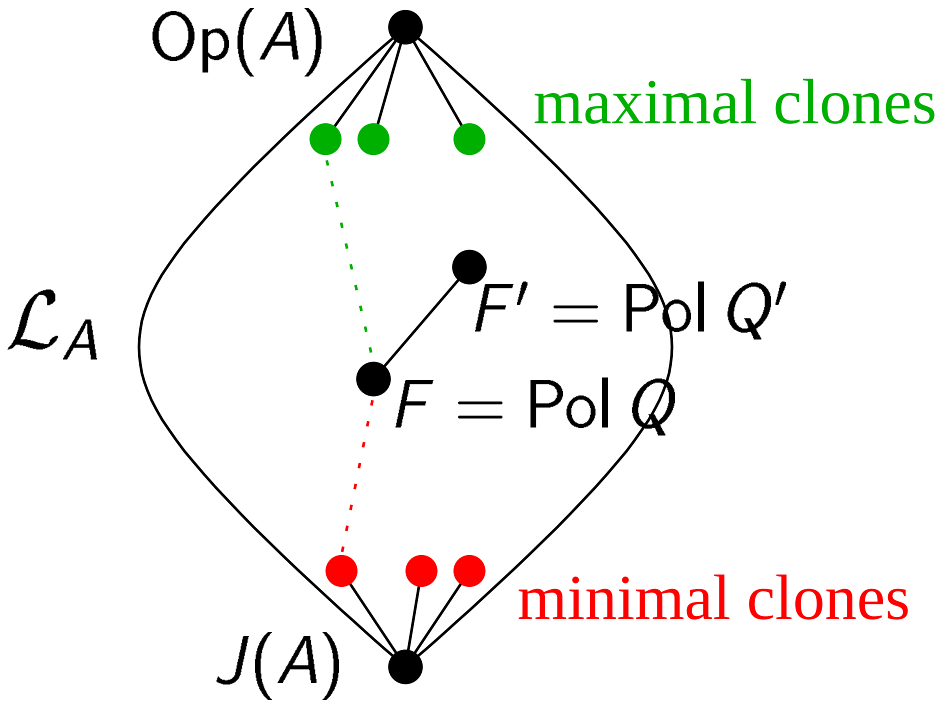
$|A|$ infinite: *I.G. Rosenberg, L. Heindorf, M. Goldstern, M. Pinsker*[a], ...

submaximal clones: *D. Lau*

maximal clones C where $C \cap \mathrm{Sym}(A)$ is maximal permutation group in $\mathrm{Sym}(A)$: *P.P. Pálfy* (2007)

[a] Goldstern/Pinsker, *A survey of clones on infinite sets.* 2007

The lattice $\mathcal{L}_A$ of clones on A



Minimal clones: complete description still open problem
$|A| = 2$: *E.L. Post* (1920/41)
$|A| = 3$: *B. Csákány* (1983)
classification: *I.G. Rosenberg* (1983)
further partial results: *G. Czédli, A. Szendrei, K. Kearnes, P.P. Pálfy, L. Szabo, B. Szszepara, T. Waldhauser,...*
essentially minimal clones: *I.G. Rosenberg, H. Machida, ...*

Completeness and maximal clones

$F \subseteq \mathrm{Op}(A)$ *complete* $:\iff \langle F\rangle_{\mathrm{Op}(A)} = \mathrm{Op}(A)$
(i.e., the algebra $\langle A, F\rangle$ is *primal*, $\implies A$ finite)

Completeness Theorem:

$\boxed{\langle F\rangle = \mathrm{Op}(A)}$ $\iff$ $\boxed{F \text{ is not contained in a maximal clone}}$

$\Updownarrow$ $\Updownarrow$

$\boxed{\mathrm{Inv}\, F = D_A}$ $\boxed{\mathrm{Inv}\, F \text{ does not contain a minimal relational clone}}$

$\iff$ $\boxed{\varrho_i \notin \mathrm{Inv}\, F \text{ for every minimal relational clone } [\varrho_i]_{\mathrm{RA}}\ (i \in I)}$ $\iff$ $\boxed{\forall i \in I \exists f_i \in F : f_i \not\rhd \varrho_i}$

maximal clones are of the form $\mathrm{Pol}\, \varrho_i$ $(i \in I)$
for relations ϱ_i described by *I. Rosenberg*

TECHNISCHE UNIVERSITÄT DRESDEN

Answer to Problem 2

> **Problem 2:** Can one represent *every* Boolean function
> $$f : \{0,1\}^n \to \{0,1\}$$
> as composition of the function
> $t(x,y,z) := \textit{if } x = y \textit{ then } z \textit{ else } x$
> (where substituting constants is allowed)?

$\iff$ $F = \{t, c_0, c_1\}$ complete ?

Answer Yes.

direct proof:

$$x \wedge y = t(x,1,y)$$
$$\neg x = t(0,x,1) \qquad \square$$

Proof using the general completeness criterion:

5 maximal clones in $\mathrm{Op}(\{0,1\})$: $\mathrm{Pol}\,\varrho_i \quad i \in \{0,1,2,3,4\}$

$\varrho_0 := \{0\}, \quad \varrho_1 := \{1\}, \quad \varrho_2 := \{(x,y) \mid x \le y\},$

$\varrho_3 := \{(x,y) \mid x = \neg y\}, \quad \varrho_4 := \{(x,y,z,u) \mid x \oplus y = z \oplus u\}$

$F := \{t, c_0, c_1\} \not\rhd \varrho_i$: $\quad c_1 \not\rhd \varrho_0,\ c_0 \not\rhd \varrho_1,\ c_0 \not\rhd \varrho_3,\ t \not\rhd \varrho_2, \varrho_4$:

$t(0$	0	$1)$	$=$	1
$t(0$	1	$1)$	$=$	0
$\in \varrho_2$	$\in \varrho_2$	$\in \varrho_2$		$\notin \varrho_2$

$t(0$	0	$1)$	$=$	1
$t(0$	1	$0)$	$=$	0
$t(0$	1	$1)$	$=$	0
$t(0$	0	$0)$	$=$	0
$\in \varrho_4$	$\in \varrho_4$	$\in \varrho_4$		$\notin \varrho_4$

Computational complexity of CSP (cf. Problem 5)

Theorem (*P. Jeavons* 1998). $\Gamma_1, \Gamma_2 \subseteq \mathrm{Rel}(A)$ finite.

$\Gamma_1 \subseteq \mathrm{Inv}\,\mathrm{Pol}\,\Gamma_2 \implies$ CSP(Γ_1) can be reduced to CSP(Γ_2) in polynomial time.

Problem 5

What can be said about the computational complexity of

Constraint Satisfaction Problems (CSP)

Γ set of (finitary) relations on a domain D.

General (algebraic) definition of CSP:

$\mathrm{CSP}(\Gamma) :=$ set of problems of the form

Does there exist a relational homomorphism
$(V, \Sigma) \to (D, \Sigma')$
(between relational systems of the same type) where $\Sigma' \subseteq \Gamma$?

Special CSP:
GRAPH COLORABILITY, GRAPH ISOMORPHISM,
SATISFIABILITY (SAT)

in particular

$\mathbf{compl}(\mathrm{CSP}(\Gamma)) = \mathbf{compl}(\mathrm{CSP}([\Gamma]_{\mathrm{RA}}))$

depends only on the clone $\mathrm{Pol}\,\Gamma$.

large $\Gamma \longleftrightarrow$ small $\mathrm{Pol}\,\Gamma$

$\implies$ Problem:

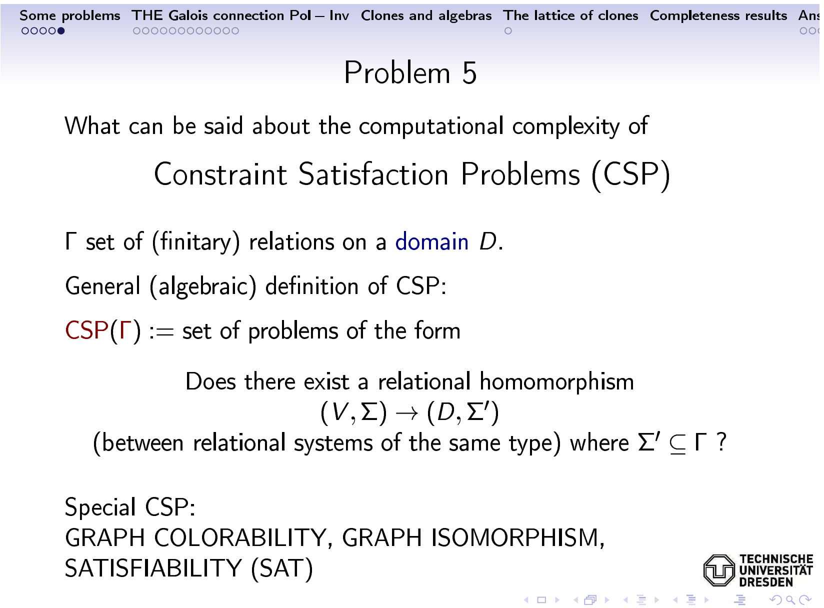
Classify minimal clones F, for which $\mathrm{CSP}(\mathrm{Inv}\,F)$ is tractable?

Jeavons, Bulatov, Krokhin, ...

Computational complexity of CSP (cf. Problem 5)

Theorem (*P. Jeavons* 1998). $\Gamma_1, \Gamma_2 \subseteq \mathrm{Rel}(A)$ finite.

$\Gamma_1 \subseteq \mathrm{Inv}\,\mathrm{Pol}\,\Gamma_2 \implies$ CSP(Γ_1) can be reduced to CSP(Γ_2) in polynomial time.



Problem 5

What can be said about the computational complexity of

Constraint Satisfaction Problems (CSP)

Γ set of (finitary) relations on a domain D.

General (algebraic) definition of CSP:

CSP(Γ) := set of problems of the form

Does there exist a relational homomorphism
$(V, \Sigma) \to (D, \Sigma')$
(between relational systems of the same type) where $\Sigma' \subseteq \Gamma$?

Special CSP:
GRAPH COLORABILITY, GRAPH ISOMORPHISM, SATISFIABILITY (SAT)

TECHNISCHE UNIVERSITÄT DRESDEN

aa

another (algebraic) approach:
P. Idziak, P. Marković, R. McKenzie, M. Valeriote, R. Willard, Tractability and learnability arising from algebras with few subpowers. (2007)

Theorem

For a finite algebra $\mathcal{A} = \langle A, F \rangle$ with few subpowers, CSP(Inv F) *is globally tractable.*

to be investigated:

- modified Galois connections (change "objects" and "attributes")
- clone lattice (e.g. minimal clones, intervals, . . .)
- dyadic view to algebraic constructions:
  $\mathrm{Inv}(\mathrm{construction}(F_i)_{i\in I}) = \text{which construction}(\mathrm{Inv}\, F_i)_{i\in I}$?
  $\mathrm{Pol}(\mathrm{construction}(Q_i)_{i\in I}) = \text{which construction}(\mathrm{Pol}\, Q_i)_{i\in I}$?
  e.g. relational view to tame congruence theory
- algorithmic problems (e.g. $f \triangleright \varrho$, free algebras, CSP)

Outline

50+25 Arbeitstagung Allgemeine Algebra with Rudolf Wille

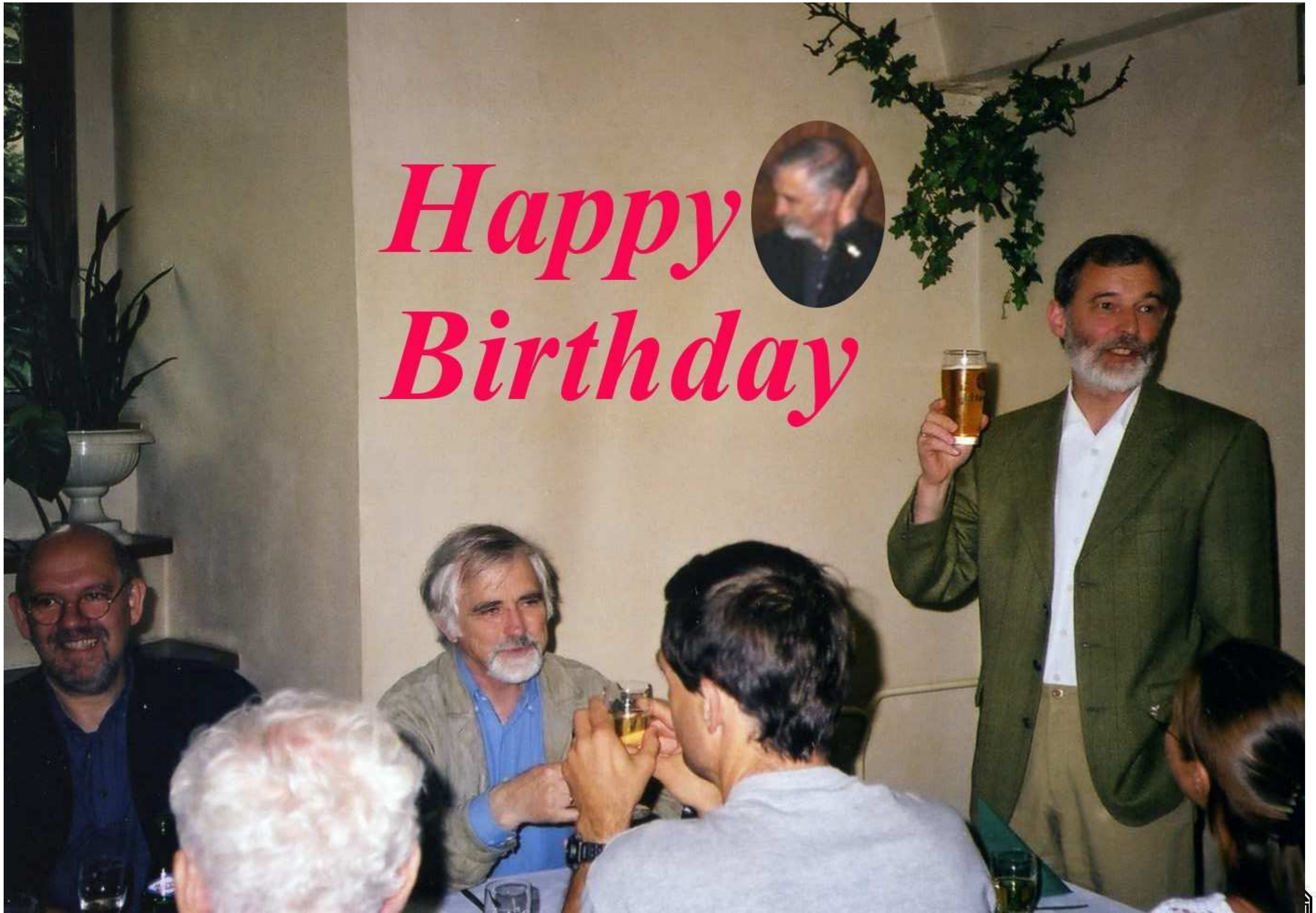
AAA series founded by
Rudolf Wille 1971

Congratulation

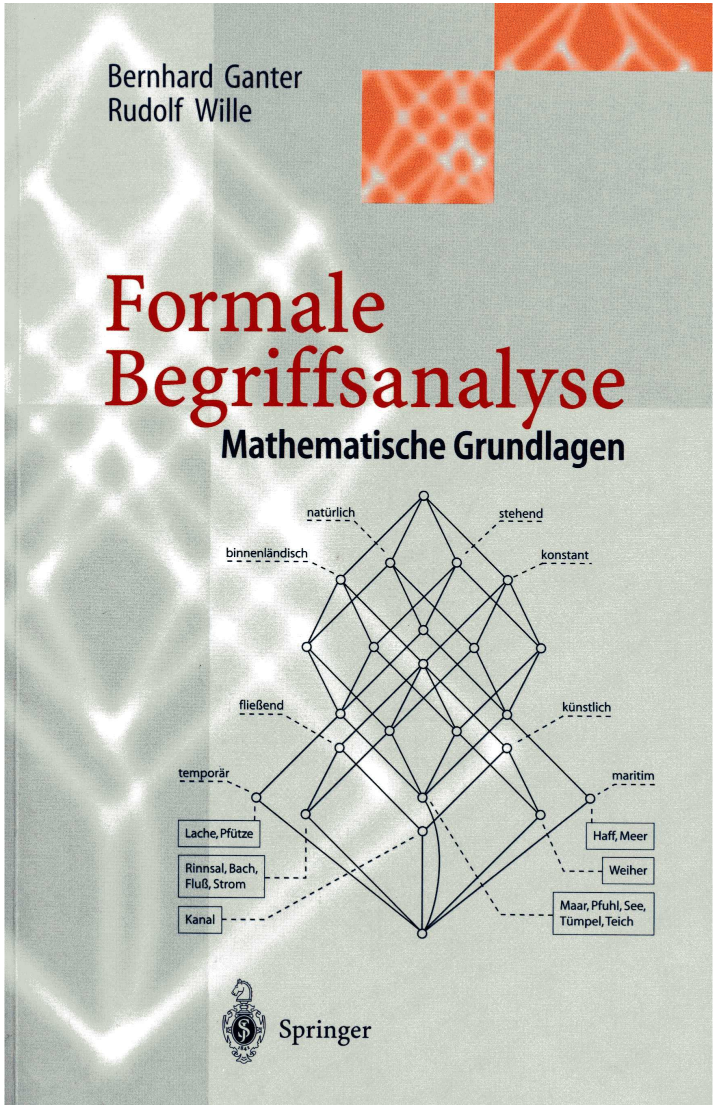
Dear Rudolf, on behalf of all participants and the whole "AAA-community" many thanks for all what you did for the development of algebra, congratulations to your 70th birthday today; good health and further success and all the best for the future.

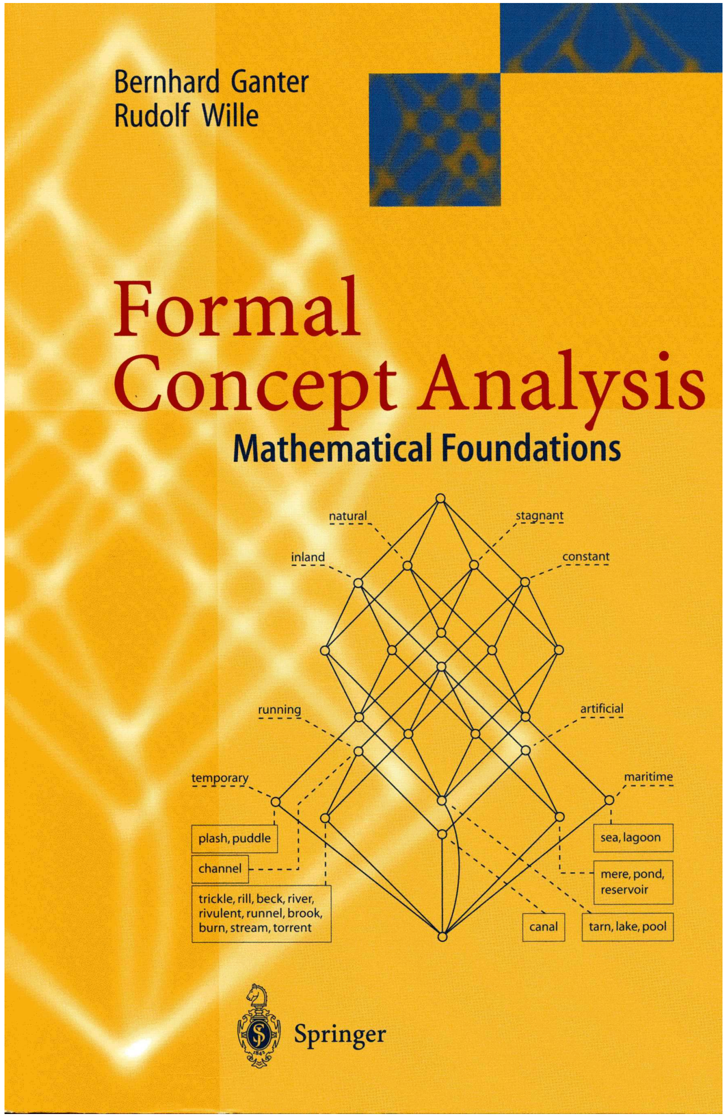
Lieber Rudolf, im Namen aller Tagungsteilnehmer und der ganzen AAA-Community sage ich Dir Dank für alles, was Du für die Entwicklung der Algebra getan hast, gratuliere ganz herzlich zu Deinem heutigen 70. Geburtstag und wünsche Dir Gesundheit, Schaffenskraft und alles Gute für die nächsten n Jahre ($n \in \mathbb{N}$)

70 years Rudolf Wille = (50+25)×AAA



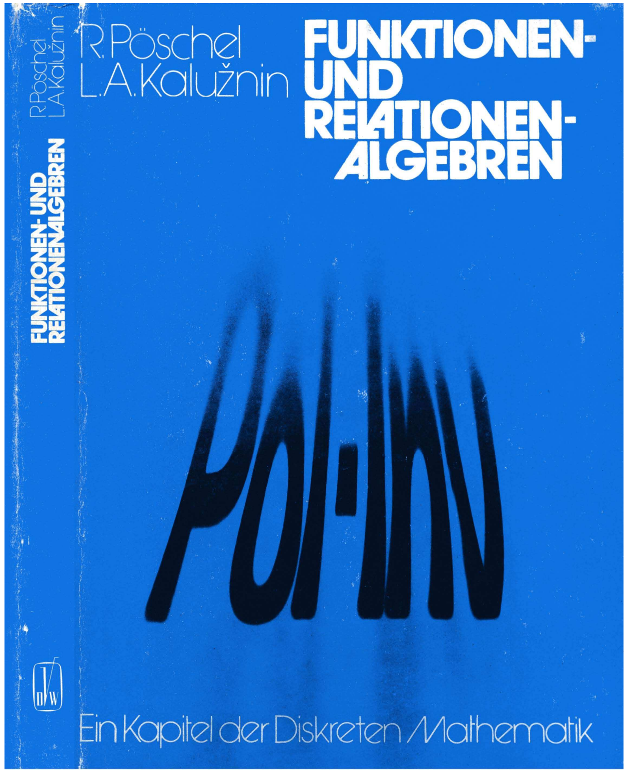
THE book of Formal Concept Analysis



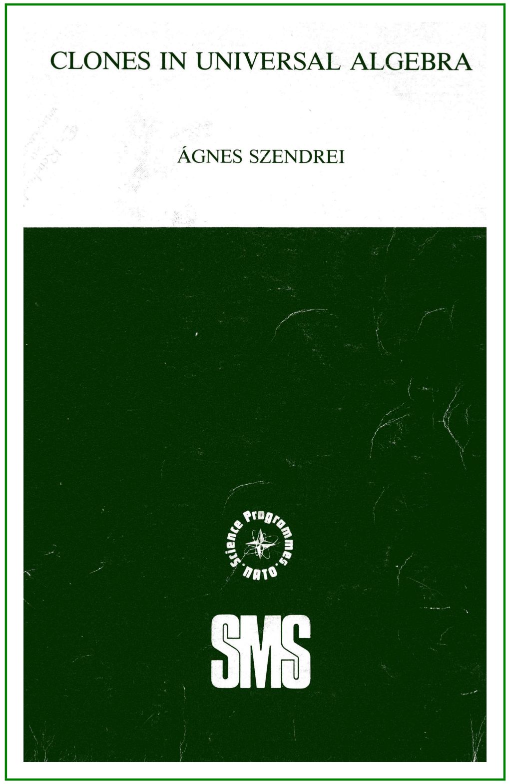


Some books about clones

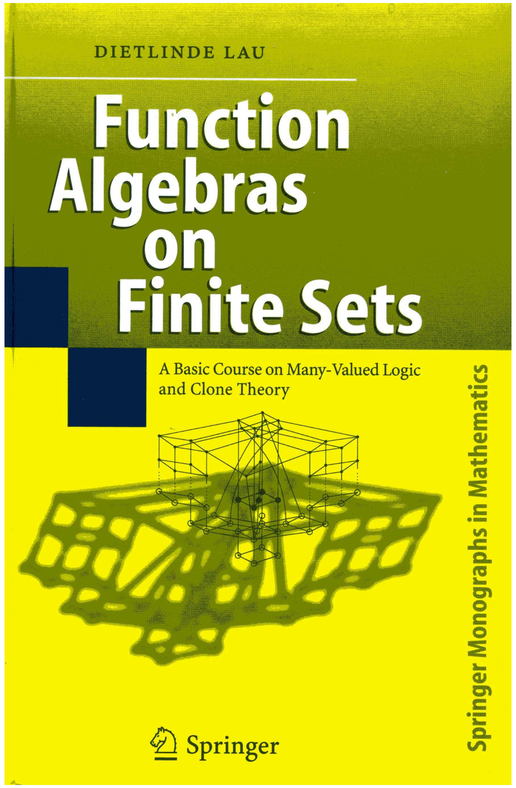
R. Pöschel
L.A. Kalužnin (1979)



A. Szendrei (1986)



D. Lau (2006)



back

TECHNISCHE UNIVERSITÄT DRESDEN