Foundations of Relations and Kleene Algebra

Peter Jipsen

Chapman University

September 4, 2006

Introduction

- Aim: cover the basics about relations and Kleene algebras within the framework of universal algebra
- This is a *tutorial*
- Slides give precise definitions, lots of statements
- Decide which statements are true (can be improved) which are *false* (and perhaps how they can be fixed)
- [Hint: a list of pages with false statements is at the end]

Prerequisites

- Knowledge of sets, union, intersection, complementation
- Some basic first-order logic
- Basic discrete math (e.g. function notation)
- These notes take an *algebraic* perspective

Conventions:

- Minimize distinction between concrete and abstract notation
- $x, y, z, x_1, \ldots$ variables (implicitly universally quantified)
- $X, Y, Z, X_1, \ldots$ set variables (implicitly universally quantified)
- $f, g, h, f_1, \ldots$ function variables
- $a, b, c, a_1, \ldots$ constants
- $i, j, k, i_1, \ldots$ integer variables, usually nonnegative
- $m, n, n_1, \ldots$ nonnegative integer constants

Algebraic properties of set operation

Let U be a set, and $\mathcal{P}(U) = \{X : X \subseteq U\}$ the *powerset* of U

$\mathcal{P}(U)$ is an algebra with operations union $\cup$, intersection $\cap$, complementation $X^- = U \setminus X$

Satisfies many identities: e.g. $X \cup Y = Y \cup X$ for all $X, Y \in \mathcal{P}(U)$

How can we describe the set of all identities that hold?

Can we decide if a particular identity holds in all powerset algebras?

These are questions about the equational theory of these algebras

We will consider similar questions about several other types of algebras, in particular relation algebras and Kleene algebras

Binary relations

An *ordered pair*, written (u, v), has the defining property

$$(u, v) = (x, y) \text{ iff } u = x \text{ and } v = y$$

The *direct product* of sets U, V is

$$U \times V = \{(u, v) : u \in U, v \in V\}$$

A *binary relation* R from U to V is a subset of $U \times V$

Write uRv if $(u, v) \in R$, otherwise write $u \not R v$

Define $uR = \{v : uRv\}$ and $Rv = \{u : uRv\}$

Operations on binary relations

Composition of relations: $R; S = \{(u, v) : uR \cap Rv \neq \emptyset\}$

$$= \{(u, v) : \exists x \ uRx \text{ and } xSv\}$$

Converse of R is $R^{\smile} = \{(v, u) : (u, v) \in R\}$

Identity relation $I_U = \{(u, u) : u \in U\}$

A binary relation *on* a set U is a subset of $U \times U$

Define $R^0 = I_U$ and $R^{n+1} = R; R^n$ for $n \geq 0$

Transitive closure of R is $R^+ = \bigcup_{n\geq 1} R^n$

Reflexive transitive closure of R is $R^* = R^+ \cup I_U = \bigcup_{n\geq 0} R^n$

Properties of binary relations

Let R be a binary relation on U

R is *reflexive* if xRx for all $x \in U$

R is *irreflexive* if $x \not R x$ for all $x \in U$

R is *symmetric* if xRy implies yRx (implicitly quantified)

R is *antisymmetric* if xRy and yRx implies $x = y$

R is *transitive* if xRy and yRz implies xRz

R is *univalent* if xRy and xRz implies $y = z$

R is *total* if $xR \neq \emptyset$ for all $x \in U$ (otherwise *partial*)

Properties in relational form

Prove (and extend) or disprove (and fix)

R is reflexive iff $I_U \subseteq R$

R is irreflexive iff $I_U \not\subseteq R$

R is symmetric iff $R \subseteq R^{\smile}$ iff $R = R^{\smile}$

R is antisymmetric iff $R \cap R^{\smile} = I_U$

R is transitive iff $R; R = R$ iff $R = R^+$

R is univalent iff $R; R^{\smile} \subseteq I_U$

R is total iff $I_U \subseteq R; R^{\smile}$

Binary operations and properties

A *binary operation* $+$ on U is a function from $U \times U$ to U

Write $+(x, y)$ as $x + y$

$+$ is *idempotent* if $x + x = x$ (all implicitly universally quantified)

$+$ is *commutative* if $x + y = y + x$

$+$ is *associative* if $(x + y) + z = x + (y + z)$

$+$ is *conservative* if $x + y = x$ or $x + y = y$

$+$ is *left cancellative* if $z + x = z + y$ implies $x = y$

$+$ is *right cancellative* if $x + z = y + z$ implies $x = y$

Connection with relations

Define R_+ on U by xR_+y iff $x + z = y$ for some $z \in U$

Prove (and extend) or disprove (and fix)

If $+$ is idempotent then R_+ is reflexive.

If $+$ is commutative then R_+ is antisymmetric.

If $+$ is associative then R_+ is transitive.

A *semigroup* is a set with an associative binary operation

A *band* is a semigroup $(U, +)$ such that $+$ is idempotent

A *quasi-ordered set (qoset)* is a set with a reflexive transitive relation

$\Rightarrow$ If $(U, +)$ is a band then (U, R_+) is a qoset

More specific connection with relations

Define $\leq_+$ on U by $x \leq_+ y$ iff $x + y = y$

Prove (and extend) or disprove (and fix)

$+$ is idempotent iff $\leq_+$ is reflexive.

$+$ is commutative iff $\leq_+$ is antisymmetric.

$+$ is associative iff $\leq_+$ is transitive.

A *semilattice* is a band $(U, +)$ such that $+$ is commutative

A *partially ordered set* is a qoset (U, R) such that R is antisymmetric

$\Rightarrow$ If $(U, +)$ is a semilattice then $(U, \leq_+)$ is a partially ordered set

A partially ordered set is called a *poset* for short

A *strict partial order* is an irreflexive transitive relation

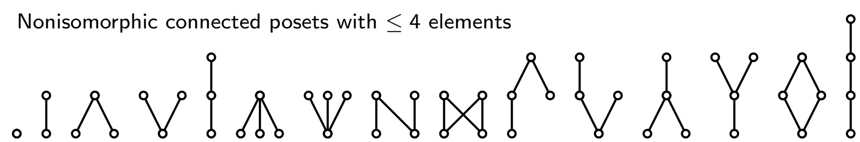
Prove (and extend) or disprove (and fix)

If $<$ is a strict partial order on U, then $(U, < \cup I_U)$ is a poset.
If $(U, \leq)$ is a poset, then $< = \leq \setminus I_U$ is a strict partial order.

For $a, b \in U$ we say that a is *covered* by b (written $a \prec b$)
if $a < b$ and there is no x such that $a < x < b$

To visualize a finite poset we can draw a *Hasse diagram*:

a is connected with an upward sloping line to b if $a \prec b$



Equivalence relations

An *equivalence relation* is a reflexive symmetric transitive relation

Prove (and extend) or disprove (and fix)

R is an equivalence relation on U iff $I_U \subseteq R = R^{\smile}; R$

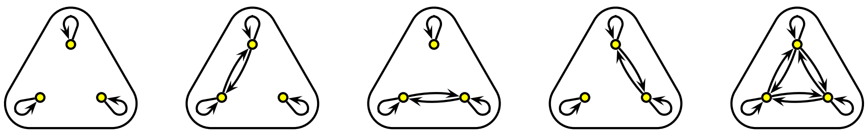
Let R be an equivalence relation on a set U, and $u \in U$

Then $uR = \{x : uRx\}$ is called an *equivalence class* of R

Usually written $[u]_R$ or simply $[u]$; u is called a *representative* of $[u]$

The *set of all equivalence classes* of R is $U/R = \{[u] : u \in U\}$

Equivalence relations on a 3-element set



Partitions

A *partition* of U is a subset P of $\mathcal{P}(U)$ such that

$$\bigcup P = U,\ \ \emptyset \notin P,\ \ \text{and } X = Y \text{ or } X \cap Y = \emptyset \text{ for all } X, Y \in P$$

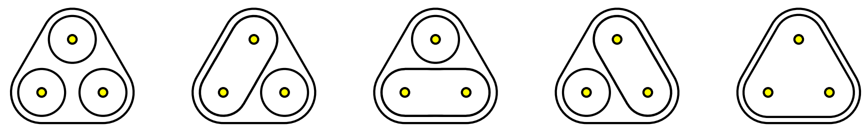
(where $\bigcup P = \{x : x \in X \text{ for some } X \in P\}$)

For a partition P define a relation by $x \equiv_P y$ iff $x, y \in X$ for some $X \in P$

Prove (and extend) or disprove (and fix)

The map $f(R) = U/R$ is a bijection from the set of equivalence relations on U to the set of partitions of U, with $f^{-1}(P)$ given by $\equiv_P$.

Partitions of a 3-element set



The poset induced by a quasi-order

For a qoset $(U, \sqsubseteq)$, define a relation on U by $x \equiv y$ iff $x \sqsubseteq y$ and $y \sqsubseteq x$

Now define $\leq$ on $U/\equiv$ by $[x] \leq [y]$ iff $x \sqsubseteq y$

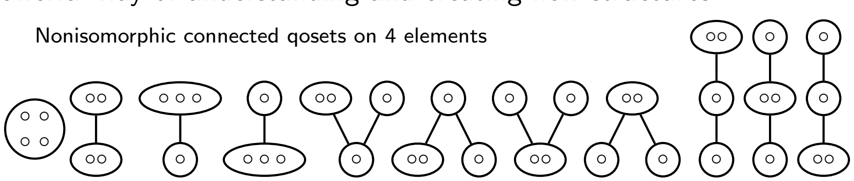
$\leq$ is said to be *well defined* if $[x'] = [x] \leq [y] = [y']$ implies $[x'] \leq [y']$

Prove (and extend) or disprove (and fix)

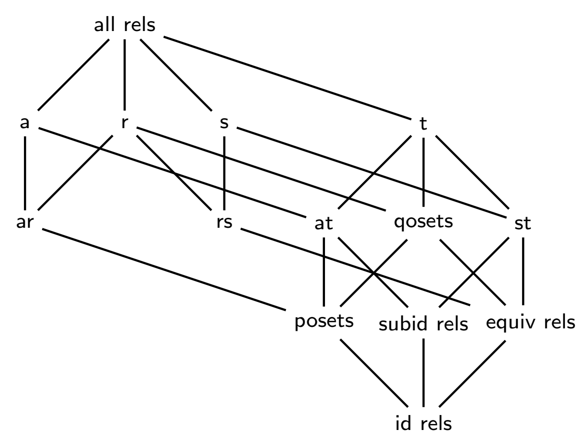
The relation $\leq$ is well defined and $(U/\equiv, \leq)$ is a poset.

Factoring mathematical structures by appropriate equivalence relations is a powerful way of understanding and creating new structures.

Nonisomorphic connected qosets on 4 elements



Some classes of binary relations



a = antisymmetric
r = reflexive
s = symmetric
t = transitive
a and s ⇒ t

Tuples and direct products

We have seen several examples of algebras and relational structures:

$(U,+)$ an algebra with one binary operation, e.g. $(\mathbb{N},+)$, $(\mathcal{P}(U),\cup)$

(U,R) a relational structure with a binary relation, e.g. $(\mathbb{N},\leq)$, $(\mathcal{P}(U),\subseteq)$

Applications usually involve several n-ary operations and relations

For a set I, an *I-tuple* $(u_i)_{i\in I}$ is a function mapping $i \in I$ to u_i.

A *tuple over $(U_i)_{i\in I}$* is an I-tuple $(u_i)_{i\in I}$ such that $u_i \in U_i$ for all $i \in I$

The *direct product* $\prod_{i\in I} U_i$ is the set of all tuples over $(U_i)_{i\in I}$

In particular, $\prod_{i\in I} U$ is the set U^I of all functions from I to U

If $I = \{1,\ldots,n\}$ then we write $U^I = U^n$ and $\prod_{i\in I} U_i = U_1 \times \cdots \times U_n$

Note: $U^0 = U^\emptyset = \{()\}$ has one element, namely the empty function $() = \emptyset$

Algebras and relational structures

A (*unsorted first-order*) *structure* is a tuple $\mathbf{U} = (U,(f^{\mathbf{U}})_{f\in\mathcal{F}_\tau},(R^{\mathbf{U}})_{R\in\mathcal{R}_\tau})$

- U is the *underlying set*
- $\mathcal{F}_\tau$ is a set of *operation symbols* and
- $\mathcal{R}_\tau$ is a set of *relation symbols* (disjoint from $\mathcal{F}_\tau$)

The *type* $\tau : \mathcal{F}_\tau \cup \mathcal{R}_\tau \to \{0,1,2,\ldots\}$ gives the *arity* of each symbol

$f^{\mathbf{U}} : U^{\tau(f)} \to U$ and $R^{\mathbf{U}} \subseteq U^{\tau(R)}$ are the *interpretation* of symbol f and R

0-ary operation symbols are called *constant symbols*

$\mathbf{U}$ is a (universal) *algebra* if $\mathcal{R}_\tau = \emptyset$; use $\mathbf{A},\mathbf{B},\mathbf{C}$ for algebras

Convention: the string of symbols $f(x_1,\ldots,x_n)$ implies that f has arity n

The superscript $^{\mathbf{U}}$ is often omitted

Monoids and involution

Recall that $(A,\cdot)$ a semigroup if $\cdot$ is an associative operation

A *monoid* is a semigroup with an *identity element*

i.e. of the form $(A,\cdot,1)$ such that $x\cdot 1 = x = 1\cdot x$

An *involutive semigroup* is a semigroup with an *involution*

i.e. of the form $(A,\cdot,^\smile)$ such that $^\smile$ has *period two*: $x^{\smile\smile} = x$, and
$^\smile$ *antidistributes over* $\cdot$: $(x\cdot y)^\smile = y^\smile \cdot x^\smile$

Prove (and extend) or disprove (and fix)

If an involutive semigroup satisfies $x\cdot 1 = x$ for some element 1 and all x then it satisfies $1^\smile = 1$ and $1\cdot x = x$

An *involutive monoid* is a monoid with an involution

A *group* is an involutive monoid such that $x\cdot x^\smile = 1$

Join-semilattices

A *semilattice* is a commutative idempotent semigroup

$(A,+,\leq)$ is a *join-semilattice* if
$(A,+)$ is a semilattice and $x \leq y \Leftrightarrow x+y = y$

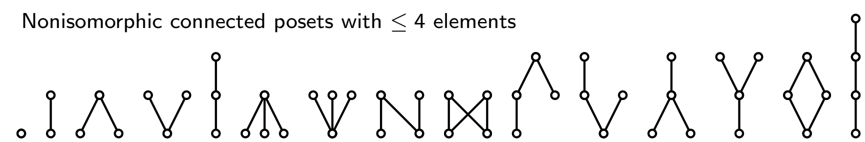
Prove (and extend) or disprove (and fix)

$(A,+,\leq)$ is a join-semilattice
iff $(A,\leq)$ is a poset and $x+y = z \Leftrightarrow \forall w(x\leq w$ and $y \leq w \Leftrightarrow z \leq w)$
iff $(A,\leq)$ is a poset and $x+y \leq z \Leftrightarrow x \leq z$ and $y \leq z$

$\Rightarrow$ any two elements x,y have a *least upper bound* $x+y$

Which of the following are join-semilattices?

Nonisomorphic connected posets with ≤ 4 elements



Lattices and duals

A *meet-semilattice* $(A, \cdot, \leq)$ is a semilattice with $x \leq y \Leftrightarrow x \cdot y = x$

$(A, +, \cdot)$ is a *lattice* if $+, \cdot$ are associative, commutative operations that satisfy the absorption laws: $x + (y \cdot x) = x = (x + y) \cdot x$

Prove (and extend) or disprove (and fix)

$(A, +, \cdot)$ is a lattice iff $(A, +, \leq)$ is a join-semilattice and $(A, \cdot, \leq)$ is a meet-semilattice where $x \leq y \Leftrightarrow x + y = y$.

Define $x \geq y \Leftrightarrow y \leq x$. The *dual* $(A, +, \leq)^d = (A, +, \geq)$
$(A, \cdot, \leq)^d = (A, \cdot, \geq)$ and $(A, +, \cdot)^d = (A, \cdot, +)$

Prove (and extend) or disprove (and fix)

The dual of a join-semilattice is a meet-semilattice and vice versa.
The dual of a lattice is again a lattice.

Distributivity and bounds

A lattice is *distributive* if it satisfies $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$

Prove (and extend) or disprove (and fix)

A lattice is distributive iff $x + (y \cdot z) = (x + y) \cdot (x + z)$ iff $(x + y) \cdot (x + z) \cdot (y + z) = (x \cdot y) + (x \cdot z) + (y \cdot z)$

$\Rightarrow$ a lattice is distributive iff its dual is distributive

A *semilattice with identity* is a commutative idempotent monoid

$(A, +, 0, \cdot, \top)$ is a *bounded lattice* if
$(A, +, \cdot)$ is a lattice and $(A, +, 0)$, $(A, \cdot, \top)$ are semilattices with identity

Prove (and extend) or disprove (and fix)

Suppose $(A, +, \cdot)$ is a lattice. Then $(A, +, 0, \cdot, \top)$ is a bounded lattice iff $0 \leq x \leq \top$ iff $x \cdot 0 = 0$ and $x + \top = \top$

Complementation and Boolean algebras

$(A, +, 0, \cdot, \top, ^-)$ is a *lattice with complementation* if $(A, +, 0, \cdot, \top)$ is a bounded lattice such that $x + x^- = \top$ and $x \cdot x^- = 0$

Prove (and extend) or disprove (and fix)

Lattices with complementation satisfy $x^{--} = x$ and DeMorgan's laws $(x + y)^- = x^- \cdot y^-$ and $(x \cdot y)^- = x^- + y^-$

A *Boolean algebra* is a distributive lattice with complementation

Prove (and extend) or disprove (and fix)

Boolean algebras satisfy $x^{--} = x$ and DeMorgan's laws $(x + y)^- = x^- \cdot y^-$ and $(x \cdot y)^- = x^- + y^-$

Prove (and extend) or disprove (and fix)

$(A, +, 0, \cdot, \top, ^-)$ is a Boolean algebra iff $+$ is commutative with identity 0, $\cdot$ is commutative with identity 1, $+$ distributes over $\cdot$, $\cdot$ distributes over $+$, $x + x^- = \top$ and $x \cdot x^- = 0$.

Boolean algebras of sets

$\mathcal{P}(U) = (\mathcal{P}(U), \cup, \emptyset, \cap, U, ^-)$ is the *Boolean algebra of all subsets of U*

A *concrete Boolean algebra* is any collection of subsets of a set U that is closed under $\cup$, $\cap$, and $^-$

The *atoms* of a join-semilattice with 0 are the covers of 0

A join-semilattice with 0 is *atomless* if it has no atoms, and

atomic if for every $x \neq 0$ there is an atom $a \leq x$

Prove (and extend) or disprove (and fix)

$\mathcal{P}(U)$ is atomic for every set U

$H = \{(a_1, b_1] \cup \cdots \cup (a_n, b_n] : 0 \leq a_i < b_i \leq 1$ are rationals, $n \in \mathbb{N}\}$ is an atomless concrete Boolean algebra with U the set of positive rationals ≤ 1

Relation algebras

An *(abstract) relation algebra* is of the form $(A, +, 0, \cdot, \top, ^-, ;, 1, ^\smile)$ where

- $(A, +, 0, \cdot, \top, ^-)$ is a Boolean algebra
- $(A, ;, 1)$ is a monoid
- $(x;y) \cdot z = 0 \;\Leftrightarrow\; (x^\smile;z) \cdot y = 0 \;\Leftrightarrow\; (z;y^\smile) \cdot x = 0$

The last line states the Schröder equivalences (or DeMorgan's Thm K)

Prove (and extend) or disprove (and fix)

In a relation algebra $x^{\smile\smile} = x$ and $^\smile$ is self-conjugated, i.e. $x^\smile \cdot y = 0 \Leftrightarrow x \cdot y^\smile = 0$. Hence $(x+y)^\smile = x^\smile + y^\smile$, $x^{-\smile} = x^{\smile -}$, $(x \cdot y)^\smile = x^\smile \cdot y^\smile$, $^\smile$ is an involution and $x;(y+z) = x;y + x;z$.

Hint: In a Boolean algebra $u = v$ iff $\forall x(u \cdot x = 0 \Leftrightarrow v \cdot x = 0)$

Prove (and extend) or disprove (and fix)

A Boolean algebra expanded with an involutive monoid is a relation algebra iff $x;(y+z) = x;y + x;z$, $(x+y)^\smile = x^\smile + y^\smile$ and $(x^\smile;(x;y)^-) \cdot y = 0$

Concrete relation algebras

$\mathrm{Rel}(U) = (\mathcal{P}(U^2), \cup, \cap, \emptyset, U^2, ^-, ;, I_U, ^\smile)$ the *square relation algebra* on U

A *concrete relation algebra* is of the form $(\mathcal{C}, \cup, \cap, \emptyset, \top, ^-, ;, I_U, ^\smile)$ where $\mathcal{C}$ is a set of binary relations on a set U that is closed under the operations $\cup$, $^-$, $;$, $^\smile$, and contains I_U

Prove (and extend) or disprove (and fix)

Every square relation algebra is concrete.

Every concrete relation algebra is a relation algebra, and the largest relation is an equivalence relation

Relation algebras have applications in program semantics, specification, derivation, databases, set theory, finite variable logic, combinatorics, . . .

Idempotent semirings

A *semiring* is an algebra $(A, +, 0, ;, 1)$ such that

- $(A, +, 0)$ is a commutative monoid
- $(A, ;, 1)$ is a monoid
- $x;(y+z) = (x;y) + (x;z)$, $\qquad (x+y);z = (x;z) + (y;z)$
- $x;0 = 0 = 0;x$

A semiring is *idempotent* if $x + x = x$

$\Rightarrow$ an idempotent semiring is a join-semilattice with $x \le y \Leftrightarrow x + y = y$, a bottom element 0, ; distributes over + and 0 is a zero for ;

Prove (and extend) or disprove (and fix)

In an idempotent semiring $x \le y$ implies $x;z \le y;z$ and $z;x \le z;y$

For any monoid $\mathbf{M} = (M, \cdot, 1)$, the *powerset idempotent semiring* is $\boldsymbol{\mathcal{P}}(\mathbf{M}) = (\mathcal{P}(M), \cup, \emptyset, ;, \{1\})$ where $X;Y = \{x \cdot y : x \in X,\ y \in Y\}$

Kleene algebras

A *Kleene algebra* is of the form $(A, +, 0, ;, 1, ^*)$ where

- $(A, +, 0, ;, 1)$ is an idempotent semiring
- $1 + x + x^*;x^* = x^*$
- $x;y \le y \Rightarrow x^*;y \le y \qquad$ (where $x \le y \Leftrightarrow x + y = y$)
- $y;x \le y \Rightarrow y;x^* \le y$

Prove (and extend) or disprove (and fix)

Let $\mathbf{M} = (M, \cdot, 1)$ be a monoid. Then $\boldsymbol{\mathcal{P}}(\mathbf{M})$ can be expanded to a Kleene algebra if we define $X^* = \bigcup_{n \ge 0} X^n$ where $X^0 = \{1\}$ and $X^{n+1} = X^n;X$

Prove (and extend) or disprove (and fix)

For any set U, $\mathrm{KRel}(U) = (\mathcal{P}(U^2), \cup, \emptyset, ;, I_U, ^*)$ is a Kleene algebra

Kleene algebras continued

Traditionally we write $x;y$ simply as xy

A Kleene expression has an *opposite* given by reversing the expression.

The opposite axioms of Kleene algebras again define Kleene algebras, so any proof of a result can be converted to a proof of the opposite result

Prove (and extend) or disprove (and fix)

In a Kleene algebra $x^n \le x^*$ *for all* $n \ge 0$ (*where* $x^0 = 1$, $x^{n+1} = x^n x$)
$x \le y \Rightarrow x^* \le y^*$
$xx^* = x^*x$ $\quad x^{**} = x^*$ *and* $x^* = 1 + x^+$ *where* $x^+ = xx^*$
$xy + z \le y \Rightarrow x^*z \le y$ (*and its opposite*)
$xy = yz \Rightarrow x^*y = yz^*$
$(xy)^*x = x(yx)^*$ *and* $(x+y)^* = x^*(yx^*)^*$

Kleene algebras have applications in automata theory, parsing, pattern matching, semantics and logic of programs, analysis of algorithms,...

Kleene algebras with tests

Kleene algebras model concatenation, nondeterministic choice and iteration, but to model programs need guarded choice and guarded iteration

A *Kleene algebra with tests* (KAT) is of the form $(A, +, 0, ;, 1, ^*, ^-, B)$ where $(A, +, 0, ;, 1, ^*)$ is a Kleene algebra, B is a unary relation ($\subseteq A$) and $x, y \in B \Rightarrow x + y,\ x;y,\ x^-,\ 0, 1 \in B,\ x;x = x,\ x;x^- = 0,\ x + x^- = 1$

Prove (and extend) or disprove (and fix)

In a KAT, $(B, +, 0, ;, 1, ^-)$ *is a Boolean algebra*

[Kozen 1996] defines KATs as two-sorted algebras, but here they are one-sorted structures with $^-$ a partial operation defined only on B

The program construct `if b then p else q` is expressed by $b;p + b^-;q$

`while b do p` is expressed by $(b;p)^*;b^-$

Idempotent semirings with domain and range

Every Kleene algebra is a KAT with $B = \{0, 1\}$

In KRel(U) the tests are a subalgebra of $\mathcal{P}(I_U)$

Can also define *idempotent semirings with tests* (just omit *)

More expressive: add a domain operator [Desharnais Möller Struth 2006]

An *idempotent semiring with predomain* is of the form $(A, +, 0, ;, 1, ^-, \delta)$ where $(A, +, 0, ;, 1, ^-, \delta[A])$ is an idempotent semiring with tests,

$$x \le \delta(x);x \quad \text{and} \quad \delta(\delta(x);y) \le \delta(x)$$

For *idempotent semirings with domain* add $\delta(x;\delta(y)) \le \delta(x;y)$

In Rel(U) the domain operator is definable by $\delta(R) = (R;R^{\smile}) \cap I_U$

Idempotent semirings with (pre)range operator are opposite

Terms and formulas

UA is a framework for studying and comparing all these algebras

Given a set X, the set of τ*-terms with variables from* X is the smallest set $T = T_\tau(X)$ such that

- $X \subseteq T$ and
- if $t_1, \ldots, t_n \in T$ and $f \in \mathcal{F}_\tau$ then $f(t_1, \ldots, t_n) \in T$.

The *term algebra over X* is $\mathbf{T}_\tau(X) = \mathbf{T} = (T_\tau(X), (f^{\mathbf{T}})_{f \in \mathcal{F}_\tau})$ with

$$f^{\mathbf{T}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n) \quad \text{for } t_1, \ldots, t_n \in T_\tau(X)$$

A *τ-equation* is a pair of τ-terms (s, t), usually written $s = t$

A *quasiequation* is an implication ($s_1 = t_1$ and ... and $s_n = t_n \Rightarrow s_0 = t_0$)

Models and theories

An *atomic formula* is a τ-equation or $R(x_1, \dots, x_n)$ for $R \in \mathcal{R}_\tau$

A *τ-formula* $\phi ::=$ atomic frm.$|\phi$and$\phi|\phi$or$\phi|\neg\phi|\phi \Rightarrow \phi|\phi \Leftrightarrow \phi|\forall x\phi|\exists x\phi$

Write $\mathbf{U} \models \phi$ if τ-formula ϕ holds in τ-structure $\mathbf{U}$ (standard defn)

Throughout $\mathcal{K}$ is a class of τ-structures, F a set of τ-formulas

Write $\mathcal{K} \models F$ if $\mathbf{U} \models \phi$ for all $\mathbf{U} \in \mathcal{K}$ and $\phi \in F$

$\mathrm{Mod}(F) = \{\mathbf{U} : \mathbf{U} \models F\}$ = class of all *models* of F

$\mathrm{Th}(\mathcal{K}) = \{\phi : \mathcal{K} \models \phi\}$ = *first order theory* of $\mathcal{K}$

$\mathrm{Th}_e(\mathcal{K}) = \mathrm{Th}(\mathcal{K}) \cap \{\tau\text{-equations}\}$ = *equational theory* of $\mathcal{K}$

$\mathrm{Th}_q(\mathcal{K}) = \mathrm{Th}(\mathcal{K}) \cap \{\tau\text{-quasiequations}\}$ = *quasiequational theory* of $\mathcal{K}$

$\mathrm{Th}_q(\mathcal{K})$ is also called the *strict universal Horn theory* of $\mathcal{K}$

Substructures, homomorphisms and products

Let $\mathbf{U}, \mathbf{V}, \mathbf{V}_i$ $(i \in I)$ be structures of type τ and let f, R range over $\mathcal{F}_\tau, \mathcal{R}_\tau$

- $\mathbf{U}$ is a *substructure* of $\mathbf{V}$ if $U \subseteq V$, $f^{\mathbf{U}}(u_1, \dots, u_n) = f^{\mathbf{V}}(u_1, \dots, u_n)$ and $R^{\mathbf{U}} = R^{\mathbf{V}} \cap \mathbf{U}^n$ for all $u_1, \dots, u_n \in U$
- $h : \mathbf{U} \to \mathbf{V}$ is a *homomorphism* if h is a function from U to V, $h(f^{\mathbf{U}}(u_1, \dots, u_n)) = f^{\mathbf{V}}(h(u_1), \dots, h(u_n))$ and $(u_1, \dots, u_n) \in R^{\mathbf{U}} \Rightarrow (h(u_1), \dots, h(u_n)) \in R^{\mathbf{V}}$ for all $u_1, \dots, u_n \in U$
- $\mathbf{V}$ is a *homomorphic image* of $\mathbf{U}$ if there exists a surjective homomorphism $h : \mathbf{U} \twoheadrightarrow \mathbf{V}$.
- $\mathbf{U}$ is *isomorphic* to $\mathbf{V}$, in symbols $\mathbf{U} \cong \mathbf{V}$, if there exists a bijective homomorphism from $\mathbf{U}$ to $\mathbf{V}$.
- $\mathbf{U} = \prod_{i \in I} \mathbf{V}_i$, the *direct product* of structures $\mathbf{V}_i$, if $U = \prod_{i \in I} V_i$, $(f^{\mathbf{U}}(u_1, \dots, u_n)_i)_{i \in I} = (f^{\mathbf{V}_i}(u_{1i}, \dots, u_{ni}))_{i \in I}$ and $(u_1, \dots, u_n) \in R^{\mathbf{U}} \Leftrightarrow \forall i(u_{1i}, \dots, u_{ni}) \in R^{\mathbf{V}_i}$ for all $u_1, \dots, u_n \in U$

Substructures are closed under all operations; give "local information"

Homomorphisms are structure preserving maps, and their images capture global regularity of the domain structure

Direct products are used to build or decompose bigger structures

A structure with one element is called *trivial*

A structure is *directly decomposable* if it is isomorphic to a direct product of nontrivial structures

A direct product has *projection maps* $\pi_i : \prod_{i \in I} \mathbf{V}_i \twoheadrightarrow \mathbf{V}_i$ where $\pi_i(u) = u_i$

Prove (and extend) or disprove (and fix)

For any direct product the projection maps are homomorphisms

Isomorphisms preserve all logically defined properties (not only first-order)

Varieties and HSP

$\mathrm{H}\mathcal{K}$ is the class of homomorphic images of members of $\mathcal{K}$

$\mathrm{S}\mathcal{K}$ is the class of substructures of members of $\mathcal{K}$

$\mathrm{P}\mathcal{K}$ is the class of direct products of members of $\mathcal{K}$

A *variety* is of the form $\mathrm{Mod}(E)$ for some set E of equations

A *quasivariety* is of the form $\mathrm{Mod}(Q)$ for some set Q of quasiequations

Prove (and extend) or disprove (and fix)

If $\mathcal{K}$ is a quasivariety then $\mathrm{S}\mathcal{K} \subseteq \mathcal{K}$, $\mathrm{P}\mathcal{K} \subseteq \mathcal{K}$ and $\mathrm{H}\mathcal{K} \subseteq \mathcal{K}$

The next characterization marks the beginning of universal algebra

Theorem (Birkhoff 1935)

$\mathcal{K}$ is a variety iff $\mathrm{H}\mathcal{K} = \mathcal{K}$, $\mathrm{S}\mathcal{K} = \mathcal{K}$ and $\mathrm{P}\mathcal{K} = \mathcal{K}$

Varieties generated by classes

$\Lambda_\tau = \{\mathrm{Mod}(E) : E \text{ is a set of } \tau\text{-equations}\} = \text{set of all } \tau\text{-varieties}$

Prove (and extend) or disprove (and fix)

For sets F_i of τ-formulas $\bigcap_{i\in I} \mathrm{Mod}(F_i) = \mathrm{Mod}(\bigcup_{i\in I} F_i)$

Hence Λ_τ is closed under arbitrary intersections

$\bigcap \Lambda_\tau = \mathrm{Mod}(\{x = y\}) =$ *the class $\mathcal{O}_\tau$ of trivial τ-structures*

The *variety generated by $\mathcal{K}$* is $\mathrm{V}\mathcal{K} = \bigcap\{\text{all varieties that contain } \mathcal{K}\}$

Prove (and extend) or disprove (and fix)

$\mathrm{SH}\mathcal{K} = \mathrm{HS}\mathcal{K}$, $\mathrm{PH}\mathcal{K} = \mathrm{HP}\mathcal{K}$ *and* $\mathrm{PS}\mathcal{K} = \mathrm{SP}\mathcal{K}$ *for any class $\mathcal{K}$*

Theorem (Tarski 1946)

$\mathrm{V}\mathcal{K} = \mathrm{HSP}\mathcal{K}$ *for any class $\mathcal{K}$ of structures*

Complete lattices

For a subset X of a poset $\mathbf{U}$ write $X \le u$ if $x \le u$ for all $x \in X$ and define $z = \sum X$ if $X \le u \Leftrightarrow z \le u$ (so $\sum X$ is the *least upper bound* of X)

$u \le X$ and the *greatest lower bound* $\prod X$ are defined dually.

Prove (and extend) or disprove (and fix)

If $\sum X$ exists for every subset of a poset then $\prod X = \sum\{u : u \le X\}$

A structure $\mathbf{U}$ with a partial order is *complete* if $\sum X$ exists for all $X \subseteq U$

$\Rightarrow$ every complete join-semilattice is a complete lattice; $x \cdot y = \prod\{x, y\}$

A complete lattice has a bottom $0 = \sum \emptyset$ and a top $\top = \prod \emptyset$

Prove (and extend) or disprove (and fix)

$\mathbf{U}$ *with partial order $\le$ is complete iff $\prod X$ exists for all $X \subseteq U$*

Λ_τ partially ordered by $\subseteq$ is a complete lattice

Congruences and quotient algebras

A *congruence* on an algebra $\mathbf{A}$ is an equivalence relation θ on A that is compatible with the operations of $\mathbf{A}$, i.e. for all $f \in Fn$

$$x_1\theta y_1 \text{ and } \ldots \text{ and } x_n\theta y_n \Rightarrow f^{\mathbf{A}}(x_1,\ldots,x_n)\theta f^{\mathbf{A}}(y_1,\ldots,y_n)$$

$\mathrm{Con}(\mathbf{A})$ is the set of all congruences on $\mathbf{A}$

Prove (and extend) or disprove (and fix)

$\mathrm{Con}(\mathbf{A})$ *is a complete lattice with $\prod = \bigcap$, bottom I_A and top A^2*

For $\theta \in \mathrm{Con}(\mathbf{A})$, the *quotient algebra* is $\mathbf{A}/\theta = (A/\theta, (f^{\mathbf{A}/\theta})_{f\in\mathcal{F}_\tau})$ where

$$f^{\mathbf{A}/\theta}([x_1]_\theta,\ldots,[x_n]_\theta) = f^{\mathbf{A}}(x_1,\ldots,x_n)$$

Prove (and extend) or disprove (and fix)

The operations $f^{\mathbf{A}/\theta}$ are well defined and $h_\theta : A \to A/\theta$ given by $h_\theta(x) = [x]_\theta$ is a surjective homomorphism from $\mathbf{A}$ onto $\mathbf{A}/\theta$

Images, kernels and isomorphism theorems

For a function $f : A \to B$ the *image* of f is $f[A] = \{f(x) : x \in A\}$

The *kernel* of f is $\ker f = \{(x, y) \in A^2 : f(x) = f(y)\}$ (an equivalence rel)

Prove (and extend) or disprove (and fix)

If $h : \mathbf{A} \to \mathbf{B}$ is a homomorphism then $\ker h \in \mathrm{Con}(A)$

$h[A]$ is the underlying set of a subalgebra $h[\mathbf{A}]$ of $\mathbf{B}$

The first isomorphism theorem: $f : \mathbf{A}/\ker h \twoheadrightarrow h[\mathbf{A}]$ given by $f([x]_\theta) = h(x)$ is a well defined isomorphism

The second isomorphism theorem: For $\theta \in \mathrm{Con}(\mathbf{A})$, the subset $\uparrow\theta = \{\psi : \theta \subseteq \psi\}$ of $Con(\mathbf{A})$ is isomorphic to $Con(\mathbf{A}/\theta)$ via the map $\psi \mapsto \psi/\theta$ where $[x]\psi/\theta[y] \Leftrightarrow x\psi y$

In a join-semilattice, u is *join irreducible* if $u = x + y \Rightarrow u \in \{x, y\}$

u is *join prime* if $u \leq x + y \Rightarrow u \leq x$ or $u \leq y$

u is *completely join irreducible* if there is a (unique) greatest element $< u$

u is *completely join prime* if $u \leq \sum X \Rightarrow u \leq x$ for some $x \in X$

(completely) meet irreducible and *(completely) meet prime* are given dually

Prove (and extend) or disprove (and fix)

In complete lattices, u is completely join irreducible iff $u = \sum X \Rightarrow u \in X$

Distributivity $\Rightarrow$ (completely) join irreducible = (completely) join prime

u is *compact* if $u \leq \sum X \Rightarrow u \leq x_1 + \cdots + x_n$ for some $x_1, \ldots, x_n \in X$

A complete lattice is *algebraic* if all element are joins of compact elements

Prove (and extend) or disprove (and fix)

$\mathrm{Con}(\mathbf{A})$ *is an algebraic lattice* (*hint: compact = finitely generated*)

Subdirect products and subdirectly irreducibles

An *embedding* is an injective homomorphism

An embedding $h : \mathbf{A} \hookrightarrow \prod_{i \in I} \mathbf{B}_i$ is *subdirect* if $\pi_i[h[A]] = B_i$ for all $i \in I$

$\mathbf{A}$ is a *subdirect product* of $(\mathbf{B}_i)_{i \in I}$ if there is a subdirect $h : \mathbf{A} \hookrightarrow \prod_{i \in I} \mathbf{B}_i$

Prove (and extend) or disprove (and fix)

Define $h : \mathbf{A} \hookrightarrow \prod_{i \in I} \mathbf{A}/\theta_i$ by $h(a) = ([a]_{\theta_i})_{i \in I}$

Then h is a subdirect embedding iff $\bigcap_{i \in I} \theta_i = I_A$

$\mathbf{A}$ is *subdirectly irreducible* if for any subdirect $h : \mathbf{A} \hookrightarrow \prod_{i \in I} \mathbf{B}_i$ there is an $i \in I$ such that $\pi_i \circ h$ is an isomorphism

Prove (and extend) or disprove (and fix)

$\mathbf{A}$ is subdirectly irreducible iff $I_A \in \mathrm{Con}(\mathbf{A})$ is completely meet irreducible iff $\mathrm{Con}(\mathbf{A})$ has a smallest nonbottom element

Meet irreducibles and subdirect representations

Zorn's Lemma states that if every linearly ordered subposet of a poset has an upper bound, then the poset itself has maximal elements

Prove (and extend) or disprove (and fix)

In an algebraic lattice all members are meets of completly meet irreducibles

The next result shows that subdirectly irreducibles are building blocks

Theorem (Birkhoff 1944)

Every algebra is a subdirect product of its subdirectly irreducible images

$\mathcal{K}_{\mathrm{SI}}$ is the *class of subdirectly irreducibles* of $\mathcal{K}$

$\Rightarrow \mathcal{V} = \mathrm{SP}(\mathcal{V}_{\mathrm{SI}})$ for any variety $\mathcal{V}$

Filters and ideals

For a poset $(U, \leq)$ the *principal ideal* of $x \in U$ is $\downarrow x = \{y : y \leq x\}$

For $X \subseteq U$ define $\downarrow X = \bigcup_{x \in X} \downarrow x$; X is a *downset* if $X = \downarrow X$

X is *up-directed* if $x, y \in X \Rightarrow \exists u \in X(x \leq u$ and $y \leq u)$

X is an *ideal* if X is an up-directed downset

principal filter $\uparrow x$, $\uparrow X$, *upset*, *down-directed* and *filter* are defined dually

An ideal or filter is *proper* if it is not the whole poset

An *ultrafilter* is a maximal (with respect to inclusion) proper filter

A filter X in a join-semilattice is *prime* if $x + y \in X \Rightarrow x \in X$ or $y \in X$

Prove (and extend) or disprove (and fix)

The set $\mathrm{Fil}(\mathbf{U})$ of all filters on a poset U is an algebraic lattice

In a join-semilattice every maximal filter is prime

In a distributive lattice every proper prime filter is maximal

Ultraproducts

$\mathcal{F}$ is a *filter over a set I* if $\mathcal{F}$ is a filter in $(\mathcal{P}(I), \subseteq)$

$\mathcal{F}$ defines a congruence on $\mathbf{U} = \prod_{i \in I} \mathbf{U}_i$ via $x \theta_{\mathcal{F}} y \iff \{i \in I : x_i = y_i\} \in \mathcal{F}$

$\mathbf{U}/\theta_{\mathcal{F}}$ is called a *reduced product*, denoted by $\prod_{\mathcal{F}} \mathbf{U}_i$

If $\mathcal{F}$ is an ultrafilter then $\mathbf{U}/\theta_{\mathcal{F}}$ is called an *ultraproduct*

$\mathsf{P}_u\mathcal{K}$ is the class of all ultraproducts of members of $\mathcal{K}$

$\mathcal{K}$ is *finitely axiomatizable* if $\mathcal{K} = \mathrm{Mod}(\phi)$ for a single formula ϕ

Prove (and extend) or disprove (and fix)

If $\mathcal{K} \models \phi$ then $\mathsf{P}_u\mathcal{K} \models \phi$ for any first order formula ϕ

If $\mathcal{K}$ is finitely axiomatizable then the complement of $\mathcal{K}$ is closed under ultraproducts

If $\mathcal{K}$ is a finite class of finite τ-structures then $\mathsf{P}_u\mathcal{K} = \mathcal{K}$

Congruence distributivity and Jónsson's Theorem

$\mathbf{A}$ is *congruence distributive* (CD) if $\mathrm{Con}(\mathbf{A})$ is a distributive lattice

A class $\mathcal{K}$ of algebras is *CD* if every algebra in $\mathcal{K}$ is CD

Theorem (Jónsson 1967)

If $\mathcal{V} = \mathsf{V}\mathcal{K}$ is congruence distributive then $\mathcal{V}_{\mathsf{SI}} \subseteq \mathsf{HSP}_u\mathcal{K}$

Prove (and extend) or disprove (and fix)

If $\mathcal{K}$ is a finite class of finite algebras and $\mathsf{V}\mathcal{K}$ is CD then $\mathcal{V}_{\mathsf{SI}} \subseteq \mathsf{HS}\mathcal{K}$

If $\mathbf{A}, \mathbf{B} \in \mathcal{V}_{\mathsf{SI}}$ are finite nonisomorphic and $\mathcal{V}$ is CD then $\mathsf{V}\mathbf{A} \neq \mathsf{V}\mathbf{B}$

$\mathcal{V}$ is *finitely generated* if $\mathcal{V} = \mathsf{V}\mathcal{K}$ for some finite class of finite algebras

Prove (and extend) or disprove (and fix)

A finitely generated CD variety has only finitely many subvarieties

Lattices of subvarieties

If $\mathcal{F}_\sigma \subset \mathcal{F}_\tau$ then the $\mathcal{F}_\sigma$-reduct of a τ-algebra $\mathbf{A}$ is $\mathbf{A}' = (A, (f^{\mathbf{A}})_{f \in \mathcal{F}_\sigma})$

Prove (and extend) or disprove (and fix)

If $\mathbf{A}'$ is a reduct of $\mathbf{A}$ then $\mathrm{Con}(\mathbf{A})$ is a sublattice of $\mathrm{Con}(\mathbf{A}')$

The variety of lattices is CD, so any variety of algebras with lattice reducts is CD

For a variety $\mathcal{V}$ the lattice of subvarieties is denoted by $\Lambda_{\mathcal{V}}$

The meet is $\bigcap$ and the join is $\sum_{i \in I} \mathcal{V}_i = \mathsf{V}(\bigcup_{i \in I} \mathcal{V}_i)$

Prove (and extend) or disprove (and fix)

For any variety $\mathcal{V}$, $\Lambda_{\mathcal{V}}$ is an algebraic lattice with compact elements = varieties that are finitely axiomatizable over $\mathcal{V}$

$\mathsf{HSP}_u(\mathcal{K} \cup \mathcal{L}) = \mathsf{HSP}_u\mathcal{K} \cup \mathsf{HSP}_u\mathcal{L}$ *for any classes $\mathcal{K}, \mathcal{L}$*

If $\mathcal{V}$ is CD then $\Lambda_{\mathcal{V}}$ is distributive and the map $\mathcal{V} \mapsto \mathcal{V}_{\mathsf{SI}}$ is a lattice embedding of $\Lambda_{\mathcal{V}}$ into "$\mathcal{P}(\mathcal{V}_{\mathsf{SI}})$" (unless $\mathcal{V}_{\mathsf{SI}}$ is a proper class)

Simple algebras and the discriminator

$\mathbf{A}$ is *simple* if $\mathrm{Con}(\mathbf{A}) = \{I_A, A^2\}$ i.e. has as few congruences as possible

Prove (and extend) or disprove (and fix)

Any simple algebra is subdirectly irreducible

$\mathbf{A}$ is a *discriminator algebra* if for some ternary term t
$\mathbf{A} \models x \neq y \Rightarrow t(x, y, z) = x$ and $t(x, x, z) = z$

Prove (and extend) or disprove (and fix)

Any subdirectly irreducible discriminator algebra is simple

$\mathcal{V}$ is a *discriminator variety* if $\mathcal{V}$ is generated by a class of discriminator algebras (for a fixed term t)

Unary discriminator in algebras with Boolean reduct

A *unary discriminator term* is a term d in an algebra $\mathbf{A}$ with a Boolean reduct such that $d(0) = 0$ and $x \neq 0 \Rightarrow d(x) = \top$

Prove (and extend) or disprove (and fix)

An algebra with a Boolean reduct is a discriminator algebra iff it has a unary discriminator term

[Hint: let $d(x) = t(0, x, \top)^-$ and $t(x, y, z) = x \cdot d(x^- \cdot y + x \cdot y^-) + z \cdot d(x^- \cdot y + x \cdot y^-)^-$]

In a concrete relation algebra the term $d(x) = \top;x;\top$ is a unary discriminator term

For a quantifier free formula ϕ we define a term ϕ^t inductively by $(r = s)^t = (r^- + s) \cdot (r + s^-)$, $\quad (\phi \text{ and } \psi)^t = \phi^t \cdot \psi^t$, $\quad (\neg\phi)^t = d((\phi^t)^-)$

Prove (and extend) or disprove (and fix)

In a discriminator algebra with Boolean reduct $\phi \Leftrightarrow (\phi^t = 1)$

Relation algebras are a discriminator variety

Let $\mathbf{A}a = (\downarrow a, +, 0, \cdot, a, {}^{-_a}, ;_a, 1\cdot a, {}^{\smile_a})$ be the *relative subalgebra* of relation algebra $\mathbf{A}$ with $a \in A$ where $x^{-_a} = x^- \cdot a$, $x;_a y = (x;y)\cdot a$, and $x^{\smile_a} = x^\smile \cdot a$

An element a in a relation algebra is an *ideal element* if $a = \top;a;\top$

Prove (and extend) or disprove (and fix)

$\mathbf{A}a$ is a relation algebra iff $a = a^\smile = a;a$

For any ideal element a the map $h(x) = (x\cdot a, x\cdot a^-)$ is an isomorphism from $\mathbf{A}$ to $\mathbf{A}a \times \mathbf{A}a^-$

A relation algebra is simple iff it is subdirectly irreducible
iff it is not directly decomposable
iff $0, \top$ are the only ideal elements
iff $\top;x;\top$ is a unary discriminator term

Representable relation algebras

The class RRA of *representable relation algebras* is $\mathrm{SP}\{\mathrm{Rel}(X) : X \text{ is a set}\}$

Prove (and extend) or disprove (and fix)

An algebra is in RRA iff it is embeddable in a concrete relation algebra

The class $\mathcal{K} = \mathrm{S}\{\mathrm{Rel}(X) : X \text{ is a set}\}$ is closed under H, S and $\mathrm{P_u}$

[Hint: $\mathrm{P_u S} \subseteq \mathrm{SP_u}$ so if $\mathbf{A} = \prod_{\mathcal{U}} \mathrm{Rel}(X_i)$ for some ultrafilter $\mathcal{U}$ over I, let $Y = \prod_{\mathcal{U}} X_i$, define $h : \mathbf{A} \to \mathrm{Rel}(Y)$ by $[x]h([R])[y] \Leftrightarrow \{i \in I : x_i R_i y_i\} \in \mathcal{U}$ and show h is a well defined embedding]

$\Rightarrow (\mathrm{V}\mathcal{K})_{\mathrm{SI}} \subseteq \mathcal{K}$ by Jónsson's Theorem

$\Rightarrow \mathrm{V}\mathcal{K} = \mathrm{SP}\mathcal{K} = \mathrm{RRA}$ by Birkoff's subdirect representation theorem

$\Rightarrow$ [Tarski 1955] RRA is a variety

Theorem

[Lyndon 1950] *There exist nonrepresentable relation algebras (i.e. $\notin$ RRA)*

[Monk 1969] RRA *is not finitely axiomatizable*

[Jonsson 1991] RRA *cannot be axiomatized with finitely many variables*

Outline of nonfinite axiomatizability: There is a sequence of finite relation algebras A_n with n atoms and the property that A_n is representable iff there exists a projective plane of order n

By a result of [Bruck and Ryser 1949] projective planes do not exist for infinitely many orders

The ultraproduct of the corresponding sequence of nonrepresentable A_n is representable, so the complement of RRA is not closed under ultraproducts

$\Rightarrow$ RRA is not finitely axiomatizable

Checking if a finite relation algebra is representable

Theorem (Lyndon 1950, Maddux 1983)

There is an algorithm that halts if a given finite relation algebra is not representable

Lyndon gives a recursive axiomatization for RRA

Maddux defines a sequence of varieties RA_n such that $\mathrm{RA} = \mathrm{RA}_4 \supset \mathrm{RA}_5 \supset \ldots \mathrm{RRA} = \bigcap_{n\geq 4} \mathrm{RA}_n$ and it is decidable if a finite algebra is in RA_n

Implemented as a GAP program [Jipsen 1993]

Comer's one-point extension method often gives sufficient conditions for representability; also implemented as a GAP program [J 1993]

Theorem (Hirsch Hodkinson 2001)

Representability is undecidable for finite relation algebras

Complex algebras

Let $\mathbf{U} = (U, T, ^\smile, E)$ be a structure with $T \subseteq U^3$, $^\smile : U \to U$, $E \subseteq U$

The *complex algebra* $\mathrm{Cm}(\mathbf{U})$ is $(\mathcal{P}(U), \cup, \emptyset, \cap, U, ^-, ;, ^\smile, 1)$ where $X;Y = \{z : (x, y, z) \in T \text{ for some } x \in X, y \in Y\}$, $X^\smile = \{x^\smile : x \in X\}$, and $1 = E$

Prove (and extend) or disprove (and fix)

$\mathrm{Cm}(\mathbf{U})$ *is a relation algebra iff* $x = y \Leftrightarrow \exists z \in E\ (x, z, y) \in T$, $(x, y, z) \in T \Leftrightarrow (x^\smile, z, y) \in T \Leftrightarrow (z, y^\smile, x) \in T$, *and* $(x, y, z) \in T$ and $(z, u, v) \in T \Rightarrow \exists w((x, w, v) \in T$ and $(y, v, w) \in T)$

An algebra $\mathbf{A} = (A, \circ, ^\smile, e)$ can be viewed as a structure $(A, T, ^\smile, E)$ where $T = \{(x, y, z) : x \circ y = z\}$ and $E = \{e\}$

Prove (and extend) or disprove (and fix)

$\mathrm{Cm}(\mathbf{A})$ *is a relation algebra iff* $\mathbf{A}$ *is a group*

Atom structures

$J(\mathbf{A})$ denotes the set of completely join irreducible elements of $\mathbf{A}$

Prove (and extend) or disprove (and fix)

In a Boolean algebra $J(\mathbf{A})$ *is the set of atoms of* $\mathbf{A}$

Every atomic BA is embeddable in $\mathcal{P}(J(\mathbf{A}))$ *via* $x \mapsto J(\mathbf{A}) \cap \downarrow x$

Every complete and atomic Boolean algebra is isomorphic to $\mathcal{P}(J(\mathbf{A}))$

The *atom structure* of an atomic relation algebra $\mathbf{A}$ is $(J(\mathbf{A}), ^\smile, T, E)$ where $T = \{(x, y, z) \in J(\mathbf{A}) : x;y \geq z\}$ and $E = J(\mathbf{A}) \cap \downarrow 1$

Prove (and extend) or disprove (and fix)

$\mathbf{U} = (U, ^\smile, T, E)$ *is the atom structure of some atomic relation algebra iff* $\mathrm{Cm}(\mathbf{U})$ *is a relation algebra*

If $\mathbf{A}$ *is complete and atomic then* $\mathrm{Cm}(J(\mathbf{A})) \cong \mathbf{A}$

Integral and finite relation algebras

A relation algebra is *integral* if $x;y = 0 \ \Rightarrow\ x = 0$ or $y = 0$

Prove (and extend) or disprove (and fix)

A relation algebra $\mathbf{A}$ *is integral iff* 1 *is an atom of* $\mathbf{A}$ *iff* $x \neq 0 \Rightarrow x;\top = \top$

Rel(2) has 4 atoms and is the smallest simple nonintegral relation algebra

Nonintegral RAs can often be decomposed into a "semidirect product" of integral algebras, so most work has been done on finite integral RAs

For finite relation algebras one usually works with the atom structure

$\mathrm{Rel}(\emptyset)$ is the one-element RA; generates the variety $\mathcal{O} = \mathrm{Mod}(0 = \top)$

$\mathrm{Rel}(1)$ is the two-element RA, with $1 = \top$, $x;y = x \cdot y$, $x^\smile = x$

It generates the variety $\mathcal{A}_1 = \mathrm{Mod}(1 = \top)$ of *Boolean relation algebras*

Varieties of small relation algebras

Define $x^s = x + x^{\smile}$ and let $\mathbf{A}^s$ have underlying set $A^s = \{x^s : x \in A\}$

A relation algebra $\mathbf{A}$ is *symmetric* if $x = x^{\smile}$ (iff $\mathbf{A}^s = \mathbf{A}$)

Prove (and extend) or disprove (and fix)

If $\mathbf{A}$ is commutative, then $\mathbf{A}^s$ is a subalgebra of $\mathbf{A}$
There are two RAs with 4 elements: $\mathbf{A}_2 = \mathrm{Cm}(\mathbb{Z}_2)$ and $\mathbf{A}_3 = (\mathrm{Cm}(\mathbb{Z}_3))^s$

The varieties generated by $\mathbf{A}_2$ and $\mathbf{A}_3$ are denoted $\mathcal{A}_2$ and $\mathcal{A}_3$

By Jónsson's Theorem $\mathcal{A}_1$, $\mathcal{A}_2$ and $\mathcal{A}_3$ are atoms of Λ_{RA}

Theorem (Jónsson)

Every nontrivial variety of relation algebras includes $\mathcal{A}_1$, $\mathcal{A}_2$ or $\mathcal{A}_3$

Group RAs and integral RAs of size 8

A complex algebra of a group is called a *group relation algebra*

GRA is the variety generated by all group relation algebras

Prove (and extend) or disprove (and fix)

If $\mathbf{U}$ is a group then $\mathrm{Cm}(\mathbf{U})$ is embedded in $\mathrm{Rel}(U)$ via Cayley's representation, given by $h(X) = \{(u, u \circ x) : u \in U, x \in X\}$

$\Rightarrow$ GRA is a subvariety of RRA

For an algebra $\mathbf{A}$ and $x \in A$, $\mathrm{Sg}^{\mathbf{A}}(x)$ is the subalgebra generated by x

There are 10 integral relation algebras with 8 elements, all 1-generated subalgebras of group relation algebras, hence representable

$\mathbf{B}_1 = \mathrm{Sg}^{\mathrm{Cm}\mathbb{Z}_4}\{2\}$	$\mathbf{B}_5 = \mathrm{Sg}^{\mathrm{Cm}\mathbb{Z}_5}\{1,4\}$	$\mathbf{C}_1 = \mathrm{Sg}^{\mathrm{Cm}\mathbb{Z}_7}\{1,2,4\}$
$\mathbf{B}_2 = \mathrm{Sg}^{\mathrm{Cm}\mathbb{Z}_6}\{2,4\}$	$\mathbf{B}_6 = \mathrm{Sg}^{\mathrm{Cm}\mathbb{Z}_8}\{1,4,7\}$	$\mathbf{C}_2 = \mathrm{Sg}^{\mathrm{Cm}\mathbb{Q}}\{r : r > 0\}$
$\mathbf{B}_3 = \mathrm{Sg}^{\mathrm{Cm}\mathbb{Z}_6}\{3\}$	$\mathbf{B}_7 = \mathrm{Sg}^{\mathrm{Cm}\mathbb{Z}_{12}}\{3,4,6,8,9\}$	$\mathbf{C}_3 = \mathrm{Cm}(\mathbb{Z}_3)$
$\mathbf{B}_4 = \mathrm{Sg}^{\mathrm{Cm}\mathbb{Z}_9}\{3,6\}$		

Integral relation algebras with 4 atoms

The 8-element integral RAs all have $\mathbf{A}_3$ as the only proper subalgebra

$\Rightarrow$ they generate join-irreducible varieties above $\mathcal{A}_3$

$\mathbf{B}_1, \ldots, \mathbf{B}_7$ are symmetric, $\mathbf{C}_1, \mathbf{C}_2, \mathbf{C}_3$ are nonsymmetric

[Comer] There are 102 integral 16-element RAs, not all representable

(65 are symmetric, and 37 are not)

[Jipsen Hertzel Kramer Maddux] 31 nonrepresentable (20 are symmetric)

Problem

What is the smallest representable RA that is not in GRA?
Is there one with 16 elements?

There are 34 candidates at `www.chapman.edu/~jipsen/gap/ramaddux.html` that are representable but not known to be group representable

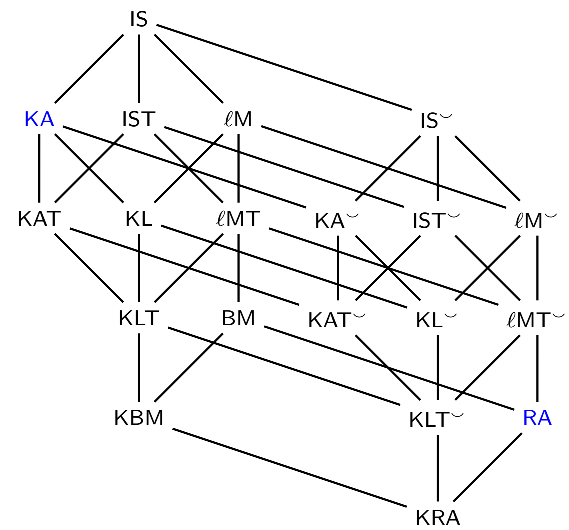
Summary of basic classes of structures

Qoset = *quasiordered sets* = sets with a reflexive and transitive relation
Poset = *partially ordered sets* = antisymmetric quosets
Equiv = *equivalence relations* = symmetric quosets
Sgrp = *semigroups* = associative groupoids
Bnd = *bands* = idempotent ($x + x = x$) semigroups
Slat = *semilattices* = commutative bands
JSlat = *join-semilattices* = semilattices with $x \le y \Leftrightarrow x + y = y$
Lat = *lattices* = two semilattices with absorption laws
Mon = *monoids* = semigroups with identity $x \cdot 1 = x = 1 \cdot x$
$\mathrm{Mon}^{\smile}$ = *involutive monoids* = monoids with $x^{\smile\smile} = x$, $(x{\cdot}y)^{\smile} = y^{\smile}{\cdot}x^{\smile}$
Grp = *groups* = involutive monoids with $x^{\smile} \cdot x = 1$
JSLat_0 = *join-semilattices with identity* $x + 0 = x$
$\mathrm{Lat}_{0\top}$ = *bounded lattices* = lattices with $x + 0 = x$ and $x{\cdot}\top = \top$
Lat^{-} = *complemented lattices* = $\mathrm{Lat}_{0\top}$ with $x + x^{-} = \top$ and $x{\cdot}x^{-} = 0$
DLat = *distributive lattices* = lattices with $x{\cdot}(y + z) = x{\cdot}y + x{\cdot}z$
BA = *Boolean algebras* = complemented distributive lattices

Some prominent subclasses of semirings

Srng = *semirings* = monoids distributing over commutative monoids and 0
IS = *(additively) idempotent semirings* = semirings with $x + x = x$
ℓM = *lattice-ordered monoids* = idempotent semirings with meet
RL = *residuated lattices* = ℓ-monoids with residuals
KA = *Kleene algebra* = idempotent semiring with *, unfold and induction
KA* = *$*$-continuous Kleene algebra* = KA with ...
KAT = *Kleene algebras with tests* = KA with Boolean subalgebra ≤ 1
KAD = *Kleene algebras with domain*
KL = *Kleene lattices* = Kleene algebras with meet
BM = *Boolean monoids* = distributive ℓ-monoids with complements
KBM = *Kleene Boolean monoids* = Boolean monids with Kleene-$*$
RA = *relation algebras* = Boolean monoids with involution and residuals
KRA = *Kleene relation algebras* = relation algebras with Kleene-$*$
RRA = *representable relation algebras* = concrete relation algebras
RKRA = *representable Kleene relation algebras* = RRA with Kleene-$*$

Subclasses from combinations of *, tests, meet, $^-$, $^\smile$



A = Algebra
B = Boolean
I = Idempotent
K = Kleene
L = Lattice
ℓ = lattice-ordered
M = Monoid
R = Relation
S = Semiring
T = with tests
$^\smile$ = with converse

Many, but not all, of these classes are varieties

Recall that quasivarietes are classes defined by implications of equations

Most notably, Kleene algebras and some of its subclasses are quasivarieties

In general, implications are not preserved by homomorphic images

To see that KA is not a variety, find an algebra in H(KA) $\setminus$ KA

Prove (and extend) or disprove (and fix)

Let $\mathbf{A}$ *be the powerset Kleene algebra of* $(\mathbb{N}, +, 0)$ *and let* θ *be the equivalence relation on* A *with blocks* $\{\emptyset\}$, $\{\{0\}\}$, $\{$*all finite sets* $\neq \{0\}, \emptyset\}$ *and* $\{$*all infinite subsets*$\}$*. Then* θ *is a congruence, but* $\mathbf{A}/\theta$ *is not a Kleene algebra.*

Theorem (Mal'cev)

A class $\mathcal{K}$ *is a quasivariety iff it is closed under* S, P *and* P_u
The smallest quasivariety containing $\mathcal{K}$ *is* $\mathrm{Q}\mathcal{K} = \mathrm{SPP}_u\mathcal{K}$

Free algebras

Let $\mathcal{K}$ be a class and let $\mathbf{F}$ be an algebra that is *generated* by a set $X \subseteq F$ (i.e. $\mathbf{F}$ has no proper subalgebra that contains X)

$\mathbf{F}$ is *$\mathcal{K}$-freely generated* by X if any $f : X \to \mathbf{A} \in \mathcal{K}$ extends to a homomorphism $\hat{f} : \mathbf{F} \to \mathbf{A}$

If also $\mathbf{F} \in \mathcal{K}$ then $\mathbf{F}$ is the *$\mathcal{K}$-free algebra on X* and is denoted by $\mathbf{F}_{\mathcal{K}}(X)$.

Prove (and extend) or disprove (and fix)

If $\mathcal{K}$ *is the class of all* τ*-algebras then the term algebra* $\mathbf{T}_\tau(X)$ *is the* $\mathcal{K}$*-free algebra on* X

If $\mathcal{K}$ *is any class of* τ*-algebras, let* $\theta_{\mathcal{K}} = \bigcap\{\ker h \mid h : \mathbf{T}_\tau(X) \to \mathbf{A}$ *is a homomorphism,* $\mathbf{A} \in \mathcal{K}\}$*. Then* $\mathbf{F} = \mathbf{T}_\tau(X)/\theta_{\mathcal{K}}$ *is* $\mathcal{K}$*-freely generated and if* $\mathcal{K}$ *is closed under subdirect products, then* $\mathbf{F} \in \mathcal{K}$

$\Rightarrow$ free algebras exist in all (quasi)varieties (since they are S, P closed)

Examples of free algebras

A free algebra on m generators satisfies only those equations with $\leq m$ variables that hold in all members of $\mathcal{K}$

$\mathbf{F}_{\mathsf{Sgrp}}(X) \cong \bigcup_{n\geq 1} X^n \qquad \mathbf{F}_{\mathsf{Mon}}(X) \cong \bigcup_{n\geq 0} X^n \qquad x \mapsto (x)$

These sets of n-tuples are usually denoted by X^+ and X^*

$\mathbf{F}_{\mathsf{Slat}}(X) \cong \mathcal{P}_{\mathrm{fin}}(X) \setminus \{\emptyset\} \qquad \mathbf{F}_{\mathsf{Slat}_0}(X) \cong \mathcal{P}_{\mathrm{fin}}(X) \qquad x \mapsto \{x\}$

$\mathbf{F}_{\mathsf{Srng}}(X) \cong \{\text{finite multisets of } X^*\} \qquad \mathbf{F}_{\mathsf{IS}}(X) \cong \mathcal{P}_{\mathrm{fin}}(X^*)$

Prove (and extend) or disprove (and fix)

If equality between elements of all finitely generated free algebras is decidable, then the equational theory is decidable

$\Rightarrow$ the equational theories of Sgrp, Mon, Slat, Srng, IS are decidable

Free distributive lattices and Boolean algebras

The free algebras for DLat and BA are also easy to describe

$\mathbf{F}_{\mathsf{DLat}}(X) \cong \mathrm{Sg}^{\boldsymbol{\mathcal{P}}(\mathcal{P}(X))}_{\mathsf{DLat}}(h[X])$

$\mathbf{F}_{\mathsf{BA}}(X) \cong \mathrm{Sg}^{\boldsymbol{\mathcal{P}}(\mathcal{P}(X))}_{\mathsf{BA}}(h[X])$

where in both cases $h(x) = \{Y \in \mathcal{P}(X) : x \in Y\}$ and $x \mapsto h(x)$

For finite X, the free BA is actually isomorphic to $\boldsymbol{\mathcal{P}}(\mathcal{P}(X))$

For lattices, the free algebra on > 3 generators is infinite but the equational theory is still decidable [Skolem 1928] (in polynomial time)

Kleene algebras and regular sets

Deciding equations in KA is also possible, but takes a bit more work

Let Σ be a finite set, called an *alphabet*

The *free monoid generated by* Σ is $\boldsymbol{\Sigma}^* = (\Sigma^*, \cdot, \varepsilon)$

Here ε is the empty sequence (), and $\cdot$ is concatenation

The *Kleene algebra of regular sets* is $\mathcal{R}_\Sigma = \mathrm{Sg}^{\boldsymbol{\mathcal{P}}(\Sigma^*)}_{\mathsf{KA}}(\{\{(x)\} : x \in \Sigma\})$

Theorem (Kozen 1994)

$\mathcal{R}_\Sigma$ is the free Kleene algebra on Σ

In particular, a *regular set* is the image of a KA term

So deciding if $(s = t) \in \mathrm{Th}_e(KA)$ is equivalent to checking if two regular sets are equal

Membership in regular sets can be determined by finite automata

Automata

A *Σ-automaton* is a structure $\mathbf{U} = (U, (a^{\mathbf{U}})_{a\in\Sigma}, S, T)$ such that $a^{\mathbf{U}}$ is a binary relation for each $a \in \Sigma$ and S, T are unary relations.

Elements of U, S, T are called *states*, *start states* and *terminal states* respectively

For $w \in \Sigma^*$ define $w^{\mathbf{U}}$ by $\varepsilon^{\mathbf{U}} = I_U$ and $(a \cdot w)^{\mathbf{U}} = a^{\mathbf{U}} ; w^{\mathbf{U}}$

The *language recognized* by $\mathbf{U}$ is $L(\mathbf{U}) = \{w \in \Sigma^* : w^{\mathbf{U}} \cap (S \times T) \neq \emptyset\}$

Rec_Σ is the set of all languages recognized by some Σ-automaton

Prove (and extend) or disprove (and fix)

$\emptyset$, $\{\varepsilon\}$, $\{a\} \in \mathrm{Rec}_\Sigma$ *for all* $a \in \Sigma$

Regular sets are recognizable

A finite automaton can be viewed as a directed graph with states as nodes and an arrow labelled a from u_i to u_j iff $(u_i, u_j) \in a^{\mathbf{U}}$

Given automata $\mathbf{U}, \mathbf{V}$, define $\mathbf{U} + \mathbf{V}$ to be the disjoint union of $\mathbf{U}, \mathbf{V}$

$\mathbf{U}; \mathbf{V} = (U \uplus V, (a^{\mathbf{U}} \uplus a^{\mathbf{V}} \uplus (a^{\mathbf{U}} T^{\mathbf{U}} \times S^{\mathbf{V}}))_{a \in \Sigma}, S', T^{\mathbf{V}})$ where

$S' = \begin{cases} S^{\mathbf{U}} & \text{if} S^{\mathbf{U}} \cap T^{\mathbf{U}} = \emptyset \\ S^{\mathbf{U}} \cup S^{\mathbf{V}} & \text{otherwise} \end{cases}$ and

$a^{\mathbf{U}} T^{\mathbf{U}} = \{u : \exists v (u, v) \in a^{\mathbf{U}}, v \in T^{\mathbf{U}}\}$

$\mathbf{U}^+ = (U, (a^{\mathbf{U}} \uplus (a^{\mathbf{U}} T^{\mathbf{U}} \times S^{\mathbf{U}}))_{a \in \Sigma}, S^{\mathbf{U}}, T^{\mathbf{U}})$

Prove (and extend) or disprove (and fix)

$L(\mathbf{U} + \mathbf{V}) = L(\mathbf{U}) \cup L(\mathbf{V})$, $L(\mathbf{U}; \mathbf{V}) = L(\mathbf{U}); L(\mathbf{V})$, and $L(\mathbf{U}^+) = L(\mathbf{U})^+$

$\Rightarrow$ every regular set is recognized by some finite automaton

Matrices in semirings and Kleene algebras

For a semiring $\mathbf{A}$, let $M_n(A) = A^{n \times n}$ be the set of $n \times n$ matrices over $\mathbf{A}$

$M_n(\mathbf{A})$ is again a semiring with usual matrix addition and multiplication

$\mathbf{0}$ is the zero matrix, and I_n is the identity matrix

If A is a Kleene algebra and $M = \left[\begin{array}{c|c} N & P \\ \hline Q & R \end{array}\right] \in M_n(A)$ define

$M^* = \left[\begin{array}{c|c} (N + PR^*Q)^* & N^*P(R + QN^*P)^* \\ \hline R^*Q(N + PR^*Q)^* & (R + QN^*P)^* \end{array}\right]$

This is motivated by the diagram:

Prove (and extend) or disprove (and fix)

The definition of M^* is independent of the chosen decomposition

If $\mathbf{A}$ is a Kleene algebra, so is $M_n(\mathbf{A})$

Finite automata as matrices

Given $\mathbf{U} = (U, (a^{\mathbf{U}})_{a \in \Sigma}, S, T)$ with $U = \{u_1, \ldots, u_n\}$ let (s, M, t) be a $0,1$-row n-vector, an $n \times n$ matrix and a $0,1$-column n-vector where

$s_i = 1 \Leftrightarrow u_i \in S$, $M_{ij} = \sum\{a : (u_i, u_j) \in a^{\mathbf{U}}\}$, and $t_i = 1 \Leftrightarrow u_i \in T$

Prove (and extend) or disprove (and fix)

$L(\mathbf{U}) = h(s; M; t)$ where $h : \mathbf{T}_{\mathsf{KA}}(\Sigma) \to \mathcal{R}_\Sigma$ is induced by $h(x) = \{(x)\}$

$\Rightarrow$ every recognizable language is a regular set [Kleene 1956]

But many different automata may correspond to the same regular set

$\mathbf{U}$ is a *deterministic* automaton if each $a^{\mathbf{U}}$ is a function on U and S is a singleton set

Prove (and extend) or disprove (and fix)

Any nondeterministic automaton $\mathbf{U}$ can be converted to a deterministic one $\mathbf{U}'$ with $U' = \mathcal{P}(U)$, $a'(X) = \{v : (u, v) \in a^{\mathbf{U}}$ for some $u \in X\}$, $S' = \{S\}$ and $T' = \{X : X \cap T \neq \emptyset\}$ such that $L(\mathbf{U}') = L(\mathbf{U})$

Minimal automata

A state v is *accessible* if $(u, v) \in w^{\mathbf{U}}$ for some $u \in S$ and $w \in \Sigma^*$

In a deterministic automaton, the accessible states are the subalgebra generated from the start state

Theorem (Myhill, Nerode 1958)

Given a deterministic automaton $\mathbf{U}$ with no inaccessible states, the relation $u\theta v$ iff $\forall w \in \Sigma^*\ w(u) \in T \Leftrightarrow w(v) \in T$ is a congruence on the automaton and $L(\mathbf{U}/\theta) = L(\mathbf{U})$

An automaton is minimal if all states are accessible and the congruence θ defined in the preceding theorem is the identity relation

Prove (and extend) or disprove (and fix)

Let $\mathbf{U}, \mathbf{V}$ be minimal automata. Then $L(\mathbf{U}) = L(\mathbf{V})$ iff $\mathbf{U} \cong \mathbf{V}$.

$\Rightarrow$ The equational theory of Kleene algebras is decidable

Try it in JFLAP: An Interactive Formal Languages and Automata Package

Th_q((idempotent)semirings) is undecidable

Theorem (Post 1947, Markov 1949)

The quasiequational theory of semigroups is undecidable

For a semigroup $\mathbf{A}$, let $\mathbf{A}_1$ be the monoid obtained by adjoining 1

Prove (and extend) or disprove (and fix)

Any semigroup $\mathbf{A}$ is a subalgebra of the ;-reduct of $\mathcal{P}(\mathbf{A})$

If $\mathcal{K} = \{$;-reducts of semirings$\}$ then $\mathsf{S}\mathcal{K}$ = the class of semigroups

A quasiequation that uses only ; holds in $\mathcal{K}$ iff it holds in all semigroups

$\Rightarrow$ the quasiequational theory of (idempotent) semirings is undecidable

Since $\mathcal{P}(\mathbf{A})$ is a reduct of KA, KAT, KAD, BM the same result holds

The equational theory of RA is undecidable

Prove (and extend) or disprove (and fix)

For any semigroup $\mathbf{A}$, the monoid $\mathbf{A}_1$ is embedded in the ;-reduct of $\mathrm{Rel}(A_1)$ via the Cayley map $x \mapsto \{(x, xy) : y \in A_1\}$

If $\mathcal{K} = \{$;-reducts of simple RAs$\}$ then $\mathsf{S}\mathcal{K}$ = the class of semigroups

The quasiequational theory of $\mathrm{RA}_{\mathrm{SI}}$, RA and RRA is undecidable

RA is a discriminator variety, hence any quasiequation (in fact any quantifier free formula) ϕ can be translated into an equation $\phi^t = 1$ which holds in RA iff ϕ holds in $\mathrm{RA}_{\mathrm{SI}}$

$\Rightarrow$ $\mathrm{Th}_e(\mathrm{RA})$ is undecidable

Undecidability is pervasive in Λ_{RA}

Theorem (Andréka Givant Nemeti 1997)

If $\mathcal{K} \subseteq$RA such that for each $n \geq 1$ there is an algebra in $\mathcal{K}_{\mathrm{SI}}$ with at least n elements below the identity then $\mathrm{Th}_e\mathcal{K}$ is undecidable

If $\mathcal{K} \subseteq$RA such that for each $n \geq 1$ there is an algebra in $\mathcal{K}$ with a subset of at least n pairwise disjoint elements that form a group under ; and $^\smile$ then $\mathrm{Th}_e\mathcal{K}$ is undecidable

Prove (and extend) or disprove (and fix)

The varieties of integral RAs, symmetric RAs and group relation algebras are undecidable

Summary of decidability and other properties

	Th_e dec	Th_q dec	Th dec	Var	CD	loc fin
Sgrp, Mon	✓	×	×	✓	×	×
Slat	✓	✓	×	✓	×	✓
Lat	✓	✓	×	✓	✓	×
DLat	✓	✓	×	✓	✓	✓
BA	✓	✓	✓	✓	✓	✓
Grp	✓	×	×	✓	×	×
Srng	✓	×	×	✓	×	×
IS	✓	×	×	✓	×	×
KA, KAT	✓	×	×	×	×	×
KAD		×	×	×	×	×
RsKA		×	×	✓	✓	×
RsL	✓	×	×	✓	✓	×
BM	×	×	×	✓	✓	×
RA	×	×	×	✓	✓	×
RRA	×	×	×	✓	✓	×
KRA	×	×	×	✓	✓	×

Categories

A *category* is a structure $\mathbf{C} = (C, O, \circ, 1, \text{dom}, \text{cod})$ such that

- C is a class of *morphisms*, O is a class of *objects*, $\text{dom}, \text{cod} : C \to O$ give the *domain* and *codomain*, $1 : O \to C$ gives an *identity morphism*, and *composition* $\circ$ is a partial binary operation on C
- $1(X)$ is denoted 1_X, $f : X \to Y$ means $\text{dom}f = X$ and $\text{cod}f = Y$
- $g \circ f$ exists iff $\text{dom}g = \text{cod}f$, in which case $\text{dom}(g \circ f) = \text{dom}f$, $\text{cod}(g \circ f) = \text{cod}g$ and if $\text{dom}g = \text{cod}h$ then $(f \circ g) \circ h = f \circ (g \circ h)$
- $\text{dom}1_X = X = \text{cod}1_X$, $1_{\text{dom}f} \circ f = f$ and $f \circ 1_{\text{cod}f} = f$
- The class $\text{Hom}(X, Y) = \{f : \text{dom}f = X \text{ and } \text{cod}f = Y\}$ is a set

Set is a category with sets as objects and functions as morphisms

Rel is a category with sets as objects and binary relations as morphisms

Functors

Category theory is well suited for relating areas of mathematics

Functors are structure preserving maps (homomorphisms) of categories

For categories $\mathbf{C}, \mathbf{D}$ a *covariant functor* $\mathbf{F} : \mathbf{C} \to \mathbf{D}$ maps $C \to D$ and $O^{\mathbf{C}} \to O^{\mathbf{D}}$ such that

- $\mathbf{F}(1_X) = 1_{\mathbf{F}X}$ and if $f : X \to Y$ then $\mathbf{F}f : \mathbf{F}X \to \mathbf{F}Y$
- if $f : X \to Y$, $g : Y \to Z$ then $\mathbf{F}(g \circ f) = \mathbf{F}g \circ \mathbf{F}f$

For a *contravariant functor* $\mathbf{F} : \mathbf{C} \to \mathbf{D}$ the definition becomes

- $\mathbf{F}(1_X) = 1_{\mathbf{F}X}$ and if $f : X \to Y$ then $\mathbf{F}f : \mathbf{F}Y \to \mathbf{F}X$
- if $f : X \to Y$, $g : Y \to Z$ then $\mathbf{F}(g \circ f) = \mathbf{F}f \circ \mathbf{F}g$

Prove (and extend) or disprove (and fix)

A category with one object is (equivalent to) a monoid, and covariant functors between such categories are monoid homomorphisms

Heterogeneous relation algebras

The category **Rel** of typed binary relations is usually enriched by adding converse and Boolean operation on the sets $\text{Hom}(X, Y)$

In this setting it is also natural to write composition $S \circ R$ as $R;S$

A *heterogeneous relation algebra* (HRA) is a structure $\mathbf{C} = (C, O, ;, 1, \text{dom}, \text{cod}, ^{\smile}, +, \top, \cdot, 0, ^{-})$ such that

- $(C, O, ;, 1, \text{dom}, \text{cod})$ is a category
- $^{\smile} : \text{Hom}(x, y) \to \text{Hom}(y, x)$ satisfies $r^{\smile\smile} = r$, $1_x^{\smile} = 1_x$, $(r;s)^{\smile} = s^{\smile};r^{\smile}$
- for all objects x, y, $(\text{Hom}(x, y), +, \top, \cdot, 0, ^{-})$ is a Boolean algebra and
- for all $r;s, t \in \text{Hom}(x, y)$, $(r;s)\cdot t = 0 \Leftrightarrow (r^{\smile};t)\cdot s = 0 \Leftrightarrow (t;s^{\smile})\cdot r = 0$

Prove (and extend) or disprove (and fix)

Relation algebras are (equivalent to) HRAs with one object

Other enriched categories

Suitably weakening the axioms of HRAs (see e.g. [Kahl 2004]) gives
ordered categories (with converse)
(join/meet)-semilattice categories
(idempotent) semiring categories
Kleene categories (with tests)
(distributive/division) allegories

Given a semiring $(A, +, \cdot)$, the set $\text{Mat}(A) = \{A^{m\times n} : m, n \geq 1\}$ of all matrices over A is an important example of a semiring category, with matrix multiplication as composition

The categorical approach is helpful in applications since it matches well with typed specification languages

Conclusion

The foundations of relation algebras and Kleene algebras span a substantial part of algebra, logic and computer science

Here we have only been able to mention some of the basics, with an emphasis on concepts from universal algebra

Participants are encouraged to read further in some of the primary sources and excellent expository works, some of which are listed below

[The following pages have at least one (intensionally) false statement in the "Prove or disprove" box(es): 8, 10, 11, 23, 36, 37, 49]

The "Prove (and extend) or disprove (and fix)" format is from Ed Burger's book "Extending the Frontiers of Mathematics: Inquiries into argumentation and proof", Key College Press, 2006

References and further reading I

[Andreka Givant Nemeti 1994] *The lattice of varieties of representable relation algebras*, J. Symbolic Logic

[Andreka Givant Nemeti 1997] *Decision problems for equational theories of relation algebras*, Memoirs AMS

[Berghammer Möller Struth (Eds) 2004] *Relational and Kleene-algebraic Methods in Computer Science*, LNCS 3051, Springer

[Birkhoff 1935] *On the structure of abstract algebras*, Proc. Camb. Phil. Soc.

[Birkhoff 1944] *Subdirect unions in universal algebra*, Bull. AMS

[Brink Kahl Schmidt (Eds) 1997] *Relational Methods in Computer Science*, Springer

[Burris Sankappanavar 1981] *A course in universal algebra*, Springer, online

[Conway 1971] *Regular algebra and finite machines*, Chapman and Hall

[Desharnais Möller Struth 2003] *Kleene algebras with domain*, online

[Desharnais Möller Struth 2004] *Modal Kleene algebras and applications*, JoRMiCS, online

[Hirsch Hodkinson 2001] *Representability is not decidable for finite relation algebras*, Trans. AMS

[Hirsch Hodkinson 2002] *Relation algebras by games*, North-Holland

[Hodkinson Mikulas Venema 2001] *Axiomatizing complex algebras by games*, Algebra Universalis

References and further reading II

[Jipsen 1993] *Discriminator varieties of Boolean algebras with residuated operators*, in "Algebraic Logic", Banach Center Publ., online

[Jipsen 2004] *From semirings to residuated Kleene lattices*, Studia Logica, online

[Jipsen Lukács 1994] *Minimal relation algebras*, Algebra Universalis

[Jipsen Maddux 1997] *Nonrepresentable sequential algebras*, J. IGPL, online

[Jipsen Tsinakis 2002] *A survey of residuated lattices*, in "Ordered algebraic structures", Kluwer, online

[Jónsson 1967] *Algebras whose congruence lattices are distributive*, Math Scand.

[Jónsson 1982] *Varieties of relation algebras*, Algebra Universalis

[Jónsson 1991] *The theory of binary relations*, in "Algebraic Logic", North-Holland

[Jonsson Tarski 1951/2] *Boolean algebras with operators I, II*, Amer. J. Math.

[Kahl 2004] *Refactoring heterogeneous relation algebras around ordered categories and converse*, JoRMiCS, online

[Kozen 1994] *A completeness theorem for Kleene algebras and the algebra of regular events*, Infor. and Comput., online

[Kozen 1994] *On action algebras*, in "Logic and Information Flow", MIT Press, online

[Kozen 1997] *Automata and computability*, Springer

References and further reading III

[Kozen 2003] *Automata on guarded strings and applications*, Matémat. Contemp., online

[Kozen and Smith 1996] *Kleene algebras with test: Completeness and decidability*, in LNCS 1258, Springer, online

[Maddux 1982] *Some varieties containing relation algebras*, Trans. AMS

[Maddux 1983] *A sequent calculus for relation algebras*, Ann. Pure and Appl. Logic

[Maddux 1985] *Finite integral relation algebras*, in LNM 1149, Springer

[Maddux 2006] *Relation algebras*, Elsevier

[Markov 1949] *The impossibility of certain algorithms in the theory of associative systems. II.* Doklady Akad. Nauk SSSR

[Post 1947] *Recursive unsolvability of a problem of Thue*, J. Symbolic Logic

[Pratt 1990] *Dynamic algebras as a well-behaved fragment of relation algebras*, in LNCS 425, Springer, online

[Pratt 1990] *Action logic and pure induction*, in LNCS 478, Springer, online

[Tarski 1946] *A remark on functionally free algebras*, Ann. Math.

[Tarski 1955] *Contributions to the theory of models III*, Konin. Nederl. Akad. Weten. Proc.