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, x₁, . . . variables (implicitly universally quantified)

X, Y, Z, X₁, . . . set variables (implicitly universally quantified)

f, g, h, f₁, . . . function variables

a, b, c, a₁, . . . constants

i, j, k, i₁, . . . integer variables, usually nonnegative

m, n, n₁, . . . 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 \(uRv\)
Define \(uR = \{v : uRv\}\) and \(Rv = \{u : uRv\}\)

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 \(xR\) 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)

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 \(R^\sim = \{(v,u) : (u,v) \in R\}\)

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 in relational form

Prove (and extend) or disprove (and fix)

\(R\) is reflexive \iff \(I_U \subseteq R\)
\(R\) is irreflexive \iff \(I_U \nsubseteq R\)
\(R\) is symmetric \iff \(R \subseteq R^\sim\) \iff \(R = R^\sim\)
\(R\) is antisymmetric \iff \(R \cap R^\sim = I_U\)
\(R\) is transitive \iff \(R; R = R\) \iff \(R = R^+\)
\(R\) is univalent \iff \(R; R^\sim \subseteq I_U\)
\(R\) is total \iff \(I_U \subseteq R; R^\sim\)
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

⇒ 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

⇒ 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 \( a < b \)) 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 \( a < b \)

Nonisomorphic connected posets with \( \leq 4 \) elements
Equivalence relations
An \textit{equivalence relation} is a reflexive symmetric transitive relation

Prove (and extend) or disprove (and fix)

\( R \) is an equivalence relation on \( U \) iff \( I_U \subseteq R = R^\sim; R \)

Let \( R \) be an equivalence relation on a set \( U \), and \( u \in U \)
Then \( uR = \{x : uRx\} \) is called an \textit{equivalence class} of \( R \)

Usually written \([u]_R\) or simply \([u]\); \( u \) is called a \textit{representative} of \([u]\)

The \textit{set of all equivalence classes} of \( R \) is \( U/R = \{[u] : u \in U\} \)

Partitions
A \textit{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 \( \equiv_P \).

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 \textit{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.

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

Nonisomorphic connected qosets on 4 elements

\[ \begin{align*}
\text{Posets} & \quad \text{Subrel} & \quad \text{Eqvrel} \\
\text{Id rels} & \quad \text{All rels} \\
\text{Antisym rels} & \quad \text{Reflexive rels} \\
\text{Sym rels} & \quad \text{Transitive rels}
\end{align*} \]
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, \(\prod_{i\in I}U_i\) is the set 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 \(U = (U,(f^U)_{f\in F_\tau},(R^U)_{R\in R_\tau})\)

- \(U\) is the underlying set
- \(F_\tau\) is a set of operation symbols
- \(R_\tau\) is a set of relation symbols (disjoint from \(F_\tau\))

The type \(\tau : F_\tau \cup R_\tau \to \{0,1,2,\ldots\}\) gives the arity of each symbol \(f^U : U^{|f|} \to U\) and \(R^U \subseteq U^{|R|}\) are the interpretation of symbol \(f\) and \(R\)

0-ary operation symbols are called constant symbols

\(U\) is a (universal) algebra if \(R_\tau = \emptyset\); use \(A,B,C\) for algebras

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

The superscript \(^U\) 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 \((A,\cdot,\sim)\) such that \(\sim\) has period two: \(x\sim\sim = x\), and \(\sim\) antidistributes over \(\cdot\): \((x\cdot y)\sim = y\sim \cdot x\sim\)

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 \(1\sim = 1\) and \(1\cdot x = x\)

An involutive monoid is a monoid with an involution

A group is an involutive monoid such that \(x \cdot x\sim = 1\)

Join-semilattices

A semilattice is a commutative idempotent semigroup

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

Prove (and extend) or disprove (and fix)

\((A,+,\leq)\) is a join-semilattice

iff \((A,\leq)\) is a poset and \(x + y = z \iff \forall w(x \leq w \text{ and } y \leq w \iff z \leq w)\)

iff \((A,\leq)\) is a poset and \(x + y \leq z \iff x \leq z \text{ and } y \leq z\)

\(\Rightarrow\) any two elements \(x,y\) have a least upper bound \(x + y\)

Which of the following are join-semilattices?

Nonisomorphic connected posets with \(\leq 4\) elements

\[\begin{array}{cccc}
   & V & N & A \\
   \downarrow & V & N & A \\
   \downarrow & V & N & A \\
   \downarrow & V & N & A \\
   \end{array}\]
Lattices and duals

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

\((A, +, \cdot)\) 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 \(x \leq y \iff x + y = y\).

Define \(x \geq y \iff y \leq x\). 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.

Complementation and Boolean algebras

\((A, +, 0, \cdot, 1, \land, \lor, \lnot)\) is a **lattice with complementation** if \((A, +, 0, \cdot, 1)\) is a bounded lattice such that \(x + x^\lor = 1\) and \(x \cdot x^\lor = 0\)

**Prove (and extend) or disprove (and fix)**

Lattices with complementation satisfy \(x^{\lor \lor} = x\) and DeMorgan’s laws

\((x + y)^\lor = x^\lor \cdot y^\lor\) and \((x \cdot y)^\lor = x^\lor + y^\lor\)

A **Boolean algebra** is a distributive lattice with complementation

**Prove (and extend) or disprove (and fix)**

Boolean algebras satisfy \(x^{\lor \lor} = x\) and DeMorgan’s laws

\((x + y)^\lor = x^\lor \cdot y^\lor\) and \((x \cdot y)^\lor = x^\lor + y^\lor\)

**Prove (and extend) or disprove (and fix)**

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

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 \((x + y) \cdot (x + z) = (x + y) \cdot (x + z)\) iff \((x + y) \cdot (x + z) = (x + y) \cdot (x + z) + (y \cdot z)\)

⇒ a lattice is distributive iff its dual is distributive

A **semilattice with identity** is a commutative idempotent monoid

\((A, +, 0, \cdot, 1)\) is a bounded lattice if \((A, +, \cdot)\) is a lattice and \((A, +, 0)\) are semilattices with identity

**Prove (and extend) or disprove (and fix)**

Suppose \((A, +, \cdot)\) is a lattice. Then \((A, +, 0, \cdot, 1)\) is a bounded lattice iff \(0 \leq x \leq 1\) iff \(x \cdot 0 = 0\) and \(x + 1 = 1\)

Boolean algebras of sets

\(\mathcal{P}(U) = (\mathcal{P}(U), \cup, \emptyset, \cap, U, \setminus)\) 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 \(\cup, \cap, \setminus\)

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 \(U\)

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

An (abstract) relation algebra is of the form $(A, +, 0, \cdot , T, \neg , ;, 1, \vdash )$ where

- $(A, +, 0, \cdot , T, \neg )$ is a Boolean algebra
- $(A, ;, 1)$ is a monoid
- $(x;y) \cdot z = 0 \iff (x\vdash z) \cdot y = 0 \iff (z;y) \cdot x = 0$

The last line states the Schröder equivalences (or De Morgan’s Thm K)

Prove (and extend) or disprove (and fix)

In a relation algebra $x \vdash \vdash = x$ and $\neg$ is self-conjugated, i.e.

$x \neg \cdot y = 0 \iff x \cdot y \neg = 0$. Hence $(x + y) \neg = x \neg + y \neg$, $x \neg \neg = x \neg \neg$, $(x \cdot y) \neg = x \neg \cdot y \neg$, $\neg$ is an involution and $x \vdash (y + z) = x \cdot y + x \cdot z$.

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

Prove (and extend) or disprove (and fix)

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

Concrete relation algebras

Rel$(U) = (\mathcal{P}(U^2), \cup, \emptyset, U^2, \neg , ;, I_U, \vdash)$ the square relation algebra on $U$

A concrete relation algebra is of the form $(C, \cup, \cap, \emptyset, T, \neg , ;, I_U, \vdash)$ where $C$ is a set of binary relations on a set $U$ that is closed under the operations $\cup, \neg , ;, \vdash$, 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
- $x(y + z) = (x;y) + (x;z)$, $(x + y)z = (x;z) + (y;z)$
- $x;0 = 0 = 0;x$

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

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

Prove (and extend) or disprove (and fix)

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

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

Kleene algebras

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

- $(A, +, 0, ;, 1)$ is an idempotent semiring
- $1 + x + x^\ast x^\ast = x^\ast$
- $x; y \leq y \Rightarrow x^\ast . y \leq y$ (where $x \leq y \iff x + y = y$)
- $y; x \leq y \Rightarrow y; x^\ast \leq y$

Prove (and extend) or disprove (and fix)

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

Prove (and extend) or disprove (and fix)

For any set $U$, KRel$(U) = (\mathcal{P}(U^2), \cup, \emptyset , ;, I_U, \vdash)$ 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

<table>
<thead>
<tr>
<th>Prove (and extend) or disprove (and fix)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In a Kleene algebra ( x^n \leq x^* ) for all ( n \geq 0 ) (where ( x^0 = 1, x^{n+1} = x^n x ))</td>
</tr>
<tr>
<td>( x \leq x^* \leq y^* )</td>
</tr>
<tr>
<td>( xx^* = x^* x ) and ( x^* = 1 + x^+ ) where ( x^+ = xx^* )</td>
</tr>
<tr>
<td>( xy + z \leq y \Rightarrow x^* z \leq y ) (and its opposite)</td>
</tr>
<tr>
<td>( xy = yz \Rightarrow x^* y = yz^* )</td>
</tr>
<tr>
<td>( (xy)^* x = x(yx)^* ) and ( (x + y)^* = x^<em>(yx)^</em> )</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Kleene algebras with tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kleene algebras model concatenation, nondeterministic choice and iteration, but to model programs need guarded choice and guarded iteration</td>
</tr>
<tr>
<td>A Kleene algebra with tests (KAT) is of the form ( (A, +, 0, ;, 1^<em>, <em>, B) ) where ( (A, +, 0, ;, 1^</em>) ) is a Kleene algebra, ( B ) is a unary relation ( (\subseteq A) ) and ( x, y \in B \Rightarrow x + y, x; y, x^</em> )</td>
</tr>
<tr>
<td>( 0, 1 \in B ), ( x; x = x ), ( x; x^* = 0 ), ( x + x^* = 1 )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prove (and extend) or disprove (and fix)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In a KAT, ( (B, +, 0, ;, 1^*) ) is a Boolean algebra</td>
</tr>
</tbody>
</table>

[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 \( (b;p)^*;b^− \)

<table>
<thead>
<tr>
<th>Terms and formulas</th>
</tr>
</thead>
<tbody>
<tr>
<td>UA is a framework for studying and comparing all these algebras</td>
</tr>
<tr>
<td>Given a set ( X ), the set of ( \tau )-terms with variables from ( X ) is the smallest set ( T = T_\tau(X) ) such that</td>
</tr>
<tr>
<td>( X \subseteq T ) and</td>
</tr>
<tr>
<td>if ( t_1, \ldots, t_n \in T ) and ( f \in F_\tau ) then ( f(t_1, \ldots, t_n) \in T ).</td>
</tr>
<tr>
<td>The term algebra over ( X ) is ( T_\tau(X) = T = (T_\tau(X), (f^T)<em>{f \in F</em>\tau}) ) with</td>
</tr>
<tr>
<td>( f^T(t_1, \ldots, t_n) = f(t_1, \ldots, t_n) ) for ( t_1, \ldots, t_n \in T_\tau(X) )</td>
</tr>
<tr>
<td>A ( \tau )-equation is a pair of ( \tau )-terms ( (s, t) ), usually written ( s = t )</td>
</tr>
<tr>
<td>A quasi-equation is an implication ( (s_1 = t_1 ) and ( \ldots ) and ( s_n = t_n \Rightarrow s_0 = t_0) )</td>
</tr>
</tbody>
</table>
Models and theories

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

A \( \tau \)-formula \( \phi := \) atomic frm. | \( \phi \) and \( \phi \) or \( \phi \) | \( \neg \phi \) \( \Rightarrow \) \( \phi \) | \( \forall x \phi \) | \( \exists x \phi \)

Write \( U \models \phi \) if \( \tau \)-formula \( \phi \) holds in \( \tau \)-structure \( U \) (standard defn)

Throughout \( \mathcal{K} \) is a class of \( \tau \)-structures, \( F \) a set of \( \tau \)-formulas

Write \( \mathcal{K} \models F \) if \( U \models \phi \) for all \( U \in \mathcal{K} \) and \( \phi \in F \)

\( \text{Mod}(F) = \{ U : U \models F \} \) = class of all models of \( F \)

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

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

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

\( \text{Th}_q(\mathcal{K}) \) is also called the strict universal Horn theory of \( \mathcal{K} \).

Substructures, homomorphisms and products

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

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

Varieties and HSP

\( HK \mathcal{K} \) is the class of homomorphic images of members of \( \mathcal{K} \)
\( SK \mathcal{K} \) is the class of substructures of members of \( \mathcal{K} \)
\( PK \mathcal{K} \) is the class of direct products of members of \( \mathcal{K} \)

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

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

Prove (and extend) or disprove (and fix)

If \( \mathcal{K} \) is a quasivariety then \( SK \mathcal{K} \subseteq \mathcal{K} \), \( PK \mathcal{K} \subseteq \mathcal{K} \) and \( HK \mathcal{K} \subseteq \mathcal{K} \)

The next characterization marks the beginning of universal algebra

Theorem (Birkhoff 1935)

\( \mathcal{K} \) is a variety iff \( HK \mathcal{K} = \mathcal{K} \), \( SK \mathcal{K} = \mathcal{K} \) and \( PK \mathcal{K} = \mathcal{K} \)
Varieties generated by classes

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

Prove (and extend) or disprove (and fix)

For sets \( F_i \) of \( \tau\) formulas \( \bigcap_{i \in I} \text{Mod}(F_i) = \text{Mod}(\bigcup_{i \in I} F_i) \)

Hence \( \Lambda_\tau \) is closed under arbitrary intersections

\[ \bigcap \Lambda_\tau = \text{Mod}\{\{x = y\}\} \text{ is the class } O_\tau \text{ of trivial } \tau\text{-structures} \]

The variety generated by \( \mathcal{K} \) is \( \mathcal{V} \mathcal{K} = \bigcap \{ \text{all varieties that contain } \mathcal{K} \} \)

Prove (and extend) or disprove (and fix)

\( \mathcal{SH} \mathcal{K} = \mathcal{HS} \mathcal{K}, \mathcal{PH} \mathcal{K} = \mathcal{HP} \mathcal{K} \) and \( \mathcal{PS} \mathcal{K} = \mathcal{SP} \mathcal{K} \) for any class \( \mathcal{K} \)

Theorem (Tarski 1946)

\( \mathcal{V} \mathcal{K} = \mathcal{HSP} \mathcal{K} \) for any class \( \mathcal{K} \) of structures

Congruences and quotient algebras

A congruence on an algebra \( A \) is an equivalence relation \( \theta \) on \( A \) that is compatible with the operations of \( A \), i.e. for all \( f \in \mathcal{F}_n \)

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

\( \text{Con}(A) \) is the set of all congruences on \( A \)

Prove (and extend) or disprove (and fix)

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

For \( \theta \in \text{Con}(A) \), the quotient algebra is \( A/\theta = (A/\theta, (f^A/\theta)_{f \in \mathcal{F}_n}) \) where

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

Prove (and extend) or disprove (and fix)

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

Complete lattices

For a subset \( X \) of a poset \( U \) write \( X \leq u \) if \( x \leq u \) for all \( x \in X \) and define \( z = \sum X \) if \( X \leq u \iff z \leq u \) (so \( \sum X \) is the least upper bound of \( X \))

\( u \leq X \) 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 \( \prod X = \sum \{ u : u \leq X \} \)

A structure \( U \) 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 \( T = \prod \emptyset \)

Prove (and extend) or disprove (and fix)

\( \mathcal{U} \) with partial order \( \leq \) is complete iff \( \sum X \) exists for all \( X \subseteq U \)

\( \Lambda_\tau \) partially ordered by \( \subseteq \) is a complete lattice

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 \( h : A \to B \) is a homomorphism then \( \ker h \in \text{Con}(A) \)

\( h[A] \) is the underlying set of a subalgebra \( h[A] \) of \( B \)

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

The second isomorphism theorem: For \( \theta \in \text{Con}(A) \), the subset \( \uparrow \theta = \{ \psi : \theta \subseteq \psi \} \) of \( \text{Con}(A) \) is isomorphic to \( \text{Con}(A/\theta) \) via the map \( \psi \mapsto \psi/\theta \) where \( [x]_\psi/\theta[y] \iff x \psi y \)
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)  
\( \text{Con}(A) \) is an algebraic lattice (hint: compact = finitely generated)

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 completely 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

\( \mathcal{K}_S \) is the class of subdirectly irreducibles of \( \mathcal{K} \)  
\( \Rightarrow \mathcal{V} = \text{SP}(\mathcal{V}_S) \) for any variety \( \mathcal{V} \)

Subdirect products and subdirectly irreducibles

An embedding is an injective homomorphism  
An embedding \( h : A \hookrightarrow \prod_{i \in I} B_i \) is subdirect if \( \pi_i[h(A)] = B_i \) for all \( i \in I \)  
\( A \) is a subdirect product of \( (B_i)_{i \in I} \) if there is a subdirect \( h : A \hookrightarrow \prod_{i \in I} B_i \)

Prove (and extend) or disprove (and fix)  
Define \( h : A \hookrightarrow \prod_{i \in I} A/\theta_i \) by \( h(a) = ([a]_{\theta_i})_{i \in I} \)  
Then \( h \) is a subdirect embedding iff \( \bigcap_{i \in I} \theta_i = I_A \)

\( A \) is subdirectly irreducible if for any subdirect \( h : A \hookrightarrow \prod_{i \in I} B_i \), there is an \( i \in I \) such that \( \pi_i \circ h \) is an isomorphism

Prove (and extend) or disprove (and fix)  
\( A \) is subdirectly irreducible iff \( I_A \subset \text{Con}(A) \) is completely meet irreducible iff \( \text{Con}(A) \) has a smallest nonbottom element

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 \( x, y \in X \Rightarrow \exists u \in X(x \leq u \text{ and } y \leq u) \)  
\( X \) 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 \( x + y \in X \Rightarrow x \in X \text{ or } y \in X \)

Prove (and extend) or disprove (and fix)  
The set \( \text{Fil}(U) \) 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 \((P(I), \subseteq)\).

\(\mathcal{F}\) defines a **congruence** on \(U = \prod_{i \in I} U_i\) via \(x \theta y \iff \{i \in I \mid x_i = y_i\} \in \mathcal{F}\).

\(U/\theta\mathcal{F}\) is called a **reduced product**, denoted by \(\prod_{\mathcal{F}} U\).

If \(\mathcal{F}\) is an ultrafilter then \(U/\theta\mathcal{F}\) is called an **ultraproduct**.

\(P_u\mathcal{K}\) is the class of all ultraproducts of members of \(\mathcal{K}\).

\(\mathcal{K}\) is **finitely axiomatizable** if \(\mathcal{K} = \text{Mod}(\phi)\) for a single formula \(\phi\).

**Prove (and extend) or disprove (and fix)**

If \(\mathcal{K} \models \phi\) then \(P_u\mathcal{K} \models \phi\) for any first order formula \(\phi\).

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 \(\tau\)-structures then \(P_u\mathcal{K} = \mathcal{K}\).

### Lattices of subvarieties

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

**Prove (and extend) or disprove (and fix)**

If \(A'\) is a reduct of \(A\) then \(\text{Con}(A)\) is a sublattice of \(\text{Con}(A')\).

The variety of lattices is \(\text{CD}\), so any variety of algebras with lattice reducts is \(\text{CD}\).

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

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

**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 \(\mathcal{V}\).

\(\text{HSP}_u(\mathcal{K} \cup \mathcal{L}) = \text{HSP}_u\mathcal{K} \cup \text{HSP}_u\mathcal{L}\) for any classes \(\mathcal{K}\), \(\mathcal{L}\).

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

### Congruence distributivity and Jónsson’s Theorem

\(\mathcal{A}\) is **congruence distributive** (CD) if \(\text{Con}(\mathcal{A})\) is a distributive lattice.

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

**Theorem (Jónsson 1967)**

If \(\mathcal{V} = \text{VK}\) is congruence distributive then \(\mathcal{V}_{SI} \subseteq \text{HSP}_u\mathcal{K}\).

**Prove (and extend) or disprove (and fix)**

If \(\mathcal{K}\) is a finite class of finite algebras and \(\mathcal{V}\) is CD then \(\mathcal{V}_{SI} \subseteq \text{HSP}_u\mathcal{K}\).

If \(A, B \in \mathcal{V}_{SI}\) are finite nonisomorphic and \(\mathcal{V}\) is CD then \(VA \neq VB\).

\(\mathcal{V}\) is **finitely generated** if \(\mathcal{V} = \text{VK}\) for some finite class of finite algebras.

**Prove (and extend) or disprove (and fix)**

A finitely generated CD variety has only finitely many subvarieties.

### Simple algebras and the discriminator

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

**Prove (and extend) or disprove (and fix)**

Any simple algebra is subdirectly irreducible.

\(\mathcal{A}\) is a **discriminator algebra** if for some ternary term \(t\)

\(A \models x \neq y \Rightarrow t(x, y, z) = x\) 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 \( A \) 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

\[ (r = s)^t = (r^r + s) \cdot (r + s^r), \quad (\phi \text{ and } \psi)^t = \phi^t \cdot \psi^t, \quad (\neg \phi)^t = d((\phi^t)^t) \]

Prove (and extend) or disprove (and fix)

In an algebra with Boolean reduct \( \phi \Leftrightarrow (\phi^t = 1) \)

Relation algebras are a discriminator variety

Let \( Aa = (\{a, +, 0, \cdot, a^{-r}, a^t\} : a \in A) \) be the relative subalgebra of relation algebra \( A \) with \( a \in A \) where \( x^{-r} = x \cdot -a, x;ay = (x; y) \cdot a, \) and \( x^{-r} = x \cdot -a \)

An element \( a \) in a relation algebra is an ideal element if \( a = \top; a; \top \)

Prove (and extend) or disprove (and fix)

\( Aa \) is a relation algebra iff \( a = a^{-r} = a^t \)

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

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 \( \text{RRA} \) of representable relation algebras is \( \text{SP} \{ \text{Rel}(X) : X \text{ is a set} \} \)

Prove (and extend) or disprove (and fix)

An algebra is in \( \text{RRA} \) iff it is embeddable in a concrete relation algebra

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

\[ \text{Hint: } P_uS \subset \text{SP}_u \text{ so if } A = \prod_{i \in I} \text{Rel}(X_i) \text{ for some ultrafilter } \mathcal{U} \text{ over } I, \text{ let } Y = \prod_{i \in I} X_i, \text{ define } h : A \rightarrow \text{Rel}(Y) \text{ by } [x]h([R])[[y]] \Leftrightarrow \{ i \in I : x_i R_i(y) \} \in \mathcal{U} \text{ and show } h \text{ is a well defined embedding} \]

\( \Rightarrow (\mathcal{K})_{\mathcal{S}U} \subset \mathcal{K} \text{ by Jónsson's Theorem} \)

\( \Rightarrow \mathcal{V}(\mathcal{K}) = \text{SP} \mathcal{K} = \text{RRA} \text{ by Birkoff's subdirect representation theorem} \)

\( \Rightarrow [\text{Tarski 1955}] \text{ RRA is a variety} \)
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
RA = RA_4 ⊃ RA_5 ⊃ ... RRA = \bigcap_{n \geq 4} 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 U = (U, T, ⊮, E) be a structure with T ⊆ U^3, ⊮ : U → U, E ⊆ U x U x U
The complex algebra Cm(U) is (P(U), ∪, ∩, E, ⊮, ⊥, ⊤, 1) where
X; Y = \{z : (x, y, z) ∈ T for some x ∈ X, y ∈ Y\},
X ⊮ = \{x ⊮ : x ∈ X\}, and 1 = E

Prove (and extend) or disprove (and fix)
Cm(U) is a relation algebra iff x = y ⇔ \exists z ∈ E (x, z, y) ∈ T,
(x, y, z) ∈ T ⇔ (x ⊮, z, y) ∈ T ⇔ (z, y ⊮, x) ∈ T, and
(x, y, z) ∈ T and (z, u, v) ∈ T ⇒ \exists w((x, w, v) ∈ T and (y, v, w) ∈ T)

An algebra A = (A, o, ⊮, e) can be viewed as a structure (A, T, ⊮, E) where
T = \{(x, y, z) : x o y = z\} and E = \{e\}

Prove (and extend) or disprove (and fix)
Cm(A) is a relation algebra iff A is a group

Atom structures
J(A) denotes the set of completely join irreducible elements of A

Prove (and extend) or disprove (and fix)
In a Boolean algebra J(A) is the set of atoms of A
Every atomic BA is embeddable in P(J(A)) via x ↦ J(A) ∩ ↓x
Every complete and atomic Boolean algebra is isomorphic to P(J(A))

The atom structure of an atomic relation algebra A is (J(A), ⊮, T, E)
where T = \{(x, y, z) ∈ J(A) : x; y ≥ z\} and E = J(A) ∩ ↓1

Prove (and extend) or disprove (and fix)
U = (U, ⊮, T, E) is the atom structure of some atomic relation algebra iff Cm(U) is a relation algebra
If A is complete and atomic then Cm(J(A)) ≅ A

Integral and finite relation algebras
A relation algebra is integral if x; y = 0 ⇒ x = 0 or y = 0

Prove (and extend) or disprove (and fix)
A relation algebra A is integral iff 1 is an atom of A iff x ≠ 0 ⇒ x; T = T

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
Rel(0) is the one-element RA; generates the variety O = Mod(0 = T)
Rel(1) is the two-element RA, with 1 = T, x; y = x · y, x ⊮ = x
It generates the variety A_1 = Mod(1 = T) of Boolean relation algebras
Varieties of small relation algebras

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

A relation algebra $A$ is symmetric if $x = x^\sim$ (iff $A^s = A$)

**Prove (and extend) or disprove (and fix)**

*If $A$ is commutative, then $A^s$ is a subalgebra of $A$*

There are two RAs with 4 elements: $A_2 = Cm(Z_2)$ and $A_3 = (Cm(Z_3))^s$

The varieties generated by $A_2$ and $A_3$ are denoted $A_2$ and $A_3$

By Jónsson’s Theorem $A_1, A_2$ and $A_3$ are atoms of $\Lambda_{\text{RA}}$

**Theorem (Jónsson)**

Every nontrivial variety of relation algebras includes $A_1, A_2$ or $A_3$

---

**Integral relation algebras with 4 atoms**

The 8-element integral RAs all have $A_3$ as the only proper subalgebra

⇒ they generate join-irreducible varieties above $A_3$

$B_1, \ldots, B_7$ are symmetric, $C_1, C_2, C_3$ are nonsymmetric

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

(65 are symmetric, and 37 are not)

[Jipsen Hertzler 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](http://www.chapman.edu/~jipsen/gap/ramaddux.html) that are representable but not known to be group representable

---

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

⇒ GRA is a subvariety of RRA

For an algebra $A$ and $x \in A$, $Sg^A(x)$ 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

$B_1 = Sg^{\text{Cm}(\mathbb{Z}_2)}(2)$  
$B_2 = Sg^{\text{Cm}(\mathbb{Z}_4)}(2)$  
$B_3 = Sg^{\text{Cm}(\mathbb{Z}_8)}(3)$  
$B_4 = Sg^{\text{Cm}(\mathbb{Z}_9)}(3, 6)$

---

**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 = monoids = semigroups with identity $x \cdot 1 = x = 1 \cdot x$

Mon$^\sim$ = involutive monoids = monoids with $x^\sim \cdot x = x$, $(x \cdot y)^\sim = y^\sim \cdot x^\sim$

Grp = groups = monoids with $x^\sim \cdot x = 1$

JSLat$_0$ = join-semilattices with identity $x + 0 = x$

Lat$^\sim_T$ = bounded lattices = lattices with $x + 0 = x$ and $x \cdot T = T$

Lat$^\sim$ = complemented lattices = Lat$^\sim_T$ with $x + x^\sim = T$ and $x \cdot x^\sim = 0$

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

\[ \text{Srng} = \text{semirings} = \text{monoids distributing over commutative monoids and 0} \]
\[ \text{IS} = (\text{additively) idempotent semirings} = \text{semirings with } x + x = x \]
\[ \ell \text{M} = \text{lattice-ordered monoids} = \text{idempotent semirings with meet} \]
\[ \text{RL} = \text{residuated lattices} = \ell \text{-monoids with residuals} \]
\[ \text{KA} = \text{Kleene algebra} = \text{idempotent semiring with } \ast, \text{ unfold and induction} \]
\[ \text{KA}^* = \ast \text{-continuous Kleene algebra} = \text{KA with } ... \]
\[ \text{KA T} = \text{Kleene algebras with tests} = \text{KA with Boolean subalgebra } \leq 1 \]
\[ \text{KAD} = \text{Kleene algebras with domain} \]
\[ \text{KL} = \text{Kleene lattices} = \text{Kleene algebras with meet} \]
\[ \text{BM} = \text{Boolean monoids} = \text{distributive } \ell \text{-monoids with complements} \]
\[ \text{KBM} = \text{Kleene Boolean monoids} = \text{Boolean monids with Kleene-} \ast \]
\[ \text{RA} = \text{relation algebras} = \text{Boolean monoids with involution and residuals} \]
\[ \text{KRA} = \text{Kleene relation algebras} = \text{relation algebras with Kleene-} \ast \]
\[ \text{RRA} = \text{representable relation algebras} = \text{concrete relation algebras} \]
\[ \text{RKRA} = \text{representable Kleene relation algebras} = \text{RRA with Kleene-} \ast \]

<table>
<thead>
<tr>
<th>\text{A} = \text{Algebra}</th>
<th>\text{B} = \text{Boolean}</th>
<th>\text{I} = \text{Idempotent}</th>
<th>\text{K} = \text{Kleene}</th>
<th>\text{L} = \text{Lattice}</th>
<th>\ell = \text{lattice-ordered}</th>
<th>\text{M} = \text{Monoid}</th>
<th>\text{R} = \text{Relation}</th>
</tr>
</thead>
<tbody>
<tr>
<td>\text{S} = \text{Semiring}</td>
<td>\text{T} = \text{with tests}</td>
<td>\leq</td>
<td>\text{≤}</td>
<td>\ast</td>
<td>\text{with converse}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Many, but not all, of these classes are varieties

Recall that quasivarieties 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

Theorem (Mal’cev)

A class \( K \) is a quasivariety iff it is closed under \( S, P \) and \( P_u \)

The smallest quasivariety containing \( K \) is \( QK = SPP_uK \).

Free algebras

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

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

If also \( F \in K \) then \( F \) is the \( K \)-free algebra on \( X \) and is denoted by \( F_K(X) \).

To prove (and extend) or disprove (and fix)

Let \( A \) be the powerset Kleene algebra of \((\mathbb{N}, +, 0)\) and let \( \theta \) be the equivalence relation on \( A \) with blocks \( \{\emptyset\}, \{\{0\}\}, \{all \ finite \ sets \neq \{0\}, \emptyset\} \)

and \( \{all \ infinite \ subsets\} \). Then \( \theta \) is a congruence, but \( A/\theta \) is not a Kleene algebra.
Examples of free algebras

A free algebra on \( m \) generators satisfies only those equations with \( \leq m \) variables that hold in all members of \( K \)

\[
\mathsf{F}_{\text{Sgrp}}(X) \cong \bigcup_{n \geq 1} X^n \quad \mathsf{F}_{\text{Mon}}(X) \cong \bigcup_{n \geq 0} X^n \quad x \mapsto (x)
\]

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

\[
\mathsf{F}_{\text{Slat}}(X) \cong \mathcal{P}(X) \setminus \{\emptyset\} \quad \mathsf{F}_{\text{Slat}_0}(X) \cong \mathcal{P}(X) \quad x \mapsto \{x\}
\]

\[
\mathsf{F}_{\text{Srng}}(X) \cong \{\text{finite multisets of } X^*\} \quad \mathsf{F}_{\text{IS}}(X) \cong \mathcal{P}(\mathcal{P}(X))
\]

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

\[ \Rightarrow \text{the equational theories of Sgrp, Mon, Slat, Srng, IS are decidable} \]

Kleene algebras and regular sets

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

Let \( \Sigma \) be a finite set, called an alphabet

The free monoid generated by \( \Sigma \) is \( \Sigma^* = (\Sigma^*, \cdot, \varepsilon) \)

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

The Kleene algebra of regular sets is \( \mathcal{R}_\Sigma = \mathcal{S}_{\mathcal{B}_{\text{KA}}}(\Sigma^*(\{(x) : x \in \Sigma\})) \)

Theorem (Kozen 1994)

\( \mathcal{R}_\Sigma \) is the free Kleene algebra on \( \Sigma \)

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

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

Membership in regular sets can be determined by finite automata

Automata

A \( \Sigma \)-automaton is a structure \( U = (U, (a^U)_{a \in \Sigma}, S, T) \) such that \( a^U \) 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 \( w^U \) by \( \varepsilon^U = I_U \) and \( (a \cdot w)^U = a^U \cdot w^U \)

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

\( \text{Rec}_\Sigma \) is the set of all languages recognized by some \( \Sigma \)-automaton

Prove (and extend) or disprove (and fix)

\( \emptyset, \{\varepsilon\}, \{a\} \in \text{Rec}_\Sigma \) 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 \( (u_i, u_j) \in a^U \)

Given automata \( U, V \), define \( U + V \) to be the disjoint union of \( U, V \)

\[
U + V = (U \uplus V, (a^U \uplus a^V \uplus (a^U T^U \times S^V))_{a \in \Sigma}, S', T')
\]

where

\[
S' = \begin{cases}
S^U & \text{if } S^U \cap T^U = \emptyset \\
S^U \uplus S^V & \text{otherwise}
\end{cases}
\]

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

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

Prove (and extend) or disprove (and fix)

\[
L(U + V) = L(U) \cup L(V), L(U; V) = L(U); L(V), \text{ and } L(U^+) = L(U)^+
\]

\( \Rightarrow \) every regular set is recognized by some finite automaton

Matrices in semirings and Kleene algebras

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

\( M_n(A) \) is again a semiring with usual matrix addition and multiplication

\( 0 \) is the zero matrix, and \( I_n \) is the identity matrix

If \( A \) is a Kleene algebra and \( M = \begin{bmatrix} N & P \\ Q & R \end{bmatrix} \in M_n(A) \) define

\[
M^* = \begin{bmatrix} (N + PR^*)^* & N^*P(R + QN^*P)^* \\ R^*Q(N + PR^*)^* & (R + QN^*P)^* \end{bmatrix}
\]

This is motivated by the diagram:

Prove (and extend) or disprove (and fix)

The definition of \( M^* \) is independent of the chosen decomposition

If \( A \) is a Kleene algebra, so is \( M_n(A) \)

Finite automata as matrices

Given \( U = (U, (a^U)_{a \in \Sigma}, S, T) \) 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

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

Prove (and extend) or disprove (and fix)

\( L(U) = h(s; M; t) \) where \( h : T_{KA}(\Sigma) \to R_\Sigma \) 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

\( U \) is a deterministic automaton if each \( a^U \) is a function on \( U \) and \( S \) is a singleton set

Prove (and extend) or disprove (and fix)

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

Minimal automata

A state \( v \) is accessible if \( (u, v) \in w^U \) 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 \( U \) with no inaccessible states, the relation \( u \not\in v \) iff \( \forall w \in \Sigma^* \ w(u) \in T \iff w(v) \in T \) is a congruence on the automaton and \( L(U/\theta) = L(U) \)

An automaton is minimal if all states are accessible and the congruence \( \theta \) defined in the preceding theorem is the identity relation

Prove (and extend) or disprove (and fix)

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

\( \Rightarrow \) 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 \(A\), let \(A_1\) be the monoid obtained by adjoining 1

**Prove (and extend) or disprove (and fix)**

Any semigroup \(A\) is a subalgebra of the \(;\)-reduct of \(P(A)\)

If \(K = \{;\text{-reducts of semirings}\}\) then \(SK = \text{the class of semigroups}\)

A quasiequation that uses only ; holds in \(K\) iff it holds in all semigroups

⇒ the quasiequational theory of (idempotent) semirings is undecidable

Since \(P(A)\) is a reduct of \(KA, KAT, KAD, BM\) the same result holds

Undecidability is pervasive in \(\Lambda_{RA}\)

**Theorem (Andréka Givant Nemeti 1997)**

If \(K \subseteq RA\) such that for each \(n \geq 1\) there is an algebra in \(K_{SI}\) with at least \(n\) elements below the identity then \(Th_KK\) is undecidable

If \(K \subseteq RA\) such that for each \(n \geq 1\) there is an algebra in \(K\) with a subset of at least \(n\) pairwise disjoint elements that form a group under ; and \(~\) then \(Th_KK\) is undecidable

**Prove (and extend) or disprove (and fix)**

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

The equational theory of RA is undecidable

**Prove (and extend) or disprove (and fix)**

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

If \(K = \{;\text{-reducts of simple RAs}\}\) then \(SK = \text{the class of semigroups}\)

*The quasiequational theory of RA\(_{SI}\), RA and RRA is undecidable*

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

⇒ \(Th_(RA)\) is undecidable

<table>
<thead>
<tr>
<th></th>
<th>(Th_{D}) dec</th>
<th>(Th_{Q}) dec</th>
<th>(Th) dec</th>
<th>Var</th>
<th>CD</th>
<th>loc fin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sgrp, Mon</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Slat</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Lat</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DLat</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>BA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Grp</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Srng</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>IS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>KA, KAT</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>KAD</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>RsKA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>RsL</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>BM</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>RA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>RRA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>KRA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
Categories

A **category** is a structure \( \mathbf{C} = (\mathbf{C}, O, \circ, 1, \text{dom}, \text{cod}) \) 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 \( \circ \) 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 \( \text{Hom}(X, Y) = \{ f : \text{dom}f = X \) and \( \text{cod}f = Y \} \) is a set

\( \text{Set} \) is a category with sets as objects and functions as morphisms

\( \text{Rel} \) is a category with sets as objects and binary relations as morphisms

Heterogeneous relation algebras

The category \( \text{Rel} \) 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 \( \mathbf{C} = (\mathbf{C}, O, ;, 1, \text{dom}, \text{cod}, \vdash, +, \top, \cdot, 0, \neg) \) such that

- \( (\mathbf{C}, O, ;, 1, \text{dom}, \text{cod}) \) is a category
- \( \vdash : \text{Hom}(x, y) \to \text{Hom}(y, x) \) satisfies \( r \vdash r = r \), \( 1_{\vdash} = 1_X \), \( (r; s) \vdash = s \vdash ; r \vdash \)
- for all objects \( x, y, (\text{Hom}(x, y), +, \top, \cdot, 0, \neg) \) is a Boolean algebra and
- for all \( r; s, t \in \text{Hom}(x, y) \), \( (r; s) \cdot t = 0 \iff (r \vdash ; t) \cdot s = 0 \iff (t ; s \vdash) \cdot r = 0 \)

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** \( F : \mathbf{C} \to \mathbf{D} \) maps \( C \to D \) and \( O^\mathbf{C} \to O^\mathbf{D} \) such that

- \( F(1_X) = 1_{FX} \) and if \( f : X \to Y \) then \( Ff : FX \to FY \)
- if \( f : X \to Y, g : Y \to Z \) then \( F(g \circ f) = Fg \circ Ff \)

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

- \( F(1_X) = 1_{FX} \) and if \( f : X \to Y \) then \( Ff : FX \to FY \)
- if \( f : X \to Y, g : Y \to Z \) then \( F(g \circ f) = Ff \circ Fg \)

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 \( (A, +, \cdot, \top, \bot, 0, 1) \), 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 “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

[Birkhoff 1944] Subdirect unions in universal algebra, Bull. AMS
[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 Maddux 1997] Nonrepresentable sequential algebras, J. IGPL, online
[Kahl 2004] Refactoring heterogeneous relation algebras around ordered categories and converse, JoRMiCS, online

References and further reading III

[Kozen 2003] Automata on guarded strings and applications, Matémat. Contemp., online
[Maddux 1982] Some varieties containing relation algebras, Trans. AMS
[Maddux 2006] Relation algebras, Elsevier
[Post 1947] Recursive unsolvability of a problem of Thue, J. Symbolic Logic