On congruences in residuated Kleene algebras and generalized ordinal sums

Peter Jipsen, Chapman University, California

- **Residuated Kleene Algebras**
- **The structure of congruences**
- **Applications of congruence distributivity**
- **Residuated Kleene algebras from ℓ-groups and relations**
- **Generalized ordinal sum decompositions**

- V. PRATT, *Action logic and pure induction*, “Logics in AI: European Workshop JELIA ’90”, ed. J. van Eijck, LNCS 478, Springer-Verlag, Amsterdam, NL, Sep, 1990, 97–120.
- D. KOZEN, *On action algebras*, In J. van Eijck and A. Visser, editors, “Logic and Information Flow”, MIT Press, 1994, 78–88.
- P. JIPSEN, *From semirings to residuated Kleene lattices* Studia Logica, vol. 76(2) (2004), 291–303.
- C. J. VAN ALTEN and J. G. RAFTERY, *Rule separation and embedding theorems for logics without weakening*, Studia Logica, vol. 76(2) (2004), 241–274.
- W. BLOK and J. G. RAFTERY, *Assertionally equivalent quasivarieties*, preprint (2004), 1–106.

- P. Jipsen and C. Tsinakis, *A survey of residuated lattices*, in "Ordered Algebraic Structures" (J. Martinez, editor), Kluwer Academic Publishers, Dordrecht, 2002, 19–56.
- P. Jipsen and F. Montagna, *On the structure of generalized BL-algebras*, preprint.

A **Kleene algebra** $(A, \vee, 0, \cdot, 1, ^*)$ is an **idempotent semiring with 0, 1 and a Kleene $*$-operation**. Specifically this means:

$(A, \cdot, 1)$ is a **monoid**,

$(A, \vee, 0)$ is a **join-semilattice with bottom**,

multiplication distributes over all finite joins, i.e. $x0 = 0 = 0x$,

$x(y \vee z) = xy \vee xz$, $\qquad (y \vee z)x = yx \vee zx$, $\qquad$ and

$*$ is a unary operation that satisfies

($*_c$) $\qquad 1 \vee x \vee x^*x^* = x^*$

($*_l$) $\qquad xy \leq y \implies x^*y = y$

($*_r$) $\qquad yx \leq y \implies yx^* = y$

The **quasivariety** of Kleene algebras is denoted by KA. It is **not** a variety: e.g. there is a 4-element algebra that fails ($*_l$) but is a homomorphic image of the Kleene algebra defined on the powerset of a 1-generated free monoid (Conway's leap).

A **residuated Kleene algebra** $(A, \vee, 0, \cdot, 1, \backslash, /, ^*)$ is a Kleene algebra expanded with

residuals $\backslash$, $/$ of the multiplication, i.e. for all $x, y, z \in A$

($\backslash$) $\quad xy \leq z \iff y \leq x\backslash z$ and

($/$) $\quad xy \leq z \iff x \leq z/y$.

Although we have **added more** quasiequations to KA, the class RKA of all residuated Kleene algebras is a **variety**:

($\backslash$) is equivalent to $y \leq x\backslash(xy \vee z)$ and $x(x\backslash z) \leq z$

($/$) is equivalent to the mirror images of these, and

($*_l$) and ($*_r$) are equivalent to $x^* \leq (x \vee y)^*$ and $(y/y)^* \leq y/y$.

Residuated Kleene algebras are also called **action algebras** by Pratt [1990] and Kozen [1994].

Kleene algebras have a long history in Computer Science, with applications in formal foundations of automata theory, regular grammars, semantics of programming languages and other areas.

Elements in a Kleene algebra can be considered as **specifications** or **programs**, with $\cdot$ as sequential composition, $\vee$ as nondeterministic choice, and * as iteration.

Residuals also have a natural interpretation: If we implement an **initial part** p of a specification s, then $px \leq s$ implies $x \leq p\backslash s$, so $p\backslash s$ is the specification for **implementing the remaining part**.

A non-commutative version of a result of Raftery and van Alten [2004] gives another reason for adding residuals:

RKA is **congruence distributive**.

What does this mean, **why** is it important, and why is it true?

A **congruence** on an algebra A is an equivalence relation θ that preserves the operations of A:

$x_i \theta y_i$ ($i = 1, \ldots, n$) implies $f(x_1, \ldots, x_n) \theta f(y_1, \ldots, y_n)$.

The congruences on A form a (algebraic) lattice $\mathrm{Con}(A)$ with

$$\theta \wedge \psi = \theta \cap \psi$$

$$\theta \vee \psi = \bigcup_{i=1}^{\infty} (\theta \circ \psi)^i$$

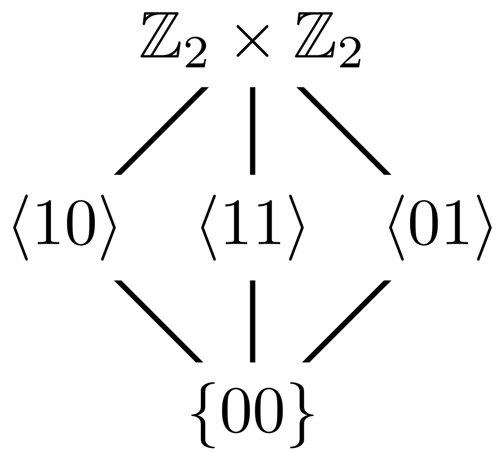
An algebra A is **congruence distributive** (CD) if $\mathrm{Con}(A)$ is a **distributive lattice**, i.e. satisfies

$$\theta \wedge (\psi \vee \varphi) = (\theta \wedge \psi) \vee (\theta \wedge \varphi)$$

A **class of algebras is CD** if each member is CD.

E.g. the variety of groups is not CD: $\mathrm{Con}(\mathbb{Z}_2 \times \mathbb{Z}_2)$

$=$ Lattice of normal subgroups $\cong$



The variety of lattices is CD (Funayama, Nakayama [1942])

To understand a variety $\mathcal{V}$ of algebras, we study its building blocks, the **subdirectly irreducible members** $\mathrm{Si}(\mathcal{V})$.

An algebra A is **subdirectly irreducible** if $\mathrm{Con}(A)$ contains a smallest nontrivial congruence.

By Birkhoff's [1944] result, any algebra is a subalgebra of a product of its subdirectly irreducible homomorphic images.

This is the universal algebra "equivalent" of the result that any natural number is a product of its prime divisors.

So, if $\mathrm{Si}(\mathcal{V}) = \mathrm{Si}(\mathcal{W})$ then $\mathcal{V} = \mathcal{W}$.

Tarski [1946] proved that for any class of algebras, $HSP(\mathcal{K})$ is the smallest variety that contains $\mathcal{K}$.

Here H, S, P stand for all **homomorphic images**, all **subalgebras**, and all **products** of members of the class they are applied to.

Jónsson's Lemma [1967] implies that if $HSP(\mathcal{K})$ is CD and of finite type, then $\mathrm{Si}(HSP(\mathcal{K})) \subseteq HSP_U(\mathcal{K})$.

Here $P_U(\mathcal{K})$ is the class of **ultraproducts** of members of $\mathcal{K}$, i.e. direct products $\prod_{i\in I} A_i$ modulo a congruence θ_U where U is an **ultrafilter** in the powerset $\mathcal{P}(I)$ and

$\underline{a}\theta_U\underline{b}$ iff $\{i \in I : a_i = b_i\} \in U$.

In particular, if all algebras in $\mathcal{K}$ have size $\leq n$,

then $P_U(\mathcal{K}) = \mathcal{K}$, so $\mathrm{Si}(HSP(\mathcal{K})) \subseteq HS(\mathcal{K})$,

hence all subdirectly irreducibles in $HSP(\mathcal{K}) - \mathcal{K}$ have size $< n$.

This can fail for varieties without CD: E.g. let

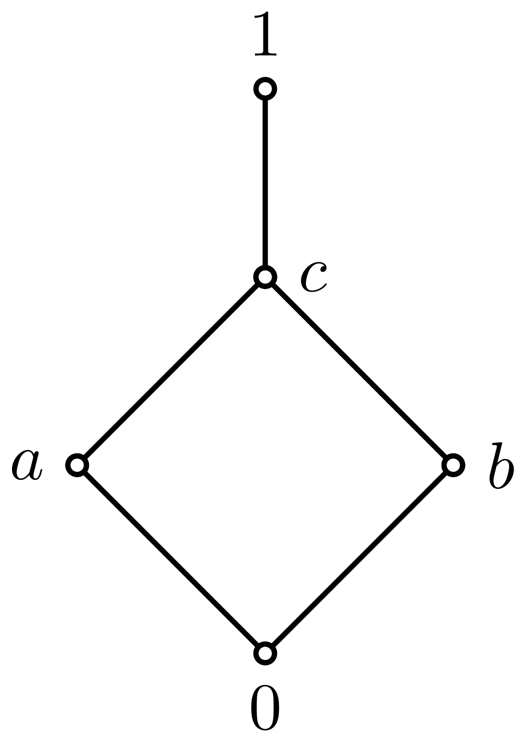
$D =$ 8-element dihedral group (i.e. symmmetries of a square),

$Q =$ 8-element quaternion group ($1, i, j, k$ and negatives, with $i^2 = j^2 = k^2 = -1, ij = k$,)

then $Q \in \mathrm{Si}(HSP(D))$ and $D \in \mathrm{Si}(HSP(Q))$.

With CD it is **much easier** to find the subdirectly irreducibles of a variety.

KA is **not** CD:



$\cdot$	0	a	b	c	1
0	0	0	0	0	0
a	0	0	0	0	a
b	0	0	0	0	b
c	0	0	0	0	c
1	0	a	b	c	1

Figure 1: A non-congruence distributive Kleene algebra

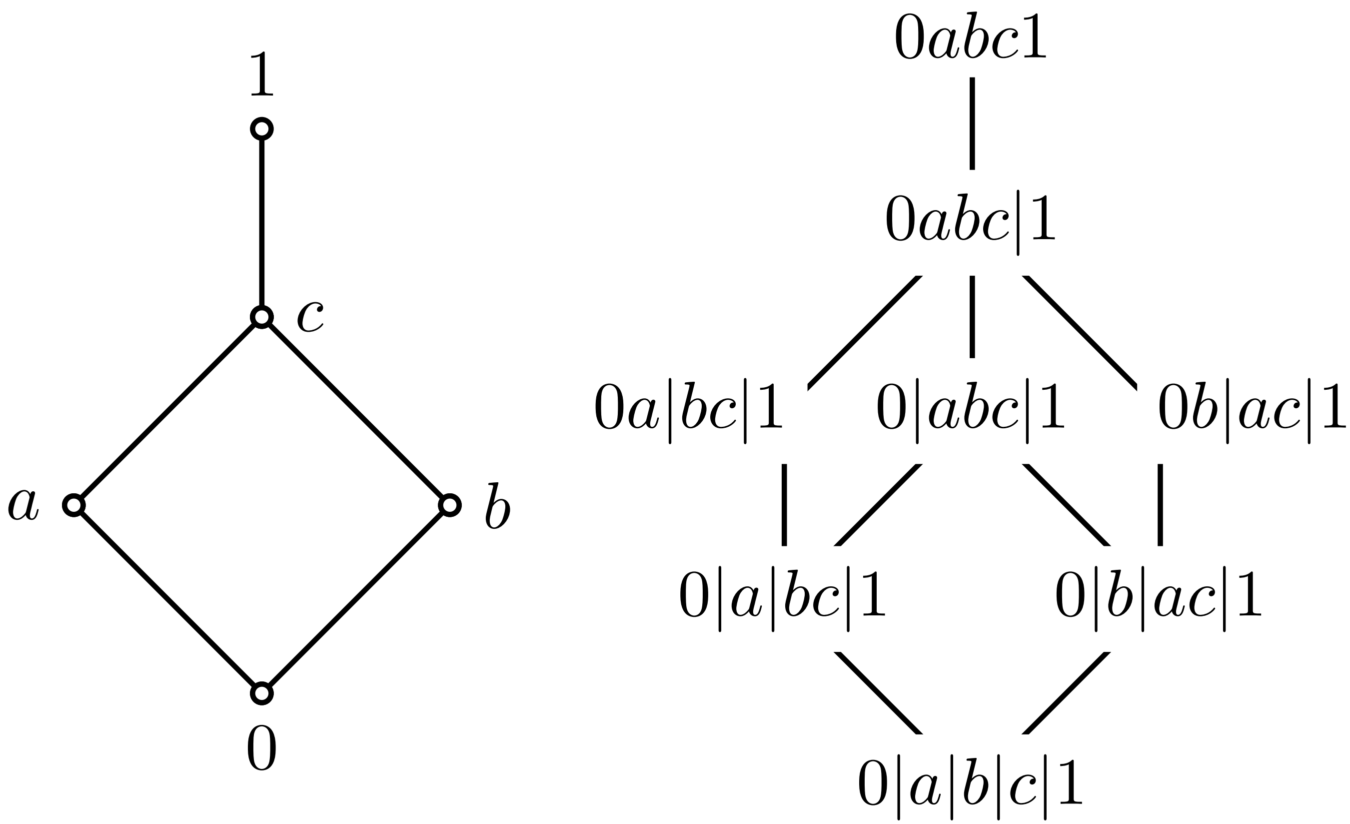


Figure 2: $\mathrm{Con}(A)$ labelled with congruence blocks

Note that $bx \le b \iff x \le 1$, hence $b\backslash b = 1$

$cx \le b \iff x \le c$, hence $c\backslash b = c$

so $b\theta c \implies 1\theta c$.

Therefore A with residuals has only two congruences.

We now give an outline of a noncommutative version of a result by Raftery and van Alten [2004] that shows RKA is CD.

Instead of congruences, we use congruence filters:

$F \subseteq A$ is a **congruence filter** if

(CF$_1$) $x, y \in F, u \in A$ implies $1, x \vee u, xy, u\backslash xu, ux/u \in F$

(CF$_2$) $x\backslash z, y\backslash z \in F$ implies $z/x, (x \vee y)\backslash z \in F$

Lemma 1. *For any residuated semilattice* A, $\mathrm{Con}(A) \cong \mathrm{CF}(A)$, *where* $F \mapsto \theta_F = \{\langle x, y\rangle : x\backslash y, y\backslash x \in F\}$ *and* $\theta \mapsto [\uparrow 1]_\theta = \{x : \exists y(x\theta y \geq 1)\}$.

The next result is adapted from Blok and Raftery [2004] Thm 14.11, and shows that joins of filters are easier to compute with residuals.

Lemma 2. $F \vee G = \{a \in A : \exists b \in F$ *with* $b\backslash a \vee a \in G\}$ *and*

$F \wedge G = F \cap G$

Theorem 3. *van Alten and Raftery [2004]*

Residuated join-semilattices are congruence distributive.

Proof. It suffices to show that for $F, G, H \in \mathrm{CF}(A)$ we have $(F \vee G) \cap (F \vee H) \subseteq F \vee (G \cap H)$.

Let $a \in (F \vee G) \cap (F \vee H)$. By the preceding lemma, $\exists b, c \in F$ such that $b\backslash a \vee a \in G$ and $c\backslash a \vee a \in H$.

By (CF$_1$) $b \leq a/(b\backslash a)$ implies $a/(b\backslash a) \in F$,

similarly $a/(c\backslash a) \in F$ and always $a/a \in F$,

hence $a/(b\backslash a \vee c\backslash a \vee a) \in F$.

Let $d = b\backslash a \vee c\backslash a \vee a$, then $a/d \in F$, so $d\backslash a \in F$ by (CF$_2$), whence $d\backslash a \vee a \in F$.

Since $d \geq b\backslash a \vee a \in G$, we have $d \in G$, and similarly $d \in H$. Therefore $d \in G \cap H$ and invoking the preceding lemma again we get $a \in F \vee (G \cap H)$. $\square$

In fact Raftery shows that even the $\vee, \backslash, /$-reducts are CD.

Since residuated Kleene algebras are expansions of residuated join-semilattices, it follows that congruence lattices of RKAs are sublattices of congruence lattices of residuated join-semilattices.

Therefore RKA is also CD.

So now we get a wealth of information about RKA from standard results about CD varieties:

Theorem 4. *If $A \in \mathsf{RKA}$ is finite, then*

(1) $Si(HSP(A))$ has only finitely many members (up to isomorphism), hence $HSP(A)$ has only finitely many subvarieties (Jónsson [1967]).

(2) $HSP(A)$ has a finite equational basis (Baker [1972]).

(1) allows us to construct (a small part of) the lattice of subvarieties of RKA from the bottom up.

Since residuated lattices are residuated join-semilattices, we can adapt Jipsen and Tsinakis [2002] Thm 6.3 as follows:

Theorem 5. *There are uncountably many minimal nontrivial varieties of residuated join-semilattices and of residuated Kleene algebras.*

$\cdot$	$\top$	1	d_0	d_1	d_2	d_3	$\dots$	c_3	c_2	c_1	c_0	b	a	0
$\top$	$\top$	$\top$	d_0	d_1	d_2	d_3	$\dots$	c_3	c_2	c_1	c_0	b	a	0
1	$\top$	e	d_0	d_1	d_2	d_3	$\dots$	c_3	c_2	c_1	c_0	b	a	0
d_0	d_0	d_0	b	b	b	b	$\dots$	b	b	b	0	0	0	0
d_1	d_1	d_1	b	b	b	b	$\dots$	b	b	0	0	0	0	0
d_2	d_2	d_2	b	b	b	b	$\dots$	b	0	0	0	0	0	0
d_3	d_3	d_3	b	b	b	b	$\dots$	0	0	0	0	0	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
c_3	c_3	c_3	b	b	s_2	a	$\dots$	0	0	0	0	0	0	0
c_2	c_2	c_2	b	s_1	a	0	$\dots$	0	0	0	0	0	0	0
c_1	c_1	c_1	s_0	a	0	0	$\dots$	0	0	0	0	0	0	0
c_0	c_0	c_0	a	0	0	0	$\dots$	0	0	0	0	0	0	0
b	b	b	0	0	0	0	$\dots$	0	0	0	0	0	0	0
a	a	a	0	0	0	0	$\dots$	0	0	0	0	0	0	0
0	0	0	0	0	0	0	$\dots$	0	0	0	0	0	0	0

Other results about residuated lattices also apply. E.g. every join-semilattice is embedded in a cancellative residuated Kleene algebra.

The **number of finite Kleene algebras of size n** is the same as the number of residuated lattices of size n:

No. of elements	1	2	3	4	5	6	7
No. of algebras	1	1	3	20	149	1488	18554

Residuated Kleene algebras from ℓ-groups and relations

What is the connection between Kleene algebras and relation algebras?

Input-output relations of programs can be viewed as elements in either framework.

What can be said about **relational residuated Kleene algebras**, i.e. RKAs obtained from collections of binary relations closed under composition, union, iteration and residuals?

The element 1 must be a unit for composition but need not correspond to the identity relation.

Examples of such Kleene algebras can be constructed from lattice-ordered groups as follows:

Let $(A, \vee, \wedge, \cdot, ^{-1}, 1)$ be an ℓ-group, i.e. $(A, \vee, \wedge)$ is a lattice, $(A, \cdot, ^{-1}, 1)$ is a group, and $\cdot$ distributes over $\vee$.

This forces the lattice to be distributive.

Instead of using $^{-1}$, we can view ℓ-groups as residuated structures with $x\backslash y = x^{-1}y$ and $x/y = xy^{-1}$.

By Holland's [1972] Embedding Theorem, every ℓ-group is embedded in an ℓ-group of order-automorphisms of a linear order.

Theorem 6. *Every ℓ-group is isomorphic to a relational residuated (join-semi)lattice.*

Proof. Let $G = \langle \text{Aut}(\Omega), \vee, \wedge, \circ, id_\Omega, \backslash, / \rangle$ be the ℓ-group of order-automorphisms of a linear order Ω.

Note that $\vee, \wedge$ are calculated pointwise.

By **Holland's embedding theorem**, it suffices to embed G into a residuated lattice of relations on Ω.

For $g \in G$, let $R_g = \{(u, v) : u \leq g(v)\}$.

$R_g \cup R_h = R_{g \vee h}$ since

$$\begin{aligned} & (u, v) \in R_g \cup R_h \\ \iff \quad & u \leq g(v) \text{ or } u \leq h(v) \\ \iff \quad & u \leq \max\{g(v), h(v)\} = (g \vee h)(v) \\ \iff \quad & (u, v) \in R_{g \vee h} \end{aligned}$$

$R_g \circ R_h = R_{g \circ h}$ since

$$
\begin{aligned}
& (u, v) \in R_g \circ R_h \\
\iff\quad & \exists w \, [(u, w) \in R_g \text{ and } (w, v) \in R_h] \\
\iff\quad & \exists w \, [u \leq g(w) \text{ and } w \leq h(v)] \\
\iff\quad & u \leq g(h(v)) \qquad\qquad (w = h(v) \text{ for } \Longleftarrow) \\
\iff\quad & (u, v) \in R_{g \circ h}
\end{aligned}
$$

$R_g \backslash R_h = R_{g \backslash h}$ since

$$
\begin{aligned}
& (u,v) \in R_g \backslash R_h \\
\iff \quad & R_g \circ \{(u,v)\} \subseteq R_h \\
\iff \quad & \forall w \, [(w,u) \in R_g \implies (w,v) \in R_h] \\
\iff \quad & \forall w \, [w \leq g(u) \implies w \leq h(v)] \\
\iff \quad & g(u) \leq h(v) \\
\iff \quad & u \leq g^{-1}(h(v)) = (g \backslash h)(v) \\
\iff \quad & (u,v) \in R_{g \backslash h}
\end{aligned}
$$

$R_g/R_h = R_{g/h}$ is similar.

Finally, $R_{id} = \{(u, v) : u \leq v\} =$ "$\leq$" is an identity element since

$$R_g \circ R_{id} = R_{g \circ id} = R_g = R_{id} \circ R_g.$$

Therefore $\{R_g : g \in G\}$ is a residuated lattice of relations that is isomorphic to G. $\square$

To ensure that 0 and * are defined, we add a bottom and top element to the residuated join-semilattice reduct of the ℓ-group.

All nontrivial ℓ-groups are infinite, but examples of finite RKAs of relations can be obtained if we restrict to intervals containing 1.

Further examples are constructed by stacking algebras on top of eachother (ordinal sums) or by constructing matrix algebras.

A generalized ordinal sum construction is the following:

Let P be a poset, and let A_i ($i \in P$) be a family of RKAs. The **poset sum** is defined as

$\bigoplus_{i\in P} A_i = \{a \in \prod_{i\in P} : i < j \implies a_i = \top$ or $a_j = 0\}$.

Here $\top$ denotes the largest element of A_i (if it exists).

This subset of the product is closed under $\vee$ and $\cdot$.

We define two auxillary operations on the poset sum:

$$(a^{\downarrow})_i = \begin{cases} 0 & \text{if } a_j < \top \text{ for some } j < i \\ a_i & \text{otherwise} \end{cases}$$

$$(a^{\uparrow})_i = \begin{cases} \top & \text{if } a_j > 0 \text{ for some } j > i \\ a_i & \text{otherwise} \end{cases}$$

Then $\backslash^{\oplus}, /^{\oplus}, 1^{\oplus}$ can be defined on the poset sum as follows:

$$a\backslash^{\oplus}b = (a\backslash b)^{\downarrow}$$

$$a/^{\oplus}b = (a/b)^{\downarrow}$$

$$1^{\oplus} = 1^{\uparrow}$$

Theorem 7. *The class of relational RKAs is closed under poset sums.*

In fact, for a particular subvariety of RKAs, this construction describes all the finite members.

Divisible join-semilattices are residuated join-semilattices that satisfy the following identities:

$$x = (x/(x \vee y))(x \vee y)$$

$$x = (x \vee y)((x \vee y)\backslash x)$$

Theorem 8. *All finite divisible join-semilattices are commutative, and can be constructed by poset sums of finite MV-chains.*

In fact, there is a 1-1 correspondence between finite divisible join-semilattices and finite posets labelled with natural numbers.

This result is useful for constructing and counting finite divisible Kleene algebras.