Right generalized hoops, varieties of loops and partial algebras

Peter Jipsen

School of Computational Sciences and
Center of Excellence in Computation, Algebra and Topology (CECAT)
Chapman University, Orange, California

ADAM 2016: Automated Deduction and its Applications to Mathematics

University of New Mexico, Albuquerque, August 5-7, 2016

Outline

- Quasigroups and groups
- Right-residuated binars
- Right-divisible residuated binars
- Right generalized hoops
- Finitely generated varieties of loops
- Partial algebras

Groups and quasigroups

Definition

A ***quasigroup*** $(A, \cdot, \backslash, /)$ is a set with 3 binary operations such that for all $x, y, z \in A$

$$xy = z \iff x = z/y \iff y = x\backslash z$$

i.e., one can solve **all equations** with no repeated variables

Quasigroups form a **variety** defined by the identities

$$(x/y)y = x = xy/y \quad \text{and} \quad y(y\backslash x) = x = y\backslash yx$$

An associative quasigroup is **term-equivalent to a group**:

$$1 = y/y \quad \text{and} \quad x^{-1} = (y/y)/x$$

Hint: $xy/z = x((y/z)z)/z = (x(y/z))z/z = x(y/z)$
hence $x = xy/y = x(y/y)$ and therefore $x\backslash x = y/y$

Residuated binars and semigroups

Definition

A ***residuated binar*** $(A, \leq, \cdot, \backslash, /)$ is a poset $(A, \leq)$ with 3 binary operations such that for all $x, y, z \in A$

$$xy \leq z \iff x \leq z/y \iff y \leq x\backslash z$$

i.e., one can solve **simple inequalities**

Residuated binars are defined (relative to posets) by the **inequations**

$$(x/y)y \leq x \leq xy/y \quad \text{and} \quad y(y\backslash x) \leq x \leq y\backslash yx$$

Farulewski 2005: The universal theory of residuated binars is **decidable**
What about the universal theory of quasigroups or loops?

Definition

A ***residuated semigroup*** is an **associative** residuated binar

If the poset is an **antichain**, then any **residuated semigroup is a group**!
$\Rightarrow$ residuated semigroups are **generalizations of groups** (replace $=$ by $\leq$)

Residuated lattices and GBL-algebras

Definition

A **residuated lattice** $(A, \wedge, \vee, \cdot, \backslash, /, 1)$ is a residuated ℓ-monoid

i.e., a lattice $(A, \wedge, \vee)$ and a residuated semigroup with unit

They are the algebraic semantics of **substructural logic**

The **equational theory** of residuated lattices is **decidable**

Definition

A residuated lattice is **divisible** if $x \leq y \implies x = y(y\backslash x) = (x/y)y$

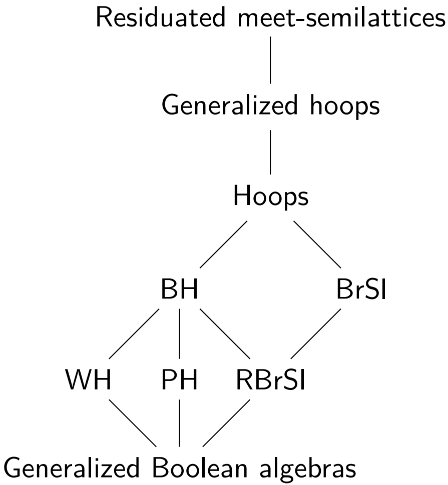
Also called a **generalized Basic Logic** algebra (GBL-algebra)

Open problem: Is the equational theory of GBL-algebras **decidable**?

GBL-algebras

- Have **distributive** lattice reducts **[J. - Tsinakis 2002]**
- All **finite** GBL-algebras are **commutative** and **integral** **[J. - Montagna 2006]**
- All **finite** GBL-algebras are **poset products** of Wajsberg chains **[J. - Montagna 2009]**

Some residuated meet-semilattices



Right-residuated binars

GBL-algebras fairly complicated, so consider **simpler** algebras

Definition

A ***right-residuated binar*** $(A, \le, \cdot, /)$ is a poset $(A, \le)$ with 2 binary operations such that for all $x, y, z \in A$

$$xy \le z \iff x \le z/y$$

Therefore $\cdot, /$ are **order-preserving in the left argument**:

Let $x \le y$. Then $yz \le yz \iff y \le yz/z \implies x \le yz/z \iff xz \le yz$

Similarly $x/z \le x/z \iff (x/z)z \le x \implies (x/z)z \le y \iff x/z \le y/z$

It would be nice if $\le$ is **definable** from the algebraic operations

Right-divisible residuated binars

Theorem

The following are equivalent in any right-residuated binar.

(i) *For all* x, y $(x \leq y \iff \exists u(x = uy))$

(ii) *For all* x, y $(x \leq y \iff x = (x/y)y)$ *(i.e. right divisibility).*

(iii) *The identities* $(y/y)x = x$ *and* $(y/x)x = (x/y)y$ *hold.*

Proof: Easy using Prover9

Right-divisible unital residuated binar

The identities for divisibility are $(y/y)x = x$ and $(y/x)x = (x/y)y$

So y/y is a left unit, and Prover9 shows $x \leq y/y$

Hence y/y is the top element of the poset, denoted by 1

A **right-divisible unital residuated binar** is a residuated binar $(A, \leq, \cdot, 1, /)$ such that $x/x = 1$, $1x = x$ and $(y/x)x = (x/y)y$ hold

The partial order is definable by $x \leq y \iff x = (x/y)y$

Note that $(x/y)y$ is a lower bound for any pair of elements x, y and we always have $1 \leq 1/x$.

Theorem

In a right-divisible unital binar the partial order is down-directed and the identity $1/x = 1$ *holds. The order is also definable by* $x \leq y \iff y/x = 1$.

Right-divisible unital residuated binars

Theorem

$(A,\cdot,1,/)$ *is a right-divisible unital residuated binar if and only if it satisfies the (quasi)identities* $x/x=1$ $\quad$ $1x=x$

$(y/x)x=(x/y)y$

$x/y=1$ *and* $y/z=1 \implies x/z=1$

$z/xy=1 \iff (z/y)/x=1$

Note: $x\le y$ if and only if $y/x=1$. This is a partial order:

- **reflexive** by $x/x=1$
- **antisymmetric** since if $x/y=1$ and $y/x=1$ then $x=1x=(y/x)x=(x/y)y=1y=y$
- **transitive** by the implication above

Open problem: Can the quasiequations be replaced by **identities**?

Open problem: Is the (quasi)equational theory **decidable**?

The right hoop identity

Adding one more identity produces an interesting sub**variety**

In the arithmetic of real numbers (or in any field) the following equation is fundamental to the **simplification of nested fractions**:

$$\frac{\frac{x}{y}}{z} = \frac{1}{z} \cdot \frac{x}{y} = \frac{x}{zy}$$

In a right-residuated binar this is the ***right hoop identity***:

$$(x/y)/z = x/zy$$

Consequences of the right hoop identity

Theorem

In a right divisible unital residuated binar the right hoop identity $x/yz = (x/z)/y$ *implies* $x(yz) = (xy)z$, $x1 = x$ *and* $x/1 = x$.

Proof.

$x(yz) = 1(x(yz))$ (left unital)
$= [(xy)z/(xy)z](x(yz))$ since $1 = x/x$
$= [((xy)z/z)/xy](x(yz))$ (right hoop id.)
$= [(((xy)z/z)/y)/x](x(yz))$ (right hoop id.)
$= [((xy)z/yz)/x](x(yz))$ (right hoop id.)
$= [(xy)z/x(yz)](x(yz))$ (right hoop id.)
$= [x(yz)/(xy)z]((xy)z)$ since $(y/x)x = (x/y)y$
$=$ reverse steps to get $= (xy)z$.
Now $x \leq 1$ implies $x = (x/1)1$, hence
$x1 = ((x/1)1)1 = (x/1)(11) = (x/1)1 = x$.
Finally $x/1 = (x/1)1 = (1/x)x = 1x = x$. □

Right generalized hoops

Definitions

A ***right generalized hoop*** $(A, \cdot, 1, /)$ is defined by the identities

$x/x = 1, \quad 1x = x, \quad (x/y)y = (y/x)x \quad$ and $\quad x/(yz) = (x/z)/y$

Define the **term-operation** $x \wedge y = (x/y)y$ and

a **binary relation** $\leq$ by $x \leq y \iff x = x \wedge y$

The next theorem shows that $\wedge$ is a **semilattice** operation

hence $\leq$ is a **partial order** on A

Moreover, A is **right-residuated** with respect to this order

and the left-unit 1 is the **top element**

Properties of right generalized hoops

Theorem

Let A be a right generalized hoop. Then
(i) *the term* $x \wedge y = (x/y)y$ *is idempotent, commutative and associative,*
(ii) $\leq$ *is a partial order and* $\wedge$ *is a meet operation with respect to* $\leq$*,*
(iii) $x \leq y \iff y/x = 1$ *for all* $x, y \in A$*,*
(iv) $xy \leq z \iff x \leq z/y$ *for all* $x, y, z \in A$*, and*
(v) $x \leq 1$ *for all* $x \in A$*, i.e.,* A *is integral.*

Proof.

Prover9 □

Right generalized hoops and polrims

There is a 4-element right generalized hoop s.t. $\cdot$ is **not order-preserving in the right argument**

$\cdot$	0	a	b	1
0	0	0	0	0
a	0	a	**b**	**a**
b	0	a	b	b
1	0	a	b	1

/	0	a	b	1
0	1	0	0	0
a	1	1	0	a
b	1	0	1	b
1	1	1	1	1

Partially ordered left-residuated integral monoids (or polrims for short) are left-residuated monoids such that the monoid operation is order-preserving in both arguments

They have been studied by **van Alten [1998]** and **Blok, Raftery [1997]**

Results on **polrims** do not automatically apply to right generalized hoops

Polrims are congruence distributive, but this is open for right generalized hoops

Generalized hoops

Definition

A ***generalized hoop*** is an algebra $(A, \cdot, 1, \backslash, /)$ such that

- $(A, \cdot, 1, /)$ is a right generalized hoop, $(A, \cdot, 1, \backslash)$ is a left generalized hoop (defined by the mirror-image identities)
- and both these algebras have the same meet operation, i. e., the identity $(x/y)y = y(y\backslash x)$ holds

Generalized hoops were first studied by **Bosbach [1969]**

The name ***hoop*** was introduced by **Büchi and Owen [1975]**

Generalized hoops are also called ***pseudo hoops***

By the preceding theorem, they are **left- and right-residuated**

They are polrims, hence **congruence distributive** (**van Alten [1998]**)

Multiplication distributes over $\wedge$

In a residuated binar, the residuation property implies that $\cdot$ distributes over any existing joins in each argument. However, this is not true for meets.The following result was proved by **N. Galatos** for **GBL-algebras** but already holds for **generalized hoops**.

Theorem

In any generalized hoop $(x \wedge y)z = xz \wedge yz$ *and* $x(y \wedge z) = xy \wedge xz$.

Proof.

From $xz \leq xz$ it follows that $x \leq xz/z$, hence $xz \leq (xz/z)z$.Likewise, from $xz/z \leq xz/z$ we deduce $(xz/z)z \leq xz$, therefore $xz = (xz/z)z$.Note that $(x \wedge y)z \leq xz \wedge yz$ always holds since $\cdot$ is order-preserving.
Now $xz \wedge yz = (xz/yz)yz = ((xz/z)/y)yz$ (right hoop id.)
$= (y/((xz)/z))(xz/z)z$ by assoc. and divisibility
$= (y/((xz)/z))xz$ by the derived identity
$\leq (y/x)xz = (y \wedge x)z$ since $x \leq (xz)/z$. The second identity is similar. □

Not true for right generalized hoops

In the last step we made use of the implication $x \le y \Rightarrow z/y \le z/x$ which holds in all residuated binars.

The preceding result requires that $\cdot$ is **order-preserving in the right argument**
Recall the 4-element right generalized hoop from earlier

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

$/$	0	a	b	1
0	1	0	0	0
a	1	1	0	a
b	1	0	1	b
1	1	1	1	1

$(a \wedge b)a = (a/b)ba = 0ba = 0$ while $aa \wedge ba = a \wedge a = (a/a)a = 1a = a$.

$1 = ((x/y)/(z/y))/(x/z)$ is equivalent to order-preserving on right

Finitely generated varieties of groups

A **variety** $\mathscr{V}$ is a class of algebras determined by identities

Birkhoff 1935 (Tarski 1942): $\mathscr{V}$ is a variety iff $\mathscr{V} = HSP(\mathscr{K})$ for some class $\mathscr{K}$

$\mathscr{V}$ is a **finitely generated** variety if $\mathscr{K}$ is a finite class of finite algebras

Varieties of groups have been studied in detail in a monograph by Hanna Neumann [1967]

The varieties generated by the finite cyclic groups $\mathbb{Z}_n$ are all distinct and, ordered by inclusion, they form a lattice isomorphic to the divisibility lattice of the natural numbers

However the dihedral group of size 8 and the quaternion group are nonisomorphic subdirectly irreducible groups with 8 elements that generate the same variety

Finitely generated varieties of loops

All loops of size 4 or less are associative, hence are groups:
$\mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$

For size 5 there are 5 nonassociative loops, denoted $5_1, 5_2, 5_3, 5_4, 5_5$

There are 107 nonassociative loops of size 6, denoted $6_1, 6_2, \ldots, 6_{107}$, with numbering taken from the library of small loops in the GAP loops package

Fact 1: A is subdirectly irreducible iff $\mathrm{Con}(A)$ has a unique atom

Fact 2: A variety is generated by its subdirectly irreducible members

$6_1, 6_2, \ldots, 6_{107}$ are subdirectly irreducible, since the only subdirectly reducible loops of size ≤ 6 are $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_6$

The subdirectly irreducible groups of size ≤ 6 are $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5$ and S_3
Hence there are a total of $1 + 1 + 1 + 6 + 108 = 117$ subdirectly irreducible loops of size up to 6

Use the Universal Algebra Calculator (`uacalc.org`) and a Sage package to check $A \in HSP(B)$ for all distinct pairs of loops in this list

UACalc finds a minimal size generating set X for the loop A, then uses a subpower algorithm to calculate the free algebra in $HSP(B)$ on $n = |X|$ generators

Simultaneously attempts to extend a bijection between the n generators and the set X to a homomorphism from the free algebra to A.

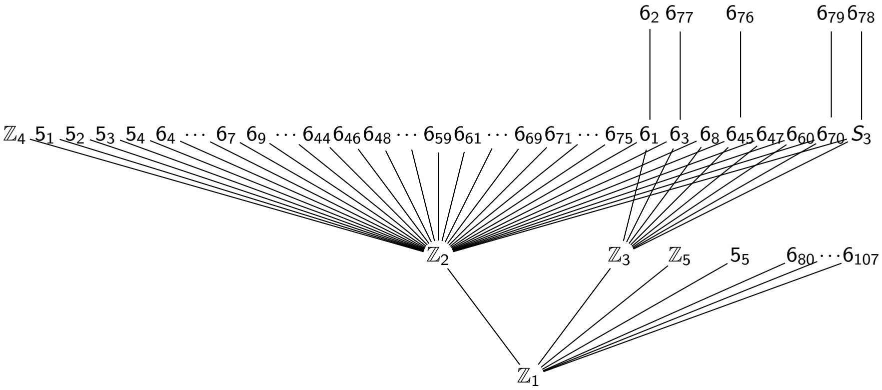
If such a homomorphism is found, the relation holds, and if not, then the Universal Algebra Calculator reports the first equation that it found which holds in B but fails in A.

$A \in HSP(B)$ is equivalent to $HSP(A) \subseteq HSP(B)$

$\Rightarrow$ **HSP-poset** of varieties generated by a subdirectly irreducible algebra

A **minimal variety** is a cover of the variety of one-element algebras

Finitely generated varieties of loops



Finitely generated varieties of loops

The nonassociative 5-element loops (omitting the identity 1):

5_1	2	3	4	5
2	1	4	5	3
3	4	5	1	2
4	5	2	3	1
5	3	1	2	4

5_2	2	3	4	5
2	1	4	5	3
3	4	5	2	1
4	5	1	3	2
5	3	2	1	4

5_3	2	3	4	5
2	1	4	5	3
3	5	1	2	4
4	3	5	1	2
5	4	2	3	1

5_4	2	3	4	5
2	1	4	5	3
3	5	2	1	4
4	3	5	2	1
5	4	1	3	2

5_5	2	3	4	5
2	3	1	5	4
3	4	5	1	2
4	5	2	3	1
5	1	4	2	3

$\Rightarrow \mathbb{Z}_2$ is a subgroup of the first 4 loops, but not of the last one

Problem (open?): Axiomatize the 5 varieties generated by these loops

Find all subvarieties of these varieties (are there any generated by a larger loop?)

Finitely generated varieties of loops

Two loops that generate comparable varieties (highlighting the differences)

6_1	2	3	4	5	6
2	1	4	3	6	5
3	4	5	6	1	2
4	3	6	5	2	1
5	6	**1**	**2**	**4**	**3**
6	5	**2**	**1**	**3**	**4**

$\leq$

6_2	2	3	4	5	6
2	1	4	3	6	5
3	4	5	6	1	2
4	3	6	5	2	1
5	6	**2**	**1**	**3**	**4**
6	5	**1**	**2**	**4**	**3**

Problem: Does $\mathrm{HSP}(6_2)$ cover $\mathrm{HSP}(6_1)$?

Are there nonisomorphic loops of size 7 that generate the same variety?

Partial algebras

math.chapman.edu/∼jipsen/uajs