Domain and Antidomain Semigroups

Jules Desharnais, Peter Jipsen and Georg Struth

Université Laval, Chapman University, University of Sheffield

Nov 4, 2009

Outline

- Domain/range and antidomain/antirange operations on relations
- Motivation for studying (anti)domain/range semigroups
- Representation results
- Hirsch-Mikulas nonrepresentability result
- Conclusion and open problems

$Rel(X)$ = set of *binary relations* R on a set X

$R; S$ = *composition* of relations

unary (anti)*domain* and (anti)*range* operations are defined by

$$\begin{aligned} d(R) &= \{(u,u) \in X^2 : (u,v) \in R \text{ for some } v \in X\}, \\ a(R) &= \{(u,u) \in X^2 : (u,v) \notin R \text{ for all } v \in X\}, \\ r(R) &= \{(v,v) \in X^2 : (u,v) \in R \text{ for some } u \in X\}, \\ r'(R) &= \{(v,v) \in X^2 : (u,v) \notin R \text{ for all } u \in X\}. \end{aligned}$$

In *relation algebras*, $\quad d(R) = R; R^\smile \cap \mathrm{id}, \qquad a(R) = \mathrm{id} - d(R),$

$$r(R) = R^\smile; R \cap \mathrm{id}, \qquad r'(R) = \mathrm{id} - r(R)$$

Elements of $Rel(X)$ represent *actions* or *computations*

Operations model the *control flow* in the system

Multiplication represents e.g. *sequential* or *parallel composition* of actions

Addition (union) represents *nondeterministic choice*

Multiplicative units model *ineffective actions* (*skip*)

Additive units model *abortive actions*

E.g. *semigroups* or *monoids* model sequential composition

Semirings model sequential composition and nondeterministic choice

Concrete models of such algebras are sets of *partial* and *total functions*, *binary relations*, *languages*, *sets of paths in graphs* or *sets of traces* ...

A *domain* operation yields *enabledness conditions* for actions

I.e. the *domain* $d(x)$ of an action x models those states from which the action x *can be executed*

The *antidomain* $a(x)$ models those states from which the action x *cannot be executed*

An axiomatisation of *domain for semirings* $(S, +, \cdot, 0, 1)$, where $d : S \to S$, is given in [Desharnais, Möller, Struth 2006] [J, Struth 2008]:

$$x = d(x) \cdot x \qquad d(x \cdot y) = d(x \cdot d(y)) \qquad d(x) + 1 = 1$$

$$d(0) = 0 \qquad d(x + y) = d(x) + d(y)$$

Consequences of the axioms

The *domain algebra* $d(S) = \{d(x) : x \in S\}$ is a *distributive lattice*

Domain semirings are *idempotent* $(x + x = x)$

Distributive lattices are suitable statespaces, but *Boolean algebras* are even better as *test algebra*

Antidomain (the Boolean complement of domain) is a map $a : S \to S$ that satisfies

$$a(x) \cdot x = 0 \qquad a(x \cdot y) = a(x \cdot a(a(y))) \qquad a(a(x)) + a(x) = 1$$

Domain operations can be obtained in *antidomain semirings* by defining $d(x) = a(a(x))$

Even *without* the additive operation, the algebras are interesting for modelling computation, and have been investigated by *semigroup theorists*

In this talk we will consider some of the following classes

domain		antidomain
LC-semigroups	LC-monoids	closable SP-semigroups
$\cup\!\!\!\!\!\!\backslash$	$\cup\!\!\!\!\!\!\backslash$	$\cup\!\!\!\!\!\!\backslash$
d-semigroups	d-monoids	a-monoids
$\cup\!\!\!\!\!\!\backslash$	$\cup\!\!\!\!\!\!\backslash$	$\cup\!\!\!\!\!\!\backslash$
twisted d-semigroups	twisted d-monoids	twisted a-monoids

Recall that a *semigroup* is a set with an associative binary operation $\cdot$

A *monoid* is a semigroup with an identity element 1

A *domain semigroup*, or *d-semigroup*, is a semigroup $(S, \cdot)$ extended by a domain operation $d : S \to S$ that satisfies the following axioms

$$\begin{aligned}
&\text{(D1)} \quad d(x)x = x \\
&\text{(D2)} \quad d(xy) = d(xd(y)) \\
&\text{(D3)} \quad d(d(x)y) = d(x)d(y) \\
&\text{(D4)} \quad d(x)d(y) = d(y)d(x)
\end{aligned}$$

A monoid that satisfies these axioms is a *domain monoid* or *d-monoid*

It is easy to check that the axioms (D1)-(D4) hold in $Rel(X)$ and, in fact, in all domain semirings

(D2) is the *locality axiom* in the context of domain semirings

In semigroups, it has also been called *left-congruence condition* [Jackson and Stokes 2001]

The class of (left/right) closure semigroups is defined by [Jackson and Stokes 2001]

A *left closure semigroup*, or *LC-semigroup*, is a semigroup that satisfies the following axioms.

$$\begin{array}{ll} \text{(D1)} & d(x)x = x \\ \textit{(L2)} & d(d(x)) = d(x) \\ \textit{(L3)} & d(x)d(xy) = d(xy) \\ \text{(D4)} & d(x)d(y) = d(y)d(x) \end{array}$$

Analogously, an *LC-monoid* is an LC-semigroup that is also a monoid.

Lemma

The class of d-semigroups is strictly contained in the class of LC-semigroups.

Lemma

d-semigroups are LC-semigroups that satisfy the locality axiom.

A *domain element* of an LC-semigroup, domain semigroup or the corresponding monoid S is an element of $d(S) = \{d(x) : x \in S\}$

Lemma

The domain elements of an LC-semigroup are precisely the fixed points of the domain operation

Hence one can express the fact that x is a domain element by $d(x) = x$

Lemma

1. *For any LC-semigroup S, the set $d(S)$ is a meet-subsemilattice of S. If S has a right unit 1, then $d(1) = 1$ is the top element of $d(S)$.*
2. *Every meet-semilattice is a domain semigroup if $d(x) = x$ is imposed, and every meet-semilattice with a top element is a domain monoid*

$d(S)$ is called the *domain algebra* of S

The semilattice-order on the domain algebra can be extended to a partial order—called the *fundamental order*—on the whole LC-semigroup by

$$x \leq y \;\Leftrightarrow\; x = d(x)y$$

On partial functions, the dual of the fundamental order is called the *refinement order*

The usual *relational demonic refinement* ordering can also be defined in this framework:

$$x \text{ refines } y \quad \text{iff} \quad d(y) \leq d(x) \;\text{ and }\; d(y)x \leq y.$$

Lemma

1. *Every monoid can be expanded to a d-monoid.*
2. *Some semigroups cannot be expanded to d-semigroups.*

Proof.

(1) The map $d(x) = 1$ for all $x \in S$ satisfies (D1) to (D4)

(2) The semigroup of positive integers under addition has no idempotents

Hence there are no candidates for membership in the domain algebra, and it is impossible to define a domain operation

Representable d-monoids

Tarski [1948] defined the class RA of abstract relation algebras and asked if every relation algebra is *representable*, i.e. embeddable into an algebra of binary relations

Monk [1964] proved that the class RRA of representable relation algebras is *not finitely axiomatizable*

Does the axiomatisation of d-monoids captures all the properties of the domain operation of binary relations?

A d-monoid is called *representable* if it can be embedded in $Rel(X)$ for some set X such that $\cdot$, d and 1 correspond to composition, relational domain and id_X

By the fundamental theorem for relation algebras [Schein 1970] the class of representable d-monoids is a *quasivariety*

Proposition

The following quasiequation fails in a 4-element d-monoid but holds in $Rel(X)$*:* $xy = d(x)$ *and* $yx = x$ *and* $d(y) = 1$ *imply* $x = d(x)$

Proof.

Finding a 4-element counterexample for d-monoids is easy with Mace4.

To prove the result for $Rel(X)$, consider $x, y \in Rel(X)$ and $(a, b) \in x$.

Then $d(y) = 1$ implies $(b, c) \in y$ for some c.

It follows from $xy = d(x)$ that $c = a$, hence $(b, a) \in y$.

Now $yx = x$ implies that $(b, b) \in x$.

Finally $xy = d(x)$ yields $(b, a) \in d(x)$, whence $b = a$.

Since (a, b) is arbitrary it follows that $x = d(x)$. □

Corollary

The quasivariety of representable d-monoids is not a variety

Twisted Domain Semigroups

Partial functions under composition satisfy another equational property called the *twisted law* by [Jackson and Stokes 2001]:

$$xd(y) = d(xy)x$$

This identity fails in $Rel(X)$ if we take x to be any relation that is not *deterministic*

A d-semigroup/monoid or LC-semigroup/monoid is *twisted* if it satisfies the twisted law

Lemma

The classes of twisted LC-semigroups and twisted d-semigroups coincide, and they are strictly contained in the class of d-semigroups.

Various *representation theorems* have been proved for families of semigroups with respect to partial functions. E.g.

• every *group* is embedded in the *symmetric group* $S(X)$ of all permutations of a set X.

• every *semigroup* is embedded in the *transformation semigroup* $T(X)$ of all functions on a set X.

Inverse semigroups are semigroups with a unary operation $^{-1}$ that satisfies the identities $x^{-1-1} = x$, $xx^{-1}x = x$ and $xx^{-1}yy^{-1} = yy^{-1}xx^{-1}$.

It is a standard result of semigroup theory (independently due to Vagner 1952 and Preston 1954) that

• every *inverse semigroup* is embedded in the *symmetric inverse semigroup* $PI(X)$ of all partial injections on X.

Theorem (Trokhimenko 1973, Jackson Stokes 2001)

Every twisted d-semigroup can be embedded in a partial transformation semigroup, hence representable.
If the semigroup has a unit, it is mapped to the identity function.

Proof (outline).

Let S be a twisted d-semigroup and consider the partial transformation semigroup $PT(S)$. For $a \in S$ define

- $D_a = \{xd(a) : x \in S\} = \{y \in S : yd(a) = y\}$,
- $f_a : D_a \to S$ by $f_a(x) = xa$, and
- $h : S \to PT(S)$ by $h(a) = f_a$.

The map h is called the *Cayley embedding* and it remains to check that

1. $d(f_a) = f_{d(a)}$,
2. $f_a;f_b = f_{ab}$, and
3. h is injective.

This is fairly straight forward, using the twisted law for (2). □

So verification of deterministic sequential programs can be done abstractly entirely within the variety of twisted d-monoids

Corollary

Every commutative d-semigroup (d-monoid) is twisted, and can be embedded in a partial transformation semigroup (monoid)

$$d(xy)x \overset{D2}{=} d(xd(y))x \overset{com}{=} d(d(y)x)x \overset{D3}{=} d(y)d(x)x \overset{D1}{=} d(y)x \overset{com}{=} xd(y)$$

Hence the classes of commutative representable d-semigroups and d-monoids are both *finitely axiomatizable* varieties

This is in contrast to relation algebras where the variety of commutative representable relation algebras is *not finitely axiomatizable*

Domain-Range Semigroups

A range operation can be defined on arbitrary semigroups by exploiting semigroup duality (with respect to opposition).

A *domain-range semigroup*, or *dr-semigroup* for short, is a semigroup with two unary operations d and r that satisfy the following axioms.

(D1)	$d(x)x = x$	(R1)	$xr(x) = x$
(D2)	$d(xy) = d(xd(y))$	(R2)	$r(xy) = r(r(x)y)$
(D3)	$d(d(x)y) = d(x)d(y)$	(R3)	$r(xr(y)) = r(x)r(y)$
(D4)	$d(x)d(y) = d(y)d(x)$	(R4)	$r(x)r(y) = r(y)r(x)$
(D5)	$d(r(x)) = r(x)$	(R5)	$r(d(x)) = d(x)$

Mace4 can show that the axioms (D5) and (R5) are not implied by the other axioms. This means that without these axioms, the domain algebra and the range algebra can be different.

Schweizer and Sklar [1967] have provided an axiomatisation for *abstract function systems*, using the following domain and range axioms.

$$d(x)x = x \quad d(xd(y)) = d(xy) \quad d(r(x)) = r(x) \quad d(x)r(y) = r(y)d(x)$$
$$xr(x) = x \quad r(r(x)y) = r(xy) \quad r(d(x)) = d(x) \quad xd(y) = d(xy)x$$

Schein [1970] has shown that adding the quasiequation

$$xy = xz \quad \Rightarrow \quad r(x)y = r(x)z$$

axiomatises precisely the quasivariety of *dr*-semigroups of partial transformations, hence this class is *finitely axiomatizable*

So these *dr*-semigroups can all be represented by binary relations

An interesting question is whether *every* *dr*-semigroup can be embedded into $Rel(X)$ for some set X

$d(r)$-monoids are not finitely axiomatizable

Theorem (Hirsch and Mikulas 2009)

The class of representable domain (and range) monoids is not finitely axiomatizable

Given a d-monoid or dr-monoid A, they define a two-player game where the existential player has a *winning strategy* iff A is *representable*

Then they define an infinite sequence of d-monoids or dr-monoids A_n that are *nonrepresentable* but the ultraproduct $(\prod A_n)/U$ for some nonprincipal ultrafilter U is *representable*

Antidomain

We use the abbreviation $x' = a(x)$ for the antidomain operation, and define an *antidomain monoid*, or *a-monoid*, $(S, \cdot, 1, ')$ as a monoid $(S, \cdot, 1)$ that satisfies

$$
\begin{array}{ll}
\text{(A1)} & x'x = 0 \\
\text{(A2)} & x0 = 0 \\
\text{(A3)} & x'y' = y'x' \\
\text{(A4)} & x''x = x \\
\text{(A5)} & x' = (xy)'(xy')' \\
\text{(A6)} & (xy)'x = (xy)'xy'.
\end{array}
$$

This axiomatisation is essentially due to Hollenberg [1997]

An expression $(xy)'$ can be understood as a modal box operator $[x]y'$

It describes the set of states from which each x-step must lead to a state where y is not enabled

Lemma

1. *The map $d(x) = x''$ is a domain operation.*
2. *The antidomain elements of an a-monoid are the fixed points of domain.*

The fixed point lemma in (2) is again a powerful tool for analysing the structure of antidomain elements

We define $x + y = (x'y')'$

Proposition

Let S be an a-monoid. Then $(S', +, \cdot, ', 0, 1)$ is a Boolean subalgebra.

An interesting observation is that using antidomain, *demonic composition* $\Box$ can be defined (it is associative in the presence of the twisted law):

$$x \Box y = (xy')'xy.$$

As in the case of *d*-monoids, by Schein's fundamental theorem, the class of representable *a*-monoids forms a quasivariety. Hollenberg has shown the following two additional results for *a*-monoids.

Theorem (Hollenberg 1997)

1. *The variety of a-monoids and the variety generated by all representable a-monoids are the same.*
2. *The quasivariety of representable a-monoids is not a variety.*

Hollenberg's counterexample for (2) is a 5-element Heyting algebra which fails the quasiequation $x''y = x'' \ \wedge \ x'y = x' \ \Rightarrow \ y = 1$ that holds in all *representable* *a*-monoids

Since each Heyting algebra is a commutative *a*-monoid, it is twisted

So, in contrast to the case of *d*-monoids, the antidomain operation need not be represented correctly by the Cayley map.

Modal operators

The question whether the quasivariety of representable a-monoids is *finitely axiomatisable* is *open*

Modal *box* and *diamond* operators can be defined for domain algebras

$|x\rangle p = (xp)''$ and $|x]p = (xp')'$ where $p = p''$

Then the diamond operator is *strict and additive* and the box operator is *costrict and multiplicative*:

$$|x\rangle 0 = 0 \qquad |x\rangle(p+q) = |x\rangle p + |x\rangle q$$

$$|x]1 = 1 \qquad |x](p \cdot q) = (|x]p) \cdot (|x]q)$$

Also $|x]p = (|x\rangle p')'$ and $|x\rangle p = (|x]p')'$ (Prover9)

Antirange

Finally, *antirange* is axiomatised dually to that of antidomain

Then the antidomain and the antirange algebra *automatically coincide*

Backward box and diamond operators $[x|$ and $\langle x|$ are defined *dually* from antirange

The following laws hold (Prover9)

demodalisation	$\lvert x\rangle p \leq q \Leftrightarrow q'xp = 0$ and $\langle x\rvert p \leq q \Leftrightarrow pxq' = 0$
conjugation	$(\lvert x\rangle p)q = 0 \Leftrightarrow p(\langle x\rvert q) = 0$
Galois connections	$\lvert x\rangle p \leq q \Leftrightarrow p \leq [x\rvert q$ and $\langle x\rvert p \leq q \Leftrightarrow p \leq \lvert x]q$

Because of the Galois connection, diamond operators are even completely additive, and box operators are completely multiplicative

Conclusion

Twisted d-semigroups and twisted d-monoids are representable

Representable d-monoids and dr-monoids are not finitely axiomatizable (Hirsch-Mikulas 2009)

Representable a-monoids are a proper subquasivariety of a-monoids

It is an *open problem* whether they are *finitely axiomatizable* (same for ar'-monoids)

Monoids with antidomain and antirange allow us to define and calculate with modal operators, giving a *unisorted* framework suitable for some automated verification

References

J. Desharnais, G. Struth, *Modal semirings revisited*. In P. Audebaud and C. Paulin-Mohring, editors, *MPC 2008*, volume 5133 of LNCS, pages 360–387. Springer, 2008

J. Desharnais, G. Struth, *Domain Axioms for a Family of Near-Semirings*. In J. Meseguer and G. Roşu, editors, *AMAST 2008*, volume 5140 of LNCS, pages 330–345. Springer, 2008

O. Frink, *Pseudo-complements in semilattices*, Duke Mathematics Journal, 29 (1962), 500–515

M. Hollenberg, *An equational axiomatization of dynamic negation and relational composition*, Journal of Logic, Language and Information, 6 (1997), 381–401

M. Jackson and T. Stokes, *An invitation to C-semigroups*, Semigroup Forum 62 (2001) 279–310

P. Jipsen and G. Struth, *The structure of the one-generated free domain semiring*, in "Relations and Kleene Algebra in Computer Science" (ed. R. Berghammer, B. Möller, G. Struth), LNCS, Vol. 4988, Springer (2008), 234–242

W. McCune, *Prover9 / Mace4*, www.prover9.org, 2007

B. Möller, G. Struth, *Algebras of modal operators and partial correctness*, Theoretical Computer Science, 351, (2006), 221–239

B. M. Schein, *Relation algebras and function semigroups*, Semigroup Forum, Vol 1 (1970) 1–62

B. Schweizer and A. Sklar, *Function systems*, Math. Annalen, 172, (1967), 1–16

V. S. Trokhimenko, *Menger's function systems*, Izv. Vyss. Učebn. Zaved. Matematika, no. 11(138), (1973) 71–78