Domain and Antidomain Semigroups

Jules Desharnais[1], Peter Jipsen[2] and Georg Struth[3]

[1] Département d'informatique et de génie logiciel, Université Laval, Canada
Jules.Desharnais@ift.ulaval.ca
[2] Department of Mathematics and Computer Science, Chapman University, USA
jipsen@chapman.edu
[3] Department of Computer Science, University of Sheffield, UK
G.Struth@dcs.shef.ac.uk

Abstract. We axiomatise and study operations for relational domain and antidomain on semigroups and monoids. We relate this approach with previous axiomatisations for semirings, partial transformation semigroups and dynamic predicate logic.

1 Introduction

We axiomatise and study the(anti)domain and (anti)range operation on semigroups and monoids, generalising the concept of domain monoid in [JS08], and those of (anti)domain and (anti)range for semirings [DS08a] and a family of near-semirings [DS08b]. Our study of the antidomain operation is strongly based on Hollenberg's axioms [Hol97] which surely deserve more attention.

Our interest in these structures is threefold: First, they play a crucial role in the study of free algebras with (anti)domain operations, for representability results with respect to functions and relations, and for algebraising multimodal logics. Second, they form a basis for comparing and consolidating axiomatisations for categories, semigroups and Kleene algebras. Third, they provide a simple flexible basis for automated theorem proving in program and system verification.

Various expansions of semigroups with unary operations have been studied in semigroup theory (cf. [Sch70,JaS01,JaS04]), mostly motivated by the semigroups of partial transformations. Our primary model of interest is the algebra $Rel(X)$ of binary relations R on a set X with composition and unary (anti)domain and (anti)range operations given as subidentity relations. These are defined by

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

The algebra $Rel(X)$ is a standard semantic model for the input-output relation of nondeterministic programs and specifications, and the domain/range operations can be used to define pre- and postconditions and modal (program) operators on a state space. The (anti)domain and (anti)range operations induce a suitable *test algebra*—a state space—on the set of subidentity relations.

In the calculus of relations, partial and total functions, injections and surjections arise as special relations. Previous work in semigroup theory and category theory has investigated domain and antidomain predominantly in the context of (partial) functions. In the same way, domain axiomatisations for functions are specialisations of domain axiomatisations for relations. Therefore, the following subalgebras of $Rel(X)$ are of interest:

$PT(X)$,	the algebra of partial transformations (i.e. partial functions) on X;
$PI(X)$,	the algebra of partial injections on X;
$T(X)$,	the algebra of transformations (i.e. total functions) on X;
$S(X)$,	the algebra of permutations on X.

The first one corresponds to models of deterministic programs. The second and fourth case also consider a unary operation R^{-1} of converse. The domain and range operations are then definable as $d(R) = R;R^{-1} \cap \mathrm{id}_X$ and $r(R) = R^{-1};R \cap \mathrm{id}_X$. For each of these algebras it is natural to study the class of all algebras that can be embedded in them. Depending on the choice of unary operations in the signature, one obtains the class of groups, semigroups, inverse semigroups, and twisted domain semigroups (axiomatisations can be found below).

Many results in this paper have been obtained by automated theorem proving and automated model generation, using the tools Prover9 and Mace4 [McC07]. Instead of presenting these proofs we add input templates for domain semigroups and antidomain monoids to the paper and encourage the reader to replay our arguments with these tools. They are easy to install and use.

2 Motivation and Overview

We are interested in algebras where elements represent actions or computations of some system and where operations model the control flow in the system. Multiplication, for instance, could represent the sequential or parallel composition of actions and addition could represent nondeterministic choice. Special actions like multiplicative units could model ineffective actions—sometimes called *skip*—and additive units could model abortive actions. Examples of such algebras are semigroups or monoids that model sequential composition, and semirings that model sequential composition and nondeterministic choice. Concrete models of such algebras are partial and total functions, binary relations, languages, sets of paths in graphs or sets of traces.

In this context, a domain operation yields enabledness conditions for actions, that is, the domain $d(x)$ of an action x abstractly models those states from which the action x can be executed. Analogously, the antidomain $a(x)$ models those states from which the action x cannot be executed.

The starting point of the current investigation is a previous axiomatisation of domain and antidomain operations for semirings $(S, +, \cdot, 0, 1)$, in which a domain

domain		antidomain
LC-semigroups	LC-monoids	closable SP-semigroups
$\rotatebox{90}{$\subsetneq$}$	$\rotatebox{90}{$\subsetneq$}$	$\rotatebox{90}{$\subsetneq$}$
d-semigroups	d-monoids	a-monoids
$\rotatebox{90}{$\subsetneq$}$	$\rotatebox{90}{$\subsetneq$}$	$\rotatebox{90}{$\subsetneq$}$
twisted d-semigroups	twisted d-monoids	twisted a-monoids

Table 1. Family of domain semigroups

operation is a map $d : S \to S$ that satisfies

$$x = d(x) \cdot x, \qquad d(x \cdot y) = d(x \cdot d(y)), \qquad d(x) + 1 = 1,$$
$$d(0) = 0, \qquad d(x + y) = d(x) + d(y).$$

It can be shown that the *domain algebra* induced by this operation—the set $d(S)$—is a distributive lattice and that each domain semiring is automatically idempotent, that is, $x + x = x$ holds for all $x \in S$. If the semiring elements represent actions of some system, then $d(S)$ represents the states from which actions are enabled. Distributive lattices are suitable statespaces, but Boolean algebras are perhaps even better. To induce a Boolean domain algebra it is convenient to axiomatise a notion of antidomain (the Boolean complement of domain) as a map $a : S \to S$ that satisfies

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

Also antidomain semirings are automatically idempotent. Domain operations can be obtained in antidomain semirings by defining $d(x) = a(a(x))$. These definitions can readily be adapted to some weaker cases of semirings—so-called near-semirings—in which some of the semiring axioms are dropped [DS08b].

A natural generalisation is to investigate how these axioms can be adapted when the operation of addition is dropped and the domain algebras induced are still meant to yield useful state spaces. We consider a whole family of domain and antidomain axiomatisations for semigroups and monoids which is presented in Table 1 as an overview. Precise definitions are given in subsequent sections. In the case of domain, the weakest axiomatisations are so-called left-closure semigroups and monoids (LC-semigroups/monoids) (cf. [JaS01]). The domain algebras of these structures are meet-semilattices, but some natural properties of domain do not hold in this class. Domain semigroups and monoids (d-semigroups/monoids) capture some of the properties of domain for binary relations, while twisted d-semigroups/monoids capture precisely the quasiequational properties of domain for partial functions. In the case of antidomain, closable semilattice pseudocomplemented semigroups (closable SP-semigroups) were introduced in [JaS04]. Their axioms induce domain algebras that are Boolean algebras, but again some natural properties of antidomain do not hold. Antidomain monoids (a-monoids) capture all the equational properties of antidomain for binary relations, while twisted a-monoids capture some of the properties of antidomain for partial functions. A more thorough investigation of the whole family is the subject of this paper.

3 Domain Semigroups

Our aim is to axiomatise domain and antidomain operations on semigroups and monoids that capture the fact that some computations may or may not be enabled from some set of states. We model the state space implicitly or internally through the images induced by the domain operations.

We consider semigroups $(S, \cdot)$ with an associative multiplication, usually left implicit, and monoids with a left and right multiplicative unit 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.

(D1) $d(x)x = x$
(D2) $d(xy) = d(xd(y))$
(D3) $d(d(x)y) = d(x)d(y)$
(D4) $d(x)d(y) = d(y)d(x)$

A monoid that satisfies these axioms is called 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. The axiom (D2) has been called *locality axiom* in the context of domain semirings. In semigroup theory, it has previously been called *left-congruence condition* [JaS01].

The axioms (D1)-(D4) are irredundant in the classes of d-semigroups and d-monoids: Mace4 found models that satisfy the semigroup or monoid axiom and three of the domain axioms, but not the fourth one, for each combination of domain axioms.

The class of right closure semigroups is defined in [JaS01]. The intended models are functions under composition. We present a dual set of axioms for relational composition.

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

(D1) $d(x)x = x$
(L2) $d(d(x)) = d(x)$
(L3) $d(x)d(xy) = d(xy)$
(D4) $d(x)d(y) = d(y)d(x)$

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

Again, it can be shown that the domain axioms of LC-semigroups and LC-monoids are irredundant.

Lemma 1. *The class of d-semigroups is strictly contained in the class of LC-semigroups.*

Prover9 has shown that the axioms (L2) and (L3) follow from the domain axioms (D1), (D3) and (D4). Mace4 presented a four-element LC-semigroup in which (D3) does not hold. It is easy to prove the same result for classes of monoids.

Lemma 2. *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 $d(S) = \{d(x) : x \in S\}$. The next lemma presents a very useful characterisation of domain elements.

Lemma 3. *The domain elements of an LC-semigroup are precisely the fixed points of the domain operation.*

Proof. If $x \in d(S)$, then $x = d(y)$ for some $y \in S$ and $d(x) = d(d(y)) = d(y) = x$ by (L2). If $x \in S$ satisfies $d(x) = x$, then $x \in d(S)$ by definition. □

This fixed point characterisation of domain elements in LC-semigroups, which a fortiori holds in domain semirings, is a key to checking closure properties of domain elements and describing the algebra of domain elements. It allows us to express the fact that x is a domain element within the language as $d(x) = x$.

Lemma 4.

(a) 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 $d(S)$.
(b) Every meet-semilattice is a domain semigroup if $d(x) = x$ is imposed, and similarly every meet-semilattice with a top element is a domain monoid.

Proof. (a) To show that domain elements are closed under composition, we use the fixed point lemma to verify that $d(d(x)d(y)) = d(x)d(y)$. Hence, by (D4), $d(S)$ is a commutative subsemigroup. Moreover $d(x)d(x) = d(x)$ holds, which implies that $d(S)$ is a subsemilattice. If $x1 = x$ holds in S, then $d(1) = d(1)1 = 1$ by (D1). The semilattice-order is defined, as usual, by $d(x) \leq d(y) \Leftrightarrow d(x)d(y) = d(x)$. Thus $d(x) \leq 1$ immediately follows from the monoidal right unit axiom.

(b) This fact is well known for LC-semigroups [JaS01]. In the case of d-semigroups we must verify that (D1)-(D4), with $d(s) = s$ for each element s, hold in every semilattice, which is trivial. □

Because of these algebraic properties we call $d(S)$ the *domain algebra* of S. It can be shown [JaS01] that 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.*

Lemma 5. *In any LC-semigroup the fundamental order coincides with the semilattice-order on the domain algebra, and is preserved by multiplication on the right.*

Note that preservation by multiplication on the left need not hold even on d-semigroups. This reflects the situation in $Rel(X)$, whereas for partial functions the fundamental order coincides with inclusion and is preserved by multiplication on both sides.

It seems interesting to compare the fundamental order $\leq$ with the usual natural order on domain semi*rings*, which is defined as $x \sqsubseteq y \Leftrightarrow x + y = y$.

Lemma 6. *The ordering $\leq$ is contained in $\sqsubseteq$ of domain semirings, but not necessarily equal.*

Proof. Prover9 has shown that $x = d(x)y \Rightarrow x + y = y$ holds in all domain semirings; Mace4 has found a three-element counterexample for the converse implication. □

We also note that the usual relational demonic refinement ordering can be defined in this framework:

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

We now outline a calculus of domain semigroups and we study some properties of their domain algebras. To formulate statements as strongly as possible from a logical point of view, we state positive properties for LC-semigroups and negative ones for domain semigroups. Automated theorem proving easily verifies the following basic laws.

Lemma 7. *Let S be an LC-semigroup and let $x, y \in S$. Then*

(a) $d(xy) \leq d(x)$.
(b) $d(x)y \leq y$, *but not necessarily* $yd(x) \leq y$.
(c) $x \leq d(x) \;\Leftrightarrow\; x = d(x)$.
(d) $x \leq 1 \Leftrightarrow x = d(x)$ *if* 1 *is a right unit.*
(e) $x \leq y \Rightarrow d(x) \leq d(y)$.
(f) $x \leq px \Leftrightarrow d(x) \leq p$ *and* $x = px \Leftrightarrow d(x) \leq p$ *hold for all* $p \in d(S)$.

Case (d) implies that, in d-monoids, the set of all domain elements is precisely the set of all subidentities. This is in contrast to the situation in domain semirings, where the domain elements can form a strict subset. There is no contradiction, since the subidentities on domain semigroups are taken with respect to $\leq$ whereas the subidentities on domain semirings are taken with respect to $\sqsubseteq$, which may admit more subidentities than $\leq$.

Case (f) captures a natural property of domain, namely

$$d(x) = \inf\{p \in d(S) : x \leq px\}.$$

Hence $d(x) = \inf\{p \in d(S) : x = px\}$ since all domain elements are left subidentities by (b). Accordingly, $d(x)$ is the least element in $d(S)$ which left preserves x, and the least domain element satisfying (D1). The assumption in (f) that $p \in d(S)$ cannot be much relaxed. The property fails if p is just a subidentity or an idempotent subidentity.

Lemma 8.

(a) Every monoid can be expanded to a d-monoid.
(b) Some semigroups cannot be expanded to d-semigroups.
(c) Domain algebras of d-monoids need not be unique.

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

(b) 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.

(c) The two d-monoids defined by

$\cdot$	0	1
0	0	0
1	0	1

with domain operations $d_1(x) = x$ and $d_2(x) = 1$ prove the claim. □

An expansion of idempotent semirings to d-semirings is not always possible. There is a three-element counterexample.

An interesting question is whether 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 Schein's fundamental theorem for relation algebras [Sch70] the class of representable d-monoids is a quasivariety.

Proposition 9. *The following quasiidentity fails in a 4-element d-monoid but holds in $Rel(X)$:*

$$xy = d(x) \text{ and } yx = x \text{ and } d(y) = 1 \quad \text{imply} \quad x = d(x).$$

Proof. Finding the counterexample for d-monoids is easy with Mace4. To prove that the result holds for binary relations, 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 10. *The quasivariety of representable d-monoids is not a variety.*

4 Twisted Domain Semigroups

Partial functions under composition satisfy another equational property called the *twisted law* in [JaS01]:

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

This identity fails in $Rel(X)$ if we take x to be any relation that is not deterministic. However it is satisfied if composition is the relational demonic composition (defined below in the section on antidomain). A d-semigroup/monoid or LC-semigroup/monoid is *twisted* if it satisfies the twisted law. The next lemma follows easily by automated theorem proving and counterexample search.

Lemma 11. *The classes of twisted LC-semigroups and twisted d-semigroups coincide, and they are strictly contained in the class of d-semigroups.*

The results of this section characterise part of the spectrum between LC-semigroups and twisted semigroups. LC-semigroups, on the one hand, yield a uniform basis for characterising domain operations for relations and functions, but they do not capture locality, which holds in relational models. Twisted semigroups, on the other hand, satisfy locality, but capture only deterministic relations, that is, partial functions. Domain semigroups are located between these two extremes and capture relations better than LC-semigroups.

The domain semigroup axioms, but not the twisted axiom (Mace4 presented a five element counterexample) hold in all domain semirings, hence domain semigroups are a natural generalisation of domain semirings. Partial functions, of course, are not closed under union hence do not form a semiring.

We have seen in Section 3 that the fundamental order $\leq$ is preserved by multiplication on the right. If the twisted identity $d(zx)z = zd(x)$ is imposed on an LC-semigroup then it is preserved by multiplication on the left as well since $x \leq y$ implies $x = d(x)y$, hence $d(zx)zy = zd(x)y = zx$, i.e. $zx \leq zy$.

Various representation theorems have been proved for families of semigroups with respect to partial functions. For example, every group is embedded in the symmetric group $S(X)$ of all permutations of a set X. Similarly, 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. We recall below a fourth instance of such an embedding due to Trokhimenko [Tro73] (cf. [JaS0a]). We present a concise variant of the proof for the domain setting because it uses a general construction that should be of interest for the RelMiCS/AKA community.

Theorem 12. *[Tro73,JaS01] Every twisted d-semigroup can be embedded in a partial transformation semigroup. If the semigroup has a unit, it is mapped to the identity function.*

Proof. 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

(a) $d(f_a) = f_{d(a)}$,
(b) $f_a;f_b = f_{ab}$, and
(c) h is injective.

By definition, $d(f_a) = \{(xd(a), xd(a)) : x \in S\}$, whereas $f_{d(a)}$ is defined on $D_{d(a)} = \{xd(d(a)) : x \in S\}$ by $f_{d(a)}(x) = xd(a)$. Since $d(d(a)) = d(a)$ and $xd(a)d(a) = xd(a)$, it follows that (a) holds.

To see that (b) holds, note that $(f_a;f_b)(x) = f_b(f_a(x)) = xab = f_{ab}(x)$, so it suffices to show that both functions have the same domain. Note that under the assumption of the twisted law we have $x = xd(y) \Leftrightarrow d(x) = d(xy)$.

Now x is in the domain of $f_a;f_b$ if and only if $x \in D_a$ and $xa \in D_b$, which means $xd(a) = x$ and $xad(b) = xa$. This can be expressed by $d(x) = d(xa)$ and $d(xa) = d(xab)$. Hence $d(x) = d(xab)$, and by the above equivalence we obtain $xd(ab) = x$, which shows that x is in the domain of f_{ab}. Conversely, if $xd(ab) = x$ then $d(x) = d(xd(ab)) = d(xd(ab)d(a)) = d(xd(a)) = d(xa)$ by (L3), (D4) and (D2), and likewise $d(xa) = d(xd(ab)a) = d(xd(ab)d(a)) = d(xd(ab)) = d(xab)$.

So h is a d-semigroup homomorphism, and it is injective since if $f_a = f_b$ then $x = xd(a)$ is equivalent to $x = xd(b)$. It follows that $d(a) = d(a)d(b) = d(b)$, whence $a = d(a)a = f_a(d(a)) = f_b(d(a)) = d(a)b = d(b)b = b$.

Finally, if S has a unit it follows immediately from the definitions that $D_1 = S$ and therefore $h(1) = f_1 = \mathrm{id}_S$. □

Corollary 13. *Every commutative d-semigroup is twisted, and can be embedded in a partial transformation semigroup.*

5 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.

$$\begin{array}{llll}
\text{(D1)} & d(x)x = x & \text{(R1)} & xr(x) = x \\
\text{(D2)} & d(xy) = d(xd(y)) & \text{(R2)} & r(xy) = r(r(x)y) \\
\text{(D3)} & d(d(x)y) = d(x)d(y) & \text{(R3)} & r(xr(y)) = r(x)r(y) \\
\text{(D4)} & d(x)d(y) = d(y)d(x) & \text{(R4)} & r(x)r(y) = r(y)r(x) \\
\text{(D5)} & d(r(x)) = r(x) & \text{(R5)} & r(d(x)) = d(x)
\end{array}$$

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. By the fixed point lemma for domain and its dual, the axioms (D5) and (R5) enforce that the domain algebra and the range algebra coincide, and both these axioms are needed for this result. (D4) and (R4) can be merged into the equivalent identity $d(x)r(y) = r(y)d(x)$.

By duality, it is clear that the identity $x = yr(x)$ also induces an ordering on S, but Mace4 can show that the order induced by domain and that by range need not coincide.

Again, the main examples of dr-semigroups are $Rel(X)$ and $PT(X)$. Inverse semigroups are also examples if we define $d(x) = xx^{-1}$, $r(x) = x^{-1}x$. In fact the twisted law holds for d, and its dual holds for r. The above representation theorem of Trokhimenko reduces to the Vagner-Preston representation theorem for inverse semigroups. However the twisted law does not hold for r in arbitrary partial transformation semigroups (simply because not all functions are injective).

Schweizer and Sklar [SS67] have provided an axomatisation for abstract function systems, using the following domain and range axioms.

$$\begin{array}{cccc} d(x)x = x & d(xd(y)) = d(xy) & d(r(x)) = r(x) & d(x)r(y) = r(y)d(x) \\ xr(x) = x & r(r(x)y) = r(xy) & r(d(x)) = d(x) & xd(y) = d(xy)x \end{array}$$

Schein has shown that adding the quasiidentity

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

axiomatises precisely the quasivariety of dr-semigroups of partial transformations (cf. [Sch70]). Prover9 easily shows that the first set of axioms without Schein's quasi-identity implies the axioms (D3) and (R3).

An interesting question is whether every *dr*-semigroup can be embedded into *Rel*(X) for some set X. We leave it open.

6 Antidomain

We have seen in Section 2 that domain semirings admit a very compact axiomatisation that induces a Boolean domain algebra. It is based on a notion of antidomain from which domain can be obtained. In this setting, antidomain is a more fundamental notion than domain.

This section shows how this approach can be generalised to the semigroup or monoid case. 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

(A1) $x'x = 0$
(A2) $x0 = 0$
(A3) $x'y' = y'x'$
(A4) $x''x = x$
(A5) $x' = (xy)'(xy')'$
(A6) $(xy)'x = (xy)'xy'$.

This axiomatisation is essentially due to Hollenberg [Hol97]. The one presented here is slightly more compact, and axiom (A5) is new, though essentially dual to one of Huntington's axioms for Boolean algebras. The axioms (A5) and (A6) might deserve further explanation. Intuitively, an expression $(xy)'$ can be understood as a modal box operator $[x]y'$, and it describes the set of states from which each x-step must lead to a state from which y is not enabled. Under this interpretation, an intuitive reading of (A5) is $x' = ([x]y') \cdot ([x]y'')$. This is a special case of the multiplicativity law $[x](p \cdot q) = ([x]p) \cdot ([x]q)$ for boxes, since $x' = [x]0$.

(A6) can be rewritten as $([x]y')x = ([x]y')xy'$, which says that executing x from those states from which each x-step must lead into y', leads into y'.

We write S' for the set $\{x' : x \in S\}$ of all *antidomain elements* of S. The constants 0 and 1 can be omitted from the language if we replace (A3) by $x'x = y'y$, (A2) by $xx'x = x'x$, and the monoid unit laws by $x(x'x)' = x$ (the left-unit law can be deduced from these axioms). In this sense the terminology *antidomain semigroup* is appropriate. However we prefer to use the more readable notation that makes the constants explicit. We can also define

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

as an abbreviation. Mace4 can show that the antidomain axioms are irredundant.

Lemma 14.

(a) A monoid is trivial if it can be extended by an antidomain operation that has a fixed point.
(b) The map $d(x) = x''$ is a domain operation.
(c) The antidomain elements of an a-monoid are the fixed points of domain.

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

Proposition 15. *Let S be an a-monoid. Then $(S', +, \cdot, ', 0, 1)$ is a Boolean subalgebra.*

Proof. We automatically verified the following properties. First, antidomain elements are are closed under addition and multiplication: $(x' + y')'' = x' + y'$ and $(x'y')'' = x'y'$. Closure under antidomain is trivial. Second, Huntington's axioms for Boolean algebras hold: $x + y = y + x$, $(x + y) + z = x + (y + z)$, and $x' = (x + y)' + (x + y')'$. Finally, $x'x'' = 0 = x''x'$ and $x' + x'' = 1$. □

In fact, Lemma 14 and Proposition 15 follow already from the antidomain axioms without (A6).

In Boolean domain semirings, the domain algebra is uniquely determined. It is the maximal Boolean subalgebra of the subalgebra of subidentities.

Lemma 16. *The antidomain algebra of an a-monoid need not be unique.*

Mace4 presented a five-element model with two different antidomain operations.

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

$$x \,\square\, y = (xy')'xy.$$

The following lemma collects some further properties of antidomain. Note that $\leq$ is the fundamental order which on the subidentities coincides with the lattice order.

Lemma 17. *Let S be an a-monoid. For all $x, y, z \in S$, the following laws hold.*

(a) $0x = 0$
(b) $(xy'')' = (xy)'$
(c) $(x'y)'' = x'y''$
(d) $x \leq 1$ *implies* $xy = 0 \Leftrightarrow x \leq y'$
(e) $x \leq 1 \Leftrightarrow x'' = x.$
(f) $x' \leq (xy)'$
(g) $xy = 0 \Leftrightarrow xy'' = 0$

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 18. *[Hol97]*

(a) The variety of a-monoids and the variety generated by all representable a-monoids are the same.
(b) The quasivariety of representable a-monoids is not a variety.

Hollenberg's counterexample for (b) is a 5-element Heyting algebra which fails the quasiidentity $x''y = x'' \wedge x'y = x' \Rightarrow y = 1$ that holds in all *representable* a-monoids. Since each Heyting algebra is a commutative a-monoid, it is twisted by Corollary 13. Consequently, in contrast to the case of d-monoids, the antidomain operation need not be represented correctly by the Cayley map. This indicates why the construction from Theorem 12 cannot even be adapted to *twisted* a-monoids. The question whether the quasivariety of representable a-monoids is finitely axiomatisable is open.

A weaker axiomatisation of an antidomain operation for semigroups is obtained as a subvariety of semilattice pseudo-complemented semigroups defined in [JaS04]. Recall that a pseudo-complement on a meet-semilattice is a unary operation $'$ that satisfies

$$xy = 0 \;\Leftrightarrow\; y \leq x'.$$

In the variety of semilattices with a unary operation, this formula is equivalent to the identities $x'x = 0$, $x0' = x$ and $x(xy)' = xy'$. The following result is proved in [Fri62].

Theorem 19. *For any pseudocomplemented meet-semilattice S, the set $B(S) = \{x'' : x \in S\}$ is a Boolean algebra with operations x', xy and $x'' + y'' = (x'y')'$.*

A *semilattice pseudo-complemented semigroup* or *SP-semigroup* is a semigroup that satisfies the following identities.

(A1) $x'x = 0$
(S2) $x0' = x$
(A3) $x'y' = y'x'$
(S4) $x'(x'y)' = x'y'$

In any SP-semigroup S the set $B(S) = \{x'' : x \in S\}$ is a meet-subsemilattice that is pseudo-complemented by the antidomain operation. As in Theorem 19, the set $B(S)$ is a Boolean algebra with join given by $x'' + y'' = (x'''y''')'$.

An SP-semigroup is called *closable* in [JaS04] if (A4), that is, $x''x = x$, holds.

Lemma 20.

(a) Every closable SP-semigroup is a d-semigroup with $d(x) = x''$*.*
(b) A closable SP-semigroup is an a-monoid if and only if (A2) and (A6) hold.

Therefore, (A5) could be replaced by (S4) in the a-monoid axioms.

The proper superclass of a-monoids defined by (A1)-(A5) is interesting in its own right. Note that (A6) holds in every antidomain semi*ring*, since

$$(xy)'x = (xy)'x(y' + y'') = (xy)'xy' + (xy'')'xy'' = (xy)'xy' + 0 = (xy)'xy'.$$

Modal box and diamond operators can be defined already in this weaker setting.

Let $\langle x\rangle p = (xp)''$ and let $[x]p = (xp')'$, where $p = p''$. Then the diamond operator is strict and additive and the box operator is costrict and multiplicative:

$$\langle x\rangle 0 = 0, \quad \langle x\rangle(p + q) = \langle x\rangle p + \langle x\rangle q, \quad [x]1 = 1, \quad [x](p \cdot q) = ([x]p) \cdot ([x]q).$$

Also $[x]p = (\langle x\rangle p')'$ and $\langle x\rangle p = ([x]p')'$. This definition of modal operators is not possible in the weaker setting of closable SP-semigroups. Hence SP-semigroups have Boolean domain algebras, but are too weak to obtain Boolean algebras with operators.

Modal algebras allow one to define a notion of determinism as $\langle x\rangle p \leq [x]p$. We therefore call an a-monoid *deterministic* if it satisfies

$$(xy'')'' \leq (xy')'.$$

Proposition 21. *An a-monoid is deterministic if and only if it is twisted.*

Note that the twisted law implies (A6), but not every a-monoid is twisted or deterministic, and determinism does not imply (A6).

Finally, a notion of antirange can be axiomatised dually to that of antidomain. Because the antidomain and the antirange algebra automatically coincide, they need no further linking. In this setting, forward box and diamond operators $|x]$ and $|x\rangle$ can be defined from antidomain, and backward operators $[x|$ and $\langle x|$ from antirange. We have the following laws.

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 $\langle x\rvert p \leq q \Leftrightarrow p \leq \lvert x]q$

In this setting, (A6) and its dual for antirange become derivable. For instance, (A6) is just the cancellation law $\langle x|x]p \leq p$ of the Galois connection. Note that because of the Galois connection, diamond operators are even completely additive, and box operators are completely multiplicative. In conclusion, monoids with antidomain and antirange allow us to define and calculate with modal operators.

7 Templates for Prover9 and Mace4

```
op(400, infix, ";").
op(500, infix, "+").
op(300, postfix, "’").

formulas(assumptions).  % domain semigroups

x;(y;z)=(x;y);z.
d(x);x=x.
d(x;y)=d(x;d(y)).
d(d(x);y)=d(x);d(y).
d(x);d(y)=d(y);d(x).

x<=y <-> x=d(x);y.

end_of_list.

formulas(assumptions). % antidomain monoid

x;(y;z)=(x;y);z.
x;1=x.
x’;x=0.
x;0=0.
x’;y’=y’;x’.
x’’;x=x.
x’=(x;y)’;(x;y’)’.
(x;y)’;x=((x;y)’;x);y’.

x<=y <-> x=x’’;y.

end_of_list.

formulas(goals). % insert goal here

end_of_list.
```

8 Conclusion

We have axiomatised operations for relational domain and antidomain for semigroups and monoids, studied the structure of the domain algebras, developed the basic calculi, and compared these algebras with previous axiomatisations. Our approach continues and also generalises previous work on axiomatisations of domain for semirings and Kleene algebras. It forms the basis for further investigations, for instance, representation theorems, free algebras and other domain algebras.

Partial and total functions and deterministic programs are central to computer science applications, while relations and nondeterminism are important for specifications and for modelling more general computing systems. But the algebraic background that has been developed in semigroup theory over the last fifty years does not seem to be widely known and, to our knowledge, no link between functional and relational domain axiomatisations has so far been provided.

Besides closing this gap, a benefit of the abstract algebraic approach is also that the analysis of functions and relations with (anti)domain can—to a large extent—be automated. This allowed us to condense the paper and focus on the conceptual development.

We would like to thank Robin Hirsch, Marcel Jackson and Szabolcs Mikulás for interesting discussions. Special thanks to Tadeusz Litak for the very interesting pointer to Marco Hollenberg's work.

References

[DS08a] 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.

[DS08b] 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.

[Fri62] O. Frink, *Pseudo-complements in semilattices*, Duke Mathematics Journal, 29 (1962), 500–515.

[Hol97] M. Hollenberg, *An equational axiomatization of dynamic negation and relational composition*, Journal of Logic, Language and Information, 6 (1997), 381–401.

[JaS01] M. Jackson and T. Stokes, *An invitation to C-semigroups*, Semigroup Forum 62 (2001), 279–310.

[JaS04] M. Jackson and T. Stokes, *Semilattice pseudo-complements on semigroups*, Comm. Algebra 32 (2004), 2895–2918.

[JaS0a] M. Jackson and T. Stokes, *Partial maps with domain and range: extending Schein's representation*, Comm. Algebra, to appear.

[JS08] 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), Lecture Notes in Computer Science, Vol. 4988, Springer-Verlag (2008), 234–242.

[McC07] W. McCune, *Prover9 / Mace4*, `www.prover9.org`, 2007.

[MS06] B. Möller, G. Struth, *Algebras of modal operators and partial correctness*, Theoretical Computer Science, 351, (2006), 221–239.

[Sch70] B. M. Schein, *Relation algebras and function semigroups*, Semigroup Forum, Vol 1. (1970), 1–62.

[SS67] B. Schweizer and A. Sklar, *Function systems*, Math. Annalen, 172, (1967), 1–16.

[Tro73] V. S. Trokhimenko, *Menger's function systems*, Izv. Vysš. Učebn. Zaved. Matematika, no. 11(138), 71–78 [in Russian].