Domain Semirings United

Uli Fahrenberg\textsuperscript{1}, Christian Johansen\textsuperscript{2}, Georg Struth\textsuperscript{3}, and Krzysztof Ziemiański\textsuperscript{4}

\textsuperscript{1}École Polytechnique, Palaiseau, France
\textsuperscript{2}University of Oslo, Norway
\textsuperscript{3}University of Sheffield, UK
\textsuperscript{4}University of Warsaw, Poland

Abstract

Domain operations on semirings have been axiomatised in two different ways: by a map from an additively idempotent semiring into a boolean subalgebra of the semiring bounded by the additive and multiplicative unit of the semiring, or by an endofunction on a semiring that induces a distributive lattice bounded by the two units as its image. This note presents classes of semirings where these approaches coincide.

1 Introduction

Domain semirings and Kleene algebras with domain \cite{DMS06,DS11} yield particularly simple program verification formalisms in the style of dynamic logics, algebras of predicate transformers or boolean algebras with operators (which are all related).

There are two kinds of axiomatisation. Both are inspired by properties of the domain operation on binary relations, but target other computationally interesting models such as program traces or paths on digraphs as well.

The initial two-sorted axiomatisation \cite{DMS06} models the domain operation as a map $d : S \to B$ from an additively idempotent semiring $(S, +, \cdot, 0, 1)$ into a boolean subalgebra $B$ of $S$ bounded by 0 and 1. This seems natural as domain elements form powerset algebras in the target models mentioned. Yet the domain algebra $B$ cannot be chosen freely: $B$ must be the maximal boolean subalgebra of $S$ bounded by 0 and 1 and equal to the set $S_d$ of fixpoints of $d$ in $S$. The alternative, one-sorted axiomatisation \cite{DS11} therefore models $d$ as an endofunction on a semiring $S$ that induces a suitable domain algebra on $S_d$—yet generally only a bounded distributive lattice. An antidomain (or domain complementation) operation is needed to obtain boolean domain algebras.

This note revisits the two axiomatisations to tie some loose ends together. We describe a natural algebraic setting in which they coincide, and which has so far been overlooked. It consists of additively idempotent semirings in which the full sets of elements below 1 form boolean algebras, as is the case, for instance, in boolean monoids and boolean quantales. We further take the opportunity to discuss domain axioms for arbitrary quantales.

The restriction to such boolean settings has little impact on applications: most models of interest are powerset algebras and hence (complete atomic) boolean algebras anyway. Yet the coincidence itself does make a difference: one-sorted domain semirings are easier to formalise in interactive proof assistants and apply in program verification and correctness.
2 Domain Axioms for Semirings

First we recall the two axiomatisations of domain semirings and their relevant properties. To distinguish them we call the first class obtained (in [DMS06]) test dioids with domain and the second one (obtained in [DS11]) domain semirings in this note.

We assume familiarity with posets, lattices and semirings. A dioid, in particular, is an idempotent semiring \((S, +, \cdot, 0, 1)\), that is, \(x + x = x\) holds for all \(x \in S\). Its additive monoid \((S, +, 0)\) is then a semilattice ordered by \(x \leq y \iff x + y = y\) and with least element 0; multiplication preserves \(\leq\) in both arguments. We write \(S_1 = \{x \in S \mid x \leq 1\}\) for the set of subidentities in \(S\) and call \(S\) bounded if it has a maximal element, \(\top\).

We call a dioid \(S\) is full if \(S_1\) is a boolean algebra, bounded by 0 and 1, with + as sup, \(\cdot\) as inf and an operation \((-)'\) of complementation that is defined only on \(S_1\).

**Definition 2.1** ([DMS06]). A test dioid \((S, B)\) is a dioid \(S\) that contains a boolean subalgebra \(B\) of \(S_1\)—the test algebra of \(S\)—with least element 0, greatest element 1, in which + coincides with sup and that is closed under multiplication.

Once again we write \((-)'\) for complementation on \(B\).

**Lemma 2.2** ([DMS06]). In every test dioid, multiplication of tests is their meet.

**Lemma 2.3** ([DMS06]). Let \((S, B)\) be a test dioid. Then, for all \(x \in S\) and \(p \in B\),

1. \(x \leq px \iff p'x = 0\),
2. \(x \leq px \iff x \leq p\top\) if \(S\) is bounded.

**Definition 2.4** ([DMS06]). A test dioid with predomain is a test dioid \((S, B)\) with a predomain operation \(d : S \to B\) such that, for all \(x \in S\) and \(p \in B\),

\[
x \leq d(x)x \quad \text{and} \quad d(px) \leq p.
\]

It is a test dioid with domain if it also satisfies, for \(x, y \in S\), the locality axiom

\[
d(xd(y)) \leq d(xy).
\]

Weak locality \(d(xy) \leq d(xd(y))\) holds already in every test dioid with predomain. Thus \(d(xd(y)) = d(xy)\) in every test dioid with domain.

**Lemma 2.5** ([DMS06]). In every test dioid \((S, B)\), the following are equivalent:

1. \((S, B, d)\) is a test dioid with predomain,
2. the map \(d : S \to B\) on \((S, B)\) satisfies, for all \(x \in S\) and \(p \in B\), the least left absorption property
   \[
d(x) \leq p \iff x \leq px,
   \] (lla)
3. in case \(S\) is bounded, \(d : S \to B\) on \((S, B)\) is, for all \(x \in S\) and \(p \in B\), the left adjoint in the adjunction
   \[
d(x) \leq p \iff x \leq p\top.
   \] (d-adj)

Interestingly, test algebras of test dioids with domain cannot be chosen ad libitum: they are formed by those subidentities that are complemented relative to the multiplicative unit [DMS06]. This has the following consequences.

**Proposition 2.6.** The test algebra \(B\) of a test dioid with domain \((S, B, d)\) is the largest boolean subalgebra of \(S_1\).
We write \( S_d = \{ x \mid d(x) = x \} \) and \( d(S) \) for the image of \( S \) under \( d \).

**Lemma 2.7** (DS11). Let \( (S, B, d) \) be a test dioid with domain. Then \( B = S_d = d(S) \).

Next we turn to the second type of axiomatisation.

**Definition 2.8** (DS11). A *domain semiring* is a semiring \( S \) with a map \( d: S \to S \) such that, for all \( x, y \in S \) and with \( \leq \) defined as for dioids,

\[
x \leq d(x)x, \quad d(xd(y)) = d(xy), \quad d(x) \leq 1, \quad d(0) = 0, \quad d(x + y) = d(x) + d(y).
\]

Every domain semiring is a dioid: \( d(1) = d(1)1 = 1 + d(1)1 = 1 + d(1) = 1 \) and then \( 1 + 1 = 1 + d(1) = 1 \) follow from the first and third axiom; hence finally \( x + x = x(1 + 1) = x \). Thus \( \leq \) is a partial order. The first axiom can be strengthened to \( d(x)x = x \).

In a domain semiring \( S \), \( d \) induces the domain algebra: \( d \circ d = d \) and therefore \( S_d = d(S) \). Moreover, \((S_d, +, \cdot, 0, 1)\) forms a subsemiring of \( S \), which is a bounded distributive lattice with + as binary sup, \( \cdot \) as binary inf, least element 0 and greatest element 1. Every domain semiring is a dioid: \( S \) is bounded. More importantly, \( (\text{lla}) \) can now be derived for all \( p \in S_d \) (it need not hold for \( p \in S_1 \)) (DS11); it can be turned into an adjunction when \( S \) is bounded.

**Proposition 2.9** (DS11). The domain algebra of a domain semiring \( S \) contains the largest boolean subalgebra of \( S \) bounded by 0 and 1.

The fifth domain axiom implies that \( d \) is order preserving. In addition, \( d(px) = pd(x) \) for all \( p \in S_d \), \( d(1) = 1 \), and \( d(\top) = 1 \) if \( S \) is bounded. More importantly, \( (\text{lla}) \) can now be derived for all \( p \in S_d \) (it need not hold for \( p \in S_1 \)) (DS11); it can be turned into an adjunction when \( S \) is bounded.

**Lemma 2.10.** In any bounded domain semiring \( S \), \((\text{lla})\) holds for all \( p \in S_d \).

**Proof.** \( d(x) \leq p \) implies \( x = d(x)x \leq px \leq p\top \) and \( d(x) \leq d(p\top) = pd(\top) = p1 = p \) follows from \( x \leq p\top \).

As mentioned in the introduction, an antidomain operation is needed to make the bounded distributive lattice \( S_d \) boolean.

**Definition 2.11** (DS11). An *antidomain semiring* is a semiring \( S \) with an operation \( ad: S \to S \) such that, for all \( x, y \in S \),

\[
ad(x)x = 0, \quad ad(x) + ad(ad(x)) = 1, \quad ad(xy) \leq ad(xad(ad(y))).
\]

Antidomain models boolean complementation in the domain algebra; the domain operation can be defined as \( d = ad \circ ad \) in any antidomain semiring \( S \). The domain algebra \( S_d \) of \( S \) is the maximal boolean subalgebra of \( S_1 \), as in Proposition 2.6. \( S \) is therefore a test dioid with \( B = S_d \).

If the domain algebra \( S_d \) of a domain semiring \( S \) happens to be a boolean algebra, it must be the maximal boolean subalgebra of \( S_1 \) by Proposition 2.9 so that \( S \) is again a test dioid with \( B = S_d \). Antidomain is then definable.

**Lemma 2.12.** Every domain semiring with boolean domain algebra is an antidomain semiring.

**Proof.** With \( ad = (\cdot)' \circ d \), the first antidomain axiom is immediate from Lemma 2.3(1); the remaining two axioms hold trivially.

### 3. Coincidence Result

The results of Section 2 suggest that the two types of domain semiring coincide when the underlying dioid is full. We now spell out this coincidence.

**Proposition 3.1.** Let \( (S, B, d) \) be a test dioid with domain. Then \((S, d)\) is a domain semiring with \( S_d = B \) and an antidomain semiring with \( ad = (\cdot)' \circ d \).
Proof. The domain semiring axioms are derivable in test dioids with domain [DMS06]; the antidomain axioms follow by Lemma 2.12. Moreover, $B$ is the maximal boolean subalgebra of $S_1$ by Proposition 2.6 and thus equal to $S_d$ by Proposition 2.9 (alternatively Lemma 2.7).

For the converse direction we consider full domain semirings $S$ where $S_d = S_1$ is a boolean algebra by Proposition 2.9. These are test dioids, hence (lla) can be used to define domain.

**Corollary 3.2.** Let $S$ be a full dioid with map $d : S \to S$. Then (lla) holds for all $x \in S$ and $p \in S_1$ if and only if $x \leq d(x)x$ and $d(px) \leq p$ hold for all $x \in S$ and $p \in S_1$.

**Proof.** As $S$ is a test dioid with $B = S_1$, Lemma 2.6 (1) applies.

**Lemma 3.3.** Let $S$ be a full dioid with map $d : S \to S$ that satisfies (lla) for all $x \in S$ and $p \in S_1$. Then $(S, S_1, d)$ is a test dioid with predomain and $S_d = S_1$.

**Proof.** $S$ is a test dioid with predomain by Corollary 3.2. $S_d \subseteq S_1$ because $d(x) \leq 1$ in any test dioid with predomain [DMS06]. $S_1 \subseteq S_d$ because $p \leq 1$ implies $p = d(p)p \leq d(p)$ and $d(p) \leq p$ because $pp = p$, using (lla).

**Proposition 3.4.** Let $(S, d)$ be a full domain semiring. Then $(S, S_d, d)$ is a test dioid with domain.

**Proof.** If $(S, d)$ is a full domain semiring, then (lla) is derivable and locality holds. Then $(S, S_d, d)$ is a test dioid with domain by Lemma 3.3 and therefore a test dioid with domain because of locality.

Our coincidence result then follows easily from Proposition 3.1 and 3.4.

**Theorem 3.5.** A full test dioid is a test dioid with domain if and only if it is a domain semiring.

On full dioids, domain can therefore be axiomatised either equationally by the domain semiring axioms or those of test dioids with domain, or alternatively by (lla) and locality. Fullness can be enforced, for instance, by requiring that every $p \leq 1$ is complemented within $S_1$, that is, there exists an element $q \in S_1$ such that $p + q = 1$ and $qp = 0$. It then follows that $S_1$ is a boolean algebra [DS11]. Alternatively, one could require that $x \leq 1 \Rightarrow d(x) = x$ holds for all $x \in S$ in order to guarantee that $S_d = S_1$.

Finally, locality need not hold in full test dioids that satisfy (lla).

**Example 3.6.** Consider the full test dioid with $S = \{0, 1, a, \top\}$ in which $a$ and $1$ are incomparable with respect to $\leq$, $aa = 0$, multiplication is defined by $a\top = \top a = a$ and $\top \top = \top$, and $d$ maps 0 to 0 and every other element to 1. Then (lla) holds, but $d(ad(a)) = d(a1) = d(a) = 1 > 0 = d(0) = d(aa)$.

## 4 Examples

The restriction to full test dioids is natural for concrete powerset algebras. It is captured abstractly, for instance, by boolean monoids and quantales.

A boolean monoid [DMS06] is a structure $(S, +, \cap, \cdot, -0, 1, \top)$ such that $(S, +, \cdot, 0, 1)$ is a semiring and $(S, +, \cap, -0, \top)$ a boolean algebra. As all sups, infs and multiplications of subidentities stay below 1, every boolean monoid is a full bounded dioid; boolean complementation on $S_1$ is given by $p' = 1 - p$ for all $p \in S_1$.

Domain can now be axiomatised as an endofunction, either equationally using the domain semiring or test dioid with domain axioms, or by the adjunction (d-adj) and locality, as in Section 3. Once again, the antidomain operation $ad$ is complementation on $S_1$. Theorem 3.5 has the following instance.

**Corollary 4.1.** A boolean monoid is a test dioid with domain if and only if it is a domain semiring.
Quantales capture the presence of arbitrary sups and infs in powerset algebras more faithfully. Formally, a quantale $\langle Q, \leq, \cdot, 1 \rangle$ is a complete lattice $\langle Q, \leq \rangle$ and a monoid $\langle Q, \cdot, 1 \rangle$ such that composition preserves all sups in its first and second argument. We write $\vee$ for the sup and $\wedge$ for the inf operator. We also write $0 = \bigwedge Q$ for the least and $\top = \bigvee Q$ for the greatest element of $Q$, and $\vee$ and $\wedge$ for binary sups and infs.

A quantale is boolean if its complete lattice is a boolean algebra. Every boolean quantale is obviously a boolean monoid, and every finite boolean monoid a boolean quantale. If $Q$ is a boolean quantale, then $Q_1$ forms even a complete boolean algebra. In boolean quantales, predomain, domain and antidomain operations can therefore be axiomatised like in boolean monoids, and we obtain another instance of Theorem 3.3 (3) analogous to Corollary 4.1, simply by replacing “boolean monoid” with “boolean quantale”.

5 Domain Quantales

Some loose ends remain to be tied together in this note as well:

- Does the interaction of $d$ with $\vee$ and $\wedge$ in quantales require additional axioms?
- Why has domain not been axiomatised explicitly using the adjunction [d-ad], at least for boolean quantales?
- And why has domain in boolean monoids or quantales not been axiomatised explicitly by $d(x) = 1 \wedge x \top$, as in relation algebra?

This section answers these questions.

First, we consider the one-sorted domain axioms in arbitrary quantales and argue that additional sup and inf axioms are unnecessary.

**Definition 5.1.** A domain quantale is a quantale that is also a domain semiring.

As every quantale is a bounded dioid, the adjunction [d-ad] holds for every $p \in Q_d$. In addition, domain interacts with sups and infs as follows.

**Lemma 5.2.** In every domain quantale,

1. $d(\bigvee X) = \bigvee d(X)$,
2. $d(\bigwedge X) \leq \bigwedge d(X)$,
3. $d(x) \wedge Y = \bigwedge d(x)Y$ for all $Y \neq \emptyset$.

**Proof.**

1. $d$ is a left adjoint by Lemma 2.10 and therefore sup-preserving. Sups over $X$ are taken in $Q$; those over $d(X)$ in $Q_d$.

2. $(\forall x \in X. \bigwedge X \leq x) \Rightarrow (\forall x \in X. d(\bigwedge X) \leq dx) \Leftrightarrow d(\bigwedge X) \leq \bigwedge d(X)$.

3. Every $y \in Y \neq \emptyset$ satisfies $d(\bigwedge d(x)Y) \leq d(d(x)y) = d(x)d(y) \leq d(x)$ and therefore $\bigwedge d(x)Y = d(\bigwedge d(x)Y) \bigwedge d(x)Y \leq d(x) \bigwedge d(x)Y \leq d(x) \bigwedge Y$. The converse inequality holds a fortiori because $x \bigwedge Y \leq \bigwedge xY$ in any quantale.

In (3), if $Y = \emptyset$, then $d(x) \wedge Y = d(x) \top$ need not be equal to $\top = \bigwedge \emptyset = \bigwedge d(x)Y$. In the quantale of binary relations over the set $\{a, b\}$, for instance, with relational composition as $\cdot$ and $R = \{(a, a)\}$, it holds that $d(R) = R$ and $d(R) \top = \{(a, a)\} \cdot \{(a, a), (a, b), (b, a), (b, b)\} = \{(a, a), (a, b)\} \subset \top$.

Moreover, (1) implies that the domain algebra $Q_d$ is a complete distributive lattice: $d(\bigvee d(X)) = \bigvee d(X)$ holds for all $X \subseteq Q$, so that any sup of domain elements is again a domain element. Yet the sups and infs in $Q_d$ need not coincide with those in $Q$. 5
Second, the adjunction $d(x) \leq p \iff x \leq p \top$ holds for all $p \in Q_1$ in a boolean quantale $Q$. General properties of adjunctions then imply that, for all $x \in Q$,

$$d(x) = \bigwedge \{ p \in Q_1 \mid x \leq p \top \}.$$ 

Lemma 3.3 then guarantees that this identity defines predomain explicitly on boolean quantales; yet Example 3.6 rules out that it defines domain: the full test dioid from this example is, in fact, a boolean quantale; it satisfies (ll) and thus (d-adj), but violates the locality axiom of domain quantales.

Finally, we give two reasons why the relation-algebraic identity $d(x) = 1 \wedge x \top$ cannot replace the domain axioms in boolean monoids and quantales.

It is too weak: In the boolean quantale $\{ \bot, 1, a, \top \}$ with $1$ and $a$ incomparable and multiplication defined by $\top \top = \top$ and $aa = a \top = \top a = a$, it holds that $d(a) = \bot$ (when defined by $d(x) = 1 \wedge x \top$), yet $d(a)a = \bot a = \bot < a$. Therefore $d(x)x = x$ is not derivable from $d(x) = 1 \wedge x \top$ even in boolean quantales.

It is too restrictive: although $d(x) = 1 \wedge x \top$ obviously holds in the quantale of binary relations, it fails, for instance, in the quantale formed by the sets of (finite) paths over some digraph $(V, E)$ mentioned in the introduction. In this model, paths $p = (v_1, \ldots, v_m)$ and $q = (w_1, \ldots, w_n)$, with $v_i, w_j \in V$ for $1 \leq i \leq m$ and $1 \leq j \leq n$, can be composed to path $pq = (v_1, \ldots, v_m, w_2, \ldots w_n)$ whenever $v_m = w_1$. The quantalic composition on sets of paths $P$ and $Q$ is then given by $PQ = \{ pq \mid p \in P, q \in Q \text{ and } pq \text{ defined} \}$; the quantalic unit is the set $V$ (of all single-vertex paths). Domain elements are subsets of $V$ given by the initial vertices of the paths in the respective set. Then $V \cap P \top = \emptyset$ unless $P$ contains a path of length one and $d(P) = \emptyset \iff P = \emptyset$, so that $d(P) = V \cap P \top$ fails for any $P$ in which all paths have length greater than 1. This type of argument applies to all powerset quantales in which the composition of underlying objects (here: paths) is generally length-increasing and the quantalic unit and domain elements are formed by fixed-length objects.

References

[DMS06] J. Desharnais, B. Möller, and G. Struth. Kleene algebra with domain. *ACM TOCL*, 7(4):798–833, 2006.

[DS11] J. Desharnais and G. Struth. Internal axioms for domain semirings. *Science of Computer Programming*, 76(3):181–203, 2011.