The Structure of the One-Generated Free Domain Semiring

Peter Jipsen[1] and Georg Struth[2]

[1] Chapman University, One University Dr, Orange, CA 92866, USA
jipsen@chapman.edu
[2] The University of Sheffield, 211 Portobello Street, Sheffield S1 4DP, UK
G.Struth@dcs.shef.ac.uk

Abstract. This note gives an explicit construction of the one-generated free domain semiring. In particular it is proved that the elements can be represented uniquely by finite antichains in the poset of finite strictly decreasing sequences of nonnegative integers. It is also shown that this domain semiring can be represented by sets of binary relations with union, composition and relational domain as operations.

1 Introduction

A *semiring* is an algebra of the form $(A, +, 0, \cdot, 1)$ such that $(A, +, 0)$ is a commutative monoid, $(A, \cdot, 1)$ is a monoid, and $\cdot$ distributes over all finite joins from the left and right (i.e. $x(y+z) = xy+xz$, $(x+y)z = xz+yz$ and $x0 = 0x = 0$). A semiring is *idempotent* if $x + x = x$. In this case, $(A, +, 0)$ is a (join-)semilattice with 0 as bottom element, and $\cdot$ preserves the join-semilattice order (denoted by $\leq$) in both arguments. The variety of idempotent semirings is denoted by IS.

Let X be a set of variables (or generators). By distributivity, every term t in the signature of semirings can be written as a finite join of terms of the free monoid $X^* = \bigcup_{n\in\mathbb{N}} X^n$ with 1 as the empty sequence and $\cdot$ as concatenation. Hence the free idempotent semiring over X, denoted by $F_{\mathsf{IS}}(X)$, is isomorphic to the set $\mathcal{P}_{\text{fin}}(X^*)$ of all finite subsets of words over the generators, with + given by union and $\cdot$ given by the complex product $U \cdot V = \{uv : u \in U, v \in V\}$.

Consequently, the equational theory of idempotent semirings is decidable. However, their quasiequational theory and their uniform word problem are undecidable: The uniform word problem for semigroups is known to be undecidable, and every semigroup S is a subreduct of its powerset semiring $\mathcal{P}(S)$.

In this note we consider *domain semirings*, which are idempotent semirings with an additional unary operation d that has the properties of a *domain operation*. Domain semirings have first been introduced in a two-sorted setting in which the domain operation maps arbitrary semiring elements to a special Boolean subalgebra [DMS06]. The reason is that arbitrary semiring elements are intended to model the actions of some program or transition system whereas the elements of the Boolean subalgebra model the states of that system. This approach has recently been generalised to a one-sorted setting [DS08] and we base our considerations on this simpler and more flexible approach.

Our aim is an explicit description of the one-generated free domain semiring $F_{\mathsf{DS}}(x)$. To this end we first describe the one-generated free domain monoid $F_{\mathsf{DM}}(x)$. We then show that these elements are the join irreducibles of $F_{\mathsf{DS}}(x)$, and we describe how they are ordered. Finally we show that $F_{\mathsf{DS}}(x)$ is isomorphic to the set of finite antichains in the poset of join irreducibles.

We conclude with the result that $F_{\mathsf{DS}}(x)$ is representable by a concrete algebra of binary relations, with union, empty relation, composition, identity relation, and relational domain as operations.

Examples of domain semirings are, for instance, reducts of relation algebras (with $d(x) = (x;x^{\smile}) \wedge 1'$), as well as reducts of Kleene algebras with domain.

Computationally meaningful models of domain semirings include the idempotent semirings of binary relations with domain defined in the standard way; the idempotent semirings formed by sets of traces of a program (which are alternating sequences of state and action symbols) with domain defined by starting states of traces; or the idempotent semirings formed by sets of paths in a graph with domain defined again by sets of starting states [DMS06].

Applications of domain semirings and Kleene algebras with domain have been intensively studied. First, domain models enabledness conditions for actions in programs and transition systems. Second, the domain operation can easily be extended into a modal diamond operator that acts on the underlying algebra of domain elements [MS06]. This links the algebraic approach with more traditional logics of programs such as dynamic, temporal and Hoare logics. Also some standard semantics of programs, including the weakest precondition and weakest liberal precondition semantics, can be modeled in this setting. Many concrete applications can be found in this and previous RelMiCS conference proceedings.

The free domain semiring is interesting in these applications since it identifies exactly those terms of domain semirings that have the same denotation in all domain semirings and because it allows the definition of efficient proof and decision procedures.

The domain axioms of domain semirings are the same as for relation algebras and for Kleene algebras with domain, and since both relation algebras and Kleene algebras have rich and complex (quasi)equational theories, we will independently study the simpler equational theory of domain semirings in this note. Even in this setting the n-generated free algebras appear to be fairly complicated, but at least we are able to handle the one-generated case.

2 Domain Semirings

A *domain monoid* is an algebra $(M, \cdot, 1, d)$ such that $(M, \cdot, 1)$ is a monoid and $d : M \to M$ is a function that satisfies

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

It follows that

$$\begin{array}{ll} d(1) = 1 & \text{[take } x = 1 \text{ in (D1)],} \\ d(d(x)) = d(x) & \text{[take } y = 1 \text{ in (D2)], and} \\ d(x)d(x) = d(x) & \text{[take } y = x \text{ in (D3)].} \end{array}$$

Hence the set $d(M) = \{d(x) : x \in M\}$ forms a meet semilattice with 1 as top element.

A *domain semiring* is an algebra $(A, +, 0, \cdot, 1, d)$ such that $(A, +, 0, \cdot, 1)$ is a semiring, $(A, \cdot, 1, d)$ is a domain monoid, and the additional axioms

$$d(x + y) = d(x) + d(y), \qquad d(0) = 0 \qquad \text{and} \qquad d(x) + 1 = 1$$

hold [DS08]. Multiplying the last axiom by x on both sides and applying (D1) shows that every domain semiring is an idempotent semiring. The varieties of domain monoids and domain semirings are denoted by DM and DS respectively.

We note that the definition of domain semiring used here is more general than the notion of $\hat{\delta}$-semiring in [DMS06] since we do not require a test-subsemiring or a complementation operation on tests.

Note also that every monoid expands to a domain monoid by taking d to be the constant function 1. Likewise, for any idempotent semiring we can obtain a domain semiring by defining $d(x) = 1$ if $x \neq 0$ and $d(0) = 0$. Therefore the quasiequational theory of domain monoids and of domain semirings is undecidable.

Lemma 1. (a) *In every domain semiring, the axioms* (D3) *and* (D4) *are implied by the remaining axioms.*
(b) *For any domain semiring A, the set $d(A) = \{d(x) : x \in A\}$ forms a distributive lattice.*

Proof. (a) Since $d(x + y) = d(x) + d(y)$ and $d(x) + 1 = 1$, it follows that d is order-preserving and $d(x) \leq 1$. Hence we use (D1) to calculate

$$d(x)d(y) = d(d(x)d(y))d(x)d(y) \leq d(1d(y))d(x)1 = d(y)d(x),$$

proving (D4). For (D3), we proceed similarly, using (D1) and (D2):

$$\begin{aligned} d(x)d(y) &= d(d(x)d(y))d(x)d(y) \\ &= d(d(x)y)d(x)d(y) \\ &\leq d(d(x)y) \\ &= d(d(d(x)y))d(d(x)y) \\ &\leq d(x)d(y). \end{aligned}$$

(b) Birkhoff [Bir67] showed that a semiring is a distributive lattice iff it satisfies $x + 1 = 1$ and $xx = x$. Note that $d(A)$ is a subsemiring of A, and these axioms hold in $d(A)$. □

Proofs of the previous lemma with an automated theorem prover (such as Prover9 [McC07]) can also be found in [DS08].

3 Reduced Terms and Normal Forms

As usual, we define $x^0 = 1$ and $x^{n+1} = x^n x$.

Lemma 2. *In a domain monoid, if $m \leq n$ then*

$$d(x^m)x^n = x^n \qquad \textit{and} \qquad d(x^m)d(x^n) = d(x^n).$$

Proof. Assuming $m \leq n$, we write $x^n = x^m x^{n-m}$, and using (D1) we have

$$d(x^m)x^n = d(x^m)x^m x^{n-m} = x^m x^{n-m} = x^n.$$

Now (D3) implies $d(x^m)d(x^n) = d(d(x^m)x^n) = d(x^n)$. □

We now describe a normal form for the elements of $F_{\mathsf{DM}}(x)$. For $i, j \geq 0$, a *basic term* is of the form $x^i d(x^j)$. A concatenation of n basic terms is thus of the form

$$x^{i_1}d(x^{j_1})x^{i_2}d(x^{j_2})\cdots x^{i_n}d(x^{j_n}).$$

Such a term is said to be *reduced* if $j_k > i_{k+1} + j_{k+1}$ and $i_{k+1} > 0$ for all $k \in \{1, 2, \ldots, n-1\}$. In particular, all basic terms are reduced.

Next we show that the domain of a reduced term is easy to determine. Together with the subsequent lemma, it follows that any term in the one-generated free domain semiring is equivalent to a term that has no nested occurrences of the domain symbol.

Lemma 3. *Let $t = x^{i_1}d(x^{j_1})x^{i_2}d(x^{j_2})\cdots x^{i_n}d(x^{j_n})$ be a reduced term. Then*

$$d(t) = d(x^{i_1+j_1}).$$

Proof. We use induction on n. For $n = 1$, the result follows from (D2). Suppose it holds for $n-1$, and let $s = x^{i_1}d(x^{j_1})\cdots d(x^{j_{n-2}})x^{i_{n-1}}$. Using (D2) twice we have

$$d(t) = d((sd(x^{j_{n-1}})x^{i_n})d(x^{j_n})) = d(sd(x^{j_{n-1}})x^{i_n+j_n}) = d(sd(d(x^{j_{n-1}})x^{i_n+j_n}))$$

and since $j_{n-1} > i_n + j_n$ we obtain $d(t) = d(sd(x^{j_{n-1}}))$ from (D3) and the preceding lemma. By the inductive hypothesis, the last term is just $d(x^{i_1+j_1})$, as required. □

The concatenation of two reduced terms need not be reduced, but the next lemma shows how to rewrite any such product to reduced form.

Lemma 4. *In any domain monoid the following identities hold:*

(a) $d(xy)xd(yz) = xd(yz)$,
(b) *if* $0 \leq i \leq j + k$ *then* $d(x^i)x^j d(x^k) = x^j d(x^k)$.

Proof. (a) First we note that (D3) and (D1) yield

$$d(y)d(yz) = d(d(y)yz) = d(yz)$$

Using (D2) and (D1) we then obtain

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

(b) If $i \leq j$ then the result follows from Lemma 2. So suppose $i > j$ and $i \leq j+k$. Then $i - j \leq k$, hence, by the result in (a),

$$d(x^i)x^j d(x^k) = d(x^j x^{i-j})x^j d(x^{i-j}x^{k-(i-j)}) = x^j d(x^{i-j}x^{k-(i-j)}).$$

□

Let $t = x^{i_1}d(x^{j_1})x^{i_2}d(x^{j_2})\cdots x^{i_n}d(x^{j_n})$ be a concatenation of basic terms. The *x-length* of t is defined to be $\sum_{k=1}^{n} i_k$. Terms with zero x-length are of the form $d(x^i)$, and they are called *domain terms*. Part (b) of the preceding lemma can be used to eliminate redundant domain terms in any concatenation of basic terms, and this is repeated until the term is in reduced normal form. This process is obviously terminating and it is not hard to see that it has the Church-Rosser property, that is, it produces the same normal form regardless of the order in which domain terms are eliminated. Note also that rewriting terms to normal form preserves the x-length.

The reduced normal form described above, though rather compact, is not convenient for describing the partial order on the elements of the free domain monoid. On elements of the form $d(x^j)$, the order is induced by the meet-semilattice structure: $d(x^j) \leq d(x^k)$ iff $j \geq k$, hence these elements form a chain (see Fig. 1).

For concatenations of basic terms, we rewrite them in *expanded normal form*:

$$d(x^{j_0})xd(x^{j_1})xd(x^{j_2})x\cdots xd(x^{j_m}).$$

where each of the j_k are chosen to be as large as possible. This is justified by using part (b) of the preceding lemma in the reverse direction and with $j = 1$. For brevity we denote such a term by the sequence $(j_0, j_1, j_2, \ldots, j_m)$ and note that this is always a strictly decreasing sequence of nonnegative integers. Let $\mathbf{P} = (P, \leq)$ be the set of all such sequences, ordered by reverse pointwise order. Thus sequences of different length are not comparable, and the maximal elements of this poset are

$$(0), \quad (1,0), \quad (2,1,0), \quad \ldots$$

corresponding to the terms

$$d(1) = 1, \quad d(x)xd(1) = x, \quad d(x^2)xd(x)xd(1) = x^2, \quad \ldots$$

A diagram of an initial part of $\mathbf{P}$ is shown in Figures 1 and 2. A multiplication is defined on P by the following "ripple product"

$$(j_0, j_1, j_2, \ldots, j_m) \cdot (k_0, k_1, k_2, \ldots, k_n) = (j'_0, j'_1, j'_2, \ldots, j'_m, k_1, k_2, \ldots, k_n)$$

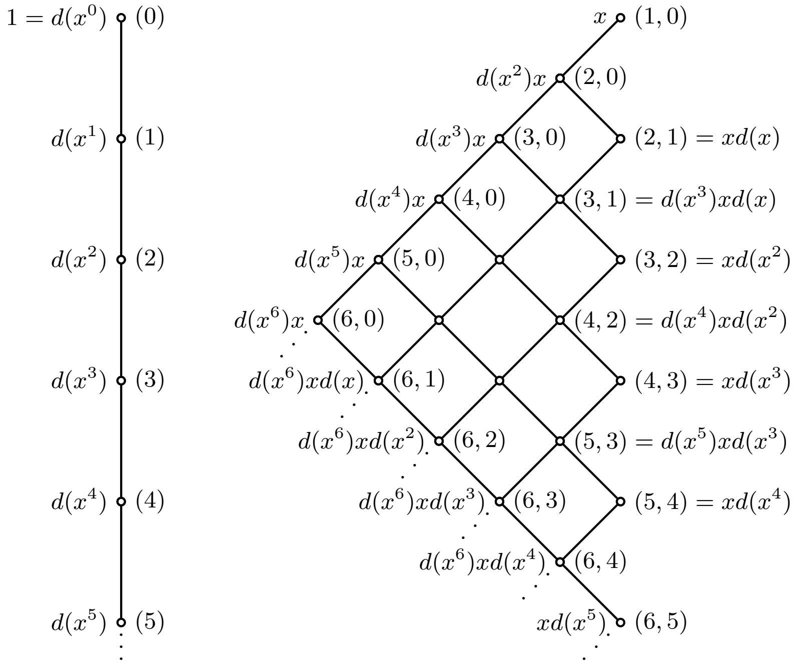


Fig. 1. Below 1 and x in the poset of join-irreducibles of $F_{\mathsf{DS}}(x)$

where $j'_m = \max(j_m, k_0)$ and $j'_i = \max(j_i, j'_{i+1}+1)$ for $i = m-1, \dots, 2, 1, 0$. For example, $(7,3,2) \cdot (4,3,1) = (7,5,4,3,1)$, while $(4,3,1) \cdot (7,3,2) = (9,8,7,3,2)$. The motivation for this definition comes from observing that this is the result if we multiply the corresponding expanded normal forms and rewrite the product again in expanded normal form. It is tedious but not difficult to check that this operation is associative.

The domain of a sequence $(j_0, j_1, j_2, \dots, j_m)$ is the length-one sequence (j_0), which corresponds to the domain term $d(x^{j_0})$.

Let $A(\mathbf{P})$ be the set of finite antichains of $\mathbf{P}$. A partial order is defined on $A(\mathbf{P})$ by $a \leq b$ iff $\downarrow a \subseteq \downarrow b$.

The multiplication is extended to antichains by using the complex product (i.e. $U \cdot V = \{uv : u \in U, v \in V\}$) and by removing all non-maximal elements.

4 Two Representation Theorems

We can now prove the main results of this note and show that the one-generated free domain semiring can be represented either in terms of antichains of integer sequences or in terms of sets of binary relations.

Theorem 1. *The join irreducibles of $F_{\mathsf{DS}}(x)$ form a poset that is isomorphic to $\mathbf{P}$, and $F_{\mathsf{DS}}(x)$ is isomorphic to $A(\mathbf{P})$.*

Proof. By distributivity, each domain semiring term $t(x)$ can be written as a finite join of expanded normal form terms. Hence any join irreducible element of $F_{\mathsf{DS}}(x)$ can be represented by an expanded normal form term.

To show that $\mathbf{P}$ is the poset of these join irreducible, it suffices to show that all expanded normal forms are join irreducible, and that two expanded normal form terms can be distinguished in some domain monoid. We use a domain monoid of relations for the second part. Let $\mathsf{j} = (j_0, \dots, j_m)$ be a decreasing sequence of natural numbers, and define a relation X_j on $\mathbb{N} \times \mathbb{N}$ by $(u, v)X_\mathsf{j}(u', v')$ iff

$$(u = u' \text{ and } v + 1 = v' \leq j_u) \text{ or } (v = v' = 0 \text{ and } u + 1 = u' \leq m)$$

Let $t_\mathsf{j}(x)$ be the term that corresponds to the sequence j. Then it is not hard to see that $((0, 0), (m, 0)) \in t_\mathsf{j}(X_\mathsf{j})$ but for any term s that is not above t_j in $\mathbf{P}$, $((0, 0), (m, 0)) \notin s(X_\mathsf{j})$ (see Fig. 3 for an illustration of X_j).

To prove that the expanded normal form terms are join irreducible, it suffices to show that each such term t is not the join of the elements $s_1, \dots, s_k$ immediately below it in $\mathbf{P}$. For this result we consider the relation X that is the union of all the relations X_j (defined on disjoint base sets), where j ranges over the sequences that correspond to the terms $t, s_1, \dots, s_k$. If we evaluate t and $s_1 + \cdots + s_k$ at this relation X, we see that t is strictly bigger, since it contains a pair from the base of its corresponding relation, which is not contained in $s_i(X)$ for any $i = 1, \dots, k$. □

We now consider the question of representing domain semirings by algebras of binary relations. We first note that for free idempotent semirings this is always possible [BS78]. For a set X of generators, a concrete construction can be obtained by considering the complex algebra of the free group $F_{\mathsf{Grp}}(X)$. This is always a representable relation algebra, with the elements of the group as disjoint relations. Since the free monoid X^* is a subset of the free group, the finite unions of the relations corresponding to singleton words give a relational representation of the free idempotent semiring with X as set of generators.

However, not all idempotent semirings can be represented by $\cup, \circ$ semirings of relations. In fact [And88,And91] showed that the class of algebras of relations, closed under $\cup, \circ$, though definable by quasiequations, is not finitely axiomatisable, hence it is strictly smaller than the finitely based variety of idempotent semirings. Similarly the class of algebras of relations closed under $\cup, \emptyset, \circ, \mathrm{id}, d$, where $d(R) = R;R^{\smile} \cap \mathrm{id}$, is a non-finitely axiomatisable quasivariety, but not a variety.

Theorem 2. *The one-generated free domain semiring can be represented by a domain semiring of binary relations.*

Proof. To see that $F_{\mathsf{DS}}(x)$ can be represented by a collection of binary relations, with operations of union, composition and domain, it suffices to construct a relation X on a set U such that $s(X) \neq t(X)$ in the relation domain semiring $\mathcal{P}(U \times U)$ for any distinct pair of elements of $F_{\mathsf{DS}}(x)$. This is done similarly to the proof of the preceding theorem, by taking X to be the union (over disjoint base sets) of all the relations X_j corresponding to the sequences $\mathsf{j} \in \mathbf{P}$.

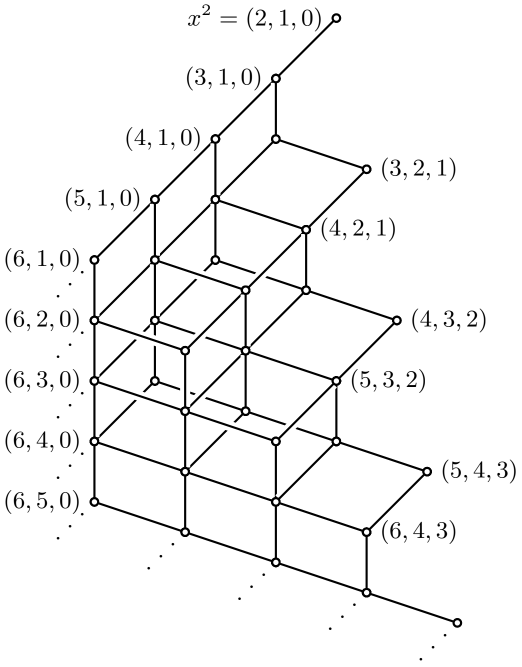
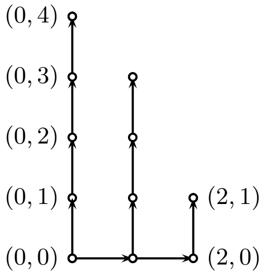


Fig. 2. Below x^2 in the poset of join-irreducibles of $F_{\mathsf{DS}}(x)$

$\mathbf{j} = (4,3,1)$

$t_{\mathbf{j}}(x) = d(x^4)xd(x^3)xd(x)$



$X_{\mathbf{j}} = \{\text{arrows}\}$

Fig. 3. The term and relation for $\mathbf{j} = (4,3,1)$

If s, t are distinct elements of the free domain semiring, then there exists a join irreducible that is below one of them, say s, but not below t. Let $\mathbf{j}$ be the decreasing sequence that corresponds to the expanded normal form $t_{\mathbf{j}}$ for this join irreducible element. Then $t_{\mathbf{j}}(X_{\mathbf{j}}) \subseteq s(X)$ but there is at least one ordered pair in $t_{\mathbf{j}}(X_{\mathbf{j}})$ that is not contained in $t(X)$, hence $s(X)$ and $t(X)$ are distinct relations. □

5 Conclusion

So far our analysis has considered only the one-generated free domain semiring. Even the two-generated case is significantly more complex, since the description of the join irreducible elements is not so transparent (e.g. a term like $d(xd(y)x)$ does not appear to be equivalent to a concatenation of basic terms).

Future research is also aiming to describe the structure of free domain semirings in the presence of additional axioms. It has been shown in [DS08] that the domain algebras $d(S)$ induced by the domain axioms can be turned into (co-)Heyting algebras or Boolean algebras by imposing further constraints. In particular, adding the three axioms

$$a(x)x = 0, \qquad a(xy) \leq a(xa(a(y))) \qquad \text{and} \qquad a(a(x)) + a(x) = 1$$

for an *antidomain* function $a : S \to S$ to the semiring axioms and defining domain as $d(x) = a(a(x))$ suffices to enforce that $d(S)$ is a Boolean algebra and to recover all theorems of the original two-sorted axiomatisation [DMS06]. Based on these results, in particular the structure of the free Boolean domain semirings certainly deserve further investigation.

References

[And88] H. Andréka, *On the representation problem of distributive semilattice-ordered semigroups*, preprint (1988), Abstracts of the AMS, Vol 10, No 2 (March 1989), p. 174.

[And91] H. Andréka, *Representations of distributive lattice-ordered semigroups with binary relations*, Algebra Universalis **28** (1991), 12–25.

[Bir67] G. Birkhoff, "Lattice Theory", 3rd ed., Vol 25 of AMS Colloquium Publications, AMS, 1967, pp. viii+420.

[BS78] D. A. Bredihin, B. M. Schein, *Representations of ordered semigroups and lattices by binary relations*, Colloq. Math. 39 (1978), 1–12.

[DMS06] J. Desharnais, B. Möller, G. Struth, *Kleene algebra with domain*, ACM Transactions on Computational Logic, Vol 7, No 4, 2006, 798–833.

[DS08] J. Desharnais, G. Struth, *Modal Semirings Revisited*, Research Report CS-08-01, Department of Computer Science, The University of Sheffield, 2008.

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

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