The Structure of Free Domain Semirings

P. Jipsen, G. Struth

Chapman U Sheffield

April 9, 2008

Outline

- Introduction
- Domain Semirings
- Free domain semiring
- Representation by by antichains of sequences
- Representation by binary relations
- Conclusion

Introduction

A *semiring* is of the form $(A, +, 0, \cdot, 1)$ such that

- $(A, +, 0)$ is a commutative monoid
- $(A, \cdot, 1)$ is a monoid
- $\cdot$ distributes over all finite joins from the left and right
  i.e. $x(y + z) = xy + xz, \quad (x + y)z = xz + yz$ and $x0 = 0x = 0$

A semiring is *idempotent* if $x + x = x$

IS is the variety of idempotent semirings

Lemma

An idempotent semiring is a (join-)semilattice with 0 *as bottom element, with* $x \le y$ *given by* $x + y = y$ *(since* $+$ *is assoc, commu and idempotent) and* $x \le y \implies wxz \le wyz \qquad$ *(since* $w(x + y)z = wxz + wyz$*)*

Examples

Examples of semirings are:

- Rings
- $(\mathbb{N}, +, 0, \cdot, 1)$
- ...

Examples of idempotent semirings are:

- Reducts of relation algebras $(A, +, 0, ;, 1)$
- Reducts of Kleene algebras $(A, +, 0, \cdot, 1)$
- Reducts of residuated lattices $(A, \wedge, \bot, \cdot, 1)$
- $(\mathbb{R} \cup \{-\infty\}, \max, -\infty, +, 0)$
- Bounded distributive lattices $(A, \vee, 0, \wedge, 1)$
- ...

Free monoids and semirings

Let X be a set of variables (or generators)

The *free monoid over X* is $X^* = \bigcup_{n\in\mathbb{N}} X^n$ with $1 =$ empty sequence and $\cdot$ as concatenation

By distributivity, every term t in the signature of semirings can be written as a finite join of terms of the free monoid X^*

Example: $x(y + xz)(x + 1) = xyx + xxzx + xy + xxz$

$\Rightarrow$ the *free idempotent semiring over X*, denoted by $F_{\mathsf{IS}}(X)$, is isomorphic to the set $\mathcal{P}_{\mathrm{fin}}(X^*)$ of all finite subsets of words over X

Here $U + V = U \cup V$ and $U \cdot V = \{uv : u \in U, v \in V\}$

Decidability

⇒ the *equational theory* of idempotent semirings is decidable:

Given terms s, t, use distributivity to write terms in normal form

However, the *quasiequational theory* (= strict universal Horn theory) is undecidable because:

- The word problem for semigroups is undecidable (Post)
- Every semiring is a semigroup under the operation "$\cdot$"
- Every semigroup S is a "$\cdot$"-subreduct of its powerset semiring $\mathcal{P}(S_e)$ (where S_e the monoid extension of S)
- ⇒ the class of "$\cdot$"-subreducts of semirings is the class of all semigroups

Domain monoids

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

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

The varieties of domain monoids is denoted by DM

Lemma

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

$\Rightarrow$ $d(M) = \{d(x) : x \in M\}$ is a meet semilattice with $1 =$ top element

Domain semirings

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 following additional axioms hold [Desharnais, Struth 2008]

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

$\Rightarrow \qquad xd(x) + x = x \qquad \Rightarrow \qquad x + x = x$

$\Rightarrow$ Every domain semiring is an idempotent semiring

The varieties of domain semirings is denoted by DS

Examples of domain semirings

Examples of domain semirings are e.g.

- reducts of relation algebras with $d(x) = (x;x^{\smile}) \wedge 1'$
- reducts of Kleene algebras with domain

Models of domain semirings in CS:

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

Idempotent semirings formed by sets of paths in a graph with domain defined by sets of starting states

Applications of domain semirings and Kleene algebras with domain have been studied intensively

Applications of domain semirings

The domain operation models enabledness conditions for actions in programs and transition systems

The domain operation can easily be extended into a modal diamond operator that acts on the underlying algebra of domain elements [Möller, Struth 2006]

Links the algebraic approach with more traditional logics of programs such as dynamic, temporal and Hoare logics

Some standard semantics of programs, including the weakest precondition and weakest liberal precondition semantics, can be modeled in this setting

Applications can be found in RelMiCS conference proceedings

Domain semirings

Domain semirings were originally introduced in a *two-sorted* setting

The domain operation maps arbitrary semiring elements to a special Boolean subalgebra [Desharnais, Möller, Struth 2006]

Arbitrary semiring elements model actions of a program or transition system

The elements of the Boolean subalgebra model the states of that system

Here we use the simpler and more general *one-sorted* approach of [Desharnais, Struth 2008]

Studying free domain semirings

The free domain semiring is interesting for applications:

Identifies exactly those terms of domain semirings that have the same denotation in all domain semirings

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

Both relation algebras and Kleene algebras have rich and complex (quasi)equational theories

Rather study the simpler equational theory of domain semirings

Outline of results

Aim: give an explicit description of free domain semirings $F_{\mathsf{DS}}(X)$

- First describe free domain monoid $F_{\mathsf{DM}}(X)$
- Then show that these elements are the join irreducibles of $F_{\mathsf{DS}}(X)$
- $\Rightarrow \quad F_{\mathsf{DS}}(X)$ is isomorphic to the set of finite antichains in the poset of join irreducibles
- Show $F_{\mathsf{DS}}(X)$ is representable by a concrete algebra of binary relations, with relational domain as operations
- $\Rightarrow \quad \mathsf{DS} = \mathsf{HSP}\{\text{Relational domain semirings}\}$
- Finally show any distributive lattice with n_i-ary operators occurs as domain elements of some domain semiring with $n_i - 1$-ary operators

One-generated domain terms

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

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

Lemma

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 $d(x^m)d(x^n) = d(d(x^m)x^n) = d(x^n)$ □

Expanded normal forms

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

For concatenations of basic terms, 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 $j_k \geq \max\{1 + j_{k+1}, 2 + j_{k+2}, \ldots, m - k + j_m\}$

E.g. $xd(x^3)x^2d(x^2) = ...$

Decreasing sequences of numbers

For brevity denote such a term by the sequence $(j_0, j_1, j_2, \dots, j_m)$

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

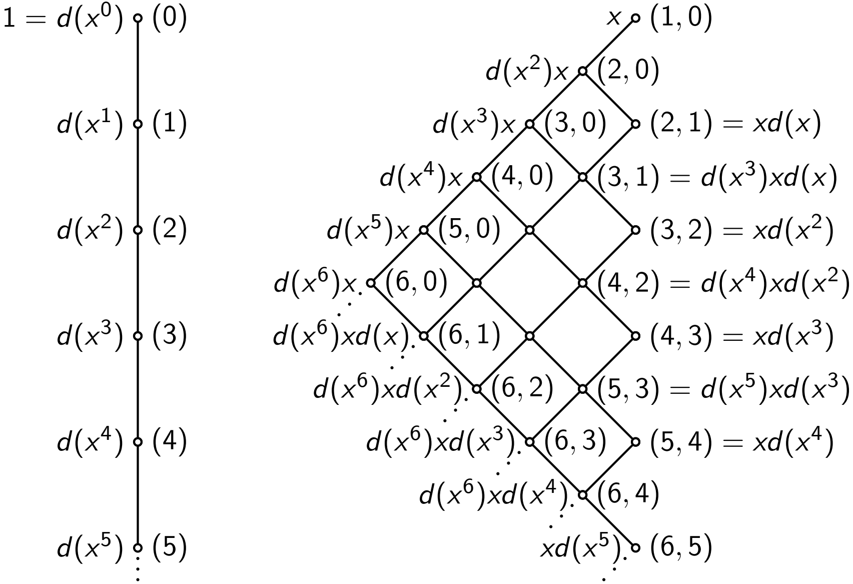
Thus sequences of different length are not comparable, and the maximal elements of this poset are

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

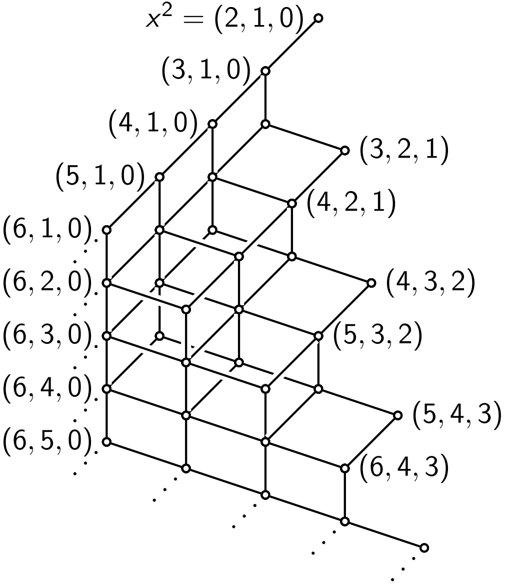
corresponding to the terms

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

The poset of join-irreducibles below 1 and x



The poset of join-irreducibles below x^2



The product of two decreasing sequences

A multiplication is defined on P by the following "ripple product"

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

where $j'_m = \max(j_m, k_0)$ and $j'_i = \max(j_i, j'_{i+1} + 1)$ for $i = m - 1, \ldots, 2, 1, 0$

For example, $(7, 3, 2) \cdot (4, 3, 1) = (7, 5, 4, 3, 1)$, while
$(4, 3, 1) \cdot (7, 3, 2) = (9, 8, 7, 3, 2)$

Can show that this is the result of multiplying the corresponding expanded normal forms and rewriting result in expanded normal form

It is tedious but not difficult to check that this operation is associative

Domain and partial order

The domain of a sequence $(j_0, j_1, j_2, \ldots, j_m)$ is the length-one sequence (j_0)

This 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

Representation Theorem

The first result shows that the one-generated free domain semiring can be represented in terms of antichains of decreasing integer sequences

Theorem

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

Proof.

(outline) By distributivity, each domain semiring term $t(x)$ can be written as a finite join of expanded normal form terms

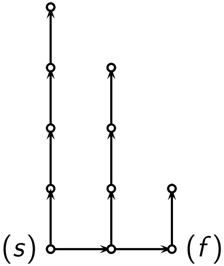
Hence any join irreducible element of $F_{\mathrm{DS}}(x)$ can be represented by an expanded normal form term

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 (details in proceedings) □

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

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

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



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

Represention of semirings by binary relations

First note that for *free* idempotent semirings this is always possible [Bredihin, Schein 1978]

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

Represention of semirings by binary relations

However, not all idempotent semirings can be represented by $\cup, \circ$ semirings of relations

[Andreka 1988, 1991] 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

Represention of semirings by binary relations

Theorem

The one-generated free domain semiring can be represented by a domain semiring of binary relations

Proof.

(outline) To see that $F_{\mathrm{DS}}(x)$ 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 $F_{\mathrm{DS}}(x)$

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 $X_{\mathbf{j}}$ corresponding to the sequences $\mathbf{j} \in \mathbf{P}$ □

n-generated case (briefly)

So far our analysis has considered the one-generated free domain semiring

The n-generated case is more complex, but has recently also been handled

A normal form is given by $d(t_0)y_1d(t_1)y_2\dots d(t_{n-1})y_nd(t_n)$ where t_i are reduced terms

Normal form is given by a reduced tree

Relational representation similar to the one-generated case

Future research is also aiming to describe the structure of free domain semirings in the presence of additional axioms

[Desharnais, Struth 2008] show 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

Anti-domain

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 ensure $d(S)$ is a Boolean algebra

⇒ recover all theorems of the original two-sorted axiomatisation of [Desharnais, Möller, Struth 2006]

Based on these results, in particular the structure of the free Boolean domain semirings certainly deserve further investigation

Boolean domain semirings generalize Jónsson-Tarski BAOs

$|x\rangle p = d(xp)$ is a modal operator on $d(A)$

In general f is an operator if
$f(\dots, x+y, \dots) = f(\dots, x, \dots) + f(\dots, y, \dots)$ and $f(\dots, 0, \dots) = 0$

BAO = BA with operators $\quad \mathbf{B} = (B, +, 0, \cdot, 1, -, (f_i)_{i\in I})$

BDSO = Boolean DS with operators $\quad \mathbf{A} = (A, +, 0, \cdot, 1, a, (g_i)_{i\in I})$

Define $d(\mathbf{A}) = (a(a(A)), +, 0, \cdot, 1, a, (|g_i\rangle)_{i\in I})$ where

$|g_i\rangle(p_0, \dots, p_n) = a(a(g_i(p_0, \dots, p_{n-1}) \cdot p_n))$

Theorem

For any BAO $\mathbf{B}$ *there exists a Boolean DSO* $\mathbf{A}$ *such that* $\mathbf{B} = d(\mathbf{A})$

Domain semirings generalize Gehrke-Jónsson DLOs

DLO = bnd distributive lattices with operators $\mathbf{B} = (B, +, 0, \cdot, 1, -, (f_i)_{i \in I})$

DSO = domain semirings with operators $\mathbf{A} = (A, +, 0, \cdot, 1, d, (g_i)_{i \in I})$

Define $d(\mathbf{A}) = (d(A), +, 0, \cdot, 1, d, (|g_i\rangle)_{i \in I})$ where

$|g_i\rangle(p_0, \dots, p_n) = d(g_i(p_0, \dots, p_{n-1}) \cdot p_n)$

Theorem

For any DLO $\mathbf{B}$ *there exists a DSO* $\mathbf{A}$ *such that* $\mathbf{B} = d(\mathbf{A})$

A is constructed from the relational domain semiring on the join-irreducibles of the canonical extension of **B**

Conclusion: Domain semirings give a simple unisorted extension of the static propositional framework to the dynamic framework of sequences

References

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

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

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

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

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

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

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

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