

ORDERED DOMAIN ALGEBRAS

ROB EGROT, ROBIN HIRSCH AND SZABOLCS MIKULÁS

ABSTRACT. We give a finite axiomatisation to representable ordered domain algebras and show that finite algebras are representable on finite bases.

Domain algebras provide an elegant, one-sorted formalism for automated reasoning about program and system verification [DS08a, DS08b]. The algebraic behaviour of domain algebras have been investigated, e.g. in [DJS09a, DJS09b]. Their primary models are algebras of relations, viz. representable domain algebras. P. Jipsen and G. Struth raised the question whether the class $\mathbf{R}(\cdot, \text{dom})$ of representable domain algebras of the minimal signature (\cdot, dom) is finitely axiomatisable. To formulate the question precisely, let us recall the definition of representable domain algebras $\mathbf{R}(\cdot, \text{dom})$.

Definition 0.1. *The class $\mathbf{R}(\cdot, \text{dom})$ is defined as the isomorphs of $\mathcal{A} = (A, \cdot, \text{dom})$ where $A \subseteq \wp(U \times U)$ for some base set U and*

$$\begin{aligned} x \cdot y &= \{(u, v) \in U \times U : (u, w) \in x \text{ and } (w, v) \in y \text{ for some } w \in U\} \\ \text{dom}(x) &= \{(u, u) \in U \times U : (u, v) \in x \text{ for some } v \in U\} \end{aligned}$$

for every $x, y \in A$.

The signature (\cdot, dom) can be expanded to larger signatures τ by including other operations. For instance, we can define

$$\begin{aligned} \text{ran}(x) &= \{(v, v) \in U \times U : (u, v) \in x \text{ for some } u \in U\} \\ x \smile &= \{(v, u) \in U \times U : (u, v) \in x\} \\ 1' &= \{(u, v) \in U \times U : u = v\} \end{aligned}$$

and the corresponding representation classes $\mathbf{R}(\tau)$ analogously to the definition of $\mathbf{R}(\cdot, \text{dom})$. We can also include bottom 0 and top 1 elements (interpreted as \emptyset and $U \times U$, respectively) and the ordering \subseteq to yield representable algebraic structures.

It turned out that the answer to the above problem is negative.

Theorem 0.2. *[[HM11]] Let τ be a similarity type such that $(\cdot, \text{dom}) \subseteq \tau \subseteq (\cdot, \text{dom}, \text{ran}, 0, 1')$. The class $\mathbf{R}(\tau)$ of representable τ -algebras is not finitely axiomatisable in first-order logic.*

Note that the above theorem does not apply to signatures where the ordering \subseteq is definable. In fact, D.A. Bredikhin proved [Bre77] that the class $\mathbf{R}(\cdot, \text{dom}, \text{ran}, \smile, \subseteq)$ of representable algebraic structures is finitely axiomatisable. Our aim is to provide an alternative, and slightly more general, proof that $\mathbf{R}(\cdot, \text{dom}, \text{ran}, \smile, 0, 1', \subseteq)$ is finitely axiomatisable. The advantage of our proof is that it uses a Cayley-type representation of abstract algebraic structures that also shows finite representability, i.e. that finite elements of $\mathbf{R}(\cdot, \text{dom}, \text{ran}, \smile, 0, 1', \subseteq)$ can be represented on finite bases. In passing we note that if composition is not definable in τ , then $\mathbf{R}(\tau)$

has the finite representation property, but every signature containing $(\cap, ;, 1')$ or $(\cap, ;, \smile)$ fails to have the finite representation property.

MAIN RESULT

Let **Ax** denote the following formulas.

Partial order: \leq is reflexive, transitive and antisymmetric, with lower bound 0.

Monotonicity and normality: the operators $\smile, ;, \text{dom}, \text{ran}$ are monotonic, e.g. $a \leq b \rightarrow a ; c \leq b ; c$ etc. and normal $0 \smile = 0 ; a = a ; 0 = \text{dom}(0) = \text{ran}(0) = 0$.

Involuted monoid: $;$ is associative, $1'$ is left and right identity for $;$, $1' \smile = 1'$ and \smile is an involution: $(a \smile) \smile = a$, $(a ; b) \smile = b \smile ; a \smile$.

Domain/range axioms:

- (1) $\text{dom}(a) = (\text{dom}(a)) \smile \leq 1' = \text{dom}(1')$
- (2) $\text{dom}(a) \leq a ; a \smile$
- (3) $\text{dom}(a \smile) = \text{ran}(a)$
- (4) $\text{dom}(\text{dom}(a)) = \text{dom}(a) = \text{ran}(\text{dom}(a))$
- (5) $\text{dom}(a) ; a = a$
- (6) $\text{dom}(a ; b) = \text{dom}(a ; \text{dom}(b))$
- (7) $\text{dom}(\text{dom}(a) ; \text{dom}(b)) = \text{dom}(a) ; \text{dom}(b) = \text{dom}(b) ; \text{dom}(a)$
- (8) $\text{dom}(\text{dom}(a) ; b) = \text{dom}(a) ; \text{dom}(b)$

A model of these axioms is called an *ordered domain algebra*.

A consequence of axioms (4) and (5) is

$$(9) \quad \text{dom}(a) ; \text{dom}(a) = \text{dom}(a)$$

Each of the axioms (1)–(8) has a dual axiom, obtained by swapping domain and range and reversing the order of compositions, and we denote the dual axiom by a ∂ superscript, thus for example, (6) ^{∂} is $\text{ran}(b ; a) = \text{ran}(\text{ran}(b) ; a)$. The dual axioms can be obtained from the axioms above, using the involution axioms and (3).

Our main result is the following.

Theorem 0.3. *The class $\mathbf{R}(; , \text{dom}, \text{ran}, \smile, 0, 1', \subseteq)$ is finitely axiomatisable:*

$$\mathcal{A} \in \mathbf{R}(; , \text{dom}, \text{ran}, \smile, 0, 1', \subseteq) \text{ iff } \mathcal{A} \models \mathbf{Ax}$$

and has the finite representation property.

Proof. First we extend the operations of a domain algebra to subsets of elements.

Definition 0.4. *Let \mathcal{A} be an ordered domain algebra.*

- (1) Write $D(\mathcal{A})$ for the set of domain elements of \mathcal{A} — those elements $d \in \mathcal{A}$ such that $\text{dom}(d) = d$. Observe that $(D(\mathcal{A}), ;)$ forms a lower semilattice ordered by \leq .
- (2) For $a \in \mathcal{A}$, let $a^\uparrow = \{b \in \mathcal{A} : a \leq b\}$ and more generally, for $X \subseteq \mathcal{A}$, let $X^\uparrow = \{b \in \mathcal{A} : (\exists a \in X) a \leq b\}$.

(3) We extend the operations so as to apply to sets of elements. If $X, Y \subseteq \mathcal{A}$, $a \in \mathcal{A}$, then

$$(10) \quad X^\smile = \{x^\smile : x \in X\}^\uparrow$$

$$(11) \quad X ; Y = \{x ; y : x \in X, y \in Y\}^\uparrow$$

$$(12) \quad \text{dom}(X) = \{\text{dom}(x) : x \in X\}^\uparrow$$

$$(13) \quad \text{ran}(X) = \{\text{ran}(x) : x \in X\}^\uparrow$$

Note that these sets are all ‘closed upwards’ by definition.

(4) A non-empty subset X of \mathcal{A} is closed if

$$(14) \quad \text{dom}(X) ; X ; \text{ran}(X) = X$$

Thus, for an ordered domain algebra \mathcal{A} , we can define another algebra on the subsets $\wp(\mathcal{A})$ of \mathcal{A} , and the partial order \leq on $\wp(\mathcal{A})$ is given by \supseteq . We will denote this ordered algebra as $\mathcal{C}(\mathcal{A})$, the elements of $\wp(\mathcal{A})$ by upper case letters X, Y, Z etc. or by a^\uparrow, b^\uparrow etc., and the elements of \mathcal{A} with lower case letters a, b, c etc. It should be clear from this notational convention whether we evaluate a term in \mathcal{A} or in $\mathcal{C}(\mathcal{A})$.

It is not difficult to check the following. Let $\tau \leq \sigma$ be an axiom of domain algebras such that every variable a occurs at most once in τ and at most once in σ . Then the inequality $\tau \supseteq \sigma$ is valid $\mathcal{C}(\mathcal{A})$. (Hint: use monotonicity and the validity of $\tau \leq \sigma$ in \mathcal{A} .) But axioms like (2) and (5) fail in general even in the subalgebra of upwards-closed elements of $\mathcal{C}(\mathcal{A})$.

Observe, from definition 0.4(3) and the transitivity of \leq , that $(\text{dom}(X) ; X ; \text{ran}(X))^\uparrow = \text{dom}(X) ; X ; \text{ran}(X)$, for any set $X \subseteq \mathcal{A}$. So every closed set is upwards closed. More equations are valid in $\mathcal{C}(\mathcal{A})$ if the variables are evaluated on closed elements, e.g. (5), but closed elements may not be closed under the operations, e.g. $X ; Y$ for closed X and Y is not closed in general, and (2) may still fail.

Let $Cl(\mathcal{A})$ be the set of all closed subsets of \mathcal{A} . Since $Cl(\mathcal{A}) \subseteq \wp(\mathcal{A})$, we have $|Cl(\mathcal{A})| \leq 2^{|\mathcal{A}|}$. Define a map F from \mathcal{A} to a structure with base $Cl(\mathcal{A})$ as follows.

$$(15) \quad (X, Y) \in a^F \iff X ; a^\uparrow \subseteq Y \text{ and } Y ; (a^\smile)^\uparrow \subseteq X$$

We claim that F yields a representation of \mathcal{A} . To this end let $0 \neq a \not\leq b$. It is easy to show that $(\text{dom}(a))^\uparrow, a^\uparrow$ are closed. By monotonicity, (5) and (2), $(\text{dom}(a))^\uparrow ; a^\uparrow \subseteq a^\uparrow$ and $a^\uparrow ; (a^\smile)^\uparrow \subseteq (\text{dom}(a))^\uparrow$, so $((\text{dom}(a))^\uparrow, a^\uparrow) \in a^F$. Also, we cannot have $\text{dom}(a) ; b \geq a$, by transitivity, monotonicity and (1), since $a \not\leq b$. Thus $((\text{dom}(a))^\uparrow, a^\uparrow) \notin b^F$, whence F is faithful.

$0^F = \emptyset$, by normality and the partial order axioms. \leq is correctly represented by the partial order axioms and monotonicity. $1^F = \{(X, X) : X \in Cl(\mathcal{A})\}$ by the involuted monoid axioms. \smile is correctly represented by the involution axioms.

Next we check composition. If $(X, Y) \in a^F$ and $(Y, Z) \in b^F$, then $X ; a^\uparrow \subseteq Y$, $Y ; (a^\smile)^\uparrow \subseteq X$, $Y ; b^\uparrow \subseteq Z$ and $Z ; (b^\smile)^\uparrow \subseteq Y$. Hence $X ; (a ; b)^\uparrow \subseteq Z$ and $Z ; ((a ; b)^\smile)^\uparrow \subseteq X$ by associativity and the involution axioms. So $(X, Z) \in (a ; b)^F$.

Conversely, assume that $(X, Z) \in (a ; b)^F$. We need a closed Y such that $(X, Y) \in a^F$ and $(Y, Z) \in b^F$.

Claim 0.5. The sets

$$\alpha = X ; a^\uparrow ; \text{ran}(Z ; (b^\smile)^\uparrow) \text{ and } \beta = Z ; (b^\smile)^\uparrow ; \text{ran}(X ; a^\uparrow)$$

and $\alpha \cup \beta$ are closed.

Thus we can define the closed element $Y = \alpha \cup \beta$. That ; is properly represented follows by the following claim.

Claim 0.6. $(X, Y) \in a^F$ and $(Y, Z) \in b^F$.

Finally, we show that dom and ran are properly represented. If $(X, Y) \in (\text{dom}(a))^F$, then $X ; (\text{dom}(a))^\dagger \subseteq Y$. Since $\text{dom}(a) \leq 1'$ by (1), we have that, for every $x \in X$, there is $y \in Y$ such that $x \geq x ; \text{dom}(a) \geq y$. Since Y is (upwards) closed, we get $X \subseteq Y$. Similarly, we get $Y \subseteq X$ by $Y ; ((\text{dom}(a))^\smile)^\dagger \subseteq Y ; (\text{dom}(a))^\dagger \subseteq X$ (using (1)). Hence $X = Y$, i.e., $(X, X) \in (\text{dom}(a))^F$. Note also that $\text{dom}(a) \in \text{ran}(X)$, since $\text{dom}(a) \in \text{ran}(Y ; (\text{dom}(a))^\dagger) \subseteq \text{ran}(x)$.

Define the closed element $Z = X ; a^\dagger$. Then $(X, Z) \in a^F$, since $X ; a^\dagger \subseteq Z$ by definition, and

$$X ; a^\dagger ; (a^\smile)^\dagger \subseteq X ; (\text{dom}(a))^\dagger \subseteq X$$

by (2) and $\text{dom}(a) \in \text{ran}(X)$. Conversely, suppose $(X, Z) \in a^F$ (for some Z). Then $X ; a^\dagger \subseteq Z$ and $Z ; (a^\smile)^\dagger \subseteq X$. Since $Z ; (a^\smile)^\dagger \subseteq X$, we have $\text{dom}(a) = \text{ran}(a^\smile) \in \text{ran}(Z ; (a^\smile)^\dagger) \subseteq \text{ran}(X)$, whence $X ; (\text{dom}(a))^\dagger \subseteq X$, i.e. $(X, X) \in (\text{dom}(a))^F$. So dom is correctly represented. Showing that ran is properly represented is similar. This finishes the proof of Theorem 0.3. \square

REFERENCES

- [Bre77] D.A. Bredikhin, “An abstract characterization of some classes of algebras of binary relations”, in *Algebra and Number Theory*, No. 2, pp. 3–19. Kabardino-Balkarsk. Gos. Univ., Nalchik, 1977. [In Russian.]
- [DJS09a] J. Desharnais, P. Jipsen and G. Struth, “Domain and antidomain semigroups”, in R. Berghammer et al. (eds.), *Relations and Kleene Algebra in Computer Science*, pages 73–87, Springer-Verlag, 2009.
- [DJS09b] J. Desharnais, P. Jipsen and G. Struth, “Internal Axioms for Domain Semirings”, presentation at *TACL'2009*, extended abstract available at http://staff.science.uva.nl/~gfontain/tac109-abstracts/tac12009_submission_73.pdf.
- [DS08a] J. Desharnais and G. Struth, “Modal semirings revisited”, in P. Audebaud and C. Paulin-Mohring (eds.), *MPC 2008*, pages 360–387, Springer-Verlag, 2008.
- [DS08b] J. Desharnais and G. Struth, “Domain axioms for a family of near-semirings”, in J. Meseguer and G. Roşu (eds.), *AMAST 2008*, pages 330–345, Springer-Verlag, 2008.
- [HM11] R. Hirsch and Sz. Mikulás, “Axiomatizability of representable domain algebras”, *Journal of Logic and Algebraic Programming*, Vol. 80(2), pp. 75–91, 2011.

Department of Computer Science
 University College London
 E-mail: R.Egrot@cs.ucl.ac.uk r.hirsch@cs.ucl.ac.uk

Department of Computer Science and Information Systems
 Birkbeck College, University of London
 E-mail: szabolcs@dcs.bbk.ac.uk