Algebra Universalis

Finite representability of semigroups with demonic refinement

Robin Hirsch and Jaš Šemrl

Abstract. The motivation for using demonic calculus for binary relations stems from the behaviour of demonic turing machines, when modelled relationally. Relational composition (;) models sequential runs of two programs and demonic refinement ($\sqsubseteq$) arises from the partial order given by modeling demonic choice ($\sqcup$) of programs (see below for the formal relational definitions). We prove that the class $R(\sqsubseteq, ;)$ of abstract $(\leq, \circ)$ structures isomorphic to a set of binary relations ordered by demonic refinement with composition cannot be axiomatised by any finite set of first-order $(\leq, \circ)$ formulas. We provide a fairly simple, infinite, recursive axiomatisation that defines $R(\sqsubseteq, ;)$. We prove that a finite representable $(\leq, \circ)$ structure has a representation over a finite base. This appears to be the first example of a signature for binary relations with composition where the representation class is non-finitely axiomatisable, but where the finite representation property holds for finite structures.

Mathematics Subject Classification. 03G15, 06F05.

Keywords. Relation algebra, Demonic refinement, Ordered semigroups, Finite representability property.

1. Introduction and motivation

A simple way of representing a $(\leq, \circ)$ structure is to interpret the binary relation $\leq$ as set inclusion $\subseteq$, and the binary function $\circ$ as composition of binary relations ;, defined for relations R, S as

$$R; S = \{(x, y) : \exists z((x, z) \in R \land (z, y) \in S)\}$$

The class $R(\subseteq, ;)$ of abstract $(\leq, \circ)$ structures isomorphic to sets of binary relations with inclusion and composition is defined exactly by the axioms
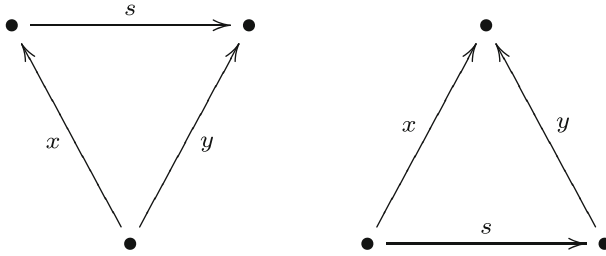
FIGURE 1. Two representations, for ordered semigroups

of ordered semigroups [15], i.e. associativity, partial order, left and right mono-tonicity. It is clear that these axioms are valid over $R(\subseteq, ;)$. Conversely, given an ordered semigroup $\mathcal{S} = (S, \leq, \circ)$ we may extend the structure to an ordered semigroup $\mathcal{S}' = (S', \leq, \circ)$ by adding a single new two-sided identity element e where $e \not\leq s$ and $s \not\leq e$ for $s \in S$, and then defining a representation $\theta : \mathcal{S} \to \wp(\mathcal{S}' \times \mathcal{S}')$ by

$$(x, y) \in s^\theta \iff y \leq x \circ s$$

illustrated in the first diagram of Figure 1. Note that the image of $s \in \mathcal{S}$ is denoted s^θ. The extra identity element is used to prove faithfulness of θ: if $s \not\leq t \in \mathcal{S}$ then $(e, s) \in s^\theta$ but $(e, s) \notin t^\theta$. A dual representation θ' of $\mathcal{S}$ over $\mathcal{S}'$, illustrated in the second part of Figure 1, is defined by

$$(x, y) \in s^{\theta'} \iff x \leq s \circ y.$$

Both inclusion and composition have demonic variants, written $(\sqsubseteq, *)$ called demonic refinement and demonic composition defined by

$$R \sqsubseteq S \iff (\text{dom}(S) \subseteq \text{dom}(R) \wedge R{\restriction}_{\text{dom}(S)} \subseteq S)$$
$$R * S = R; S \cap \{(x, y) : \forall z((x, z) \in R \to z \in \text{dom}(S))\}$$

where $\text{dom}(S) = \{x : \exists y (x, y) \in S\}$ and $R{\restriction}_{\text{dom}(S)}$ denotes the restriction of R to pairs (x, y) where $x \in \text{dom}(S)$. Closely related to the demonic refinement relation is the demonic join operator $\sqcup$, defined by

$$R \sqcup S = (R \cup S){\restriction}_{\text{dom}(R) \cap \text{dom}(S)}$$

In the set of all binary relations over a set X, $R \sqcup S$ is the join (least upper bound) of R, S with respect to $\sqsubseteq$. Conversely, given the operator $\sqcup$ we may recover the relation $\sqsubseteq$ by defining $R \sqsubseteq S \iff R \sqcup S = S$. Note, however, that an operator $\sqcap$ that returns the greatest lower bound of two relations may not be defined, it is not in general the case that two binary relations have any common lower bound with respect to $\sqsubseteq$, see Section 5. Roughly speaking, these operations were motivated by relational modelling of the behaviour of a Turing Machine, when the demon is in control whereas their analogous 'angelic' counterparts can be used to relationally model the behaviour of the same machine when the angel makes the nondeterministic choices.

It is known [3] that $R(\sqsubseteq, *)$ is also axiomatised by the same three axioms of ordered semigroups that axiomatise $R(\subseteq, ;)$. This suggests a wider duality

between angelic and demonic operators and relations for algebras of binary relations; such a duality deserves further investigation. Certainly, algebras of binary relations with mixed signatures are not so nicely behaved. For example over $R(\subseteq, *)$, although $*$ remains associative, $\subseteq$ is still a partial order and $*$ is right monotonic with respect to $\subseteq$, we find that left monotonicity fails, and it was shown recently that $R(\subseteq, *)$ is not finitely axiomatisable [9].

Our main focus here is the representation class $R(\sqsubseteq, ;)$, a second example of a mixed signature, this time with angelic composition and demonic refinement. The motivation for using $\sqsubseteq$ in conjunction with ; is based on the Refinement Algebra described in [14], but adapted for relational reasoning. Consider a Hoare triple (P, A, Q), where A is a nondeterministic program and P, Q are pre and post conditions. We can model A as the binary relation over the base of all configurations C consisting of all pairs (c_1, c_2) where program A can terminate in configuration c_2, starting from c_1. A condition, such as $P, Q, \neg Q$ etc., can be modelled as the set of all (c, c) such that c satisfies the condition, so that programs and conditions are modelled as binary relations over C. We can model the partial correctness of (P, A, Q) by $P; A = P; A; Q$ which implies, by associativity and monotonicity, $P; A; (\neg Q) = P; A; Q; (\neg Q) = P; A; 0 \subseteq 0$ where 0 is the empty relation, the bottom element with respect to $\subseteq$. One reason why this fails to model total correctness is that programs without terminating runs will also be modelled as 0. However, if we add a new point $\perp$ to the base C, extend A to A' by including $(c, \perp)$ in A' whenever c is in the domain of A, and extend each condition P to P' by including $(\perp, \perp)$ (so all conditions hold at $\perp$), as we mention in Section 5, we find the bottom element with respect to $\sqsubseteq$ to be $\mathbf{0} = \{(c, \perp) : c \in C\}$ (note the bold font, to distinguish it from the empty relation), and we can still model the partial correctness of (P, A, Q) as $P'; A' = P'; A'; Q'$, but this does not imply $P'; A'; (\neg Q)' \sqsubseteq P'; \mathbf{0}$ as monotonicity fails. In fact, if $P'; A'; (\neg Q)' \sqsubseteq P'; \mathbf{0}$ holds then from any configuration c satisfying P the only configuration reachable by A' where $\neg Q$ holds is $\perp$ (hence partial correctness), and the domain of A' (which is the same as the domain of A) includes all configurations satisfying P, hence from any configuration satisfying P there is a terminating run of A to a configuration satisfying Q. Thus $P'; A'; (\neg Q)' \sqsubseteq P'; \mathbf{0}$ is equivalent to the total correctness of (P, A, Q).

Over $R(\sqsubseteq, ;)$ we find that both left and right monotonicity fail. A key problem we address is to axiomatise this representation class. To find an axiomatisation, of course we may use the axioms of associativity and partial order, but what additional axioms should be included in order to fill the gap created by the omission of the two monotonicity axioms? The main results here are a recursively defined infinite set of axioms that defines $R(\sqsubseteq, ;)$ and a proof that no finite set of axioms can do it. Our proof that the recursive axiomatisation is complete also shows that a finite representable $(\sqsubseteq, ;)$-structure has a representation over a finite base set.

Algebras of binary relations have been used extensively to model program semantics [11,5], and the introduction of demonic choice ($\sqcup$) and demonic composition ($*$) has extended this framework towards reasoning about the total

correctness of non-deterministic Turing Machines [5, 1]. The introduction of the demonic refinement predicate led to further verification applications, for example utilising Refinement Algebras [14, 4]. Furthermore, relaxing the requirement that composition is a total binary operator we obtain *refined semigroupoids*, which have been of interest in relation-algebraic programming [10].

The fairly extensive literature on demonic relations and operators includes a variety of different notations. In the context of Kleene Algebra extensions, such as Refinement Algebra, where the emphasis is on the behaviour of tests, $\sqcap, \sqsupseteq$ are sometimes used in place of $\sqcup, \sqsubseteq$.

2. Axiomatising $R(\sqsubseteq, ;)$

We focus on the signature $(\sqsubseteq, ;)$, in the abstract case the corresponding symbols will be $(\leq, \circ)$. A binary relation over the base X is a subset of $X \times X$. A *concrete* $(\sqsubseteq, ;)$ structure is a set of binary relations over some base, closed under composition, with demonic refinement. An isomorphism from an abstract $(\leq, \circ)$ structure to a concrete $(\sqsubseteq, ;)$ structure is called a representation. $R(\sqsubseteq, ;)$ denotes the class of all $(\leq, \circ)$ structures isomorphic to concrete $(\sqsubseteq, ;)$ structures.

The signature does not include the domain operation, nor does it include 'angelic' (ordinary) set inclusion. However, we will define with infinitary $(\leq, \circ)$-formulas, the predicates $\blacktriangleleft, \vartriangleleft^s$ to signify the domain inclusion and inclusion of the restriction to the domain of s respectively, see Lemma 2.2 below.

Let

$$a \blacktriangleleft b \Leftrightarrow \bigvee_{n < \omega} a \blacktriangleleft_n b$$

$$a \vartriangleleft^s b \Leftrightarrow \bigvee_{n < \omega} a \vartriangleleft^s_n b$$

where

$$a \blacktriangleleft_0 b \Leftrightarrow a \geq b \vee \exists c (a \geq b \circ c)$$

$$a \vartriangleleft^s_0 b \Leftrightarrow (a \leq b \wedge s = b)$$

$$a \blacktriangleleft_{n+1} b \Leftrightarrow \left\{ \begin{array}{l} (a \vartriangleleft^a_n b) \vee \\ \exists c\, (a \blacktriangleleft_n c \wedge c \blacktriangleleft_n b) \vee \\ \exists d, f, f'\, (a = d \circ f \wedge f \blacktriangleleft_n f' \wedge b = d \circ f')) \end{array} \right\}$$

$$a \vartriangleleft^s_{n+1} b \Leftrightarrow \left\{ \begin{array}{l} (\exists c\, (a \vartriangleleft^s_n c \wedge c \vartriangleleft^s_n b)) \vee \\ \exists c, c', d, d'\, (a = c \circ d \wedge c \vartriangleleft^s_n c' \wedge d \vartriangleleft^d_n d' \wedge b = c' \circ d') \vee \\ \exists s'(a \vartriangleleft^{s'}_n b \wedge s \blacktriangleleft_n s') \end{array} \right\}$$

Lemma 2.1. (1) Reflexivity holds for both $\blacktriangleleft, \vartriangleleft^s$ for any s
(2) $a \blacktriangleleft_n b \wedge b \blacktriangleleft_n c \to a \blacktriangleleft_{n+1} c$, $a \vartriangleleft^s_n b \wedge b \vartriangleleft^s_n c \to a \vartriangleleft^s_{n+1} c$, so $\blacktriangleleft$ and $\vartriangleleft^s$ are transitive, for each $s \in S$
(3) $a \vartriangleleft^s_n b \circ c$, $b \vartriangleleft^s_n b'$, $c \vartriangleleft^c_n c'$ implies $a \vartriangleleft^s_{n+1} b' \circ c'$,
(4) $d \blacktriangleleft_n a \circ c$, $a \leq a'$, $d \blacktriangleleft_n a'$, $c \blacktriangleleft_n c'$ implies $d \blacktriangleleft_{n+3} a' \circ c'$,
(5) $s \blacktriangleleft_n s'$, $a \vartriangleleft^{s'}_n b$ implies $a \vartriangleleft^s_{n+1} b$

Proof. (1), (2), (3), (5) follow directly from the definitions of $\blacktriangleleft, \lhd$. For (4), observe how from $a \leq a'$ we have $a \lhd_0^{a'} a'$ which, together with $a \circ c' \blacktriangleleft_0 a'$, give us $a \lhd_1^{a \circ c'} a'$. From this and $c' \lhd_0^{c'} c'$ we get $a \circ c' \lhd_2^{a \circ c'} a' \circ c'$ and thus $a \circ c' \blacktriangleleft_3 a' \circ c'$. We also have $c \blacktriangleleft_n c'$ and hence $a \circ c \blacktriangleleft_{n+1} a \circ c'$. So, by the transitive steps $d \blacktriangleleft_n a \circ c \blacktriangleleft_{n+1} a \circ c' \blacktriangleleft_3 a' \circ c'$ we obtain $d \blacktriangleleft_{n+3} a' \circ c'$. $\square$

Lemma 2.2. *Let $\mathcal{S} \in R(\sqsubseteq, ;)$ and let θ be a representation of $\mathcal{S}$. For all $a, b, s \in \mathcal{S}$*

$$a \blacktriangleleft b \Rightarrow \mathrm{dom}(a^\theta) \subseteq \mathrm{dom}(b^\theta), \text{ and}$$

$$a \lhd^s b \Rightarrow a^\theta \!\restriction_{\mathrm{dom}(s^\theta)} \subseteq b^\theta.$$

Proof. We prove both claims by a single induction over n. In the base case, if $a \blacktriangleleft_0 b$ then either $a^\theta \sqsupseteq b^\theta$ or $a^\theta \sqsupseteq b^\theta; c^\theta$ (for some c) hence $\mathrm{dom}(a^\theta) \subseteq \mathrm{dom}(b^\theta)$. And if $a \lhd_0^s b$ then $s = b$, $a \leq b$, so $a^\theta\!\restriction_{\mathrm{dom}(s^\theta)} = a^\theta\!\restriction_{\mathrm{dom}(b^\theta)} \subseteq b^\theta$.

For the inductive step, suppose $a \blacktriangleleft_{n+1} b$, from the recursive definition, there are three alternatives. In the first case, $a \lhd_n^a b$ then inductively $a^\theta = a^\theta\!\restriction_{\mathrm{dom}(a^\theta)} \subseteq b^\theta$ so $\mathrm{dom}(a^\theta) \subseteq \mathrm{dom}(b^\theta)$. In the second case, inductively $\mathrm{dom}(a^\theta) \subseteq \mathrm{dom}(c^\theta) \subseteq \mathrm{dom}(b^\theta)$. In the third case, there are d, f, f' where $a = d \circ f$, $f \blacktriangleleft_n f'$ and $b = d \circ f'$. For any $x \in \mathrm{dom}(a^\theta)$, there is y such that $(x, y) \in a^\theta$ and there is z such that $(x, z) \in d^\theta$, $(z, y) \in f^\theta$. Inductively, $z \in \mathrm{dom}(f^\theta) \subseteq \mathrm{dom}((f')^\theta)$ so there is w such that $(z, w) \in (f')^\theta$, hence $(x, w) \in d^\theta; (f')^\theta = b^\theta$, so $x \in \mathrm{dom}(b^\theta)$, proving $\mathrm{dom}(a^\theta) \subseteq \mathrm{dom}(b^\theta)$.

Now suppose $a \lhd_{n+1}^s b$. There are three alternatives in the recursive definition. In the first case, inductively $a^\theta\!\restriction_{\mathrm{dom}(s^\theta)} \subseteq c^\theta$ and $c^\theta\!\restriction_{\mathrm{dom}(s^\theta)} \subseteq b^\theta$, so $a^\theta\!\restriction_{\mathrm{dom}(s^\theta)} \subseteq b^\theta$. In the second case, there are c, c', d, d' as in the definition. If $x \in \mathrm{dom}(s^\theta)$ and $(x, y) \in a^\theta$ then there is z such that $(x, z) \in c^\theta$, $(z, y) \in d^\theta$. Inductively, $(x, z) \in (c')^\theta$ and $(z, y) \in (d')^\theta$, hence $(x, y) \in (c' \circ d')^\theta = b^\theta$. In the third case, $\mathrm{dom}(s^\theta) \subseteq \mathrm{dom}((s')^\theta)$, so $a\!\restriction_{\mathrm{dom}(s^\theta)} \subseteq a\!\restriction_{\mathrm{dom}((s')^\theta)} \subseteq b^\theta$. This proves $a^\theta\!\restriction_{\mathrm{dom}(s^\theta)} \subseteq b^\theta$, as required. $\square$

Let

$$\sigma_n = ((b \blacktriangleleft_n a \wedge a \lhd_n^b b) \to a \leq b)$$

$$\sigma = ((b \blacktriangleleft a \wedge a \lhd^b b) \to a \leq b)$$

For finite n, σ_n is a first-order formula, while σ is infinitary and is equivalent to $\bigwedge_{n < \omega} \sigma_n$.

Lemma 2.3.

$$R(\sqsubseteq, ;) \models \sigma.$$

Proof. Let $\mathcal{S} \in R(\sqsubseteq, ;)$ and let θ be a representation. Assume the premise of σ, $\mathcal{S} \models (b \blacktriangleleft a \wedge a \lhd^b b)$. By the previous Lemma, $\mathrm{dom}(b^\theta) \subseteq \mathrm{dom}(a^\theta)$ and $a^\theta\!\restriction_{\mathrm{dom}(b^\theta)} \subseteq b^\theta$, i.e. $a^\theta \sqsubseteq b^\theta$. Since θ represents $\leq$ as $\sqsubseteq$ we must have $\mathcal{S} \models a \leq b$. Thus $\mathcal{S} \models \sigma$. $\square$

We now define an explicit construction of a representation to prove completeness. It will be loosely based on representation for ordered semigroups θ'
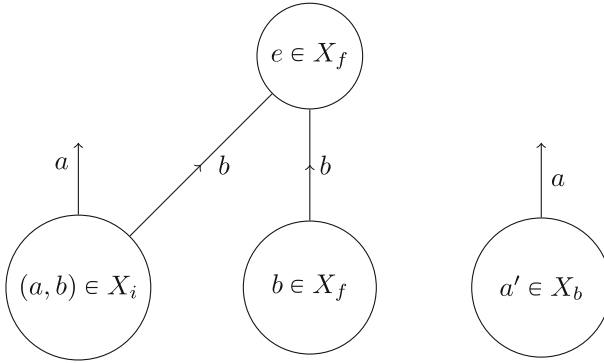
FIGURE 2. Points $(a,b) \in X_i$, $b \in X_f$, $a' \in X_b$

as described in Section 1 and visualised on the second part of Figure 1, but where at each point we also record information about the domain of outgoing labels. We begin by defining the base X.

Definition 2.4. Let $\mathcal{S}$ be a $(\leq, \circ)$-structure. Consider the base set

$$X = X_i \,\dot\cup\, X_f \,\dot\cup\, X_b$$

where $\dot\cup$ denotes disjoint union and

$$X_i = \{(a,b) : a, b \in \mathcal{S}, \ a \blacktriangleleft b\}$$
$$X_f = \{b : b \in \mathcal{S}\}$$
$$X_b = \{a' : a \in \mathcal{S}\}.$$

We may use a prime symbol $'$ for points in X_b in order to distinguish them from points in X_f. For $x = (a,b) \in X_i$ let $\lambda(x) = b$, $\delta(x) = a$, for $b \in X_f$ let $\lambda(b) = \delta(b) = b$, and for $a' \in X_b$ let $\lambda(a')$ be undefined and $\delta(a') = a$.

We refer to the points in X_i, X_f, X_b as *initial points*, *follow points* and *branch points*, respectively. For $x \in X$ we may refer to $\delta(x)$ as the *domain* of x and for $x \in X_i \cup X_f$, $\lambda(x)$ is the *label* of x. Suppose $\mathcal{S}$ contains a left and right identity e for $\circ$. In Definition 2.5 below, we will define a representation where for $x \in X_i \cup X_f$, $\lambda(x)$ will label the edge from x to the fixed point $e \in X_f$, and for $x \in X$, $\delta(x)$ will be a tight lower $\blacktriangleleft$-bound for the label of any outgoing edge from x. Note that the label of a follow point equals the domain of that point, the label of a branch point is undefined. An example of an initial, follow and a branch point is visualised in Figure 2.

Definition 2.5. For each $a \in \mathcal{S}$ define a binary relation $a^\theta \subseteq X \times X$ by letting $(x, y) \in a^\theta$ if and only if

(1) $y \notin X_i$,
(2) $x \in X_b \Rightarrow y \in X_b$,
(3) $\delta(x) \blacktriangleleft a \circ \delta(y)$ and
(4) $x \in X_i \,\dot\cup\, X_f, \ y \in X_f \Rightarrow \lambda(x) \vartriangleleft^{\delta(x)} a \circ \lambda(y)$.
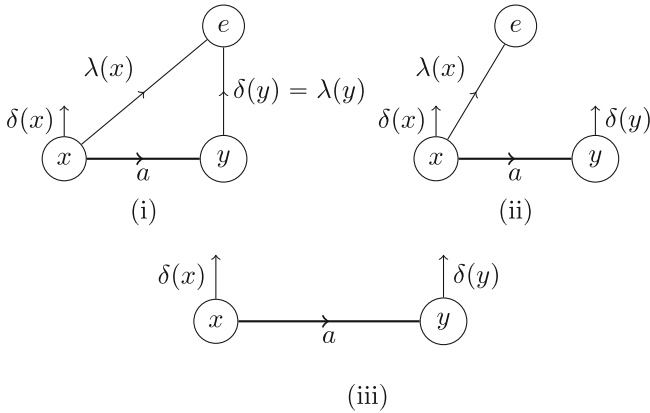
FIGURE 3. $(x, y) \in a^\theta$ with (i) $x \in X_i \overset{\bullet}{\cup} X_f$ and $y \in X_f$, (ii) $x \in X_i \overset{\bullet}{\cup} X_f$ and $y \in X_b$, and (iii) $x \in X_b$, $y \in X_b$. It is required in each case that $\delta(x) \blacktriangleleft a \circ \delta(y)$, and in case (i) additionally that $\lambda(x) \vartriangleleft^{\delta(x)} a \circ \lambda(y)$. In (i) and (ii) if $x \in X_f$ then the $\delta(x)$ and $\lambda(x)$ arrows coincide, see Definitions 2.4, 2.5.

We visualise θ in Figure 3.

Lemma 2.6. *Let $\mathcal{S} = (S, \leq, \circ)$ be a structure where $\circ$ is associative, $\leq$ is a partial order, $\mathcal{S} \models \sigma$ and suppose there is an identity $e \in \mathcal{S}$. Let θ be from Definition 2.5. Then $a \leq b \in \mathcal{S}$ if and only if $a^\theta \sqsubseteq b^\theta$.*

Proof. Assume $a \nleq b$, so either $\neg b \blacktriangleleft a$ or $\neg a \vartriangleleft^b b$, by σ. In the former case, consider $b' \in X_b$, and recall that $\delta(b') = b$. Then $b' \in \text{dom}(b^\theta)$ (since $(b', e') \in b^\theta$) but $b' \notin \text{dom}(a^\theta)$ (since $\neg b \blacktriangleleft a$). Otherwise $b \blacktriangleleft a$ and $\neg a \vartriangleleft^b b$, but then define $x = (b, a) \in X_i$ and observe that (x, e) is in a^θ but not in b^θ, yet $x \in \text{dom}(b^\theta)$ (since $(x, e') \in b^\theta$). Either way, $a^\theta \nsqsubseteq b^\theta$.

Now suppose $a \leq b$. First we check that $\text{dom}(b^\theta) \subseteq \text{dom}(a^\theta)$. If $x \in \text{dom}(b^\theta)$ there is $y \in X$ where $(x, y) \in b^\theta$. It follows that $\delta(x) \blacktriangleleft b \blacktriangleleft a$, so $(x, e') \in a^\theta$ and $x \in \text{dom}(a^\theta)$. Secondly, if $x \in \text{dom}(b^\theta)$ (so $\delta(x) \blacktriangleleft b$) and $(x, y) \in a^\theta$ we know that (3)–(4) hold for a, in particular $\delta(x) \blacktriangleleft a \circ \delta(y)$. It follows that $\delta(x) \blacktriangleleft b \circ \delta(y)$, by Lemma 2.1(4), as required by (3). Conditions (1),(2) remain true for b^θ. For (4) if $x \in X_f$ then $\lambda(x) \vartriangleleft^{\delta(x)} a \circ \lambda(y) \vartriangleleft^{\delta(x)} b \circ \lambda(y)$, by Lemma 2.1(3). Hence $(x, y) \in b^\theta$, thus $a^\theta \sqsubseteq b^\theta$. $\square$

Lemma 2.7. *Let $\mathcal{S} = (S, \leq, \circ)$ be a structure where $\circ$ is associative, $\leq$ is a partial order, $\mathcal{S} \models \sigma$ and let θ be from from Definition 2.5. For any $a, b \in \mathcal{S}$, we have $(a \circ b)^\theta = a^\theta; b^\theta$.*

Proof. First, let's show that $a^\theta; b^\theta \subseteq (a \circ b)^\theta$. Take any $(x, y) \in a^\theta$ and $(y, z) \in b^\theta$. We have $\delta(x) \blacktriangleleft a \circ \delta(y)$ and $\delta(y) \blacktriangleleft b \circ \delta(z)$, so $\delta(x) \blacktriangleleft a \circ b \circ \delta(z)$, by Lemma 2.1(4). If $x \in X_i \cup X_f$ then $y, z \in X_f$, by (1), (2), so $\lambda(y) = \delta(y)$,

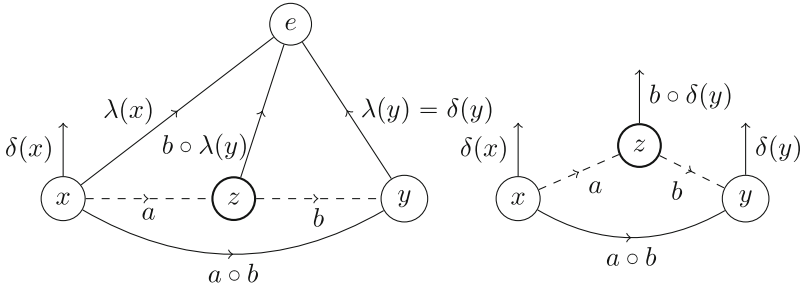FIGURE 4. Witness z for $(x,y) \in (a \circ b)^\theta$ where $x \in X_i \overset{\bullet}{\cup} X_f$ and $y \in X_f$ (left), $x \in X$, $y \in X_b$ (right).

$\lambda(x) \vartriangleleft^{\delta(x)} a \circ \lambda(y)$, $\lambda(y) \vartriangleleft^{\lambda(y)} b \circ \lambda(z)$, and then $\lambda(x) \vartriangleleft^{\delta(x)} a \circ b \circ \lambda(z)$, by Lemma 2.1(3). Hence $(x,z) \in (a \circ b)^\theta$.

Conversely, to show that $(a \circ b)^\theta \subseteq a^\theta ; b^\theta$, take any $(x,y) \in (a \circ b)^\theta$. By (1) $y \notin X_i$. If $y \in X_b$ let $z = (b \circ \delta(y))' \in X_b$ (Figure 4 right), otherwise $y \in X_f$ and we let $z = (b \circ \lambda(y)) \in X_f$ (Figure 4 left). In each case $\delta(z) = b \circ \delta(y)$, in the latter case $\lambda(z) = (b \circ \lambda(y))$, so $(x,z) \in a^\theta$, $(z,y) \in b^\theta$, as required.   □

Theorem 2.8. $R(\sqsubseteq, ;)$ *is axiomatised by partial order, associativity and* $\{\sigma_n : n < \omega\}$. *Finite structures* $\mathcal{S} \in R(\sqsubseteq, ;)$ *are representable over a finite base* X *with* $|X| \leq (1 + |\mathcal{S}|)^2 + 2 \cdot (1 + |\mathcal{S}|)$.

Proof. Soundness of partial order, associativity is clear, soundness of σ_n is from Lemma 2.3. For completeness, take any associative, partially ordered $(\leq, \circ)$-structure $\mathcal{S} \models \{\sigma_n : n < \omega\}$. We may define $\mathcal{S}'$ be adding a new identity e to $\mathcal{S}$ unordered with other elements. By Lemmas 2.6 and 2.7 , the map θ of Definition 2.5 is a $(\sqsubseteq, ;)$-representation of $\mathcal{S}'$, hence it restricts to a $(\sqsubseteq, ;)$-representation of $\mathcal{S}$. The representation θ has base contained in a disjoint union of a copy of $(\mathcal{S}')^2$ and two copies of $\mathcal{S}'$ and thus contains at most $(1 + |\mathcal{S}|)^2 + 2 \cdot (1 + |\mathcal{S}|)$ elements.   □

3. $R(\sqsubseteq, ;)$ is not finitely axiomatisable

Definition 3.1. Let $n < \omega$, $N = 1 + 2^n$ and let $\mathcal{S}_n$ be a $(\leq, \circ)$-structure whose underlying set S_n has $3 + 3N$ elements

$$S_n = \{0, b, c\} \cup \{a_i, a_i b, a_i c : i < N\}$$

where composition $\circ$ is defined by $a_i \circ b = a_i b$, $a_i \circ c = a_i c$ (all $i < N$) and all other compositions result in 0, and the refinement operation $\leq$ is defined as the reflexive closure of

$$\{(s, 0) : s \in S_n\} \cup \{(a_{i+1} b, a_i), (a_i, a_{i+1} c), (a_i b, a_i c) : i < N\}$$

where here and below the operator $+$ denotes addition modulo N.

Observe that $\circ$ is associative and $\leq$ is a partial order.

Lemma 3.2. *For $n \geq 2$, $\mathcal{S}_n$ is not representable, but $\mathcal{S}_n \models \sigma_k$ for $k < n$.*

Proof. Since $s \leq 0$ we have $0 \blacktriangleleft_0 s$. Also, for $i < N$, since $a_{i+1} \circ b \leq a_i$ we have $a_i \blacktriangleleft_0 a_{i+1}b \blacktriangleleft_0 a_{i+1}$, $a_i \blacktriangleleft_0 a_{i+1}$, so $a_i \blacktriangleleft_k a_{i+2^k}$ for $k \geq 1$, using Lemma 2.1((2)). Hence $\{a_i, a_ib : i < N\}$ is a clique of $\blacktriangleleft_n$, but for $k < n$ we do not have $a_{i+1} \blacktriangleleft_k a_i$ nor do we have $a_{i+1}c \blacktriangleleft_k a_ib$.

For $\triangleleft$, we have

- $t \triangleleft_0^s u$ iff $t \leq u$ and $s = u$, i.e. $s \triangleleft_0^s s$, $s \triangleleft_0^0 0$ (all s), $a_{i+1}b \triangleleft_0^{a_i} a_i$, $a_i \triangleleft_0^{a_{i+1}c} a_{i+1}c$ and $a_ib \triangleleft_0^{a_ic} a_ic$ (all $i < N$), but $\triangleleft_0$ holds in no other cases.
- Since $a_{i+1}b \circ c = 0$ and $a_{i+1}b \triangleleft_0^{a_i} a_i$, it follows by Lemma 2.1((3)) that $0 \triangleleft_1^{a_i} a_ic$, similarly $0 \triangleleft_1^{a_i} a_ib$. Also by Lemma 2.1((3)), since $a_i \triangleleft_0^{a_{i+1}c} a_{i+1}c$ and $a_{i+1}c \circ b = 0$ we get $a_ib \triangleleft_1^{a_{i+1}c} 0$, similarly $a_ic \triangleleft_1^{a_{i+1}c} 0$. And from $a_i \triangleleft_0^{a_i} a_i$ and $c \triangleleft_0^c c$ we get $a_ic \triangleleft_1^{a_i} a_ic$, similarly $a_ib \triangleleft_1^{a_i} a_ib$. The only non-zero products are $a_i \circ b$ and $a_i \circ c$, so the only remaining case of $\triangleleft_1$ we obtain from Lemma 2.1((3)) is $0 \triangleleft_1^s 0$, which follows since $s \triangleleft_0^s s$, for all $s \in \mathcal{S}_n$ and $0 \triangleleft_0^0 0$. By Lemma 2.1((5)), from $a_{i+1}b \triangleleft_0^{a_i} a_i$ we get $a_{i+1}b \triangleleft_1^s a_i$ for $s \blacktriangleleft_0 a_i$. This concludes the exhaustive enumeration of elements in $\triangleleft_1$, not covered by $\triangleleft_0$.
- If $a \triangleleft_1^s b$ and $s' \blacktriangleleft_1 s$ we get $a \triangleleft_2^{s'} b$, in particular $0 \triangleleft_2^{a_ic} a_ic$.
- Since $a_ib \triangleleft_1^{a_{i+1}c} 0 \triangleleft_2^{a_{i+1}c} a_{i+1}c$, it follows by Lemma 2.1((2)) that

$$a_ib \triangleleft_3^{a_{i+1}c} a_{i+1}c.$$

- The remaining cases of $\triangleleft$ can be enumerated as follows. We have $0 \triangleleft^s a_{i+1}c$, $0 \triangleleft^s a_{i+1}b$, $a_ic \triangleleft^s a_ic$ for $s \blacktriangleleft a_0$, by Lemma 2.1((4)). Additionally, since $a_{i+1}b \triangleleft^s a_i$, we get $0 \triangleleft^s a_i$, by Lemma 2.1((2)). Also by Lemma 2.1((2)), for any $s \in \mathcal{S}_n$ since $s \triangleleft^0 0$ and $0 \triangleleft^0 a_ib$, $0 \triangleleft^0 a_ic$, $0 \triangleleft^0 a_i$, we have $s \triangleleft^0 a_ib$, $s \triangleleft^0 a_ic$, $s \triangleleft^0 a_i$, and if $a \in \{a_ib, a_ic : i < N\}$, and $b \in \{a_i, a_ib, a_ic : i < N\}$ we have $a \triangleleft^{a_{i+1}c} b$.

This covers all triples (a, s, b) where $a \triangleleft^s b$. It follows that $\mathcal{S}_n \not\models \sigma_{n+1}$ for $n \geq 2$, since $a_{i+1}c \blacktriangleleft_1 a_{i+1} \blacktriangleleft_n a_ib$, $a_ib \triangleleft_3^{a_{i+1}c} a_{i+1}c$ but $\mathcal{S}_n \not\models a_ib \leq a_{i+1}c$. By Theorem 2.8, $\mathcal{S}_n$ is not representable. The only cases where $a \triangleleft^b b$ and $a \not\leq b$ are $a_ib \triangleleft^{a_{i+1}c} a_{i+1}c$, but for $k < n$ we do not have $a_{i+1}c \blacktriangleleft_k a_ib$, hence $\mathcal{S}_n \models \sigma_k$. $\square$

Theorem 3.3. $R(\sqsubseteq, ;)$ *cannot be defined by finitely many axioms.*

Proof. Each structure $\mathcal{S}_n \notin R(\sqsubseteq, ;)$. For any $k < \omega$ almost all $\mathcal{S}_n$ satisfy σ_k (in fact, all $\mathcal{S}_n$ where $n > k$) and they are all associative and partially ordered, hence any non-principal ultraproduct $\mathcal{S} = \Pi_U \mathcal{S}_n$ is associative, partially ordered and satisfies all σ_ks, so by Theorem 2.8, $\mathcal{S} \in R(\sqsubseteq, ;)$. By Łoś' theorem, $R(\sqsubseteq, ;)$ has no finite axiomatisation. $\square$

4. Finite axiomatisability and representability

For any relation algebra signature Σ, the representation class $R(\Sigma)$ may be finitely axiomatisable or not, and it may be that finite representable structures have finite representations or not. All four combinations of these two properties are possible.

Theorem 4.1. *The representation class $R(\Sigma)$ is finitely axiomatisable, and finite structures in $R(\Sigma)$ have finite representations, according to the following incomplete table.*

	fin. ax.	not fin. ax.
fin. rep	$(\subseteq, D, R, {}^{\smile}, ;)$	$(\sqsubseteq, ;)$
	$(\subseteq, ;), (\sqsubseteq, *)$	
not fin. rep.	$(\cap, ;)$	$(\cap, \cup, ;) \subseteq \Sigma$
		$(\subseteq, \backslash, ;) \subseteq \Sigma$

where $\Sigma' \subseteq \Sigma$ signifies the language characterised by Σ being an expansion of the language characterised by Σ'.

Proof. Finite axiomatisability of $R(\subseteq, D, R, {}^{\smile}, ;)$ is proved in [2] and the finite representation property for this signature is proved in [8]. Both $R(\subseteq, ;)$ and $R(\sqsubseteq, *)$ are defined by the axioms of ordered semigroups and have the finite representation property [15, 9].

The finite representation property is proved for $R(\sqsubseteq, ;)$ in Theorem 2.8, non-finite axiomatisability is proved in Theorem 3.3. The failure of the finite representation property for signatures containing $(\cap, ;)$ is proved in [13], finite axiomatisability of $R(\cap, ;)$ is proved in Proposition 4.2 below.

For the final quadrant of the diagram, if the representation problem for finite structures in $R(\Sigma)$ is undecidable, we know that there can be no finite axiomatisation, and since the set of formulas valid over $R(\Sigma)$ is recursively enumerable the finite representation property cannot hold. The representation problem for finite structures is proved undecidable for signatures containing $(\cap, \cup, ;)$ in [7] and for signatures containing $(\subseteq, -, ;)$, where negation is interpretted as complementation relative to a universal relation $X \times X$, in [12]. We extend that result to prove failure of the finite representation property for representations where $-$ denotes complementation relative to an arbitrary maximal binary relation in Proposition 4.3, below. $\qquad\square$

Proposition 4.2. $R(\cap, ;)$ *is finitely axiomatisable.*

Proof. A $(\cap, ;)$-representable $(\cdot, \circ)$-structure clearly satisfies the semilattice laws, associativity and monotonicity. Conversely, in a representation game played over an associative, monotonic semilattice $\mathcal{S}$, $\exists$ plays a sequence of networks — graphs N whose edges are labelled by upward closed subsets of $\mathcal{S}$, such that $N(x, y); N(y, z) \subseteq N(x, z)$ for all $x, y, z \in N$. [See Definition 7.7 of [6] for more details of a representation game for the full signature of relation algebra, and Chapter 9 for representation games in a more general setting.] In the initial round suppose $\forall$ picks $a \neq b$. By antisymmetry either $a \not\leq b$ or $b \not\leq a$, without loss assume the former. $\exists$ plays a network N_0 with two nodes labelled $N(x, y) = a^{\uparrow}$, all other edges have empty labels, note that $b \notin N(x, y)$. In a subsequent round let N be the current network and suppose $\forall$ picks nodes $x, y \in N$ and $a, b \in \mathcal{S}$ such that $a \circ b \in N(x, y)$, see Figure 5. $\exists$ adds a single new node z and lets $N'(w, z) = N(w, x); a^{\uparrow}$, $N'(z, w) = b^{\uparrow}; N(y, w)$ for all $w \in N$ to define N'. Edges within N are not refined. If $u, w \in N$ then
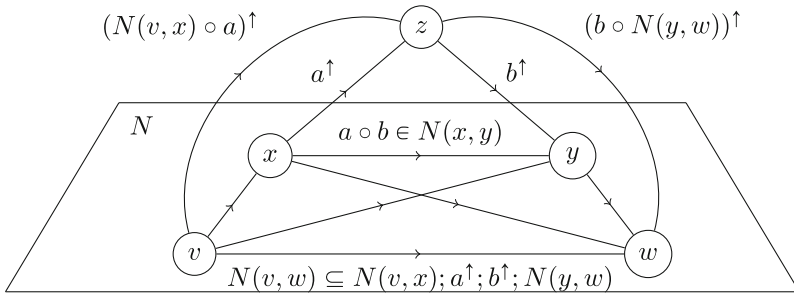
FIGURE 5. Node Addition in a Representation Game for $(\cdot, \circ)$

$N'(u, z); N'(z, w) = N(u, x); a^{\uparrow}; b^{\uparrow}; N(y, w) \subseteq N(u, x); N(x, y); N(y, w)$, since $a; b \in N(x, y)$, using associativity, left and right monotonicity. It is easily seen that N' is a consistent network, a legal response to $\forall$'s move not refining the initial edge. It follows that $\mathcal{S} \in R(\cap, ;)$ $\square$

Let $\mathcal{S}$ be a $(\leq, -, \circ)$-structure. A $(\subseteq, \backslash, ;)$-representation of $\mathcal{S}$ over base X is a map $\theta : \mathcal{S} \to \wp(X \times X)$ such that for all $a, b \in \mathcal{S}$,

- $a \leq b \to a^\theta \subseteq b^\theta$,
- $(x, y) \in a^\theta \to (x, y) \in \Delta(b^\theta, (-b)^\theta)$ (the symmetric difference of b^θ and $(-b)^\theta$),
- $(x, y) \in (a \circ b)^\theta \leftrightarrow \exists z((x, z) \in a^\theta \wedge (z, y) \in b^\theta)$.

According to this definition, $-$ is represented as $\backslash$, the complementation in the union of all the represented binary relations.

Proposition 4.3. *For any Relation Algebra (RA) reduct $(\subseteq, \backslash, ;) \subseteq \Sigma$, the representation class $R(\Sigma)$ fails to have the finite representation property for finite representable structures.*

Proof. The point algebra $\mathcal{P}$ is a relation algebra whose boolean part has three atoms e, l, g (so 8 elements, $0, e, l, g, -e, -l, -g, 1$), where e is the identity, the converse of l is g, composition for atoms is given by

$$
\begin{array}{c|ccc}
\circ & e & l & g \\
\hline
e & e & l & g \\
l & l & l & 1 \\
g & g & 1 & g
\end{array}
$$

and the operators extend to arbitrary elements by additivity. A representation of $\mathcal{P}$ over $\mathbb{Q}$ may be obtained by representing e, l, g as the identity $\{(q, q) : q \in \mathbb{Q}\}$, less than $\{(q, q') : q < q'\}$ and greater than, respectively. It follows that the reduct of $\mathcal{P}$ to $(\leq, -, \circ)$ is $(\subseteq, \backslash, ;)$-representable. We claim it has no finite $(\subseteq, \backslash, ;)$-representation.

Let θ be any $(\subseteq, \backslash, ;)$-representation of $\mathcal{P}$ over the base X.

Claim 1. If $(x, y) \in g^\theta$ then $x \neq y$. To prove the claim, suppose for contradiction that there is a point $x \in X$ with $(x, x) \in g^\theta$. As $g \leq -e$, $(x, x) \in$
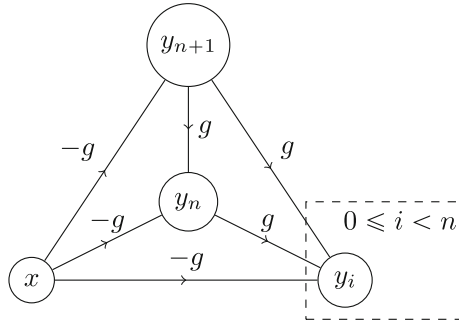
FIGURE 6. Induction showing a new node is needed for representation of P

$g^\theta \subseteq (-e)^\theta$. And since $g = g \circ e$, there exists a y s.t. $(x, y) \in g^\theta$, $(y, x) \in e^\theta$. Since $e \circ g = g$, we also have $(y, x) \in g^\theta$. But $e \leq -g$, so $(y, x) \in (-g)^\theta$. Since $(y, x) \in g^\theta$ we have reached a contradiction and proved claim 1.

Claim 2. For $n \geq 0$ there will exist an $x \in X$ and a set of distinct points $y_0, \ldots, y_n \in X$ such that for all $i \leq n$ we have $(x, y_i) \in (-g)^\theta$ and for all $i < j \leq n$ we have $(y_j, y_i) \in g^\theta$. See Figure 6. Claim 2 is proved by induction over n. For the base case, $n = 0$, since $(-g) \not\leq 0$ there are x, y_0 where $(x, y_0) \in (-g)^\theta$. Assume the hypothesis for some $n \geq 0$. Since $(x, y_n) \in (-g)^\theta$ and $(-g) \leq 1 = (-g) \circ g$, there must be $y_{n+1} \in X$ where $(x, y_{n+1}) \in (-g)^\theta$ and $(y_{n+1}, y_n) \in g^\theta$. Since $(y_n, y_i) \in g^\theta$ it follows that $(y_{n+1}, y_i) \in (g \circ g)^\theta = g^\theta$, for $i \leq n$. By the previous claim, y_{n+1} is distinct from y_i, for $i \leq n$, as required. This proves Claim 2.

Since X contains a set of n distinct points, for all $n < \omega$, it follows that X must be infinite. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

5. Demonic lattice and semilattice

We have seen in the introduction that demonic join $\sqcup$ is the join operation for demonic refinement $\sqsubseteq$. A demonic meet $\sqcap$, acting as a least upper bound of its two arguments, may not in general be defined, as there are binary relations having no common lower bound at all. If a point x is in the domain of two binary relations R, S, but not in the domain of $R \cap S$, then any lower bound of R, S would be below the intersection $R \cap S$, hence x would be outside its domain, yet in order to be a lower bound its domain should contain both the domain of R and the domain of S, a contradiction. This problem could solved be adding a single new point $\bot$ to the base X of the representation θ and letting $\theta'(R) = \theta(R) \cup \{(x, \bot) : x \in \mathrm{dom}(R)\}$ to obtain an alternative representation of the refinement algebra, with $\sqsubseteq$-least element $\{(x, \bot) : x \in X \cup \{\bot\}\}$. Over such a representation, a greatest lower bound may be defined by

$$R \sqcap S = \{(x, y) : (x, y) \in R, \ x \notin \mathrm{dom}(S)\}$$

$$\cup \, (R \cap S)$$
$$\cup \, \{(x, y) : (x, y) \in S, \ x \notin \operatorname{dom}(R)\}$$

Hence, every representable $(\sqsubseteq, ;)$-structure embeds into a representable $(\sqcap, \sqcup, ;)$-structure forming a distributive lattice with composition. We expect that additional properties are required to ensure that such a representation exists.

Problem 5.1. Is the class of representable semigroups with demonic semilattice $R(\sqcup, ;)$ finitely axiomatisable and are the finite structures in $R(\sqcup, ;)$ representable over finite bases?

Problem 5.2. Find axioms for the class of all $(\sqcup, \sqcap, ;)$-structures of binary relations with demonic join and meet under composition.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

[1] Berghammer, R., Zierer, H.: Relational algebraic semantics of deterministic and nondeterministic programs. Theor. Comput. Sci. **43**, 123–147 (1986)

[2] Bredikhin, D.: Abstract characteristic of some classes of algebras of relations. Algebra Theory Numbers **2**, 3–19 (1977). (**In Russian**)

[3] De Carufel, J., Desharnais, J.: Demonic algebra with domain, relations and Kleene algebra in computer science. Lect. Notes Comput. Sci. **4136**, 120–134 (2006)

[4] De Carufel, J.L., Desharnais, J.: On the structure of demonic refinement algebras with enabledness and termination. In: International conference on relational methods in computer science, pp. 69–83. Springer (2008)

[5] Dijkstra, E.W., Scholten, C.S.: Predicate Calculus and Program Semantics. Springer, Berlin, Heidelberg (1990)

[6] Hirsch, R., Hodkinson, I.: Relation Algebras by Games. Elsevier Science, Amsterdam (2002)

[7] Hirsch, R., Jackson, M.: Undecidability of representability as binary relations. J. Symbol. Logic **77**(4), 1211–1244 (2012)

[8] Hirsch, R., Mikulás, S.: Ordered domain algebras. J. Appl. Logic **11**(3), 266–271 (2013)

[9] Hirsch, R., Mikulas, S., Stokes, T.: The algebra of non-deterministic programs: demonic operations, order and axioms. arxiv:2009.12081 (2020)

[10] Kahl, W.: Relational semigroupoids: abstract relation-algebraic interfaces for finite relations between infinite types. J. Logic Algebr. Program. **76**(1), 60–89 (2008)

[11] Mili, A., Desharnais, J., Mili, F.: Relational heuristics for the design of deterministic programs. Acta Informatica **24**(3), 239–276 (1987)

[12] Neuzerling, M.: Undecidability of representability for lattice-ordered semigroups and ordered complemented semigroups. Algebra Univ. **76**, 431–443 (2016)

[13] Neuzerling, M.D.: Representability of finite algebras of relations. Ph.D. thesis, La Trobe University (2017)

[14] von Wright, J.: Towards a refinement algebra. Sci. Comput. Program. **51**(1–2), 23–45 (2004)

[15] Zareckiĭ, K.: The representation of ordered semigroups by binary relations. Izvestiya Vysšhikh. Uchebnykh. Zavedeniĭ. Matematika **6**(13), 48–50 (1959)

Robin Hirsch and Jaš Šemrl
Department of Computer science
University College London
London WC1E 6BT
UK
e-mail [R. Hirsch]: r.hirsch@ucl.ac.uk
URL: http://www.cs.ucl.ac.uk/staff/robin_hirsch/
e-mail [J. Šemrl]: j.semrl@cs.ucl.ac.uk
URL: http://www.cs.ucl.ac.uk/staff/j.semrl/