

Undecidable Varieties of Semilattice-ordered Semigroups, of Boolean Algebras with Operators, and logics extending Lambek Calculus

Á. KURUCZ, I. NÉMETI, I. SAIN AND A. SIMON, *Mathematical Institute of the Hungarian Academy of Sciences, Budapest, PO Box 127, H-1364, Hungary. E-mail: kurucz@rmk530.rmki.kfki.hu, {h1469nem,h1468sain}@ella.hu, andras@rmk530.rmki.kfki.hu*

Abstract

We prove that the equational theory of semigroups becomes undecidable if we add a semilattice structure with a 'touch of symmetric difference'. As a corollary we obtain that the variety of all Boolean algebras with an associative binary operator has a 'hereditarily' undecidable equational theory. Our results have implications in logic, e.g. they imply undecidability of modal logics extending the Lambek Calculus and undecidability of Arrow Logics with an associative arrow modality.

Below we prove that semilattice-ordered semigroups with a 'touch of symmetric difference' have a 'hereditarily' undecidable equational theory.

There were results and methods available showing that many discriminator varieties having an associative binary operation are undecidable. See e.g. Andréka-Givant-Németi [2] for a relatively large variety of such methods and references. For completeness we note that Tarski around 1950 and Maddux around 1977 already had such kinds of results.

One of the main aims of our method herein is to elaborate a *general method* which works for varieties which are very far from discriminator varieties. By 'very far' we mean that we do not use discriminator algebras at any point of our proof. E.g. one of the proofs in Kurucz-Németi-Sain-Gyuris [10] proves that a certain variety, say, V is undecidable by proving that for every algebra $A \in V$ one can define a new structure B (with both universe and operations different from those of A) being a subdirect product of discriminator algebras, then one can use the discriminator property of B . In contrast, the present proof method does not use discriminator algebras even in this indirect way.

THEOREM 0.1

Let K be a class of algebras such that the binary operations \vee , $*$, \circ and the constant 1 are term definable in K . Assume that conditions (1)–(5) below hold in K .

1. \vee is an upper semilattice (i.e. $x \leq y$ iff $x \vee y = y$) with greatest element 1

- 2(i) $(x * y) * (x * y) \leq x * y$
- (ii) $y * y \leq x \implies x * x \leq y * y$.
- (iii) $x \leq (x * y) \vee y$
- 3. \circ distributes over \vee
- 4. \circ is associative
- 5. For infinitely many nonisomorphic monadic-generated¹ simple Relation Algebras \mathcal{A} , the $\{0, \vee, \circ\}$ -reduct of \mathcal{A} is a subreduct of some element of \mathbf{K} and $\mathcal{A} \models x * x = 0$.

Then the equational theory of \mathbf{K} is undecidable.

PROOF. Fix a unary term $c(x)$ of type t . Let Qeq denote the set of all quasiequations in the language of semigroups (using \circ for the semigroup operation). For any $q \in Qeq$ of form

$$[(\tau_1 = \sigma_1) \wedge \dots \wedge (\tau_n = \sigma_n)] \rightarrow (\tau_0 = \sigma_0)$$

an equation $e_c(q)$ of type t is defined as follows.

$$e_c(q) \stackrel{\text{def}}{=} [(\tau_0 \vee c(\tau)) * (\sigma_0 \vee c(\tau))] \vee [(\sigma_0 \vee c(\tau)) * (\tau_0 \vee c(\tau))] \leq c(\tau),$$

where $\tau \stackrel{\text{def}}{=} (\tau_1 * \sigma_1) \vee (\sigma_1 * \tau_1) \vee \dots \vee (\tau_n * \sigma_n) \vee (\sigma_n * \tau_n)$. ■

Let \mathbf{SG} denote the class of all semigroups.

LEMMA 0.2

If

- (a) c is increasing, i.e. $\mathbf{K} \models x \leq c(x)$;
- (b) 'dual'-relativizing with $c(x)$ is a \circ -homomorphism for every x , i.e.

$$\mathbf{K} \models (y \circ z) \vee c(x) = [(y \vee c(x)) \circ (z \vee c(x))] \vee c(x)$$

then for any $q \in Qeq$

$$\mathbf{SG} \models q \implies \mathbf{K} \models e_c(q).$$

To prove Lemma 0.2 we need Claims 0.3 and 0.4 below.

CLAIM 0.3

For any algebra $\mathcal{A} \in \mathbf{K}$, $\bar{a} \in {}^\omega A$

$$\mathcal{A} \not\models e_c(q)[\bar{a}] \implies (\tau_0 \vee c(\tau))[\bar{a}] \neq (\sigma_0 \vee c(\tau))[\bar{a}].$$

PROOF. For every k ($k = 1, \dots, n$)

$$((\tau_k * \sigma_k) * (\tau_k * \sigma_k))[\bar{a}] \stackrel{(2)(i)}{\leq} (\tau_k * \sigma_k)[\bar{a}] \stackrel{(1)}{\leq} \tau[\bar{a}] \stackrel{(a)}{\leq} c(\tau)[\bar{a}] \stackrel{(1)}{\leq} (\tau_0 \vee c(\tau))[\bar{a}].$$

Assume that $((\tau_0 \vee c(\tau))[\bar{a}] = (\sigma_0 \vee c(\tau))[\bar{a}])$ holds. Then by (2)(ii)

$$[(\tau_0 \vee c(\tau)) * (\sigma_0 \vee c(\tau))][\bar{a}] \leq ((\tau_k * \sigma_k) * (\tau_k * \sigma_k))[\bar{a}] \stackrel{(2)(i)}{\leq} (\tau_k * \sigma_k)[\bar{a}] \stackrel{(1)}{\leq} \tau[\bar{a}] \stackrel{(a)}{\leq} c(\tau)[\bar{a}].$$

Similarly, $[(\sigma_0 \vee c(\tau)) * (\tau_0 \vee c(\tau))][\bar{a}] \leq c(\tau)[\bar{a}]$ also holds, contradicting $\mathcal{A} \not\models e_c(q)[\bar{a}]$. ■

¹A Relation Algebra is monadic-generated iff it is generated by a set of elements x satisfying $x \circ 1 = x$.

CLAIM 0.4

For every k ($k = 1, \dots, n$),

$$\mathbf{K} \models (\tau_k \vee c(\tau) = \sigma_k \vee c(\tau)).$$

PROOF.

$$\mathbf{K} \models \tau_k \vee c(\tau) \stackrel{(a)}{=} \tau_k \vee \tau \vee c(\tau) \stackrel{(1)}{\geq} \tau_k \vee (\sigma_k * \tau_k) \vee c(\tau) \stackrel{(2)(iii)}{\geq} \sigma_k \vee c(\tau).$$

The other direction can be proved similarly, thus the proof of Claim 0.4 is completed. ■

PROOF. [of Lemma 0.2] Assume $\mathbf{K} \not\models e_c(q)$ that is, there is some $\mathcal{A} \in \mathbf{K}$ and $\bar{a} \in {}^\omega \mathcal{A}$ such that $\mathcal{A} \not\models e_c(q)[\bar{a}]$. Let $B \stackrel{\text{def}}{=} \langle B, \circ^B \rangle$ be the following algebra:

$$\begin{aligned} B &\stackrel{\text{def}}{=} \{x \vee c(\tau)(\bar{a}) : x \in \mathcal{A}\} \\ x \circ^B y &\stackrel{\text{def}}{=} (x \circ^{\mathcal{A}} y) \vee c(\tau)(\bar{a}), \quad \text{for any } x, y \in B. \end{aligned}$$

Then, by (b), B is a semigroup. Also by (b) and by Claims 0.3 and 0.4 above,

$$B \models (\tau_0 \neq \sigma_0)[\bar{a}'] \quad \text{and} \quad B \models (\tau_k = \sigma_k)[\bar{a}'] \quad (k = 1, \dots, n),$$

where $\bar{a}' \stackrel{\text{def}}{=} \langle \dots, a_j \vee c(\tau)(\bar{a}), \dots \rangle_{j \in \omega}$. Thus $B \not\models q[\bar{a}']$, i.e. $\mathbf{SG} \not\models q$. ■

Now let **FSG** denote the class of all finite semigroups.

LEMMA 0.5

If

(c) c is normal² in the special relation algebras occurring in condition (5)

then for any $q \in Qeq$

$$\mathbf{K} \models e_c(q) \implies \mathbf{FSG} \models q.$$

PROOF. Assume $\mathbf{FSG} \not\models q$. Then there is a finite semigroup \mathcal{G} in which q does not hold. Then condition (5) of the Theorem ensures³ that there is some $\mathcal{A} \in \mathbf{K}$ such that the Cayley-representation⁴ of \mathcal{G} can be embedded into the 'o'-reduct of \mathcal{A} , thus $\mathcal{A} \not\models q$. Again by (5), $x *^{\mathcal{A}} x$ is the empty set for any $x \in \mathcal{A}$. Thus by (c) $c(\tau) = \emptyset$ that is, the right hand side of $e_c(q)$ is equal to \emptyset . But the left hand side is not, since for any $x, y \in \mathcal{A}$ if $(x * y) \vee (y * x) = \emptyset$ then

$$x \stackrel{(2)(iii)}{\leq} (x * y) \vee y \stackrel{(1)}{\leq} (x * y) \vee (y * x) \vee y = y,$$

and similarly, $y \leq x$. Thus $\mathcal{A} \not\models e_c(q)$ that is, $\mathbf{K} \not\models e_c(q)$. ■

LEMMA 0.6

Let \mathbf{Q} be a quasivariety of semigroups. Assume $\mathbf{FSG} \subseteq \mathbf{Q}$. Then the set $Qeq(\mathbf{Q})$ of quasiequations valid in \mathbf{Q} is undecidable⁵.

² c is normal in an algebra \mathcal{A} iff $\mathcal{A} \models c(0) = 0$.

³Cf. Andr  ka-Givant-N  meti [2] and N  meti [11] for detail.

⁴For any semigroup \mathcal{G} , the Cayley representation of \mathcal{G} is a semigroup whose elements are functions and the semigroup operation is the composition of functions.

⁵We do not need to assume that the whole of **FSG** is in \mathbf{Q} , but the present form is simpler to state.

PROOF. This lemma is essentially known, therefore we include here only an outline of the proof⁶. The full proof is included e.g. in the long, tutorial version of the present paper, also in Andr  ka-Givant-N  meti [2], and in the long, tutorial version of N  meti [11]; from the latter we recall below all that seem important.

Outline of the proof By a *Turing machine-input (TM-input) pair* we understand a pair $\langle T, b \rangle$ where T is a Turing machine and b is a possible input for T .

A pair $\langle T, b \rangle$ is called *bounded* if the execution of $\langle T, b \rangle$ involves only finitely many configurations of T . (If $\langle T, b \rangle$ terminates then it is obviously bounded.) ■

CLAIM 0.7

Among the bounded TM-input pairs the terminating and nonterminating ones are recursively inseparable. In other words, there is no decidable set H of TM-input pairs such that

$$(\text{for all bounded } \langle T, b \rangle) [\langle T, b \rangle \in H \iff \langle T, b \rangle \text{ terminates}].$$

Note that H above was *not* restricted to contain only bounded pairs.

PROOF. The proof is exactly the same as that of undecidability of the Halting Problem. (The only extra consists in noticing that the Turing machine constructed by diagonalization is bounded for every possible input.) ■

Next, exactly as in the Handbook of Math. Logic [3], to every TM-input pair $\langle T, b \rangle$ we associate a quasiequation $q_{T,b}$ in the language of semigroups. This is a standard construction, and it is also standard to show that

$$SG \models q_{T,b} \iff \langle T, b \rangle \text{ terminates,}$$

cf. e.g. op. cit.

Next we consider the standard proof of $(\langle T, b \rangle \text{ diverges} \implies SG \not\models q_{T,b})$. There, from the divergent pair $\langle T, b \rangle$, one constructs a semigroup S in which $q_{T,b}$ fails (for some evaluation of the variables).

The next step is to observe that if $\langle T, b \rangle$ is *bounded* then we can make S finite. This is done in the following way. The standard construction of S is as a quotient of a free semigroup G^* generated by a finite G . The elements of G^* code the possible configurations of the Turing machine T . But if $\langle T, b \rangle$ is bounded, then we need only finitely many configurations. Hence we need only a finite part $P \subseteq G^*$ of G^* . Let $m \in \omega$ be large enough such that all words in P are shorter than m . Let $\sim \subseteq G^* \times G^*$ be defined by

$$(\forall w, u \in G^*) [w \sim u \stackrel{\text{def}}{\iff} (w = u \text{ or } (|w| > m \text{ and } |u| > m))].$$

Then instead of G^* we can use G^* / \sim since all what is relevant to the execution of $\langle T, b \rangle$ is inside P which is isomorphically represented in G^* / \sim . Therefore if in the construction of S we replace G^* with G^* / \sim , we will obtain a (perhaps new) version S_1 of S , which still has the property $S_1 \not\models q_{T,b}$.

⁶This outline is detailed enough such that using the Handbook of Math. Logic [3] the interested reader can fill in the gaps. In this outline we explain how to modify the standard proof of undecidability of $Qeq(SG)$ e.g. in the above quoted handbook, to obtain the present Lemma 0.6.

Since $G * / \sim$ is finite, so is S_1 . This proves that, for any bounded $\langle T, b \rangle$,

$$\langle T, b \rangle \text{ diverges} \implies \text{FSG} \not\models q_{T,b}.$$

Assume now, $\text{FSG} \subseteq Q \subseteq \text{SG}$. Then by the above,

$$(\text{for all bounded } \langle T, b \rangle) [\langle T, b \rangle \text{ terminates} \iff Q \models q_{T,b}].$$

Therefore if $\text{Qeq}(Q)$ were decidable then the set

$$H \stackrel{\text{def}}{=} \{\langle T, b \rangle : Q \models q_{T,b}\}$$

would be decidable too. But this would contradict our Claim 0.7. Thus $\text{Qeq}(Q)$ is undecidable, as was desired.

Now it is left to show a unary term $c(x)$ of type t with properties (a)–(c) of Lemmas 0.2 and 0.5 above. Let

$$c(x) \stackrel{\text{def}}{=} x \vee (1 \circ x) \vee (x \circ 1) \vee (1 \circ x \circ 1).$$

Then (a) and (c) obviously hold for c .

To prove (b) it is enough to show that $1 \circ c(x) \leq c(x)$ and $c(x) \circ 1 \leq c(x)$, which, by conditions (3) and (4), obviously hold for the term c above.

Now, since the function c above is clearly recursive, Lemmas 0.2–0.6 above imply that the equational theory of \mathbf{K} is undecidable, completing the proof of Theorem 0.1. ■

REMARK 0.8

The operation $*$ is really only a ‘touch’ of symmetric difference in \mathbf{K} . Even $x * x$ is far from being 0-like. Indeed, let $A \in \mathbf{K}$ be arbitrary and let

$$\begin{aligned} H &\stackrel{\text{def}}{=} \{x \in A : x = y * z \text{ for some } y, z \in A\} \\ \text{At}(H) &\stackrel{\text{def}}{=} \{(x * x) * (x * x) : x \in A\} = \{(x * x) * (x * x) : x \in H\}. \end{aligned}$$

Then H is ‘atomic’, i.e. below each element of H there is an element of $\text{At}(H)$. This set $\text{At}(H)$ of ‘atoms’ can be almost anything, it can form an arbitrarily large antichain, or there can be a lot of elements below $\text{At}(H)$ (but not members of H). ■

COROLLARY 0.9

- (i) The equational theory of the variety \mathbf{BAO}° of all Boolean Algebras with an associative binary operator (which distributes over \vee) is undecidable.
- (ii) \mathbf{BAO}° is ‘hereditarily’ undecidable in the sense that any $\mathbf{K} \subseteq \mathbf{BAO}^\circ$ satisfying condition (5) of Thm 0.1 is undecidable.
- (iii) The equational theories of Residuated Boolean Monoids (RM) and of Euclidean Residuated Boolean Monoids (ERM) (as defined in Birkhoff [5] §XIV.5, Jipsen [8], Jónsson–Tsinakis [9]) are undecidable.
- (iv) The equational theory of the variety of dual Brouwerian semilattices with an associative binary operator ‘ \circ ’ is ‘hereditarily’ undecidable (in the sense of (ii) above).⁷

⁷ Cf. e.g. Pigozzi [12] for dual Brouwerian semilattices with operators.

PROOF. We prove only (i), the others are similar.

Take $*$ to be the real symmetric difference. Condition (5) is satisfied, because now the $\{0, \vee, \circ\}$ -reduct of any full representable Relation Algebra is a subreduct of some algebra in \mathbf{K} . ■

REMARK 0.10

We note that the methods of Andr  ka-Givant-N  meti [2] and Simon-Kurucz [14] yield that the varieties Commutative ERM, Integral ERM, Symmetric ERM and AERM (cf. Jipsen [8]) have hereditarily undecidable equational theories. For detail see Simon-Sain-N  meti [15], where the methods and results are extended to residuated Boolean Algebras with Operators (EUR's in the notation of Jipsen [8]).

Note that the dual version of Theorem 0.1 above also holds.

COROLLARY 0.11

The equational theory of the variety of all Heyting Algebras with an associative binary operator (which distributes over \wedge) is undecidable.

Before formulating the corollaries in logic we recall some conventions from the logic literature (cf. e.g. Venema [16]).

In the literature of multi-modal logics by a (\Diamond -type) *modality* we understand an n -ary logical connective, say, $\Diamond_i(\varphi_1, \dots, \varphi_n)$ such that \Diamond_i distributes over ' \vee ' in each of its arguments. In the same multi-modal logic there may be several such connectives, like $\Diamond_0, \dots, \Diamond_k$. There is no other restriction on what we recall a multi-modal logic (except that the Boolean connectives are assumed to be available). A modality is either \Diamond -type or \Box -type. The \Box -type differs from the \Diamond -type only in that it distributes over ' \wedge ' instead of ' \vee '.

COROLLARY 0.12 (Corollaries in logic)

- (i) Any multi-modal logic extending (conservatively) the Lambek Calculus is undecidable.
- (ii) Any Arrow Logic (cf. e.g. van Benthem [4], Venema [16]) with an associative arrow modality is undecidable.
- (iii) Let L be any multi-modal logic with an associative binary \Diamond -type modality \circ (and with other arbitrarily 'strange' connectives). Let $Th_L(\circ)$ denote those theorems of L which involve only \circ and Boolean connectives. If for every $n < \omega$ there is some set U with $|U| \geq n$ such that $Th_L(\circ)$ is valid in the full relational Kripke frame $U \times U$ then the logic L is undecidable.
- (iv) Any multi-modal intuitionistic logic with an associative binary \Box -type modality is 'hereditarily' undecidable (in a sense similar to item (iv) above).

As contrast we mention the following theorems.

THEOREM 0.13

The equational theory of the variety of all Boolean Algebras with an associative binary operator (which does not necessarily distribute over \vee) is decidable.

PROOF. It can be found in Gyuris [6]. ■

THEOREM 0.14

The equational theory of the variety of all distributive lattices with an associative binary operator (which does distribute over \vee) is decidable.

PROOF. It can be found in Andr  ka [1]. ■

Applications to Pratt's algebras and logics

In §3 of Pratt [13] Pratt lists as 'work needed' the problem of settling the decidability properties of the equational theories of the classes of algebras he discussed in that paper.

Below, we settle some of these questions: The classes we will mention below are collected on the figure at the beginning of §2 in Pratt's paper.

The variety **ISR** of idempotent semirings is decidable. (This follows from results in Andr  ka [1].)

It looks likely that the methods of Andr  ka [1] can be extended to decide **SLM** too but we did not check this.

It would be good to know if instead of residuated monoids **RES** we studied its more mundane version obtained the following way. Add to **ISR** the operation of classical equivalence ' \leftrightarrow '. Here, $(x \leftrightarrow y) = -(\neg x \oplus \neg y)$, where \oplus is Boolean symmetric difference. Let **ISR** $^{\sim}$ denote this variety. Is the equational theory of **ISR** $^{\sim}$ decidable?

Let us return to answering questions from Pratt [13] instead of generating new ones. The variety **BSR** of Boolean semirings is hereditarily undecidable, e.g. by our Thm. 0.1. Therefore for any class **K** such that $\mathbf{K} \subseteq \mathbf{BSR}$ or for some reduct $Rd(\mathbf{K})$ of **K**, $Rd(\mathbf{K}) \subseteq \mathbf{BSR}$, whenever **K** satisfies Condition (5) of Thm. 0.1, then the equational theory of **K** is undecidable. Therefore all the classes **BSRT**, **RBM**, etc. below **BSR** on the figure in Pratt [13] are undecidable. Moreover, all the classes in Pratt [13] which strengthen **BSR** either by new axioms or by new operations are undecidable. (Also the equational theory of **LL** is undecidable, but we think this was known.)

With the above (together with classical results) more than 2/3-rd of the varieties on the picture in Pratt [13] seems to be settled (from the point of view of equational decidability). The only varieties whose decision problems remain open seem to be **RES** and **ACT**.

Acknowledgements

The proof we present herein was implicitly contained in [10] (cf. also [7]).

Research supported by Hungarian National Foundation for Scientific Research grants No 1911, No 2258 and No T7255.

References

- [1] Andr  ka, H. Distributive lattice-ordered semigroups are decidable Manuscript, Math. Inst., Budapest.
- [2] Andr  ka, H., Givant, S. and N  meti, I. Which *RA*-varieties are decidable? Manuscript, Mills College, Oakland, Jan 1992. A shorter version to appear at *Bulletin of Section of Logic* (Univ. of Lodz) as 'Decision problems for Equational Theories of Relation Algebras'.
- [3] Barwise, J. (editor) *Handbook of Mathematical Logic*. North-Holland, 1977.
- [4] van Benth  m, J. Dynamic Arrow Logic. In: *Logic and Information Flow* (eds.: Jan van E  ck & Albert
- [5] Birkhoff, G. *Lattice Theory*. Amer. Math. Soc., 1948 (revised in 1973).
- [6] Gyuris, V. Decidability of semigroups with a Boolean ordering (and non-distributive modal logics). Preprint, Math. Inst., Budapest, 1992
- [7] Gyuris, V., Kurucz,   ., N  meti, I. and Sain, I. Associativity implies undecidability in Arrow Logics. In *Proceedings of the Applied Logic Conference Logic At Work*, Amsterdam, Dec 1992.

- [8] Jipsen, P. *Computer Aided Investigations of Relation Algebras*. Dissertation, Vanderbilt University, Nashville, Tennessee, 1992.
- [9] Jónsson, B. and Tsinakis, C. Relation algebras as residuated Boolean algebras. *Algebra Universalis*, to appear.
- [10] Kurucz, Á., Németi, I., Sain, I. and Gyuris, V. Associativity implies undecidability in Arrow Logics. Preprint, Math. Inst., Budapest, 1992.
- [11] Németi, I. Exactly which varieties of cylindric algebras are decidable? Preprint, Math. Inst., Budapest, 1985.
- [12] Pigozzi, D. Fregean Algebraic Logic. In: *Algebraic Logic* (Andréka, H. Monk, J.D. and Németi, I., eds) Proc. Conf. Budapest 1988, Colloq. Math. Soc. J. Bolyai, Vol 54. North-Holland, Amsterdam, 1991, pp. 473–502.
- [13] Pratt, V. A Roadmap of some two dimensional logics. In: *Lecture Notes for TEMPUS Summer School*, July 1992, Prague (ed.: Jiri Adamek)
- [14] Simon, A. and Kurucz, Á. The equational theory of Euclidean Residuated Boolean Monoids is undecidable. Preprint, Math. Inst., Budapest, 1993
- [15] Simon, A., Sain, I. and Németi, I. Some classes of residuated Boolean algebras with operators, their equational undecidability. Preprint, Math. Inst., Budapest, Spring 1993.
- [16] Venema, Y. *Many-Dimensional Modal Logic*. Ph.D. Dissertation, Institute for Logic, Language and Computation, Univ. of Amsterdam, 1992.

Received 18 May 1993