Theoretical Computer Science 19 (1982) 331–335
North-Holland Publishing Company

NOTE

ON DIRECT PRODUCTS OF AUTOMATON DECIDABLE THEORIES

Bernard R. HODGSON*

Département de mathématiques, Université Laval, Québec, Canada G1K 7P4

Communicated by E. Engeler
Received August 1981

Abstract. This paper is concerned with connections between two different ways to prove decidability results: methods of automata theory and methods related to products of algebraic systems. Some basic automaton-theoretic conditions on relational structures are presented which give preservation theorems for decidability under certain direct products.

1. Introduction

In this paper, we present a brief description of some connections between two approaches to the decision problem of logical theories. On the one hand, we are interested in the use of finite automata in solving decision problems. This method originated with the works of Büchi and Elgot in the early sixties and was subsequently brought to a high level of sophistication, culminating in the deep results of Rabin [6] about the decidability of various second-order theories via automata on infinite trees. (See Rabin [7] for a survey of these results and also for a general discussion of different methods for establishing decidability of theories.) On the other hand, we are also interested in the study of the decidability properties of certain products of structures. An investigation of such properties was initiated by Mostowski [4] and then further developed in a more general setting by Feferman and Vaught [3].

Our concern will be with decision problems in first-order logic. After identifying rather weak and natural conditions on structures ensuring that the corresponding first-order theories are automaton decidable, we will show that these conditions are sufficient to give us preservation results for automaton decidability under certain direct products, namely finite direct products and countable direct powers (weak or strong).

* The author's work was supported by the Natural Sciences and Engineering Research Council of Canada.

2. Preliminary definitions and results

We use two types of finite state automata, namely the usual Rabin–Scott model and the Muller–McNaughton model accepting ω-words (see for example [1] or [11] for definitions). The languages and ω-languages respectively accepted by such automata are called *regular*. As is well known, the *emptiness problem* for regular (ω-) languages is effectively decidable. Moreover, regular (ω-) languages both satisfy various closure properties. More precisely, we will need the following:

(a) The family of regular languages is closed under union, complementation, concatenation, iteration closure, homomorphisms and inverse homomorphisms. (See any textbook on formal languages.)

(b) The family of regular ω-languages is closed under union, complementation, concatenation with a regular language, homomorphisms and inverse homomorphisms. The strong (or ω-) iteration closure of a regular language is a regular ω-language. (See [1, 2, 9 or 11].)

Given a relational structure $\mathscr{D} = \langle D, \{R_i \mid i \in I\}\rangle$ with domain D and relations $R_i \subseteq D^{n_i}$, the *theory* $\mathrm{Th}(\mathscr{D})$ is the set of all sentences (from the appropriate first-order language $\mathscr{L}_{\mathscr{D}}$) true in $\mathscr{D}$. It follows immediately from the solvability of the emptiness problem for regular (ω-) languages that if there is, modulo an appropriate encoding of elements and tuples of elements of D, an effective procedure assigning to every formula of $\mathscr{L}_{\mathscr{D}}$ a finite automaton accepting its truth-set (i.e. the codes for tuples of elements satisfying the formula), then the theory $\mathrm{Th}(\mathscr{D})$ is decidable. We will emphasize such a situation by saying that $\mathrm{Th}(\mathscr{D})$ is *automaton decidable*.

When looking for automaton decidable theories, it is quite natural in a first step to consider a class of relational structures which are, in a way, archetypal, their domains and relations being encoded in a "simple" fashion. To be more explicit, let D be such that its elements can be expressed directly as words or ω-words over some appropriate alphabet (typical cases: natural numbers written in binary notation; p-adic numbers encoded as infinite strings, each component being a coefficient written in base p). Then our archetypal structures will be those for which encoding of relations can be done in a most straightforward manner, namely by *convolution* of the codes for the domain. We recall that, given two ω-words $u = (u_i)_{i<\omega}$ and $v = (v_i)_{i<\omega}$ over an alphabet Σ, their convolution is the ω-word $u * v$ over the alphabet Σ^2 defined by $(u * v)_i = (u_i, v_i)$. Convolution of finite words of equal length is defined similarly. This operation can be canonically extended to finite words of unequal length by introducing an arbitrary marker repeatedly used to "fill the gap" between the shorter word and the longer one (such a "parallel" encoding was used by Myhill [5]).

Definition. A relational structure is *automatic* (resp. *ω-automatic*) if, modulo an appropriate effective convolution-encoding, its domain and relations are regular languages (resp. ω-languages).

The $(\omega\text{-})$ automatic structures are basic to the study of automaton decidability.

Theorem 1. *The theory of an $(\omega\text{-})$ automatic structure is automaton decidable.*

The proof goes by induction on the complexity of formulas, using the closure properties of regular $(\omega\text{-})$ languages. We suppress the details.

Examples of $(\omega\text{-})$ automatic structures are addition of natural numbers (i.e. Presburger arithmetic) and addition of p-adic numbers.

3. Direct products of $(\omega\text{-})$ automatic structures

We consider the following three constructions on families of relational structures: finite direct products, weak (countable) direct powers and strong (countable) direct powers. Recall that, given a non-empty family $\{\mathcal{D}^{(j)} \mid j \in J\}$ of similar relational structures $\mathcal{D}^{(j)} = \langle D^{(j)}, \{R_i^{(j)} \mid i \in I\}\rangle$, its *strong direct product* is the structure $\mathcal{P} = \langle P, \{S_i \mid i \in I\}\rangle$ with domain $P = \prod_{j\in J} D^{(j)}$ and relations $S_i \subseteq P^{n_i}$ defined by $(g, \ldots, h) \in S_i$ iff, for all $j \in J$, $(g(j), \ldots, h(j)) \in R_i^{(j)}$. Given an arbitrary element $e \in P$, the *weak direct product* is the structure $\mathcal{P}_e$ with domain $P_e = \{f \in P \mid f(j) = e(j)$ for all but finitely many $j \in J\}$ and whose relations are the restrictions of the S_i's to P_e. The product is *finite* or *countable* according to whether the index set J is so. If J is countable and all the factors $\mathcal{D}^{(j)}$ are equal to a fixed structure $\mathcal{D}$, then the result is called a strong or weak countable direct *power*, which we denote respectively by $\mathcal{D}^{\omega}$ or $\mathcal{D}^{*}$.

We have the following three preservation theorems for automaton decidability.

Theorem 2. *The theory of a finite direct product of $(\omega\text{-})$ automatic structures is automaton decidable.*

Theorem 3. *The theory of a weak countable direct power of an automatic structure is automaton decidable.*

Theorem 4. *The theory of a strong countable direct power of an automatic structure is automaton decidable.*

We postpone the proof of these theorems to the next section, giving first some examples of applications.

(1) Every finitely generated abelian group $\mathcal{G}$ is isomorphic to a finite direct product of cyclic groups (see [8, p. 193]). Since any cyclic group (finite or infinite) can be seen to be an automatic structure, it follows from Theorem 2 that the theory $\mathrm{Th}(\mathcal{G})$ is automaton decidable.

(2) Skolem arithmetic (i.e. the theory of multiplication of positive natural numbers) is automaton decidable. This follows from Theorem 3, since (cf. [4]) the

structure $\langle \mathbb{N}-\{0\}, \times\rangle$ is isomorphic to the weak countable direct power of $\langle \mathbb{N}, +\rangle$ through the mapping

$$n = \prod_{i=1}^{k} p_i^{n_i} \mapsto (n_1, n_2, \ldots, n_k, 0, 0, \ldots)$$

where p_i denotes the ith prime and n_i is its exponent in the prime decomposition of n.

(3) More generally, the theory of any free abelian group (of countable rank) is automaton decidable, since each element has a unique finite expression $\prod_{i=1}^{k} \gamma_i^{m_i}$ for generators γ_i and integers m_i (see [8, p. 187]).

(4) The theory of addition of countable-dimensional vectors of natural numbers (with addition defined componentwise) is automaton decidable by Theorem 4.

(5) Similarly, multiplication of Steinitz' g-numbers is automaton decidable. These numbers [10, p. 250] are formal expressions $\prod_{i=1}^{\infty} p_i^{x_i}$ where p_i ranges over all primes and x_i is either a natural number or the symbol ∞. They are multiplied by adding exponents with the convention that for every natural x, $\infty + x = x + \infty = \infty + \infty = \infty$.

4. Proof of the theorems

We now give some indications how to prove the theorems. In each case, the basic step is to find a suitable encoding for the elements of the product structure.

For example, the case of a finite direct product of (ω-) automatic structures can be handled quite easily: the elements of the product can be encoded by convolution of the codes for the elements of the factors, or even by simple concatenation in the automatic case. (It can thus be seen that a finite direct product of (ω-) automatic structures is (ω-) automatic.)

The elements of a weak (countable) direct power represent a finite but arbitrarily large amount of "informations": the operation of iteration closure can thus be used for encoding. For example, consider the structure $\langle \mathbb{N}-\{0\}, \times\rangle$ for Skolem arithmetic. The number $n = \prod_{i=1}^{k} p_i^{n_i}$ can be encoded as a word $\underline{n}_1\Box\underline{n}_2\Box\cdots\Box\underline{n}_k$ over the alphabet $\{0, 1, \Box\}$, where $\underline{n}_i$ is the binary notation for the natural n_i and $\Box$ is used as a marker. Encoding of tuples of numbers is done in a similar fashion, first by adding null exponents if necessary to ensure that all numbers have prime decompositions of the same length, and then by iterating the convolution of the exponents for the successive primes.

Finally, a strong (countable) direct power is encoded through the operation of ω-iteration closure, which allows to encode an infinite (countable) amount of "informations".

Once the appropriate encoding has been chosen, the proof is done by induction on the complexity of formulas. We outline the proof for the case of a weak direct power.

Let us consider $\mathscr{D}^*$, the weak countable direct power of an automatic structure $\mathscr{D}$. We thus have to prove that for any formula $\phi(x_1, \ldots, x_n)$ of the appropriate language for $\mathscr{D}^*$, the set of codes for tuples of elements satisfying ϕ is regular. Now the domain and relations of $\mathscr{D}$ being regular languages, the same is true of those of the power structure, as encoding is done by iteration. It then follows that the truth-set of any atomic formula is regular. The case of an existentially quantified formula $\exists x_i \phi$ is treated by projecting the truth-set of ϕ along the ith axis, and then using erasing homomorphisms to get rid of useless markers left there by the convolution. The case of a disjunction $\phi \vee \psi$ is treated analogously, using closure of regular languages under inverse homomorphisms, while the case of a negation $\sim\phi$ is immediate.

The automaton decidability of the strong countable direct power $\mathscr{D}^\omega$ can be shown similarly, using closure properties of regular ω-languages.

Acknowledgment

The author is indebted to Professor Shuichi Takahashi of the Université de Montréal for many stimulating and fruitful discussions about the subject of this paper, during the preparation of the author's Ph.D. thesis under his supervision.

References

[1] Y. Choueka, Theories of automata on ω-tapes: a simplified approach, *J. Comput. Systems Sci.* **8** (1974) 117–141.

[2] R.S. Cohen and A.Y. Gold, Theory of ω-languages. II: A study of various models of ω-type generation and recognition, *J. Comput. Systems Sci.* **15** (1977) 185–208.

[3] S. Feferman and R.L. Vaught, The first order properties of products of algebraic systems, *Fund. Math.* **47** (1959) 57–103.

[4] A. Mostowski, On direct products of theories, *J. Symbolic Logic* **17** (1952) 1–31.

[5] J. Myhill, Linear bounded automata, WADD Technical Note 60-165, Wright-Patterson Air Force Base (1960).

[6] M.O. Rabin, Decidability of second-order theories and automata on infinite trees, *Trans. Amer. Math. Soc.* **141** (1969) 1–35.

[7] M.O. Rabin, Decidable theories, in: J. Barwise, Ed., *Handbook of Mathematical Logic* (North-Holland, Amsterdam, 1977) 595–629.

[8] J.J. Rotman, *The Theory of Groups* (Allyn and Bacon, Boston, 2nd ed., 1973).

[9] L. Staiger and K. Wagner, Zur Theorie der Abstrakten Familien von ω-Sprachen (ω-AFL), in: F. Bolck, Ed., *Tagungsbericht II. Int. Symp. für Algorithmische Kompliziertheit von Lern- und Erkennungsprozessen* (Friedrich-Schiller-Universität, Jena, 1976) 79–91.

[10] E. Steinitz, Algebraische Theorie der Körper, *J. Reine Angew. Math.* **137** (1910) 167–309.

[11] B.A. Trakhtenbrot and Ya.M. Barzdin', *Finite Automata: Behavior and Synthesis* (North-Holland, Amsterdam, 1973).