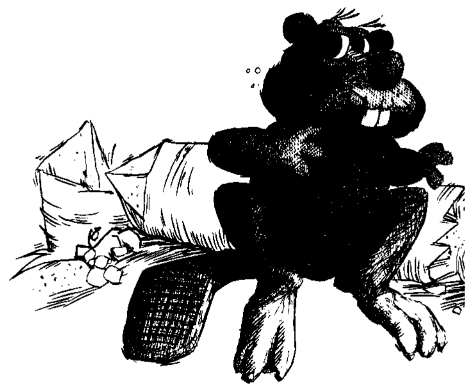
UNIVERSITY OF WATERLOO COMPUTER SCIENCE DEPARTMENT
UNIVERSITY OF WATERLOO COMPUTER SCIENCE DEPARTMENT
UNIVERSITY OF WATERLOO COMPUTER SCIENCE DEPARTMENT
UNIVERSITY OF WATERLOO COMPUTER SCIENCE DEPARTMENT



Systems of Equations over a Finitely Generated Free Monoid Having an Effectively Findable Equivalent Finite Subsystem

Karel Culik II
Juhani Karhumäki

CS-86-38

September, 1986

SYSTEMS OF EQUATIONS OVER A FINITELY GENERATED FREE MONOID HAVING AN EFFECTIVELY FINDABLE EQUIVALENT FINITE SUBSYSTEM*

K. Culik II

Department of Computer Science
University of Waterloo
Ontario, Canada
and

J. Karhumäki

Department of Mathematics
University of Turku
Finland

ABSTRACT

It has been proved recently, cf, [AL], that each system of equations over a finitely generated free monoid having only a finite number of variables has an equivalent finite subsystem. We discuss the problem when such a finite subsystem can be effectively found. We show that this is the case when the system is defined by finite, algebraic or deterministic two-way transducers.

1. Introduction

Throughout the history of mathematics compactness results, that is results stating that something which is specified by an infinite way is actually specified by a finite subpart of this infinite specification, have been eagerly looked for. In recent years a remarkable compactness property of free monoids has been revealed. More precisely, it has been shown in [AL] and [Gu] that each system of equations over a finitely generated free monoid and having a finite number of variables is equivalent to its finite subsystem.

This compactness result is closely related to the *Ehrenfeucht Conjecture*, cf. [K], which is as follows: For each subset L of a finitely generated free monoid Σ^* there exists a finite subset F of L such that for any two morphisms h and g from Σ^* into another free monoid the equation $h(x) = g(x)$ holds for all x in L if and only if it holds for all x in F. F is called a *test set* for L. It is

This work was supported by the Natural Sciences and Engineering Research Council of Canada under Grant A-2403

straightforward

to conclude that the Ehrenfeucht Conjecture follows directly from the above compactness property of systems of equations, which, hence, could be called the *Generalized Ehrenfeucht Conjecture*. It was shown in [CK1], as a first step towards the solution of the Ehrenfeucht Conjecture, that these two statements are in fact equivalent.

After knowning that each system of equations possesses an equivalent finite subsystem a natural question to be asked is "under which conditions such a finite subsystem can be effectively found?" This is the topic of this note.

We first recall from [CK1] a connection between the Ehrenfeucht Conjecture and its generalized version showing that the conjecture holds effectively for certain types of subsets of Σ^* if and only if systems of equations of the "corresponding" type possess effectively equivalent finite subsystems. Then we start to consider systems of equations defined by different kinds of transducers, that is automata with outputs. Such devices suit very well to describe infinite systems of equations - for each successful computation the input word defines the lefthand side of an equation and the corresponding output word defines the righthand side of the same equation.

We consider three types of transducers: finite transducers, pushown transducers and determinisitic two-way transducers. We show that in each of these cases the corresponding systems of equations possess effectively equivalent finite subsystems. In the first two cases proofs are based on pumping properties of sets of words, and the results are proved already in [CK1] and [ACK]. In the third case the detailed proof is much more complicated as is shown here.

2. Preliminaries

We assume that the reader is familiar with the basic facts of formal language theory, cf. e.g. [H], as well as those of free monoids. Consequently, we define here in details only a few most infrequently used notions as well as our special terminology, while some other notions are described only informally.

Let Σ be a finite alphabet and $N=\{x_1,..,x_n\}$ a finite set of *variables* such that $\Sigma \cap N = \emptyset$. An *equation* with n variables (or unknowns) over a free monoid Σ^* generated by Σ is of the form

$$(1) \qquad u = v \quad \text{with} \quad u,v \in N^*.$$

A *system of equations* is any collection of equations. A *solution* of a system of equations over Σ^* is a morphism $h: N^* \to \Sigma^*$ satisfying $h(u) = h(v)$ for all equations $u = v$ in the system. Thus, a solution can be identified with an n-tuple of words. Two systems of equations are called *equivalent* if they have exactly the same solutions.

Observe that in defining equations we did not allow constants, i.e., u and v in (1) were in N^* rather than in $(N \cup \Sigma)^*$. This was done only for the sake of convenience, since without affecting our considerations constants in equations can be eliminated by introducing for each symbol a in Σ a new variable X_a and replacing

each occurrence of a by X_a and adding a finite set of new equations $X_a = a$.

Following [CK1] we next introduce our special notion. In what follows we identify an equation $u = v$ with the pair (u,v). Consequently, a system S of equations with unknowns N can be viewed as a binary relation over N, i.e., $S \subseteq N^* \times N^*$. Now, let L be a family of languages (over the same alphabet) and R a family of binary relations over N. We say that **R** is *morphically characterized* by **L** if the following holds: A binary relation R is in **R** if and only if there exist a language L in **L** and two morphisms h and g such that $R = \{(h(w), g(w) \mid w \in L\}$. Finally, we say that a system of equations (that is a binary relation) is of *type* **L** if it belongs to the family of relations morphically characterized by **L**.

A connection between the Ehrenfeucht Conjecture for a family **L** of languages and its generalized version for systems of equations of type **L** (for definitions cf. Introduction) can now be obtained, as is shown in [CK1]:

Theorem 1. For any family **L** of languages the following statements are equivalent :

(i) For each effectively given L in **L** a test set can be effectively found,

(ii) For each effectively given system S of equations of type **L** a finite equivalent subsystem can effectively be found.

A natural way (at least for computer scientists) to define infinite systems of equations is to use transducers that is to say automata with outputs. In this paper we shall be considering three types of transducers which are informally described in the following lines (for more details cf. [H]). A *finite transducer* is a finite (nondeterministic) automaton provided with an output structure, that is for each transition a (possibly empty) output is produced. Similarly, a *pushdown transducer* is an ordinary pushdown automaton provided with an output structure. Finally, a *deterministic two-way transducer* is obtained from a deterministic two-way automaton by adding a single output to each transition rule.

Let T be an arbitrary transducer of any of the above types. Then if N denotes the input alphabet (that is the alphabet of the underlying automaton) and M denotes the output alphabet then T defines via successful computations a binary relation $S_T \subseteq N \times M$. Consequently, each transducer defines a system of equation with $N \cup M$ as the set of variables.

Next we argue in favour of our above special notion by using some known results from the theory of transducers. Let *Reg* and *CF* denote the families of regular (or rational) and context free (or algebraic) languages, respectively. We said that a system of equations is of type *Reg* iff it is morphically characterized by the family *Reg*, which, in turn, means by the well known Nivat Theorem, cf. [B], that the system is defined by a finite transducer. We call such systems of equations *rational*. Similarly, a system of equations is of type *CF* iff it is defined by a pushdown transducer, cf. [CC]; hence, we call these relations *algebraic*. Finally, it is clear that the family of arbitrary binary relations is of type "the family of all languages".

We proceed by giving two examples of systems of equations.

Example 1. Let $L \subseteq N^*$ be a regular language. Then the system of equations defined by

$$S = \{x = x^R \mid x \in L\},$$

when x^R denotes the reverse of the word x, is algebraic, since it is obvious how to construct a pushdown transducer for S.

Example 2. Let $d: N^* \to N^*$ be a morphism defined by $d(a) = aa$ for each a in N. Then the relation defined by

$$S = \{d(x) = xx^R \mid x \in \Sigma^*\}$$

can be realized by a deterministic two-way transducer. The same conclusion holds if x ranges over an arbitrary given regular language instead of Σ^*.

In order to be able to express relations defined by deterministic two-way transducers in terms of type **L** for some family **L** of language we shall need the following definitions. Let w be a word in the alphabet Σ and $h_1, \ldots, h_k$, for $k \geq 1$, be a set of endomorphisms of Σ^*.
Define

$$L_o = \{w\}$$

$$L_{i+1} = L_i \cup \bigcup_{j=1}^{k} h_j(L_i) \quad \text{for} \quad i \geq 0$$

and

$$L = \bigcup_{i=0}^{\infty} L_i .$$

Languages **L** thus defined are called *DTOL Languages*. Further a language L is called an *HDTOL Language* iff it is a morphic image of a DTOL language. The family of all HDTOL languages is denoted by *HDTOL*. More about these and related language families can be found from [RS].

The family *HDTOL* has the following properties. Firstly, it contains all regular or even all linear context-free languages as is easy to see. Secondly, it is incomparable with the family of context-free languages, cf. [RS]. Finally, the most important property of HDTOL languages from the point of view of this note is that these languages are "purely morphically defined". As an illustration of the power of HDTOL languages we give the following example.

Example 3. The language

$$L' = \{x x^R x \mid x \in \{a,b\}^*\}$$

is an HDTOL language. Indeed, $L' = h(\bigcup_{i=o}^{\infty} L_i)$, where

$$L_o = \{w\}$$

$$L_{i+1} = L_i \cup h_a(L_i) \cup h_b(L_i), \quad \text{for} \quad i \geq o,$$

and the morphisms $h_a, h_b : \{w,a,b,A,\overline{A},B,\overline{B}\}^* \to \{a,b,A,\overline{A},B,\overline{B}\}^*$ and the morphism $h : \{w,a,b,A,\overline{A},B,\overline{B},\}^* \to \{a,b\}^*$ are defined as follows:

h_a:	$w \to A\overline{A}A$	h_b:	$w \to B\overline{B}B$	h:	$w \to \epsilon$
	$A \to aA$		$A \to bA$		$A \to a$
	$\overline{A} \to \overline{A}a$		$\overline{A} \to \overline{A}b$		$\overline{A} \to a$
	$B \to aB$		$B \to bB$		$B \to b,$
	$\overline{B} \to \overline{B}a$		$\overline{B} \to \overline{B}b$		$\overline{B} \to b$
	$a \to a$		$a \to a$		$a \to a$
	$b \to b$		$b \to b$		$b \to b$

where ϵ denotes the empty word.

3. Results

In this section we consider systems of equations defined by the above three types of transducers, and conclude that in each case an equivalent finite subsystem can be effectively found.

Theorem 2. For each rational system S of equations (given by a finite transducer) an equivalent finite subsystem S' can be effectively found.

Outline of the proof. A straightforward consequence of pumping properties of regular languages and of the following implication, cf. [ACK] or [K] : For any words $w,y,u,v,\overline{x},\overline{y},\overline{u}$ and $\overline{v}$ we have

$$\left.\begin{aligned} xy &= \overline{x}\,\overline{y} \\ xuy &= \overline{x}\,\overline{u}\,\overline{y} \\ xvy &= \overline{x}\,\overline{v}\,\overline{y} \end{aligned}\right\} \Rightarrow xuvy = \overline{x}\,\overline{u}\,\overline{v}\,\overline{y}$$

□

It follows from the proof of Theorem 2 that not only an equivalent finite subsystem S' can be found but it can also be strongly bounded. Indeed, assume without loss of generality that S is given by a *normalized* finite transducer (that is to say that inputs read and outputs produced in single transition steps are of the length at most 1). Then the S' can be chosen to contain only those equations in which the words (in unknowns) are shorter than two times the cardinality of the state set of the finite transducer.

The proof of Theorem 2 used pumping properties of regular languages. Similarly we can use pumping properties of context-free languages to establish the Ehrenfeucht Conjecture for this family. However, in this case the detailed proof is quite lengthy, cf. [ACK], but since everything can be done effectively we conclude by Theorem 1 the following.

Theorem 3. For each algebraic system of equations (given by a pushdown transducer) there effectively exists an equivalent finite subsystem.

Next we turn to consider systems of equations defined by deterministic two-way transducers. In order to establish the above compactness property also in this case we need a different approach. In this case the systems of equations are not characterized by any family of languages (cf. discussion after Theorem 5), however, the family of HDTOL languages plays an important role. For this family we have:

Theorem 4. Each system of equations of the type *HDTOL* possesses effectively an equivalent finite subsystem.

Proof: By Theorem 1 it is enough to show that the Ehrenfeucht Conjecture holds effectively for HDTOL languages. This, in turn, was shown in [CK2], cf. also [CK1], using the (noneffective) validity of the Ehrenfeucht Conjecture, cf. [AL], and a decidability result of Makanin cf. [Mak], stating that it can be tested whether a given equation over a free monoid has a solution.

□

From Theorem 4 we obtain

Theorem 5. Each system S of equations defined by a deterministic two-way transucer possesses effectively an equivalent finite subsystem.

Proof. Let S be defined by a deterministic two-way transducer T which means that

$$(u,v) \in S \quad iff \quad v = T(u).$$

Without loss of generality we may assume that the input and output alphabets of T coincide, say are equal to N. Since we can allow endmarkers in our transducers it is easy to construct from T another deterministic two-way transducer, say T_1, such that

$$T_1(u) = \bar{u}\, T(u) \quad \text{for } all \quad u \in N^*$$

where $\bar{u}$ is the barred copy of u.

Next we define the language

$$L = \{T_1(u) \mid u \in N^*\}. \tag{2}$$

Then, clearly

$$S = \{(h(u), \bar{h}(u)) \mid u \in L\}$$

where the morphisms $h, \bar{h} : \{N U \bar{N}\}^*$ are defined by

$$h(a) = \epsilon \quad \text{and} \quad \bar{h}(a) = a \quad \text{for all} \quad a \; in \; N$$
$$h(\bar{a}) = a \quad \text{and} \quad \bar{h}(\bar{a}) = \epsilon \quad \text{for all} \quad \bar{a} \; in \; \bar{N}.$$

So, by Theorem 4, it remains to be shown that L is an HDTOL language.

In order to see this we first note that the domain of T is regular, cf. [H]. Secondly, it was shown in [ERS] that the image of an EDTOL language, which is, by definition, of the form $K \cap \Sigma^*$ where K is a DTOL language and Σ is an alphabet, under a deterministic two-way transducer is an EDTOL language, too. Finally, it is known that the families of EDTOL and HDTOL languages coincide, cf. [NRSS], and so by the fact that each regular language is an HDTOL language we conclude that L in (2) is an HDTOL language. Furthermore, by the above references, it can be effectively constructed from T completing the proof of Theorem 5.

□

By the proof of Theorem 5, each system of equations defined by a deterministic two-way transducer is of type *HDTOL*. The converse is not true. In fact, the family of systems of equations defined by deterministic two-way transducers cannot be morphically characterized by any family of languages, since, for example the domains and the images of these transucers determine different families of languages, as was seen in the proof of Theorem 5. It also follows from the proof of Theorem 5 that systems of equations of the form

(3) $\{(u, T(u)) \mid u \in L\}$ with $L \in HDTOL$ and T a deterministic two-way transducer

are of type *HDTOL*, yielding the following strengthing of Theorem 5:

Theorem 6. For each system of equations of the form (3) there effectively exists an equivalent finite subsystem.

The fact that deterministic two-way transducers are single-valued implies that (3) does not give all systems of equations of type *HDTOL* either.

4. Applications and concluding remarks

We start this final section by pointing out a couple of applications of our previous results. We hope (and believe) that more will be found in the future.

Application 1. Let X be a finite set of words over an alphabet Σ. We consider the semigroup X^+ generated by X, and we are particularly interested in the set of all identities of X^+ in Σ^*. It is straightforward to see, cf. e.g. [Mak], that this set of identities forms, in our terms, a rational system of equations with X as the set of variables. Consequently, by Theorem 2, it has a finite equivalent subsystem which, moreover, can be effectively found. This means that all the identities of X^+ are actually implied by a finite effectively findable set of identities of X^+, cf. also [HK] and [S] for a more general result. As a conclusion we have found a short proof for the following result:

Corollary 1. It is decidable whether two finitely generated subsemigroups of a free semigroup are isomorphic.

Application 2. Let us call a word x palindromic if $x = x^R$. Now we raise the question of deciding whether a given language is a subset of the set of all palindromic words. For regular languages the problem can be settled by Example 1 and Theorem 3. Indeed, let L be a regular language. Then the relation $\{(x,x^R) \mid x \in L\}$ is algebraic and hence equivalent with a finite relation $\{(x,x^R) \mid x \in F\}$, where $F \subseteq L$ and can be effectively found. Now, the result follows since L is palindromic iff the relation $\{(x,x^R) \mid x \in L\}$ holds.

A similar argumentation can be used to solve the problem for HDTOL languages, since the relation $\{(x,x^R) \mid x \in L\}$, where $L \in$ *HDTOL*,, is of type *HDTOL*, cf. Example 3 and the proof of Theorem 5. More about these and similar problems can be found in [HKK].

As a concluding remark we want to compare our results to some related results. We first observe, cf. also [CK1] and [ACK]:

Corollary 2. The equivalence problem for rational (resp. algebraic or of type *HDTOL*) systems of equations is decidable.

Proof. By our theorems in Section 3, in each case systems of equations can be replaced by finite systems of equations. Hence, the result follows since the equivalence of two finite systems of equations can be tested as was shown in [CK1].

□

By Corollary 2 we can decide whether two finite transducers defines equivalent systems of equations. On the other hand it is a well-known result cf. [Gr] or [B] that it is undecidable whether two finite transducers are equivalent, that is whether they define the same relation.

References

[ACK] Albert, J., Culik II, K. and Karhumäki, J., Test sets for context-free languages and algebraic systems of equations, Inform. Control 52 (1982) 172-186.

[AL] Albert, M.H. and Lawrence, J., A proof of Ehrenfeucht's Conjecture, Theoret. Comput. Sci. 41 (1985) 121-123.

[B] Berstel, J., Transductions and Context-Free Languages (Teubner, Stuttgrard, 1979).

[CC] Culik II, K., and Choffrut, C., Properties of finite and pushdown transducers, SIAM, J. Comput. 12 (1983) 300-315.

[CK1] Culik II, K., and Karhumäki, J., Systems of equations over a free monoid and Ehrenfeucht's Conjecture, Discrete Mathematics 43 (1983) 139-153.

[CK2] Culik II, K., and Karhumäki, J., The decidability of the DTOL sequence equivalence problem and related decision problems, University of Waterloo, Department of Computer Science, Research Report CS-85-05 (1985).

[ERS] Engelfriet, J., Rozenberg, G., and Stutzki, G., Tree transducers, L systems and two-way machines, J. Comput. Systems Sci. 20 (1980) 150-202.

[Gr] Griffiths, T., The unsolvability of the equivalence problem for ϵ-free nondeterministic generalized machines, J. Assoc. Comput. Mach. 15 (1968) 409-413.

[Gu] Guba, V.S., personal communication (1985).

[H] Harrison, M.A., Introduction to Formal Language Theory (Addison-Wesley, Reading MA, 1982).

[HK] Harju, T., and Karhumäki, J., On the defect theorem and simplifiability, semigroup Forum 33 (1986) 199-217.

[HKK] Horváth, S., Karhumäki, J., and Kleijn, H.C.M., Decidability and Characterization results concerning palindromicity manuscript (1986).

[K] Karhumäki, J., The Ehrenfeucht Conjecture: A compactness claim for finitely generated free monoids, Theoret. Comput. Sci. 29 (1984) 285-308.

[Mak] Makanin, G.S., The Problem of solvability of equations in a free semigroup, Mat. SG. 103 (1977) 147-236 (English transl. in : Math USSR SG. 32 (1977) 129-198).

[Mar] Markov, Al. A., On finitely generated subsemigroups of a free semigroup, Semigroup Forum 3 (1971) 251-258.

[NRSS] Nielsen, M., Rozenberg, G., Salomaa, A. and Skyum S., Nonterminals, homomorphisms and codings in different variations of OL-systems, I. Deterministic systems, Acta Informatica 4 (1974) 87-106.

[S] Spehner,J.-C., Tout sous-monoide finiment engendré d'un monoide libre admet une présentation de Malcev finie, C.R. Acad. Sc. Paris, 301, Série I, no. 18 (1985).

[RS] Rozenberg, G., and Salomaa, A., The Mathematical Theory of L Systems (Academic Press, New York, 1980).