Theoretical Computer Science 41 (1985) 121-123
North-Holland

NOTE

A PROOF OF EHRENFEUCHT'S CONJECTURE

M.H. ALBERT* and J. LAWRENCE**
Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

Communicated A. Salomaa
Received March 1985

Abstract. Ehrenfeucht's Conjecture states that each subset S of a finitely generated free monoid has a finite subset T such that if two endomorphisms of the monoid agree on T, then they agree on S. It is the purpose of this note to verify the conjecture.

Ehrenfeucht's Conjecture states that if $\mathbb{M}_k$ is the k-generated free monoid and S is a subset of $\mathbb{M}_k$, then there is a finite subset T of S such that if two endomorphisms on $\mathbb{M}_k$ agree on T, then they agree on S. This conjecture was made by Ehrenfeucht at the beginning of the 1970's and was motivated by formal language theory. It was first proved for $k=2$ in [4]. In this paper we prove the following theorem.

1. Theorem. *Ehrenfeucht's Conjecture is true.*

There are several interesting consequences of Theorem 1. In particular, we have the following theorem.

2. Theorem. *The* HD0L *sequence equivalence problem is decidable.*

That Theorem 1 implies Theorem 2 is proved in [3].

The reader is referred to [6] for an excellent survey of the work around the Ehrenfeucht's Conjecture including some consequences of Theorem 1.

Suppose that $\mathbb{M}_k(x_1, \ldots, x_k)$ is the free monoid generated by the set $\{x_1, \ldots, x_k\}$ and that M is another monoid. A monoid equation in k variables $x_1, \ldots, x_k$ is one of the form $w_1(x_1, \ldots, x_k) = w_2(x_1, \ldots, x_k)$, where w_1 and w_2 are elements of $\mathbb{M}_k(x_1, \ldots, x_k)$. We say that a k-tuple $(v_1, \ldots, v_k)$ of elements in M is a solution to the equation if $w_1(v_1, \ldots, v_k) = w_2(v_1, \ldots, v_k)$. Two systems of equations in k variables are said to be equivalent over M, if they have the same solution set. In [3] it is proven that Theorem 1 is equivalent to the following theorem.

* Research supported by an NSERC Postdoctoral Fellowship.
** Research partially supported by a grant from NSERC.

3. Theorem. *A system of monoid equations in k variables is equivalent, over the countably generated free monoid, to a finite subsystem.*

We can look at equations over groups by replacing the k-generated free monoid by the k-generated free group and the monoid M by a group G.

Recall that a group is said to be metabelian if it is an extension of an abelian group by an abelian group, or, equivalently, if it satisfies the identity $[[w, x], [y, z]] = 1$, where $[a, b] = a^{-1}b^{-1}ab$. In order to prove Theorem 3, we need the following two theorems.

4. Theorem ([7]). *A free monoid freely generated by a set can be embedded into the free metabelian group freely generated by the same set.*

This can be proved by considering the wreath product $\mathbb{Z} \wr \mathbb{Z}$, where $\mathbb{Z}$ is the infinite cyclic group (see [2]).

5. Theorem ([5, Theorem 3]). *A finitely generated metabelian group satisfies the ascending chain condition on normal subgroups.*

The proof of the above theorem uses the Hilbert Basis Theorem.

Proof of Theorem 3. Embed the countably generated free monoid $\mathbb{M}$ into the countably generated free metabelian group $\mathbb{A}$. A system of monoid equations in k variables $x_1, \ldots, x_k$ can be considered as a system of group equations. If we can prove that this system is equivalent over $\mathbb{A}$ to a finite subsystem, then it is equivalent over $\mathbb{M}$ to the same subsystem. We now turn our attention to group equations over $\mathbb{A}$.

Suppose that $\mathbb{G}_k = \mathbb{G}_k(x_1, \ldots, x_k)$ is the free group generated by the set $\{x_1, \ldots, x_k\}$ and that $\mathbb{A}_k(x_1, \ldots, x_k)$ is the free metabelian group generated by the same set. By Theorem 5, $\mathbb{A}_k$ satisfies the ascending chain condition on normal subgroups. Now by [1, Theorem 1], a system of equations in k variables is equivalent over $\mathbb{A}$ to a finite subsystem. For completeness we reproduce the part of the proof of [1, Theorem 1] that we need to justify the above claim.

Suppose that $\{w_i(x_1, \ldots, x_k) = 1\}_{i=1}^{\infty}$ is a system of group equations in k variables $x_1, \ldots, x_k$ (thus the w_i's are words in the free group $\mathbb{G}_k$). Now suppose that the k-tuple $(a_1, \ldots, a_k)$ of elements of $\mathbb{A}$ is a solution to $w_1 = 1$, $w_2 = 1, \ldots, w_l = 1$ but is not a solution to $w_{l+1} = 1$. Let α be the map from $\mathbb{G}_k$ to $\mathbb{A}_k$ that sends x_j to x_j and let β be the map from $\mathbb{A}_k$ to $\mathbb{A}$ that sends x_j to a_j. We have

$$\beta(\alpha(w_i(x_1, \ldots, x_k))) = w_i(a_1, \ldots, a_k) = 1 \quad \text{if } 1 \leqslant i \leqslant l,$$

while

$$\beta(\alpha(w_{l+1}(x_1, \ldots, x_k))) = w_{l+1}(a_1, \ldots, a_k) \neq 1.$$

Therefore, $\alpha(w_i(x_1, \ldots, x_k))$ is in the kernel of β if $1 \leq i \leq l$, while $\alpha(w_{l+1}(x_1, \ldots, x_k))$ is not in the kernel of β. It follows that the normal subgroup of $\mathbb{A}_k$ generated by the set $\{\alpha(w_i(x_1, \ldots, x_k))\}_{i=1}^{l}$ does not contain the element $\alpha(w_{l+1}(x_1, \ldots, x_k))$. Therefore, if the system of equations is not equivalent to a finite subsystem, then we have an infinite ascending chain of normal subgroups of $\mathbb{A}_k$, contradicting Theorem 5.

This completes the proof of Theorem 3 and, hence, also of Theorem 1. □

References

[1] M.H. Albert and J. Lawrence, The descending chain condition on solution sets for systems of equations in groups, *Proc. Edinburgh Math. Soc.*, to appear.

[2] G. Baumslag and Y. Roitberg, Groups with free 2-generator subsemigroups, *Semigroup Forum* **25** (1982) 135–143.

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

[4] K. Culik, II and A. Salomaa, Test sets and checking words for homomorphism equivalence, *J. Comput. System Sci.* **20** (1980) 379–395.

[5] P. Hall, Finiteness conditions for soluble groups, *Proc. London Math. Soc.* (3) **4** (1954) 419–436.

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

[7] A.I. Mal'cev, Nilpotent semigroups, *Ivanov. Gos. Ped. Last. Ucen Zap. Fiz.-Mat. Nauki* **4** (1953) 107–111.