Theoretical Computer Science 44 (1986) 333-339
North-Holland

NOTE

THE EHRENFEUCHT CONJECTURE: AN ALGEBRA-FRAMEWORK FOR ITS PROOF

Ebbe Thue POULSEN
Matematisk Institut, Aarhus University, DK-8000 Århus C, Denmark

Communicated by A. Salomaa
Received December 1985

Abstract. We describe an algebraic framework including, in particular, the affine monoid of a given ring. Within this framework it is a simple matter to deduce Ehrenfeucht's Conjecture from Hilbert's Basis Theorem.

1. Introduction

Ehrenfeucht's Conjecture in formal language theory goes back to the beginning of the 1970s (cf. [4]), and was recently proved by Albert and Lawrence [1]. It can be formulated as follows.

Theorem 1.1 (Ehrenfeucht's Conjecture). *Let A be an alphabet (i.e., a finite nonempty set), and let A^* denote the set of finite words in the letters of A. If L is an arbitrary subset of A^*, then there exists a finite subset F of L which is a test set for L in the following sense: if B is any alphabet and $h_1, h_2: A^* \to B^*$ are any two homomorphisms, then*

$$\forall w \in F: h_1(w) = h_2(w) \text{ implies that } \forall w \in L: h_1(w) = h_2(w).$$

According to Salomaa [6], various proofs of Theorem 1.1 have been given, all of them ultimately based upon Hilbert's Basis Theorem (see Section 3 below). See also Perrin [5], a paper which, in addition, comments upon some related results and open problems.

The aim of the present paper is primarily to clarify: we believe that our proof is quite transparent, and, in particular, that it makes clear how a result in commutative algebra (namely Hilbert's Basis Theorem) can contribute to proving an essentially noncommutative result (namely Ehrenfeucht's Conjecture).

The main tool for passing between commutative rings and noncommutative monoids is the construction which to any ring R associates its affine monoid Aff(R) (Definition 2.3). Essential ingredients in the transfer of information between the two areas mentioned are the 'homomorphism lemma' (Lemma 2.4), the 'injectivity lemma' (Lemma 2.5), and Lemma 2.6, which asserts the existence of a ring-homomorphism representing a given monoid-homomorphism. These results are collected in Section 2.

The proof given in Section 3 is in its essence modelled after the proof in [6]. According to that author, basic parts of the proof are due to McNaughton.

2. Algebraic preliminaries

In this section we shall explicitly formulate the universal properties of the monoid A^* and of the polynomial ring $\mathbb{Z}[A]$ (Lemmas 2.1 and 2.2), we shall define the affine monoid Aff(R) associated with a given ring R and state a simple 'homomorphism lemma' (Lemma 2.4). The less trivial Lemmas 2.5 and 2.6 are proved in detail.

Lemma 2.1. *Let A be an alphabet.*

(1) *A^* is a monoid (with concatenation as operation and the empty word as neutral element).*

(2) *If M is any monoid and $f: A \to M$ any function, then f has a unique extension to a monoid-homomorphism $\bar{f}: A^* \to M$.*

In addition to the monoid A^* we shall consider the set $\mathbb{Z}[A]$ of all polynomials with indeterminates belonging to A and integer coefficients.

Note. We require all rings to have a unit element and all ring-homomorphisms to map unit element into unit element.

Lemma 2.2. *Let A be an alphabet.*

(1) *$\mathbb{Z}[A]$ is a commutative ring (with the usual operations of polynomial addition and multiplication).*

(2) *If K is any commutative ring and $f: A \to K$ any function, then f has a unique extension to a ring-homomorphism $\tilde{f}: \mathbb{Z}[A] \to K$.*

Lemmas 2.1 and 2.2 are often formulated as: "*A^* is the free monoid generated by the set A*" and "*$\mathbb{Z}[A]$ is the free commutative ring generated by the set A*" respectively. Both of these results are easy to prove, Lemma 2.1 by the general associative law, and Lemma 2.2 by the general associative, the general commutative, and the general distributive laws.

2.1. The affine monoid

Let R be any ring. A function $f: R \to R$ of the form

$$f(x) = r + sx,$$

where $(r, s) \in R^2$ is called *affine*. It is clear that if

$$g(x) = t + ux,$$

then

$$(f \circ g)(x) = (r + st) + (su)x,$$

which shows that the set of affine functions is closed under composition, and therefore, is a monoid. This observation motivates the following definition.

Definition 2.3. Let R be a ring. By the *affine monoid* $\mathrm{Aff}(R)$ *of* R we understand the set R^2 organised with the binary operation

$$(r, s) \bullet (t, u) = (r + st, su).$$

The following result is obvious.

Lemma 2.4. *Let R_1 and R_2 be rings, and let $\hat{h}: R_1 \to R_2$ be a ring-homomorphism. Then the map $\hat{h} \times \hat{h}: \mathrm{Aff}(R_1) \to \mathrm{Aff}(R_2)$ defined by component-wise application of $\hat{h}$ is a monoid-homorphism.*

The injectivity result of Lemma 2.5 is crucial.

Lemma 2.5. *Let A be any alphabet, and let A^*, $\mathbb{Z}[A]$, and $\mathrm{Aff}(\mathbb{Z}[A])$ be the monoid, the polynomial ring, and the affine monoid described above. Let $\alpha: A \to \mathrm{Aff}(\mathbb{Z}[A])$ be defined by*

$$\alpha(a) = (a, a) \quad \textit{for all } a \in A,$$

and let $\bar{\alpha}: A^* \to \mathrm{Aff}(\mathbb{Z}[A])$ denote its extension to a monoid-homomorphism. Let π_1 denote the projection of $\mathrm{Aff}(\mathbb{Z}[A])$ onto its first coordinate, i.e.,

$$\pi_1(p_1, p_2) = p_1 \quad \textit{for } (p_1, p_2) \in \mathrm{Aff}(\mathbb{Z}[A]).$$

Then $\pi_1 \circ \bar{\alpha}: A^* \to \mathbb{Z}[A]$ is injective.

Proof. It is easy to see that if $w = a_1 a_2 \ldots a_k \in A^*$ is a word of length k, then $\pi_1 \circ \bar{\alpha}(w)$ is a sum of the k monomials $a_1, a_1a_2, a_1a_2a_3, \ldots, a_1a_2 \ldots a_k$. Thus, $\pi_1 \circ \bar{\alpha}(w)$ tells us not only which characters occur in w, but also their order. □

aab -> a + aa + aab = a + a^2 + a^2b

2.2. *The disjoint sum $A+A$*

Let A be an alphabet. We denote by A_1 respectively A_2 the two disjoint copies of A obtained by providing each element with the index '1' respectively '2', and we define *the disjoint sum* $A+A$ by

$$A+A=A_1\cup A_2.$$

We define two maps $\varphi_1,\varphi_2:A\to A+A$ by

$$\varphi_i(a)=a_i \quad \text{for } a\in A,\ i=1,2.$$

In view of Lemmas 2.1 and 2.2 these maps have extensions to monoid-homomorphisms $\bar{\varphi}_i:A^*\to(A+A)^*$ and to ring-homomorphisms $\tilde{\varphi}_i:\mathbb{Z}[A]\to\mathbb{Z}[A+A]$. (The extensions simply consist in providing each letter occurring in a word or a polynomial with the index in question.)

The next lemma is one of the main ingredients in the proof of Ehrenfeucht's Conjecture.

Lemma 2.6. *Let A be an alphabet, let $A+A$, φ_1 and φ_2 be defined as above, and define $\sigma:A\to\mathrm{Aff}(\mathbb{Z}[A+A])$ by*

$$\sigma(a)=(a_1,a_2)=(\varphi_1(a),\varphi_2(a)) \quad \textit{for } a\in A.$$

Let B be any alphabet, and let $\bar{\beta}:B^*\to\mathrm{Aff}(\mathbb{Z}[B])$ be the monoid-homomorphism corresponding to the map $\bar{\alpha}$ of Lemma 2.5.

Then, if $h:A^*\to B^*$ is any monoid-homomorphism, there exists a unique ring-homomorphism $\hat{h}:\mathbb{Z}[A+A]\to\mathbb{Z}[B]$ such that

$$\bar{\beta}\circ h=(\hat{h}\times\hat{h})\circ\bar{\sigma}, \tag{1}$$

i.e., such that the following diagram is commutative.

$$\begin{tikzcd}
A^* \arrow[r, "h"] \arrow[d, "\bar{\sigma}"'] & B^* \arrow[d, "\bar{\beta}"] \\
\mathrm{Aff}(\mathbb{Z}[A+A]) \arrow[r, "\hat{h}\times\hat{h}"] & \mathrm{Aff}(\mathbb{Z}[\mathrm{B}])
\end{tikzcd}$$

Proof. The proof is easy. First assume that (1) holds, and consider any $a\in A$. The element $\bar{\beta}\circ h(a)$ in $\mathrm{Aff}(\mathbb{Z}[B])$ is of the form $(p_1(a),p_2(a))$, where the two polynomials $p_i(a)\in\mathbb{Z}[B]$ depend upon a. By (1), we have

$$(\hat{h}\times\hat{h})(\sigma(a))=(p_1(a),p_2(a)),$$

i.e., $\hat{h}(a_1)=p_1(a)$ and $\hat{h}(a_2)=p_2(a)$.

Thus, $\hat{h}$ is uniquely determined on $A+A$. By the uniqueness part of Lemma 2.2, $\hat{h}$ is uniquely determined on $\mathbb{Z}(A+A)$.

To see that $\hat{h}$ exists, let $f:A+A\to\mathbb{Z}[B]$ be determined by

$$f(a_1)=p_1(a), \qquad f(a_2)=p_2(a),$$

where $a \in A$ is arbitrary, and $(p_1(a), p_2(a)) = \bar{\beta} \circ h(a)$ as above. By Lemma 2.2, f has an extension $\hat{h} = \tilde{f}$ to a ring-homomorphism from $\mathbb{Z}[A+A]$ into $\mathbb{Z}[B]$, and by Lemma 2.4, $\hat{h} \times \hat{h}$ is a monoid-homomorphism of $\mathrm{Aff}(\mathbb{Z}[A+A])$ into $\mathrm{Aff}(\mathbb{Z}[B])$.

Thus, both sides of (1) are monoid-homomorphisms, and since they coincide on all $a \in A$, they coincide on A^* by the uniqueness part of Lemma 2.1. □

3. Proof of Ehrenfeucht's Conjecture

It was proved by Culik and Karhumäki (see [4]) that Ehrenfeucht's Conjecture is equivalent to the following statement.

Theorem 3.1. *Let A be an alphabet and let I be an index-set. Let $(w_{i,1}, w_{i,2})_{i \in I}$ be a family of pairs of words in A^*:*

$$\forall i \in I: (w_{i,1}, w_{i,2}) \in A^* \times A^*.$$

Then there exists a finite subset J of I such that if B is any alphabet and $h: A^* \to B^*$ any monoid-homomorphism, then

$$\forall j \in J: \; h(w_{j,1}) = h(w_{j,2}) \tag{2}$$

implies that

$$\forall i \in I: \; h(w_{i,1}) = h(w_{i,2}). \tag{3}$$

Both of the implications in the statement that Theorem 1.1 and Theorem 3.1 are equivalent can be proved by means of constructions involving the direct sum $A+A$.

We shall prove Theorem 3.1 from the following theorem.

Hilbert's Basis Theorem. *Let A be an alphabet and let I be an index set. Let $(p_i)_{i \in I}$ be a family of polynomials in $\mathbb{Z}[A]$. Then there exists a finite subset J of I such that the ideal generated by the set $\{p_j \mid j \in J\}$ contains the set $\{p_i \mid i \in I\}$.*

We note that the theorem means that each polynomial p_i, $i \in I$, can be written as a linear combination of the polynomials $p_j, j \in J$, in the sense that there exist polynomials $q_{ij} \in \mathbb{Z}[A]$, $i \in I$, $j \in J$, such that

$$\forall i \in I: \; p_i = \sum_{j \in J} q_{ij} p_j. \tag{4}$$

A proof of this—not very deep—theorem can, for instance, be found in [2, p. 81; 3, p. 240; or 7, p. 200].

Proof of Theorem 3.1. Let A, I, and $(w_{i,1}, w_{i,2})_{i\in I}$ be given, and construct $A+A$, φ_1, φ_2, and σ as in Lemma 2.6. Also, let π_1 denote the projection of $\mathrm{Aff}(\mathbb{Z}[A+A])$ onto its first coordinate.

For each $i \in I$, define the polynomial $p_i \in \mathbb{Z}[A+A]$ by

$$p_i = \pi_1 \circ \bar{\sigma}(w_{i,1}) - \pi_1 \circ \bar{\sigma}(w_{i,2}). \tag{5}$$

By Hilbert's Basis Theorem there exists a finite subset J of I and polynomials $q_{ij} \in \mathbb{Z}[A+A]$ such that (4) holds. We shall now show that if B is any alphabet and $h: A^* \to B^*$ any monoid-homomorphism, then (2) implies (3).

To see this, let $\bar{\beta}$ and $\hat{h}$ be determined as in Lemma 2.6, and let π_1 denote the projection of $\mathrm{Aff}(\mathbb{Z}[B])$ onto its first coordinate, too.

Consider any two words w_1 and w_2 in A^*. Since $\pi_1 \circ \bar{\beta}$ is injective (Lemma 2.5), we have

$$h(w_1) = h(w_2) \tag{6}$$

if and only if

$$\pi_1 \circ \bar{\beta} \circ h(w_1) = \pi_1 \circ \bar{\beta} \circ h(w_2). \tag{7}$$

Using (1) we see that (7) is the same as

$$\pi_1 \circ (\hat{h} \times \hat{h}) \circ \bar{\sigma}(w_1) = \pi_1 \circ (\hat{h} \times \hat{h}) \circ \bar{\sigma}(w_2)$$

or

$$\hat{h} \circ \pi_1 \circ \bar{\sigma}(w_1) = \hat{h} \circ \pi_1 \circ \bar{\sigma}(w_2),$$

and since $\hat{h}$ is a ring-homomorphism, it follows that (6) holds if and only if

$$\hat{h}(\pi_1 \circ \bar{\sigma}(w_1) - \pi_1 \circ \bar{\sigma}(w_2)) = 0.$$

Thus, by the definition (5) of the p_i's, (2) is equivalent to

$$\forall j \in J: \ \hat{h}(p_j) = 0. \tag{8}$$

Since $\hat{h}$ is a ring-homomorphism, it follows from (4) and (8) that

$$\forall i \in I: \ \hat{h}(p_i) = \sum_{j\in J} \hat{h}(q_{ij})\hat{h}(p_j) = 0.$$

which is equivalent to (3). □

References

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

[2] M.F. Atiyah and I.G. MacDonald, *Introduction to Commutative Algebra* (Addison-Wesley, Reading, MA, 1969).

[3] P. Dubreil et M.L. Dubreil-Jacotin, *Leçons d'Algèbre Moderne* (Dunod, Paris, 1961).

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

[5] D. Perrin, On the solution of Ehrenfeucht's Conjecture, *Bull. EATCS No. 27* (October 1985) 68-70.

[6] A. Salomaa, The Ehrenfeucht Conjecture: A proof for language theorists, *Bull. EATCS No. 27* (October 1985) 71-82.

[7] O. Zariski and P. Samuel, *Commutative Algebra I* (Van Nostrand, Princeton, NJ, 1958).