EHRENFEUCHT TEST SET THEOREM AND HILBERT BASIS THEOREM: A CONSTRUCTIVE GLIMPSE

Cristian CALUDE and Dragoş VAIDA
Department of Mathematics, University of Bucharest
14 Academiei str.,70109 Bucharest, Romania

Ehrenfeucht Test Set Theorem, highly significant in Formal Language Theory, and Hilbert Basis Theorem are constructively correlated. A constructive version of Ehrenfeucht Test Set Theorem is proved; it is, classically, equivalent with the original result, which in turn is constructively equivalent with the classical Hilbert Basis Theorem. Our proof is given within Bishop Constructive Mathematics and it relies upon Tennenbaum's version of Hilbert Basis Theorem.

1. INTRODUCTION

The proof of Ehrenfeucht's Conjecture at the end of 1985 (see Albert and Lawrence (1985), Perrin (1985), Salomaa (1985)) has established a rather unexpected link between a result in Commutative Algebra, Hilbert Basis Theorem (Hilbert (1888-9), Waerden (1950)) and a relevant property in Formal Language Theory, of a non-commutative character (see Karhumaki (1984) for an overview).

The present paper is a continuation of CALUDE (1986). Our main aim is to offer a constructive version of Ehrenfeucht Test Set Theorem which is classically equivalent to the original result and allows us to constructively contrast the classical forms of Ehrenfeucht and Hilbert theorems. Our analysis is made using Tennenbaum's version of the notion of a **Noetherian discrete module**, a constructive notion classically equivalent to the ascending chain condition (see Bridges and Richman (1987), Mines, Richman and Ruitenburg (1988)). **We work within Bishop Constructive Mathematics**, shortly **BISH** (Bridges and Richman (1987)). Our basic notation is taken from the above quoted monographs.

By N and Z we denote, respectively, the set of naturals and the set of integers. For every finite non-empty set X (denoted alphabet) we construct X^*, the free monoid generated by X and Z [X] (i.e. the set of all polynomials in X over Z), the free commutative ring generated by X. In view of the universality properties it follows that: i) for every monoid M and for every function $f:X \to M$ there exists a unique monoid-morphism $m(f) : X^* \to M$ which extends f, ii) for every function $f:A \to R$, where R is a commutative ring, there is a unique ring-morphism $r(f) : Z[A] \to R$ which extends f. Let R_1, R_2 be two rings and $f : R_1 \to R_2$ be a ring-morphism . By $aff(f) : Aff(R_1) \to Aff(R_2)$ we denote the monoid-morphism $aff(f)(s,t) = (f(s),f(t))$, where Aff(R) is the affine monoid of R (i.e. the set R organized with the binary operationn $(r,s).(t,u) = (r+st,su)$). By $\pi_i (i=1,2)$ we denote the projection functions $\pi_1(s,t)=s$, $\pi_2(s,t) = t$. Finally, X+X is the disjoint union $\{x_1 / x \in X\} \cup \{x_2 / x \in X\}$, and $\underline{X} = \{\underline{x} / x \in X\}$ is a disjoint copy of X.

Classicaly, Ehrenfeucht and Hilbert results can be stated as follows:

Ehrenfeucht's Test Set Theorem. For every non-empty subset $L \subset A^*$ (A finite) there exists a finite subset $F \subset L$ (called test set for L) such that for every pair of monoid-morphisms $f,g:A \to B$ (B finite), if $f(u) = g(u)$, for every $u \in F$, then $f(u) = g(u)$, for every $u \in L$.

Hilbert Basis Theorem. For every non-empty subset $T \subset Z[A]$ (A finite) there exists a finite subset $P \subset T$ such that every element of T can be written as a linear combination of elements of P with coefficients polynomials in Z [A] (in all variables in A except a fixed one).

Both results presented above use the existential quantification in an essential way. The interpretation of the "existence" is the root of the distinction between the traditional or classical mathematics

and its constructive counterpart: whereas, classically, the existence of an object x with property P can be stated by deducing a contradiction from the assumption that no such x exists, constructively, the proof of the existence of such an x must embody two algorithms, one for the construction of x and another for checking that x has the property P.

From the very beginning Hilbert Basis Theorem was confronted with constructive requirements (see the objections of Gordan, Cayley and Kronecker in Reid (1970)) and was a challenge for the search of various constructive substitutes. Following Seidenberg (1975), "any condition on R classically equivalent to the ascending chain condition on ideals and which can be shown, constructively, to transfer to R [X] can be reasonably be considered as a definition of **Noetherian** for constructive purposes".In what follows we shall use Tennenbaum's condition. Let R be a ring and M a discrete R-module (see Bridges and Richman (1987)). A **Noetherian basis function** for M is a sequence $(\varphi_n)_{n\geq 2}$ of functions, $\varphi_n : M^n \longrightarrow R^{n-1}$ such that if $(x_n)_{n\geq 1}$ is an infinite sequence of elements of M, then there exists arbitrarily large n such that $x_n = \sum_{i=1}^{n-1} r_i x_i$, where $\varphi_n(x_1,\ldots,x_n) = (r_1,\ldots,r_{n-1})$. One can prove (see Mines, Richman, Ruitenberg (1988), p.204-207) that every discrete R-module M admitting a Noetherian basis function is (constructively) Noetherian (i.e.,for every ascending chain of ideals $I_1 \subset I_2 \subset \ldots$ in M, there exists a natural n such that $I_n = I_{n+1}$) and M[X] also admits a Noetherian base function. Our basic example is the ring Z of integers, as a module over itself, which admits a Noetherian basis function and therefore Z[A] also admits a Noetherian basis function. The above constructive definition of Noetherian R-module is classically, but not constructively, equivalent to the traditional definition (for every ascending chain of ideals $I_1 \subset I_2 \subset \ldots$ in M there exists a natural n such that $I_m = I_n$, for all $m > n$). The above definitions can be correlated by means of Brouwer-Bishop **limited principle of omniscience (LPO)**: if (a_n) is a binary sequence, then either there exists m such that $a_m = 1$ or else $a_n = 0$, for each n. Now, the constructive ascending chain condition appended with **LPO** is constructively equivalent to the classical ascending chain condition (Bridges and Richman, 1987). As **LPO** is rejected in constructive mathematics (it is provably false within some varieties of constructive mathematics, for example INT and RUSS; see Bridges and Richmann(1987), p.4), it follows that we must content our-selves with the more restricted definition, i.e. with the requirement that we can find a place where the chain **pauses**.

A subset $S \subset A^* \times A^*$ is called a system of word equations, shortly a **word-system**. A **solution** for S is a monoid morphism $f: A \longrightarrow B$ such that $f(u) = f(v)$, for every $(u,v) \in S$. Two word-systems S and S' are **equivalent** in case they have exactly the same solutions. Finally, we state the

Word-System Theorem. For every $S \subset A^* \times A^*$ (A finite) there exists a finite word-system $S' \subset S$ which is equivalent to S.

2. BASIC TRANSFER RESULTS

Our aim is to present, within **BISH**, two results relating Ehrenfeucht's condition to word-systems and to systems of polynomial equations. These results appear, more or less, in Culik II and Karhumäki (1983) and Thue Poulsen (1985), but proofs are included to insure that there are no problems from the constructive point of view.

Theorem 1. For every $u,v \in A^*$ there exists a polynomial $p_{u,v} \in Z[A+A]$ (depending upon u and v) satisfying the following condition:

(1) for every monoid-morphism $h : A^* \longrightarrow B^*$ there exists a ring-morphism $F : Z[A+A] \longrightarrow Z[B]$ (depending only upon h, but **not** on u and v) such that $h(u) = h(v)$ iff $F(p_{u,v}) = 0$.

Proof. Consider the mapping $\alpha : A \longrightarrow Aff(Z[A+A])$ defined by $\alpha(a) = (a_1, a_2)$, $a \in A$ and put

(2) $p_{u,v} = \pi_1 \circ m(\alpha)(u) - \pi_1 \circ m(\alpha)(v)$.

Given the alphabet B we consider the function $\beta : B \longrightarrow Aff(Z[B])$; $\beta(b) = (b,b)$, $b \in B$ and we observe that

(3) the monoid-morphism $\pi_1 \circ m(\beta)$ is injective.

Finally, given a monoid-morphism $h : A^* \longrightarrow A^*$, we define the function $f : A+A \longrightarrow Z[B]$ by the formula

(4) $f(a_i) = \pi_i \circ m(\beta) \circ h(a)$, $a \in A$, $i = 1,2$,

and we set

(5) $F = r(f)$.

By construction, F : Z[A+A] $\longrightarrow$ Z[B] is a ring-morphism. Moreover, F has the following useful property : aff(F) is the unique monoid-morphism such that

(6) $aff(F) \circ m(\alpha) = m(\beta) \circ h$.

Indeed, in view of the universality of A^* it is enough to show that (6) is valid in every point $a \in A$: $aff(F)(m(\alpha)(a)) = aff(F)(\alpha(a)) = aff(F(a_1, a_2)) = (F(a_1), F(a_2)) = (r(f)(a_1), r(f)(a_2)) = (f(a_1), f(a_2)) = (\pi_1 \circ m(\beta) \circ h(a), \pi_2 \circ m(\beta) \circ h(a)) = (m(\beta) \circ h)(a)$.

To end the proof we display the following equivalences:

$h(u) = h(v) \iff \pi_1 \circ m(\beta)(h(u)) = \pi_1 \circ m(\beta)(h(v))$; (3)

$\iff \pi_1 \circ (m(\beta) \circ h)(u) = \pi_1 \circ (m(\beta) \circ h)(v)$

$\iff \pi_1 \circ (aff(F) \circ m(\alpha))(u) = \pi_1 \circ (aff(F) \circ m(\alpha))(v)$; (6)

$\iff \pi_1 \circ (aff(r(f)) \circ m(\alpha))(u) = \pi_1 \circ (aff(r(f)) \circ m(\alpha))(v)$; (5)

$\iff \pi_1 \circ aff(r(f))(\pi_1 \circ m(\alpha)(u), \pi_2 \circ m(\alpha)(u)) = \pi_1 \circ aff(r(f))(\pi_1 \circ m(\alpha)(v), \pi_2 \circ m(\alpha)(v))$

$\iff \pi_1 \circ (r(f)(\pi_1 \circ m(\alpha)(u)), r(f)(\pi_2 \circ m(\alpha)(u))) = \pi_1 \circ (r(f)(\pi_1 \circ m(\alpha)(v)), r(f)(\pi_2 \circ m(\alpha)(v)))$; def. of aff

$\iff r(f)(\pi_1 \circ m(\alpha)(u)) = r(f)(\pi_1 \circ m(\alpha)(v))$

$\iff r(f)(\pi_1 \circ m(\alpha)(u) - \pi_1 \circ m(\alpha)(v)) = 0$;
$r(f)$ is a ring-morphism

$\iff F(p_{u,v}) = 0$; (2), (5). #

Theorem 2. (Culik II and Karhumäki) Ehrenfeucht Test Set Theorem is equivalent to Word-System Theorem.

Proof. Assume that Word-System Theorem is vaid. Let L be a non-empty subset of A^*. Construct the word-system $S(L) = \{(u, \underline{u})/u \in L\} \subset (A \cup \underline{A})^*$. In view of the Word-System Theorem there exists a finite word-system $S' \subset S(L)$, equivalent to S(L). Take $F = \{u \in L/(u, \underline{u}) \in S'\}$; and note that for each pair of monoid-morphisms $f, g : A^* \to B^*$ we can construct the monoid-morphism $h : (A \cup \underline{A})^* \to B^*$ given by $h(a) = f(a)$; $h(\underline{a}) = g(a)$, for every $a \in A$ such that the following equivalences hold: f, g agree on F $\iff$ h is a solution for S' $\iff$ h is a solution for S $\iff$ f, g agree on L.

Conversely, given a word-system $S \subset A^* \times A^*$ we construct the set $L = \{uv/ (u,v) \in S\} \subset (A \cup \underline{A})^*$ and the monoid-morphisms $f, g : (A \cup \underline{A})^* \to A^*$ given by $f(a) = a$, $f(\underline{a}) = e$ (the null string), $g(a) = e$, $g(\underline{a}) = a$; for all $a \in A$. Clearly, $S = \{(f(u), g(u))/ u \in L\}$. It is obvious that $S' = \{(f(u), g(u))/ u \in F\}$, (where F is a test set for L) is a finite word-system, $S' \subset S$ and S' is equivalent to S. #

3. CONTRASTING HILBERT AND EHRENFEUCHT THEOREMS

Our aim is to show that, **within BISH**, Ehrenfeucht Test Set Theorem and Hilbert Basis Theorem are both equivalent to **LPO**; extending the results in Calude (1986) and Calude and Vaida (1987).

Theorem 3. The following assertions are equivalent :

(i) **LPO**,

(ii) Hilbert Basis Theorem,

(iii) Ehrenfeucht Test Set Theorem.

Proof. (i) $\Rightarrow$ (ii). The proof is by induction on the number of elements of A. If A is empty, then Z[A] reduces to Z. Given now a non-empty subset $T \subset Z$ we construct the subgroup $\langle T \rangle$ generated by T, i.e. the set of all linear combinations of elements in T with integer coefficients. In view of **LPO** there exists a natural n such that $\langle T \rangle = nZ$. We injectively generate, using a dovetailing procedure, all the elements of $\langle T \rangle$ and we compare them to the generator n. Using **Markov's Principle** (if (a_m) is a binary sequence so that it is impossible that $a_m = 0$, for all m , then there exists a natural k such that $a_k = 1$), which is an easy consequence of **LPO**, we get a representation of the form $n = \sum_{i=1}^{m} a_i \cdot t_i$ ($a_i \in Z$, $t_i \in T$), and therefore the basis is $P = \{t_1, \ldots, t_m\}$.

For the induction step we follow Hilbert's original reasoning (see Hilbert (1988-9), Waerden (1950)). As usual one considers a non-empty subset $T \subset Z[A][Y]$, where Y is a new variable, and the ideal (T) generated by T. Let J be the set of the leading coefficients of the polynomials in (T), according to their Y's expansions. The induction hypothesis applies to $J \subset Z[A]$, so that J is generated by a finite number of polynomials $p_1, \ldots, p_m$. In view of the construction of J we can find a finite set of polynomials q_i in (T), of degree d_i, $1 \leq i \leq m$, which have as corresponding leading coefficients exactly the polynomials p_i . We repeat the above procedure for the sets J_k ($1 \leq k \leq \max(d_i)$) which contain the leading coefficients of the polynomials in (T) of degree k.

From now on Hilbert's original proof is constructive and will not be repeated.

(ii) $\Rightarrow$ (iii) Given $L \subset A^*$ we construct the word-system S(L) as in the proof of Theorem 2. For every pair $(u, \underset{\sim}{u}) \in S(L)$ we construct a polynomial $p_u = p_{u,\underset{\sim}{u}}$ as in Theorem 1. Using (ii), from the set of polynomials $T = \{ p_u / u \in L \}$ we can construct a finite subset P such that each polynomial in T is in the ideal generated by P. Take now

$F = \{ u/\ p_u \in P\}$ and notice that $F \subset L$ is finite and by Theorems 1 and 2 it satisfies the requirement in (iii).

(iii) ===> (i). Let (a_n) be a binary sequence and construct the set $L = \{0^{a_{n+1}}\ 1^{a_n} / n \geq 1\} \subset \{0, 1\}^*$. Here for every $x \in \{0,1\}$, $x^0 = e$, $x^k = xx...x$, k copies, for $k > 0$. Let $f, g : \{0,1\}^* \longrightarrow \{0,1\}^*$ be the morphisms given by $f(0) = f(1) = g(0) = 0$, $g(1) = 00$. Obviously, f and g agree on L iff $a_n = 0$, for all n. By (iii) we construct a finite subset $F \subset L$ so that f and g agree on F iff they agree on L, i.e.iff $a_n = 0$ for all n. #

Comment. In Bridges and Richmann (1987),p. 92-93 one sketches a proof of Hilbert Basis Theorem (for a countable discrete ring) by invoking **Markov's Principle** and using some classical reasoning. The present proof does not rely upon any classical reasoning; it makes use of **LPO** (and, as a consequence,of **Markov's Principle**), and it shows that the use of **LPO** cannot be avoided.

The implications (ii) ===> (iii) and (iii) ===> (i) do not use **LPO** or **Markov's Principle**.

4. CONSTRUCTIVE EHRENFEUCHT TEST SET THEOREM

In this section we present a constructive version of Ehrenfeucht Test Set Theorem using Tennenbaum's form of Hilbert Basis Theorem.

Theorem 4. Let $L \subset A^*$. For every sequence $(x_n)_{n \geq 1}$ of elements in L and for every natural k, there exists a natural $s > k$ such that for every pair of monoid-morphisms $f, g : A^* \longrightarrow B^*$, f and g agree on $\{x_1, ..., x_s\}$ iff they agree on $\{x_1, ..., x_{s-1}\}$.

Proof. Given L we construct the language $S(L)$ as in the proof of Theorem 2 and the set of polynomials $T = \{p_u = p_{u,\underline{u}} / u \in L\} \subset Z[X]$ where $X = (A \cup \underline{A}) + (A \cup \underline{A})$. Using Tennenbaum's Theorem (see Mines, Richman and Ruitenberg (1988), Theorems 4.4 and 4.2, p.205-207) we can find a Noetherian basis function for $Z[X]$. The proof is concluded by Theorem 1. #

Comment. In view of Theorems 1 and 2 it follows that Theorem 4 classically implies Hilbert Basis Theorem. By Theorem 3, we deduce that Theorem 4 is classically equivalent to Ehrenfeucht Test Set Theorem, so, according to Seidenberg point of view, it can be considered as a possible constructive version of Ehrenfeucht's condition.

5. REFERENCES

1. M.H.ALBERT and J.LAWRENCE. A proof of Ehrenfeucht's conjecture, **Theoret.Comput.Sci.** 41 (1985),121 - 123 .

2. D. BRIDGES and F.RICHMAN . **Varieties of Constructive Mathematics**, Cambridge University Press, Cambridge, London, New York, New Rochelle, Melbourne, Sydney, 1987.

3. C.CALUDE. Note on Ehrenfeucht's conjecture and Hilbert's basis theorem, **Bull.European Assoc.Theoret.Comput.Sci.** 29(1986), 18-22.

4. C.CALUDE and D.VAIDA. The Ehrenfeucht property and constructivity, **INFO-IASI'87, Proc. 5-th Colloquium on Computer Science**, Iasi, October 9-10, 1987, 1-16 (in Romanian).

5. K.CULIK II and J.KARHUMÄKI. Systems of equations over a free monoid and Ehrenfeucht's conjecture. **Discrete Math.**43 (1983), 139-155.

6. D.HILBERT. Theorie der algebraischen Gebilde, I-III, **Gottinger Nachrichten** (1888), 450-457; (1889), 25-34, 423-430, in D.HILBERT. **Gesammelte Abhandlungen**, Verlag Von Julius Springer, Berlin, 1933.

7. J.KARHUMÄKI. The Ehrenfeucht's conjecture: a compactness claim for finitely generated monoids, **Theoret.Comput.Sci.** 29 (1984), 285-308.

8. R.MINES, F.RICHMAN and W.RUITENBURG. **A Course in Constructive Algebra**, Springer Verlag, New York, Heidelberg, London, Paris, Tokyo, 1988.

9. D.PERRIN. On the solution of Ehrenfeucht's conjecture, **Bull: European Assoc.Theoret.Comput.Sci.** 27 (1985),68-70.

10. E.T.POULSEN. **The Ehrenfeucht Conjecture: An algebra Framework for Its Proof**, Mathematik Institut, Aarhus Universitet 86 (19855), no.14:

11. C.REID. **Hilbert** (with an appreciation of Hilbert's mathematical work by Herman Weyl), Springer-Verlag, Berlin, 1970.

12. A.SALOMAA. The Ehrenfeucht conjecture : a proof for language theorists, **Bull.European Assoc.Theoret.Comput.Sci.** 27 (1985), 71-82.

13. A.SEIDENBERG. What is Noetherian? **Rendiconti del Seminario Matematico e fisico di Milano**, 11 (1975), 55-61.

14. B.L.VAN DER WAERDEN. **Modern Algebra**, vol.II, Friedrik Ungar Publishing Comp., New York, 1950.