ALGEBRAIC METHODS OF AUTOMATED REASONING IN MONADIC LOGIC

by José A. Alonso in Sevilla (Spain)

Introduction

The purpose of this paper is to explain how the theory of Gröbner bases can be used for automated proving in Monadic Logic.

The paper is organized as follows: in Section 1 we recall the syntax and semantics of Monadic Logic, and we describe the aim of this paper: the resolution by an algebraic algorithm of the deduction problem in Monadic Logic. Successively, we reduce the deduction problem in Monadic Logic to the propositional calculus (Section 2), to the ideal membership problem (Section 3), and, finally, to find a Gröbner Base (Section 4). In Section 5 we give some algorithms that solve the problems described above.

Main sources of the paper are Shoenfield [5] and Boolos & Jeffrey [1] for the sections 1 and 2; Hsiang [3] and Kapur & Narendran [4] for the section 2; and Buchberger [2] for the sections 4 and 5.

1.- Preliminaries

A monadic language L consists of: an enumerable set of variables, a set of constants, a set of monadics predicate symbols, the connectives $\neg$ (negation) and $\wedge$ (conjunction) and the universal quantifier $\forall$. The terms of L are the variables and the constants. We shall use the letter t as metavariable ranging over the terms of L. A formula of L is any sequence of symbols of L obtained using the following rules:

(1) if P is a predicate symbol of L and t is a term of L, then Pt is a formula of L (named atomic formula).

(2) if A and B are formulas, then $(\neg A)$ and $(A \wedge B)$ are formulas.

(3) if x is a variable and A is a formula, then $(\forall x A)$ is again a formula.

We shall use capital letters $A, B, C \dots$ as metavariables about formulas. Let us write $(A \vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$ and $(\exists x A)$ to represent $(\neg((\neg A) \wedge (\neg B)))$, $((\neg A) \vee B)$, $((A \rightarrow B) \wedge (B \rightarrow A))$ and $(\neg(\forall x(\neg A)))$, respectively. We shall use the usual rules of elimination of parentheses.

An occurrence of a variable x in a formula A is bound in A if it occurs in a part of A of the form $\exists x B$; otherwise, it is free in A. By $A_{x_1,\dots,x_s}[t_1,\dots,t_s]$ we represent the formula obtained by sustitution, simultaneously, of all free occurrences of the variables $x_1,\dots,x_s$ in A by $t_1,\dots,t_s$, respectively. A variable x is free in a formula A if there is a free occurrence of x in A. A sentence is a formula in which there are no free occurrences of any variables. The set of the sentences of L is denoted by $Sent(L)$.

A L-structure $\mathbf{M}$ consists of: (1) a nonempty set M, called the universe of $\mathbf{M}$; (2) for each constant c of L an element $\mathbf{M}(c)$ in M; (3) for each predicate symbol P of

L, a subset $\mathbf{M}(P)$ of M. For each element a of M, we choose a new constant $\mathbf{a}$. By $L(\mathbf{M})$ we represent the new language obtained by adding to L a new constant $\mathbf{a}$ for each element a of M. For each new constant $\mathbf{a}$ we let $\mathbf{M}(\mathbf{a}) = a$. The set of truth values is the field $\mathbf{Z}_2 = \{0, 1\}$, where 1 means "truth", and 0 means "false". The truth functions $H_\neg : \mathbf{Z}_2 \to \mathbf{Z}_2$ and $H_\wedge : \mathbf{Z}_2^2 \to \mathbf{Z}_2$ of the connectives $\neg$ and $\wedge$ are defined by:

$$H_\neg(u) = \begin{cases} 1, & \text{if } u = 0; \\ 0, & \text{if } u = 1. \end{cases} \qquad H_\wedge(u_1, u_2) = \begin{cases} 1, & \text{if } u_1 = u_2 = 1; \\ 0, & \text{if } u_1 = 0 \text{ or } u_2 = 0. \end{cases}$$

Let A be a sentence of $L(A)$. The truth value of A, $\mathbf{M}(A)$, is defined recursively, by:

$$\mathbf{M}(A) = \begin{cases} 1, & \text{if } A \text{ is } Pt \text{ and } \mathbf{M}(t) \in \mathbf{M}(P); \\ H_\neg(\mathbf{M}(B)), & \text{if } A \text{ is } \neg B; \\ H_\wedge(\mathbf{M}(B), \mathbf{M}(C)), & \text{if } A \text{ is } B \wedge C; \\ 1, & \text{if } A \text{ is } \forall x B \text{ and } \mathbf{M}(B_x[\mathbf{a}]) = 1 \text{ for all } a \in M. \end{cases}$$

An $\mathbf{M}$-occurrence of a formula A is a sentence of $L(\mathbf{M})$ $A_{x_1,\ldots,x_n}[\mathbf{a}_1, \ldots, \mathbf{a}_n]$, where $x_1, \ldots, x_n$ are the free variables of A and $a_1, \ldots, a_n$ are elements of M. A formula A of L is valid in $\mathbf{M}$, $\mathbf{M} \models A$, if $\mathbf{M}(A') = 1$ for every $\mathbf{M}$-occurrence A' of A. $\mathbf{M}$ is a model of A if $\mathbf{M} \models A$. A is valid, $\models A$, if all L-structures are models of A. A is consistent if A has a model. $\mathbf{M}$ is a model of a set Γ of formulas of L, $\mathbf{M} \models \Gamma$, if all the formulas in Γ are valid in $\mathbf{M}$. If Γ has a model, we said that Γ is consistent. A is a consequence of Γ, $\Gamma \models A$, if A is valid in every model of Γ.

The aim of this paper is the resolution by an algebraic algorithm, of the following:

Problem 1. *(Deduction problem in Monadic Logic)*
Given a finite set Γ *of sentences of* L *and a sentence* A *of* L*. Decide whether* $\Gamma \models A$.

2.- From Monadic Logic to Propositional Calculus

From now on let L be the monadic language with constants $c_1, \ldots, c_r$ and predicate symbols $P_1, \ldots, P_m$ and L', the language obtained from L by adding the new constants $c_{r+1}, \ldots, c_n$, where $n = r + 2^m$. For each natural number k, we represent by $[k]$ the set $\{1, 2, \ldots, k\}$.

A proposition of L' is a sentence of L' with no quantifiers. By $\mathbf{P}(L')$ we denote the set of propositions of L'. A valuation of L' is a map v from $\{P_i c_j : i \in [m], j \in [n]\}$ to $\mathbf{Z}_2$. For each valuation v, we consider a map $V : \mathbf{P}(L') \to \mathbf{Z}_2$, defined, recursively, by

$$V(A) = \begin{cases} v(A), & \text{if } A \text{ is atomic;} \\ H_\neg(V(B)), & \text{if } A \text{ is } \neg B; \\ H_\wedge(V(B), V(C)), & \text{if } A \text{ is } B \wedge C. \end{cases}$$

An element A of $\mathbf{P}(L')$ is a tautology, $\models_0 A$, if $V(A) = 1$ for every valuation v. $B \in \mathbf{P}(L')$ is a tautological consequence of a finite subset $\Gamma = \{A_1, \ldots, A_s\}$ of $\mathbf{P}(L')$, $\Gamma \models_0 B$, if $V(B) = 1$ for every valuation v such that $V(A_1) = \cdots = V(A_s) = 1$.

Let us consider the map $\varphi : Sent(L') \to \mathbf{P}(L')$, defined, recursively, by

$$\varphi(A) = \begin{cases} A, & \text{if } A \text{ is atomic;} \\ \neg\varphi(B), & \text{if } A \text{ is } \neg B; \\ \varphi(B) \wedge \varphi(C), & \text{if } A \text{ is } B \wedge C; \\ \varphi(B_x[c_1]) \wedge \cdots \wedge \varphi(B_x[c_n]), & \text{if } A \text{ is } \forall x B. \end{cases}$$

A L'-structure $\mathbf{M}$ is good if for each element a of M there is an element $i \in [n]$ such that $\mathbf{M}(c_i) = \mathbf{a}$.

Lemma 1. *Let* $\mathbf{M}$ *be a good* L*-structure . For every* $A \in Sent(L)$, $\mathbf{M}(A) = \mathbf{M}(\varphi(A))$

Proof: By induction on the length of A. If A is $\forall x B$, we use that $\mathbf{M}(B_x[\mathbf{a}]) = 1$ for all $a \in M$ if and only if $\mathbf{M}(B_x[c_i]) = 1$ for all $i \in [n]$. ∎

Lemma 2. *Let* $A \in Sent(L)$ *be consistent. There exists a model* $\mathbf{M}$ *of* A *such that* $\mathrm{card}(M) \leq 2^m$.

Proof: Let $\mathbf{M}_1$ be a model of A. In the universe M_1 of $\mathbf{M}_1$ we define the following relation $a \equiv b$ if and only if $\mathbf{M}_1(P_i\mathbf{a}) = \mathbf{M}_1(P_i\mathbf{b})$ for every $i \in [m]$. $\equiv$ is an equivalence relation. Let $f : M_1 \to M_1/\equiv$ be such that $f(a) = a/\equiv$ for all $a \in M_1$. Let $\mathbf{M}_2$ be the $L(\mathbf{M}_1)$-structure with universe $M_2 = \{f(a) : a \in M_1\}$ defined by

$$\begin{aligned} \mathbf{M}_2(\mathbf{a}) &= f(a) && \text{for all } a \in M_1; \\ \mathbf{M}_2(c_i) &= f(\mathbf{M}(c_i)) && \text{for all } i \in [r]; \\ \mathbf{M}_2(P_j) &= \{f(a) : a \in \mathbf{M}_1(P_j)\} && \text{for all } j \in [m]. \end{aligned}$$

Let $\mathbf{M}$ be the restriction of $\mathbf{M}_2$ to L (i.e. the universe of $\mathbf{M}$ is M_2, $\mathbf{M}(c_i) = \mathbf{M}_2(c_i)$ for all $i \in [n]$ and $\mathbf{M}(P_j) = \mathbf{M}_2(P_j)$ for all $j \in [m]$). Then $\mathbf{M}$ verifies that $\mathrm{card}(M) \leq 2^m$, since the map $g : M_2 \to \mathbf{Z}_2^m$ defined by $g(f(a)) = (\mathbf{M}_1(P_1(f(a))), \ldots, \mathbf{M}_1(P_m(f(a))))$ is injective. $\mathbf{M} \models A$ since $\mathbf{M}_1(A) = 1$ and

$$\mathbf{M}_1(B_{x_1,\ldots,x_s}[\mathbf{a}_1, \ldots, \mathbf{a}_s]) = \mathbf{M}(B_{x_1,\ldots,x_s}[\mathbf{f}(\mathbf{a_1}) \ldots, \mathbf{f}(\mathbf{a_s})])$$

for every formula B of $L(\mathbf{M}_1)$ and every $(a_1, \ldots, a_s) \in M_1^s$. ∎

Lemma 3. *Let* $A \in Sent(L)$ *and* $\mathbf{M}$ *a model of* A*. There exists a model* $\mathbf{M}'$ *of* A *such that* $\mathrm{card}(\mathbf{M}') = \mathrm{card}(\mathbf{M}) + 1$.

Proof: Let b_0 be an element which is not in M, a_0 a fixed element of M and $M' = M \cup \{b_0\}$. Let $\mathbf{M}'$ be the L'-structure with universe M' defined by:

$$\mathbf{M}'(c_i) = \mathbf{M}(c_i) \qquad \text{for } i \in [n];$$

$$\mathbf{M}'(P_j) = \begin{cases} \mathbf{M}(P_j), & \text{if } a_0 \notin \mathbf{M}(P_j); \\ \mathbf{M}(P_j) \cup \{b_0\}, & \text{if } a_0 \in \mathbf{M}(P_j). \end{cases}$$

We consider that the constants added to L to get $L(\mathbf{M})$ and $L(\mathbf{M}')$ are the same.

$\mathrm{card}(\mathbf{M}') = \mathrm{card}(\mathbf{M}) + 1$ since $b_0 \notin M$.

$\mathbf{M}' \models A$ since $\mathbf{M} \models A$ and $\mathbf{M}(B_{x_1,\ldots,x_s}[\mathbf{a}_0, \ldots, \mathbf{a}_0]) = \mathbf{M}'(B_{x_1,\ldots,x_s}[\mathbf{b}_0, \ldots, \mathbf{b}_0])$ for every formula B of $L(\mathbf{M}')$ with s $(s \geq 0)$ free variables $x_1, \ldots, x_s$. ∎

Lemma 4. *Let $A \in Sent(L)$ be consistent. There exists a model* $\mathbf{M}$ *of* A *with cardinal* 2^m.

Proof: Consequence of lemmas 2 and 3. ∎

Lemma 5. *Let us assume that* $A \in Sent(L')$ *is consistent. Then there exists a good* L*-structure* $\mathbf{M}$ *such that* $\mathbf{M}(A) = 1$.

Proof: Let $\mathbf{M}'$ be a model of A of cardinal 2^m, $M' = \{a_i : i \in [2^m]\}$ and $\mathbf{M}$ the L'-structure with universe M defined by

$$\mathbf{M}(c_i) = \begin{cases} \mathbf{M}'(c_i), & \text{if } i \in [r]; \\ a_{i-r}, & \text{if } i \in [n] - [r]. \end{cases}$$

$$\mathbf{M}(P_j) = \mathbf{M}'(P_j).$$

Then M is good and $\mathbf{M}(A) = \mathbf{M}'(A) = 1$. ∎

Theorem 1. *For each* $A \in Sent(L)$,

$$\models A \text{ if and only if } \models_0 \varphi(A).$$

Proof:

($\Longrightarrow$) Let us assume that $\varphi(A)$ is not a tautology. Then there exists a valuation v of L' such that $V(\varphi(A)) = 0$. Let $\mathbf{M}'$ be the L'-structure with universe $M' = \{c_1, \ldots, c_n\}$ defined by:

$$\begin{array}{ll} \mathbf{M}'(c_i) = c_i, & \text{for } i \in [n]\ ; \\ \mathbf{M}'(P_j) = \{c_i : v(P_j c_i) = 1\} & \text{for } j \in [m]. \end{array}$$

$\mathbf{M}'$ is a good L'-structure. By Lemma 1

$$\mathbf{M}'(A) = \mathbf{M}'(\varphi(A)) = V(\varphi(A)) = 0$$

So, A is no valid.

($\Longleftarrow$) Assume that A is no valid. Then $\neg A$ is consistent. By Lemma 5, there exists a good L'-structure $\mathbf{M}$ such that $\mathbf{M}(\neg A) = 1$. Let v be the valuation defined by

$$v(P_i c_j) = \mathbf{M}(P_i c_j)$$

for $i \in [m]$ and $j \in [n]$. By Lemma 1,

$$V(\varphi(A)) = \mathbf{M}(\varphi(A)) = \mathbf{M}(A) = 0.$$

So, $\varphi(A)$ is not a tautology. ∎

Theorem 2. *Let* $A_1, \ldots, A_s, B$ *be elements of* $Sent(L)$. *Then*

$$\{A_1, \ldots, A_s\} \models B \text{ if and only if } \{\varphi(A_1), \ldots, \varphi(A_s)\} \models_0 \varphi(B).$$

Proof:

$$\begin{array}{lll} \{A_1, \ldots, A_s\} \models B & \Longleftrightarrow & \models A_1 \wedge \cdots \wedge A_s \to B \\ & \Longleftrightarrow & \models_0 \varphi(A_1 \wedge \cdots \wedge A_s \to B) \\ & \Longleftrightarrow & \models_0 \varphi(A_1) \wedge \cdots \wedge \varphi(A_s) \to \varphi(B) \\ & \Longleftrightarrow & \{\varphi(A_1), \ldots, \varphi(A_s)\} \models_0 \varphi(B). \ \blacksquare \end{array}$$

This theorem allows us to reduce Problem 1 to

Problem 2. *(Deduction problem in Propositional Calculus)*
Given a finite subset Γ *of* $\mathbf{P}(L')$ *and an element* A *of* $\mathbf{P}(L')$*. Decide whether* $\Gamma \models_0 A$*.*

3.- From Propositional Calculus to Polynomial Ring

Let $R = \mathbf{Z}_2[X_1, \ldots, X_{mn}]$ be the polynomial ring with coefficients in $\mathbf{Z}_2$. The ideal generated by the finite set $F = \{p_1, \ldots, p_s\}$ is

$$I(F) = I(p_1, \ldots, p_s) = \left\{ \sum_{i=1}^{s} q_i p_i : q_i \in R \right\}$$

In the following, will be denoted by I the ideal generated by

$$F = \{X_1^2 + X_1, \ldots, X_{mn}^2 + X_{mn}\}$$

and for every $p \in R$, $\overline{p} = p + I$.

Let $\theta : P(L') \to R$ be the map defined, recursively, by

$$\theta(A) = \begin{cases} X_{(i-1)n+j}, & \text{if } A \text{ is } P_i c_j; \\ \theta(B) + 1, & \text{if } A \text{ is } \neg B; \\ \theta(B).\theta(C), & \text{if } A \text{ is } B \wedge C. \end{cases}$$

For each valuation v we define a homomorphim $V^* : R \to \mathbf{Z}_2$ by

$$V^*(p) = \begin{cases} 0, & \text{if } p = 0; \\ 1, & \text{if } p = 1; \\ v(P_i c_j), & \text{if } p = X_{(i-1)n+j}; \\ V^*(q) + V^*(r), & \text{if } p = q + r; \\ V^*(q) V^*(r), & \text{if } p = qr \end{cases}$$

By induction on polynomials, we have

Lemma 6. *For each valuation* v*,* $V = V^* \circ \theta$*.*

In the set of monomials of R we define the following relation

$$X_1^{\alpha_1} \cdots X_{mn}^{\alpha_{mn}} >_M X_1^{\beta_1} \cdots X_{mn}^{\beta_{mn}}$$

if and only if (1) $\sum_{1 \le i \le mn} \alpha_i > \sum_{1 \le i \le mn} \beta_i$ or (2) $\sum_{1 \le i \le mn} \alpha_i = \sum_{1 \le i \le mn} \beta_i$ and there exists an element $k \in [mn]$ such that $\alpha_k > \beta_k$ and $\alpha_i = \beta_i$ for all $i \in \{1, \ldots, k-1\}$. The relation $>_M$ is a noetherian total ordering.

Lemma 7. *For every $p \in R$, $p \in I$ if and only if $V^*(p) = 0$ for every valuation v.*

Proof:

($\Longrightarrow$) Is an immediate consequence of the definition of I , since that V^* is a homomorphism and $u^2 + u = 0$ for all $u \in \mathbf{Z}_2$.

($\Longleftarrow$) Let us assume that $p \notin I$. Then there exists an element $q \in p + I$ such that $q = \sum a_{\alpha_1,\ldots,\alpha_{mn}} X_1^{\alpha_1} \cdots X_{mn}^{\alpha_{mn}}$, with $\alpha_i \in \{0, 1\}$. Let $X_1^{\alpha_1} \cdots X_{mn}^{\alpha_{mn}}$ be the minor monomial of q. Let v be the valuation such that $V^*(X_i) = \alpha_i$ for all $i \in [mn]$. Then $V^*(q) = 1$, and $V^*(p) = 1$. ∎

Lemma 8. *Let p, q be elements of R. $\overline{p} = \overline{q}$ if and only if $V^*(p) = V^*(q)$ for every valuation v.*

Proof:

$$\begin{aligned} \overline{p} = \overline{q} \quad &\Longleftrightarrow \quad p - q \in I \\ &\Longleftrightarrow \quad V^*(p - q) = 0 \text{ for every valuation } v \text{ [by Lemma 7]} \\ &\Longleftrightarrow \quad V^*(p) = V^*(q) \text{ for every valuation } v. \ \blacksquare \end{aligned}$$

We define, in $P(L')$, the relation:

$$A \sim B \text{ if and only if } \models_0 A \leftrightarrow B$$

$\sim$ is an equivalence relation in $P(L')$. Let us denote by $[A]$ the class of A (i.e. $[A] = \{B \in P(L') : B \sim A\}$) and by $\mathbf{B}$ the quotient set. We define in $\mathbf{B}$ the operations $+$ and $\cdot$ as follows:

$$\begin{aligned} [A] + [B] &= [\neg(A \leftrightarrow B)] \\ [A] \cdot [B] &= [A \wedge B] \end{aligned}$$

and the elements 0 and 1 by

$$\begin{aligned} 0 &= [\neg(P_1 c_1 \leftrightarrow P_1 c_1)] \\ 1 &= [P_1 c_1 \leftrightarrow P_1 c_1] \end{aligned}$$

$(\mathbf{B}, +, \cdot, 0, 1)$ is a Boolean ring.

Lemma 9. *The map $\theta' : \mathbf{B} \to R/I$ defined by*

$$\theta'([A]) = \overline{\theta(A)}$$

is a ring isomorphism.

Proof:

(a) θ' is well defined and injective: For all $A, B \in P(L')$,

$$\begin{aligned} [A] = [B] \quad &\Longleftrightarrow \quad V(A) = V(B) \text{ for every valuation } v \\ &\Longleftrightarrow \quad V^*(\theta(A)) = V^*(\theta(B)) \text{ for every valuation } v \text{ [by Lemma 6]} \\ &\Longleftrightarrow \quad \overline{\theta(A)} = \overline{\theta(B)} \text{ [by Lemma 8].} \end{aligned}$$

(b) θ' is suprajective, since for every $p \in R$, $\overline{\theta(\theta''(p))} = \overline{p}$, where $\theta'' : R \to P(L')$ is the map defined by

$$\theta''(p) = \begin{cases} X_i, & \text{if } p = X_i; \\ P_1c_1 \leftrightarrow P_1c_1, & \text{if } p = 1; \\ \neg(\theta''(q) \leftrightarrow \theta''(r)), & \text{if } p = q + r; \\ \theta''(q) \wedge \theta''(r), & \text{if } p = qr; \end{cases}$$

(c) θ' is a homomorphism: the proof is straighforward. ∎

By induction on s we can prove the following Lemmas

Lemma 10. *Let $A_1, \ldots, A_s, B$ be elements of $P(L')$.*

$$\theta'([A_1 \wedge \cdots \wedge A_s \to B]) = \overline{p_1 \cdots p_s q + p_1 \cdots p_s + 1},$$

where $p_i = \theta(A_i)$ and $q = \theta(B)$.

Lemma 11. *Let $p_1, \ldots, p_s, q$ be elements of R. Then $\overline{p_1 \cdots p_s(q+1)} = I$ if and only if $\overline{q+1} \in (\overline{p_1 \cdots p_s + 1})$, where $(\overline{p_1 \cdots p_s + 1})$ is the ideal of R/I generated by $\overline{p_1 \cdots p_s + 1}$.*

Lemma 12. *Let $p_1, \ldots, p_s$ be elements of R. Then*

$$(\overline{p_1 \cdots p_s + 1}) = (\overline{p_1 + 1}, \ldots, \overline{p_s + 1}).$$

Theorem 3. *Let $A_1, \ldots, A_s, B$ be elements of $P(L')$. $\{A_1, \ldots, A_s\} \models_0 B$ if and only if*

$$\theta(B) + 1 \in I(\theta(A_1) + 1, \ldots, \theta(A_s) + 1, X_1^2 + X_1, \ldots, X_{mn}^2 + X_{mn}).$$

Proof:

$\{A_1, \ldots, A_s\} \models_0 B \iff$

$\iff \models_0 A_1 \wedge \cdots \wedge A_s \to B$

$\iff [A_1 \wedge \cdots \wedge A_s \to B] = 1$

$\iff \theta'([A_1 \wedge \cdots \wedge A_s \to B]) = \overline{1}$

$\iff \overline{p_1 \cdots p_s q + p_1 \cdots p_s + 1} = \overline{1}$ [by Lemma 10]

$\iff \overline{p_1 \cdots p_s(q+1)} = I$

$\iff \overline{q+1} \in (\overline{p_1 \cdots p_s + 1})$ [by Lemma 11]

$\iff \overline{q+1} \in (\overline{p_1 + 1}, \ldots, \overline{p_s + 1})$ [by Lemma 12]

$\iff$ there exist $r_1, \ldots, r_s \in R$ such that
$\overline{q+1} = \sum_{i=1}^{s} \overline{r_i} \cdot \overline{p_i + 1}$

$\iff$ there exist $r_1, \ldots, r_s, r'_1, \ldots, r'_{mn} \in R$ such that
$(q+1) = \sum_{i=1}^{s} r_i(p_i + 1) + \sum_{j=1}^{mn} r'_j(X_j^2 + X_j)$

$\iff q + 1 \in I(p_1 + 1, \ldots, p_s + 1, X_1^2 + X_1, \ldots, X_{mn}^2 + X_{mn})$

$\iff \theta(B) + 1 \in I(\theta(A_1) + 1, \ldots, \theta(A_s) + 1, X_1^2 + X_1, \ldots, X_{mn}^2 + X_{mn})$. ∎

This theorem allows us to reduce Problem 2 to

Problem 3. *(Ideal membership problem)*
Given a finite subset F of R and an element q of R. Decide whether q is an element of $I(F)$.

4.- Gröbner bases

From now on, we shall use the following syntacticals variables $p, q, q', \ldots$ to represent the polynomials of R; $u, u_1, u_2, \ldots$ for the monomials of R; and $F, G, \ldots$ for finite subsets of R.

Let us assume that the nonzero polynomials are represented by a decreasing sum of monomials, i.e., $p = u_1 + \cdots + u_k$ with $u_1 >_M \cdots >_M u_k$. Let us put $L(p) = u_1$ and $R(p) = u_2 + \cdots + u_k$ to represent the leader of p and the rest of p, respectively.

We consider the relation in R: $p > q$ if and only if (1) $p \neq 0$ and $q = 0$, or (2) $p \neq 0$, $q \neq 0$ and $L(p) >_M L(q)$, or (3) $p \neq 0$, $q \neq 0$, $L(p) = L(q)$ and $R(p) > R(q)$. $>$ is a noetherian total ordering in R.

For each polynomial p and monomial u, we define a map $\rho(p,u) : R \to R$ by $\rho(p,u)(q) = q - \mathrm{coef}(uL(p), q)up$, where $\mathrm{coef}(u,p)$ is the coefficient of u in p.

We say that the polynomial q reduces to q' using the polynomial p and the monomial u, $q \longrightarrow_{p,u} q'$, if $q' = \rho(p,u)(q) \neq q$. $q \longrightarrow_p q'$ means that there exists a monomial u such that $q \longrightarrow_{p,u} q'$, and, if F is a finite set of polynomials, $q \longrightarrow_F q'$ means that there exists a polynomial $p \in F$ such that $q \longrightarrow_p q'$.

It is clear that $\longrightarrow_F \subseteq >$ (i.e. $q \longrightarrow_F q'$ implies that $q > q'$), and so, $\longrightarrow_F$ is noetherian.

By $\stackrel{*}{\longrightarrow}_F$ we represent the reflexive-transitive closure of $\longrightarrow_F$. We say that a polynomial q is F-irreducible if there exists no polynomial q' of R such that $q \longrightarrow_F q'$, and we say that q' is an F-irreducible form of q if q' is F-irreducible and $q \stackrel{*}{\longrightarrow}_F q'$.

Since $\longrightarrow_F$ is noetherian, then for each polynomial there exists, at least, an F-irreducible form. (The F-irreducible form of a polynomial is not unique in general. For instance, if $R = \mathbf{Z}_2[X_1, X_2, X_3]$, and $F = \{X_1 + X_2, X_1 + X_3\}$, then X_2 and X_3 are F-irreducible forms of X_1).

F is a Gröbner base if for each polynomial there exists one and only one F-irreducible form. G is a Gröbner base of $I(F)$ if G is a Gröbner base and $I(G) = I(F)$.

Theorem 4. *(Buchberger 1976) G is a Gröbner base of $I(F)$ iff $I(F) = \{q \in R : q \stackrel{*}{\longrightarrow}_G 0\}$.*

This theorem allows us to reduce Problem 3 to:

Problem 4. *Given a finite set F of polynomials. Find a Gröbner base G of $I(F)$.*

Problem 5. *Given a finite set F of polynomials and a polynomial p. Find an F-irreducible form of p.*

5.- Algorithms and Examples

5.1 Irreducible form

The following algorithm solves Problem 5.

Algorithm 1

Input: A polynomial $p = u_1 + \cdots + u_k$ and a finite set of polynomials $F = \{q_1, \ldots, q_m\}$.

Output: A polynomial q such that q is an F-irreducible form of p.

Procedure $FN(p, F)$:

$$\begin{array}{l} \textbf{while } q \text{ is not } F\text{-irreducible } \textbf{do} \\ \quad j := inf\{i \in [m] : (\exists u)[\rho(q_i, u)(q) \neq q]\} \\ \quad j' := inf\{i \in [k] : (\exists u)[uL(q_j) = u_i]\} \\ \quad q := FN\left(\rho\left(q_j, \dfrac{u'_j}{L(q_j)}\right)(q), F\right) \end{array}$$

Example 1. If $F = \{X_1X_2 + X_1 + 1, X_1^2 + 1\}$ and $p = X_1^3 + X_1X_2^2$, then

$$\begin{aligned} FN(p, F) &= FN(X_1^3 + X_1X_2^2, F) = \\ &= FN(X_1^3 + X_1X_3 + X_2, F) = \\ &= FN(X_1^3 + X_1 + X_2 + 1, F) = \\ &= FN(X_2 + 1, F) = \\ &= X_2 + 1 \end{aligned}$$

5.2 Gröbner bases

We define the S-polynomial of the polynomials q_1 and q_2 by

$$S(q_1, q_2) = \sum_{i=1}^{2} \frac{\text{lcm}((L(q_1), L(q_2))}{L(q_i)} \cdot q_i$$

Since

Theorem 5. *(Buchberger 1976) F is a Gröbner base if and only if for every $q_1, q_2 \in F, S(q_1, q_2) \overset{*}{\longrightarrow}_F 0$.*

The following algorithm solves Problem 4:

Algorithm 2 (Buchberger's algorithm)

Input: A finite set of polynomials $F = \{p_1, \ldots, p_k\}$.
Output: A Gröbner base G of $I(F)$.
Procedure $BG(F)$:

$$
\begin{array}{l}
G := F \\
B := \{(p_i, p_j) : 1 \leq i < j \leq k\} \\
\textbf{while } B \neq \emptyset \textbf{ do} \\
\qquad (q_1, q_2) := \text{first element of } B \\
\qquad B := B - \{(q_1, q_2)\} \\
\qquad h := FN(S(q_1, q_2), G) \\
\qquad \textbf{if } h \neq 0 \textbf{ then } B := B \cup (\{h\} \times G) \\
\qquad \qquad \qquad \qquad G := G \cup \{h\}
\end{array}
$$

Example 2. If

$$F = \{X_2X_4 + X_1 + X_4 + 1, X_3X_4 + X_4, X_1X_2 + X_2\},$$

then

$$BG(F) = F \cup \{X_1X_4 + X_1 + X_4 + 1, X_1X_3 + X_1 + X_3 + 1\}.$$

5.3 Ideal membership problem

The following algorithm solves Problem 3:

Algorithm 3

Input: F and q.
Output: "yes", if $q \in F$; "not", if $q \notin F$.
Procedure:

$$
\begin{array}{l}
\textbf{let } G := BG(F)\textbf{, } q' := FN(q, G) \\
\textbf{if } q' = 0 \textbf{ then } \text{"yes"} \\
\qquad \qquad \textbf{else } \text{"not"}
\end{array}
$$

Example 3. If F is the set of example 2, then $p = X_1X_4 + X_2X_4 \in I(F)$, since $FN(p, BG(F)) = 0$, but $p' = X_1X_4 + X_3X_4 \notin I(F)$, because $FN(p', BG(F)) = X_1 + 1$.

5.4 Deduction in Propositional Calculus

The following algorithm solves the deduction problem in Propositional Calculus (Problem 2):

Algorithm 4

Input: A finite set Γ of propositions in L' and a proposition B of L'.
Output: "yes" if $\Gamma \models_0 B$, "not" otherwise.
Procedure:

$$\begin{aligned}
&F := \{\theta(A)+1 : A \in \Gamma\} \cup \{X_i^2 + X_i : i \in [mn]\}\\
&G := BG(F)\\
&h := FN(\theta(B)+1, G)\\
&\textbf{if } h = 0 \textbf{ then } \text{"yes"} \textbf{ else } \text{"not"}
\end{aligned}$$

Example 4. If

$$\Gamma = \{X_1 \vee X_2, X_2 \leftrightarrow (X_1 \to X_3), X_3 \vee (X_2 \wedge X_4), X_4 \leftrightarrow (X_3 \to X_2)\}$$

and

$$B = X_2 \wedge X_4,$$

then

$$\begin{aligned}
F = \{&X_1X_2 + X_1 + X_2 + 1, X_1X_3 + X_1 + X_3 + 1, X_2X_3X_4 + X_2X_4 + X_3 - 1,\\
&X_2X_3 + X_3 + X_4 + 1, X_1^2 + X_1, X_2^2 + X_2, X_3^2 + X_3, X_4^2 + X_4\}\\
G = F &\cup \{X_2 + 1, X_4 + 1\}\\
h = F&N(X_2X_4 + 1, G) = 0
\end{aligned}$$

So, $\Gamma \models_0 B$.

Using that $F = \{X_i^2 + X_i : i \in [mn]\}$ is a Gröbner bases, the following algorithm solves the validity problem in propositional calculus:

Algorithm 5

Input: A proposition A of $P(L')$.
Output: "yes" if $\models_0 A$, "not" otherwise.
Procedure:

$$\begin{aligned}
&F := \{X_i^2 + X_i : i \in [mn]\}\\
&\textbf{if } FN(\theta(A), F) = 1 \textbf{ then } \text{"yes"} \textbf{ else } \text{"not"}
\end{aligned}$$

Example 5. If $A = (X_1 \to X_2) \vee (X_2 \to X_1)$, then $\theta(A) = X_1^2X_2^2 + X_1^2X_2 + X_1X_2^2 + X_1X_2 + 1$, $FN(\theta(A), F) = 1$ and $\models_0 A$. If $A' = (X_1 \leftrightarrow X_2) \wedge (X_1 \leftrightarrow \neg X_2)$, then $\theta(A') = X_1^2 + X_1 + X_2$, $FN(\theta(A'), F) = 0$ and $\not\models_0 A'$.

5.5 Deduction in Monadic Logic

Let $\psi : Sent(L') \to R$ be the map defined by

$$\psi(A) = \begin{cases} X_{(i-1)n+j}, & \text{if } A \text{ is } P_ic_j;\\ \psi(B)+1, & \text{if } A \text{ is } \neg B;\\ \psi(B)\psi(C), & \text{if } A \text{ is } B \wedge C;\\ \prod_{1\le j\le n} \psi\left(B_x[c_j]\right), & \text{if } A \text{ is } \forall x B \end{cases}$$

It is clear that $\psi = \theta \circ \varphi$, and by Theorems 2 and 3, we obtain the

Theorem 6. *Let* $A_1, \ldots, A_s, B$ *be elements of* $Sent(L)$. *Then* $\{A_1, \ldots A_s\} \models B$ *if and only if*

$$\psi(B) + 1 \in I(\psi(A_1) + 1, \ldots, \psi(A_s) + 1, X_1^2 + X_1, \ldots, X_{mn}^2 + X_{mn}).$$

This theorem allows us to describe an algorithm that solves the deduction problem in the Monadic Logic (Problem 1)

Algorithm 6

Input: A finite set Γ of sentences of L and a sentence B of L.
Output: "yes" if $\Gamma \models A$, "not" otherwise.
Procedure:

$F := \{\psi(A) + 1 : A \in \Gamma\} \cup \{X_i^2 + X_i : i \in [mn]\}$
$G := BG(F)$
$h := FN(\psi(B) + 1, G)$
if $h = 0$ **then** "yes" **else** "not"

Example 6. If

$$\Gamma = \{P_1 c_1, \neg P_1 c_2\}$$

and

$$B = \neg(\forall x)(\forall y)[P_1 x \leftrightarrow P_1 y]$$

then

$$G = \{X_1 + 1, X_2\} \cup \{X_i^2 + X_i : i \in [4]\},$$

$$h = FN(\prod_{1 \leq i,j \leq 4} (X_i + X_j + 1), G) = 0,$$

and

$$\Gamma \models B.$$

The following algorithm solves the validity problem in Monadic Logic:

Algorithm 7

Input: A sentence A of L.
Output: "yes" if $\models A$, "not" otherwise.
Procedure:

$F := \{X_i^2 + X_i : i \in [mn]\}$
if $FN(\psi(A), F) = 1$ **then** "yes" **else** "not"

Example 7. If

$$A = (\exists x)(\forall y)[P_1 x \to P_1 y],$$

then

$$\begin{aligned}\psi(A) = {} & \psi((\forall y)[P_1 c_1 \to P_1 y]) + \psi((\forall y)[P_1 c_2 \to P_1 y]) \\ & + \psi((\forall y)[P_1 c_1 \to P_1 y])\psi((\forall y)[P_1 c_2 \to P_1 y]),\end{aligned}$$

$\psi((\forall y)[P_1c_1 \to P_1y]) = \psi(P_1c \to P_1c_1)\psi(P_1c \to P_1c_2)$,
$\psi(P_1c_1 \to P_1c_1) = X_1^2 + X_1 + 1 \xrightarrow{*}_F 1$,
$\psi(P_1c_1 \to P_1c_2) = X_1X_2 + X_1 + 1$,
$\psi((\forall y)[P_1c_1 \to P_1y]) \xrightarrow{*}_F X_1X_2 + X_1 + 1$.
In the same way,
$\psi((\forall y)[P_1c_2 \to P_1y]) \xrightarrow{*}_F X_1X_2 + X_2 + 1$.
So,

$$\begin{aligned}\psi(A) &\xrightarrow{*}_F (X_1X_2 + X_1 + 1) + (X_1X_2 + X_2 + 1) + (X_1X_2 + X_1 + 1)(X_1X_2 + X_2 + 1) \\ &\xrightarrow{*}_F 1\end{aligned}$$

and $\models A$.

REFERENCES

[1] Boolos, G. and R. Jeffrey Computability and logic. Cambridge Univ. Press, London, 1974.
[2] Buchberger, B., Gröbner Bases: An algorithmic method in polynomial ideal theory. In: Recent trends in multidimensional systems theory (ed. by N.K. Rose), Reidel, 1985, pp. 185–232.
[3] Hsiang, J., Refutational theorem proving using term-rewriting systems. Artificial Intelligence, **25** (1985), 255–300.
[4] Kapur, D. and P. Narendran, An equational approach to theorem proving in first–order predicate calculus. In: 9th IJCAI, Los Angeles, CA, August 1985.
[5] Shoenfield, J.R., Mathematical Logic. Addison Wesley, Mass., 1967.

J.A. Alonso
Departamento de Algebra
Facultad de Matemáticas
Universidad de Sevilla
C/Tarfia s/n
41012–Sevilla
Spain