Instituto de Ciências Matemáticas e de Computação

ISSN - 0103-2577

AN ALGEBRAIC PROBLEM AND THE SOFTWARE MAPLE

MIRIAN PERCIA MENDES

Nº 73

NOTAS DO ICMC
Série Matemática

São Carlos
Mar./1999

An Algebraic Problem and the Software Maple

Mirian Percia Mendes*

February 25, 1999

Abstract

The purpose of this note is to show how we managed to answer an algebraic question that researchers have put for years, namely, if a polynomial in the polynomial ring in several variables belongs to an ideal of this ring. Using the software Maple V, Release 4, we present an algorithm that decides whether a particular polynomial belongs to a particular ideal of the mentioned polynomial ring. A brief introduction describes how our specific algebraic problem appeared and then it is presented together with the notation used.

Key Words. algebraic problem, polynomial ring in several variables, ideal, membership problem

1 Introduction

Studying the immersion problem of some differential manifolds in Euclidean spaces, it was noticed that, from the topological point of view, a good invariant - the first topological invariant - which could give us some results in our research would be the Stiefel-Whitney characteristic classes. As these cohomology classes deal with the specific ring $\mathbb{Z}_2$, we began to work on it. Besides this, we observe "symmetries", or rather, "polynomial symmetries" and finally we came to our algebraic problem. How to arrive at this problem is outside the scope of this note[1], which is to show how the software Maple V, Release 4, helped us in the solution of our specific problem. Introducing some notation and the problem, we would like to draw the readers' attention to the "symmetries" that appear as well as the matrices that arise from them.

2 Presentation of the problem

Here we are going to introduce our problem fixing the notation that will be used.

*Universidade de São Paulo, Instituto de Ciências Matemáticas e de Computação, Departamento de Matemática, São Carlos, SP, Brazil, mpmendes@icmc.sc.usp.br

[1] Please refer to [2] for further information.

Let $\mathbb{Z}_2[x_1,\ldots,x_n]$ be the polynomial ring in n variables $x_1,\ldots,x_n$ and $\sigma_i = \sigma_i(x_1,\ldots,x_n)$ the i^{th} elementary symmetric polynomial in these variables. Then

$$\begin{aligned}
\sigma_1 &= \sigma_1(x_1,\ldots,x_n) = x_1 + \ldots + x_n;\\
\sigma_2 &= \sigma_2(x_1,\ldots,x_n) = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n;\\
&\vdots\\
\sigma_n &= \sigma_n(x_1,\ldots,x_n) = x_1\ldots x_n.
\end{aligned}$$

Let $\mathcal{I}_n =< \sigma_1,\ldots,\sigma_n >$ be the ideal of $\mathbb{Z}_2[x_1,\ldots,x_n]$ generated by the n elementary symmetric polynomials $\sigma_1,\ldots,\sigma_n$.

Let $\tau_k = \tau_k(t_{12},\ldots,t_{n-1n})$ be the k^{th} elementary symmetric polynomial of $\mathbb{Z}_2[x_1,\ldots,x_n]$ in h variables t_{ij} with $i<j$ where $t_{ij} = x_i + x_j$, $h = \sum_{i=1}^{s}\binom{n_i}{2}$ and $\{n_1,\ldots,n_s\}$ is an increasing partition of n with $n_1\ldots n_s \neq 1$. So,

$$\begin{aligned}
\tau_1 = {} & t_{12} + t_{13} + \ldots + t_{1n_1} +\\
& t_{23} + \ldots + t_{2n_1} +\\
& \cdots\\
& t_{n_1-1n_1} +\\
& t_{n_1+1n_1+2} + \ldots + t_{n_1+1n_1+n_2} +\\
& \cdots\\
& t_{n_1+n_2-1n_1+n_2} +\\
& \ddots\\
& \ddots\\
& t_{n_1+\ldots+n_{s-1}+1n_1+\ldots+n_{s-1}+2} + \ldots + t_{n_1+\ldots+n_{s-1}+1n_1+\ldots+n_s} +\\
& \cdots\\
& t_{n_1+\ldots+n_s-1n_1+\ldots+n_s};\\
& \vdots
\end{aligned}$$

$$\begin{aligned}
\tau_h = {} & t_{12}\ t_{13}\ \ldots\ t_{1n_1}\\
& t_{23}\ \ldots\ t_{2n_1}\\
& \cdots\\
& t_{n_1-1n_1}\\
& \ddots\\
& t_{n_1+\ldots+n_{s-1}+1n_1+\ldots+n_{s-1}+2}\cdots t_{n_1+\ldots+n_{s-1}+1n_1+\ldots+n_s}\\
& \cdots\\
& t_{n_1+\ldots+n_s-1n_1+\ldots+n_s}.
\end{aligned}$$

Our problem consists in knowing if the polynomial $\tau_k = \tau_k(t_{ij})$ $(k = 1,\ldots,h)$ belongs to $\mathcal{I}_n$.

First it should be noted that the h variables t_{ij} described previously can be put in an antisymmetric matricial form with blocks of order n_i, $i = 1,\ldots,s$.

Then we have, with the first block of order n_1, a matrix $n_1 \times n_1$ of the form:

$$\begin{pmatrix} 0 & t_{12} & t_{13} & \cdots & t_{1n_1} \\ -t_{12} & 0 & t_{23} & \cdots & t_{2n_1} \\ -t_{13} & -t_{23} & 0 & \cdots & t_{3n_1} \\ \vdots & \vdots & \vdots & & \vdots \\ -t_{1n_1} & -t_{2n_1} & -t_{3n_1} & \cdots & 0 \end{pmatrix}$$

and, with the i^{th} block of order n_i $(i > 1)$, a matrix $n_i \times n_i$ of the form:

$$\begin{pmatrix} 0 & \cdots & t_{n_{i-1}+1n_{i-1}+n_i} \\ -t_{n_{i-1}+1n_{i-1}+2} & \cdots & t_{n_{i-1}+2n_{i-1}+n_i} \\ \vdots & & \vdots \\ -t_{n_{i-1}+1n_{i-1}+n_i} & \cdots & 0 \end{pmatrix}$$

Considering only the upper triangular part of these blocks, we have $\binom{n_1}{2}$ variables with the first block and $\binom{n_i}{2}$ variables with the i^{th} block $(i > 1)$. Bearing this consideration in mind, we finally obtain the h variables t_{ij} $(i < j)$ of $\mathbb{Z}_2[x_1, \ldots, x_n]$ at which we aimed.

3 Preliminaries

All the information here can be found in [1] and [3].

3.1 Orderings on the monomials in $\mathbb{Z}_2[x_1, \ldots, x_n]$

In the case of one variable, the division algorithm gives us the solution of our problem. It must be observed that the key point of this algorithm consists in the idea of ordering on terms in the polynomials in decreasing order by their degree.

So as to generalize this idea for several variables, we need an ordering on terms in the polynomials in $\mathbb{Z}_2[x_1, \ldots, x_n]$. Our ordering must be "compatible" with the algebraic structure of polynomial rings.

Besides this, since a polynomial is a sum of monomials, we would like to be able to arrange these monomials in an unambiguously way so that we can compare them and then establish their positions.

In this sense, we introduce some more notation.

Definition 3.1 *A monomial ordering on $\mathbb{Z}_2[x_1, \ldots, x_n]$ is a total well-ordering $<$ on the set of monomials*

$$\{X^\alpha \in \mathbb{Z}_2[x_1, \ldots, x_n]; X^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}, \alpha_i \in \mathbb{N}, i = 1, \ldots, n\}$$

such that if X^α, X^β are monomials in this set with $X^\alpha < X^\beta$ then $X^\alpha X^\gamma < X^\beta X^\gamma$, for each X^γ monomial in it.

One example of a monomial ordering in our polynomial ring is the lexicographic order. For more examples see [3].

Therefore, if p is a nonzero polynomial in this ring, we can write, for each $\alpha_i = (\alpha_{i_1}, \ldots, \alpha_{i_n}) \in \mathbb{N}^n$, $p = X^{\alpha_1} + X^{\alpha_2} + \ldots + X^{\alpha_r}$ where $X^{\alpha_r} < \ldots < X^{\alpha_2} < X^{\alpha_1}$.

Under this condition, we put $lt(p) = 1X^{\alpha_1}$ and $lt(0) = 0$ and we call it *leading term* (the term of highest degree) of p.

3.2 A division algorithm in $\mathbb{Z}_2[x_1, \ldots, x_n]$

Our goal now is to extend the division algorithm to the polynomial ring that we are dealing with. We have:

Theorem 3.2 *Fix a monomial ordering $<$ on $\mathbb{Z}_2[x_1, \ldots, x_n]$ and let $(g_1, \ldots, g_t)$ be an ordered t-tuples of nonzero polynomials in that ring. Then each $p \in \mathbb{Z}_2[x_1, \ldots, x_n]$ can be written as $p = q_1 g_1 + \ldots + q_t g_t + r$ where $q_i (i = 1, \ldots, t)$ and r belong to this ring. Besides this, either $r = 0$ or it is a $\mathbb{Z}_2$-linear combination of monomials none of which is divisible by any $lt(g_1), \ldots, lt(g_t)$. Under these conditions, we call r a remainder of p in the division of it by the ordered t-tuples $(g_1, \ldots, g_t)$.*

With this result, if after the division of p by $(g_1, \ldots, g_t)$ we get $r = 0$ then $p = q_1 g_1 + \ldots + q_t g_t$ and therefore $p \in < g_1, \ldots, g_t >$, the ideal of $\mathbb{Z}_2[x_1, \ldots, x_n]$ generated by the polynomials $g_1, \ldots, g_t$.

The converse is not true since the remainder r, in the above algorithm, is not uniquely characterized by the requirement that no term of r is divisible by one of $lt(g_1), \ldots, lt(g_t)$ (see [3]). In other words, even if $p \in < g_1, \ldots, g_t >$ we can obtain a nonzero remainder in our division. In this case, we did not have a perfect generalization.

In order to solve such inconvenience, we are going to determine a set of "good" generators for the ideal where the remainder r of the division by them is unique and the condition $r = 0$ is equivalent to p belongs to it.

3.3 Gröbner Bases

The set of "good" generators was introduced for the first time in the middle of the sixties by H. Hironaka and later by B. Buchberger in his PhD thesis. The name "Gröbner bases" was created by Buchberger in honour of W. Gröbner (1899 - 1980).

The idea involved is that once we choose a monomial ordering, each $p \in \mathbb{Z}_2[x_1, \ldots, x_n]$ has a unique leading term $lt(p)$.

Definition 3.3 *Fix a monomial order. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal $\mathcal{I}$ is a Gröbner basis if $< lt(g_1), \ldots, lt(g_t) > = < lt(\mathcal{I}) >$ where $lt(\mathcal{I})$ is the set of leading terms of elements of $\mathcal{I}$.*

We can show that every nonzero ideal $\mathcal{I}$ of $\mathbb{Z}_2[x_1, \ldots, x_n]$ has a Gröbner basis, which is a basis of $\mathcal{I}$.

In the seventies and eighties, Buchberger *et al* devised an algorithm that calculates such bases. With this algorithm, $\tau_k \in \mathcal{I}_n$ if and only if, the remainder r in the division of this polynomial by G, a Gröbner basis for this ideal, is zero. Under these conditions, we call r by normal form of τ_k related to G and we write normalf(τ_k, G).

4 The Software Maple

As it can be observed we have to follow seven steps:

step 1

Given n, the elementary symmetric polynomials σ_i, $i = 1, \ldots, n$ in the n variables $x_1, \ldots, x_n$ needs to be constructed.

step 2

Having the polynomials σ_i and with them the ideal $\mathcal{I}_n$, a Gröbner basis G for this ideal needs to be obtained.

step 3

All the increasing partitions of n, indexing each of them by $PART_i$, must be described.

step 4

Working with partition $PART_i$, our next need is the construction of the matrix $n \times n$, whose blocks are obtained according to this partition.

step 5

Having the matrix, h_i is determined, i.e., the number of variables t_{ij} of the required elementary symmetric polynomial τ_k.

step 6

Now it is possible to know if the polynomial τ_k belongs to the ideal $\mathcal{I}_n$ through the uniqueness of the remainder $RFINAL$.

step 7

Finally, the result is printed.

Considering all this information, by using the software Maple [5] we developed an initial algorithm that gives us:

(1) the elementary symmetric polynomials σ_i in n variables $x_1, \ldots, x_n$;
(2) a Gröbner basis G for the ideal $\mathcal{I}_n$;
(3) the remainders R, in $\mathbb{Z}$, of the division of the polynomials $P_k = \tau_k$ by G;
(4) the remainders $RFINAL$, in $\mathbb{Z}_2$, of the division of P_k by G.

(1) algorithm that calculates the elementary symmetric polynomials σ_i in n variables

```
> n:= : X:=[seq(x[i],i=1..n)]:

> for i from 1 to n do
    with(combinat,choose):
    CB[i]:=choose(X,i):
    with(combinat,numbcomb):
    NCB[i]:=numbcomb(n,i):
    for j from 1 to NCB[i] do
        PCB[i,j]:=product(CB[i][j][kp],kp=1..i)
    od:
    sigma[i]:=sum(PCB[i,l],l=1..NCB[i])
  od:
```

(2) algorithm that calculates a Gröbner basis G for the ideal $\mathcal{I}_n$

```
> with(grobner):
  IDEAL:=[seq(sigma[i],i=1..n)]:
  G:=gbasis(IDEAL,X):
```

algorithm that separates the blocks of a matrix $n \times n$ according to some increasing partition of this n

```
> with(combinat,partition):
  PART:=partition(n):
  with(combinat,numbpart):
  NPART:=numbpart(n)-1:
  for i from 2 to NPART do
   PART[i]:
   with(linalg,vectdim):
   s[i]:=vectdim(PART[i]):
   for jb from 1 to s[i] do
            d[i,jb]:=PART[i][jb]
   od:
   d[i]:=[seq(d[i,kb],kb=1..s[i])]:
   for i1 from 1 to d[i,1]-1 do
            for j1 from i1+1 to d[i,1] do
                     t[i1,j1]:=x[i1]+x[j1]
            od:
            t[i1]:=seq(t[i1,l1],l1=i1+1..d[i,1])
   od:
   y[1]:=seq(t[k1],k1=1..d[i,1]-1):
   for lb from 2 to s[i] do
            A:=sum(d[i,a],a=1..lb-1):
            B:=sum(d[i,b],b=1..lb):
            for ig from A+1 to B-1 do
                     for jg from ig+1 to B do
                              t[ig,jg]:=x[ig]+x[jg]
                     od:
                     t[ig]:=seq(t[ig,lg],lg=ig+1..B)
            od:
            M[lb]:=seq(t[kg],kg=A+1..B-1)
   od:
   y[2]:=seq(M[i2],i2=2..s[i]):
```

algorithm that calculates h the number of variables t_{ij} of a given increasing partition of n

```
YG[i]:=[seq(y[k2],k2=1..2)]:
with(linalg,vectdim):
h[i]:=vectdim(YG[i]):
```

(3) algorithm that calculates the remainders R in $\mathbb{Z}$ of the division of polynomials τ_k by the Gröbner basis G

```
for k from h[i] by -1 to 1 do
 with(combinat,choose):
 COMB[k]:=choose(YG[i],k):
 with(combinat,numbcomb):
 NCOMB[k]:=numbcomb(h[i],k):
 for j from 1 to NCOMB[k] do
          PCOMB[k,j]:=product(COMB[k][j][kr],kr=1..k)
 od:
 tau[i][k]:=sum(PCOMB[k,lr],lr=1..NCOMB[k]):
 with(grobner):
 R[i][k]:=normalf(tau[i][k],G,X):
```

(4) algorithm that calculates the remainders $RFINAL$ in $\mathbb{Z}_2$ of the division of polynomials τ_k by G

```
RFINAL[i][k]:=modp(R[i][k],2):
PR[i,k][1]:=tau[k]=tau[i][k]:
PR[i,k][2]:=RF[k]=RFINAL[i][k]:
PR[i,k]:=[seq(PR[i,k][j],j=1..2)]
  od
od:
```

algorithm that shows us the final result

```
[ >  n:=n;

[ >  for p from 1 to n do sigma[p]:=sigma[p] od;

[ >  G:=G;

[ >  for p from 2 to NPART do PART[p]:= PART[p]:
     h[p]:=h[p]:
     for m from 1 to h[p] do print(PR[p,m]) od
     od;
```

References

[1] ADAMS, W.W.; LOUSTAUNAU, P. *An introduction to Gröbner bases.* Providence, A.M.S., 1994. (Graduate Studies in Mathematics v. 3).

[2] CONDE, A.; MENDES, M.P.; Gröbner bases and the immersions of real flag manifolds in euclidean spaces. Awaiting publication.

[3] COX, D.; LITTLE, J.; O'SHEA, D. *Ideals, varieties and algorithms.* New York, Springer, 1992. (Undergraduate Text Mathematics)

[4] LANG, S. *Linear Algebra.* 3 ed. New York, Springer, 1987.

[5] MAPLE V, RELEASE 4. University of Waterloo. Waterloo Maple Inc. Waterloo, Province of Ontario, Canada, June 1996.

Biography

Mirian P. Mendes received her Doctorate in Mathematical Sciences from the Institute of Mathematical Sciences of São Carlos of the University of São Paulo, Brazil, in 1997 and currently is an assistant professor in the Mathematics Department of that Institute, where she has taught for the last eleven years. Her research interests focus on Differential Topology, but she is also interested in Abstract Algebra.

Resumo

O propósito desta nota é mostrar como nós respondemos, em um caso específico, a uma questão algébrica que pesquisadores têm colocado por anos, a saber: se um polinônmio em um anel polinomial em várias variáveis pertence a um ideal deste anel. Usando o softwre Maple V, Release 4, nós apresentamos um algoritmo que soluciona esse nosso problema. Uma breve introdução descreve como o mesmo surgiu nos nossos estudos e apresenta também a notação usada.

NOTAS DO ICMC

SÉRIE MATEMÁTICA

072/99 BRUCE, J.W.; TARI, F. – Duality and implicit differentials equations.

071/99 SUN, X.; MENEGATTO, V.A. – Stricly positive definite functions on the complex Hilbert sphere.

070/99 MÀNCINI, S.; RUAS, M.A.S.; TEIXEIRA, M.A. – On divergent diagrams of finite codimension.

069/98 LINHARES, O. L.; ANDRADE, E.X.L. DE – Matrizes especiais matrizes de teste.

068/98 CONDE, A.; MENDES, M.P. – Gröbner bases and the immersions of real flag manifolds in Euclidean spaces.

067/98 MOCHIDA, D.K.H.; ROMERO-FUSTER, M.C.; RUAS, M.A.S. – Osculating hyperplanes and asymptotic directions of condimension two submanifolds of euclidean spaces.

066/98 CARVALHO, A.N.; PRIMO, M.R.T. – Boundary synchronization in parabolic problems with nonlinear boundary conditions.

065/98 BRUCE, J.W.; FLETCHER, G.J.; TARI, F. – Bifurcations of binary differential equations.

064/98 BRUSCHI, S.; CARVALHO, A. N.; RUAS-FILHO, J.G. – The dynamics of a one-dimensional scalar parabolic problem versus the dynamics of its discretization.

063/98 LEIVA, H. - A new sufficient algebraic condition for the controllability and observability of linear time varying systems.