Gröbner Bases with ***DERIVE***

Alessandro Perotti

Dip. di Matematica, Università di Milano, Via Saldini 50, I-20133 Milano, Italy

This paper describes an experiment in the use of DERIVE in learning mathematical concepts at an advanced undergraduate level. The chosen topic is the theory of Gröbner bases for ideals of multivariate polynomials, a fundamental tool in computational commutative algebra with applications in many fields. The project led to the preparation of a series of DERIVEfunctions to implement the relevant algorithms for Gröbner basis computation. This work in turn stimulated some research on the explicit description of monomial orderings, a key ingredient of the theory, in a form which can be easily used in computer algebra systems.

1. INTRODUCTION

The work described in this article began as a student project, supervised by the author, to implement Buchberger's algorithm for Gröbner basis computation with *DERIVE*. Computations with multivariate polynomials depend critically on the choice of the ordering for the terms of the polynomials. On one hand, the efficiency of Buchberger's algorithm is influenced by the ordering. On the other hand, the theoretical questions which can be answered using a Gröbner basis impose restrictions on the choice of the ordering. It is then fundamental, in the use of a computer algebra system for Gröbner basis computation, to have great freedom in specifying the ordering. This need stimulated some theoretical work about orderings on $\mathbf{Z}^n$, which in turn gave a simple method to implement in *DERIVE* computations with respect to different monomial orderings.

In sections 2 to 4 we briefly recall definitions and some relevant facts about Gröbner bases. A good reference to Buchberger's theory is, for example, Cox et al, 1992, whose notation we have tried to follow. In section 5 is described the implementation of Buchberger's algorithm for the lexicographic order. Section 6 is devoted to orderings on $\mathbf{Z}^n$. They have been studied by many authors (see for example Carrà Ferro and Sit, 1994, for the vast literature on the subject and for much more). Here we use some results of Robbiano (1985 and 1986) to show that a large class of monomial orderings can be described by means of integral non-singular matrices with nonnegative entries. In sections 7 and 8 the preceding results are applied to implement Buchberger's algorithm in the general case.

The *DERIVE*functions given below have been tested on many examples using version 2.58 of the program. The time necessary to compute Gröbner bases can be quite long compared to other systems. This is due in part to the non-availability of some basic computations involving polynomials (degree, coefficients, etc.) as built in functions.

2. NOTATION AND DEFINITIONS

Let k be the coefficient field and $k[x_1, \ldots, x_n]$ the polynomial ring in n indeterminates $x_1, \ldots, x_n$. Every polynomial f is a sum $\sum_{\alpha \in A} a_\alpha x^\alpha$ of *terms* $a_\alpha x^\alpha$ ($a_\alpha \neq 0$), where A is a finite subset of n-tuples of nonnegative integers $\alpha_1, \ldots, \alpha_n$. A *term* is a product of a nonzero coefficient a_α and a *monomial* $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. The sum $|\alpha| = \alpha_1 + \ldots + \alpha_n$ of the exponents in a monomial is called the *total degree* of the monomial.

Once the order of the variables has been fixed, every monomial is uniquely determined by the n-tuple $\alpha_1, \ldots, \alpha_n$ of its exponents in $\mathbf{Z}^n_{\geq 0}$. A *monomial ordering* is a total ordering on $\mathbf{Z}^n_{\geq 0}$ (or equivalently, on the set of monomials) which is a well-ordering, compatible with the sum of the exponents in $\mathbf{Z}^n_{\geq 0}$: if $\alpha > \beta$, then $\alpha + \gamma > \beta + \gamma$ for any $\gamma \in \mathbf{Z}^n_{\geq 0}$.

Examples: the *lexicographic* order *lex*, defined by $x^\alpha >_{lex} x^\beta$ if the first non-zero component of the vector $\alpha - \beta$ is positive, is a monomial ordering. Another example is the *graded* (or *total*) *lexicographic* order *grlex*, defined by $x^\alpha >_{grlex} x^\beta$ if $|\alpha| > |\beta|$, or $|\alpha| = |\beta|$ and $\alpha >_{lex} \beta$.

Let $f = \sum_{\alpha \in A} a_\alpha x^\alpha$ be a non-zero polynomial and let $>$ be a fixed monomial ordering. The *multidegree* of f is the n-tuple $\mathrm{MDEG}(f) = \max\{\alpha \in \mathbf{Z}^n_{\geq 0}$ such that $a_\alpha \neq 0\}$. The *leading coefficient* of f is $\mathrm{LC}(f) = a_{\mathrm{MDEG}(f)}$, the *leading monomial* is $\mathrm{LM}(f) = x^{\mathrm{MDEG}(f)}$ and the *leading term* is $\mathrm{LT}(f) = \mathrm{LC}(f)\,\mathrm{LM}(f)$.

Examples: with respect to the *lex* order with $x > y$, the polynomial $2x^2y^3 + 5xy^5 - 3xy - 2y + 4$ has multidegree $(2, 3)$ and leading term $2x^2y^3$; with respect to the *grlex* order, the multidegree is $(1, 5)$ and the leading term is $5xy^5$.

3. THE DIVISION ALGORITHM

The choice of a monomial ordering makes it possible to extend the well-known division algorithm for univariate polynomials. Let $F = (f_1, \dots, f_s)$ be an ordered s-tuple of polynomials in $k[x_1, \dots, x_n]$. Every polynomial f can be written as

$$f = q_1 f_1 + q_2 f_2 + \cdots + q_s f_s + r$$

where $\mathrm{MDEG}(f) > \mathrm{MDEG}(q_i f_i)$ for any i such that $q_i f_i \neq 0$ and the *remainder* r is a sum of terms, none of which is divisible by a $\mathrm{LT}(f_i)$.

Remark: the quotients $q_1, \dots, q_s$ and the remainder r depend on the choice of the monomial ordering and, in general, also on the ordering of the divisors $f_1, \dots, f_s$.

The following algorithm gives $q_1, \dots, q_s$ and the remainder r:

```
$q_1 := 0; \dots ; q_s := 0; r := 0$
$p := f$
WHILE $p \neq 0$ DO
    IF there exists a first index $i$ such that $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$ THEN
        $q_i := q_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$
        $p := p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i$
    ELSE
        $r := r + \mathrm{LT}(p)$
        $p := p - \mathrm{LT}(p)$
```

4. GRÖBNER BASES AND BUCHBERGER'S ALGORITHM

Let I be an ideal of polynomials. The subset $\{g_1, \dots, g_s\}$ of I is a *Gröbner basis* of I with respect to a fixed monomial ordering if the monomials $\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)$ generate the *initial ideal* $\langle \mathrm{LT}(I) \rangle$ generated by all the leading terms of elements in I. The set $G = \{g_1, \dots, g_s\}$ is a *reduced Gröbner basis* for I if it is a Gröbner basis such that every element has leading coefficient 1 and for every $g_i \in G$, no monomial of g_i is generated by the leading terms of the other elements of G. This condition guarantees the uniqueness of the reduced Gröbner basis of an ideal.

If $G = \{g_1, \dots, g_s\}$ is a Gröbner basis of an ideal I, then the ambiguity in the definition of a remainder of f on division by $g_1, \dots, g_s$ disappears. In this case, the remainder r is also called the *normal form* of f with respect to G, and denoted by $\mathrm{NF}(f, G)$. Otherwise, it is called the normal form of f with respect to the *ordered* set $(g_1, \dots, g_s)$.

The division algorithm gives the following useful characterization of Gröbner bases. In particular, it provides a membership criterion for the ideal.

Proposition 1: the subset $\{g_1, \dots, g_s\}$ of I is a Gröbner basis of I if and only if for every $f \in I$ the normal form of f with respect to $g_1, \dots, g_s$ is zero.

Buchberger's algorithm is based on a stronger version of the last result. We recall the definition of the *S-polynomial* of f and g:

$$S(f,g) = \frac{x^\gamma}{\mathrm{LT}(f)} f - \frac{x^\gamma}{\mathrm{LT}(g)} g$$

where the monomial x^γ is the *least common multiple* of $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$.

Proposition 2: the subset $G = \{g_1, \ldots, g_s\}$ of I is a Gröbner basis of I if and only if for every pair (i,j), $i \neq j$, the normal form of $S(g_i, g_j)$ with respect to G is zero.

Buchberger's algorithm

Let $F = (f_1, \ldots, f_s)$ be a set of generators of the ideal I. A Gröbner basis $G = (g_1, \ldots, g_t)$ of I is obtained by the following algorithm:

```
$B := \{(i,j) | 1 \leq i < j \leq s\}$
$G := F$
$t := s$
WHILE $B \neq \emptyset$ DO
    select $(i,j) \in B$
    $g := \mathrm{NF}(S(g_i, g_j), G)$
    IF $g \neq 0$ THEN
        $t := t + 1$
        $G := G \cup \{g\}$
        $B := B \cup \{(i,t) | 1 \leq i \leq t - 1\}$
    $B := B - \{(i,j)\}$
```

This algorithm can be made more efficient by giving conditions to know in advance if the normal form of $S(g_i, g_j)$ does not need to be included in the new generating set. We refer the reader to section 2.9 of Cox et al, 1992 for a complete treatment and to the following section for an implementation in *DERIVE*.

5. IMPLEMENTATION OF BUCHBERGER'S ALGORITHM: THE LEX ORDER CASE

In this section we give a set of *DERIVE* functions which implement Buchberger's algorithm with respect to the *lex* order. The symbols `f` and `g` denote polynomials, `v` is a vector containing the (ordered) variables, `ltf` and `ltg` are leading terms, `m1` and `m2` are monomials. Firstly, we must compute the leading term, the multidegree and the S-polynomial of a pair.

```
DEGREE(f,x):=DIMENSION(ITERATES(DIF(ff,x,1),ff,f))-3
TERM(f,i,x):=LIM(DIF(f,x,i),x,0)/i!*x^i
LT_X(f,x):=TERM(f,DEGREE(f,x),x)
LT_LEX_1(f,v,i):=IF(i>DIMENSION(v),f,LT_LEX_1(LT_X(f,ELEMENT(v,i)),v,i+1))
LT_LEX(f,v):=LT_LEX_1(f,v,1)
LT(f,v):=LT_LEX(f,v)
MDEG_AUX(ltf,v):=VECTOR(ELEMENT(v,k)*DIF(ltf,ELEMENT(v,k))/ltf,k,1,DIMENSION (v))
MDEG(f,v):=MDEG_AUX(LT(f,v),v)
MON_LCM_AUX(v,md):=PRODUCT(ELEMENT(v,i)^ELEMENT(md,i),i,DIMENSION(v))
MON_LCM(m1,m2,v):=~
  MON_LCM_AUX(v,MAX(APPEND([MDEG_AUX(m1,v),MDEG_AUX(m2,v)] ‘,[[0,0]])))
S_POLY_AUX(f,g,v,ltf,ltg):=MON_LCM(ltf,ltg,v)*(f/ltf-g/ltg)
S_POLY(f,g,v):=S_POLY_AUX(f,g,v,LT(f,v),LT(g,v))
```

In the definition of the function MON_LCM, which computes the LCM of two monomials, it has been necessary to append the row $(0, 0)$ to the row of the multidegrees in order to let the function MAX behave coherently in the univariate case.

Now we implement the division algorithm. For our purpose, it is sufficient to give the normal form of f with respect to the vector of divisors denoted by ff. The vector ltff contains the leading terms of the divisors, ltp and mdegp are respectively the leading term and the multidegree of the polynomial p.

```
NF_4(p,ltp,mdegp,ff,ltff,v,r,i):=~
  IF(mdegp>=MDEG_AUX(ELEMENT(ltff,i),v),[p-ELEMENT(ff,i)*ltp/ELEMENT(ltff,i),r],~
  IF(i<DIMENSION(ff),NF_4(p,ltp,mdegp,ff,ltff,v,r,i+1),[p-ltp,r+ltp]))
NF_3(p,ltp,ff,ltff,v,r,i):=NF_4(p,ltp,MDEG_AUX(ltp,v),ff,ltff,v,r,i)
NF_2(w,ff,ltff,v):=IF(ELEMENT(w,1)=0,w,~
  NF_3(ELEMENT(w,1),LT(ELEMENT(w,1),v),ff,ltff,v,ELEMENT(w,2),1),~
  NF_3(ELEMENT(w,1),LT(ELEMENT(w,1),v),ff,ltff,v,ELEMENT(w,2),1))
NF_1(f,ff,ltff,v):=ELEMENT(ITERATE(NF_2(w,ff,ltff,v),w,[f,0]),2)
NF(f,ff,v):=NF_1(f,ff,VECTOR(LT(ELEMENT(ff,i),v),i,DIMENSION(ff)),v)
```

Here is Buchberger's algorithm. The input $F = (f_1, \dots, f_s)$ is stored as the first line of the matrix g, which contains also the leading terms and the multidegrees of the polynomials. This matrix is updated every times a new element of the Gröbner basis is found. The order of selection of the pairs (i, j), $i < j$, is inverse lexicographic: $(1, 2), (1, 3), (2, 3), \dots$. The function SUCC(ij) finds the successor of (i, j) in the list, and j is used for the stopping test: when it is greater than the number t of generators, the Gröbner basis has been found.

Two criteria to exclude useless pairs have been implemented: the first one (COND1) tests for equality of the product $\mathrm{LT}(g_i)\,\mathrm{LT}(g_j)$ and the $\mathrm{LCM}(\mathrm{LT}(g_i), \mathrm{LT}(g_j))$; the second one (COND2) checks for divisibility of $\mathrm{LCM}(\mathrm{LT}(g_i), \mathrm{LT}(g_j))$ by $\mathrm{LT}(g_k)$, for a $k \neq i, j$ belonging to a previously considered pair.

```
COND1(mdegi,mdegj):=IF(mdegi+mdegj=MAX([mdegi,mdegj]`),0,1,1)
COND2_AUX(g,i,mdegi,mdegj,k):=IF(k=i,1,~
  IF(MAX([mdegi,mdegj]`)>=ELEMENT(g,3,k),0,COND2_AUX(g,i,mdegi,mdegj,k+1)))
COND2(g,i,mdegi,mdegj):=COND2_AUX(g,i,mdegi,mdegj,1)
SUCC(ij):=IF(ELEMENT(ij,1)+1<ELEMENT(ij,2),ij+[1,0],[1,ELEMENT(ij,2)+1])
S_POLY_AUX1(f,g,v,ltf,ltg,mdegf,mdegg):=~
  MON_LCM_AUX(v,MAX(APPEND([mdegf,mdegg]`,[[0,0]])))*(f/ltf-g/ltg)
B_5(ij,g,v,t,ss,ltss):=[SUCC(ij),APPEND(g`,[[ss,ltss,MDEG_AUX(ltss,v)]])`,t+1]
B_4(ij,g,v,t,ss):=~
  IF(ss=0,[SUCC(ij),g,t],B_5(ij,g,v,t,ss,LT(ss,v)),B_5(ij,g,v,t,ss,LT(ss,v)))
B_3(ij,g,v,t,gi,gj):=~
  IF(NOT(COND1(ELEMENT(gi,3),ELEMENT(gj,3))),~
  IF(NOT(COND2(g,ELEMENT(ij,1),ELEMENT(gi,3),ELEMENT(gj,3))),~
  B_4(ij,g,v,t,NF_1(S_POLY_AUX1(ELEMENT(gi,1),ELEMENT(gj,1),v,ELEMENT(gi,2),~
  ELEMENT(gj,2),ELEMENT(gi,3),ELEMENT(gj,3)),ELEMENT(g,1),ELEMENT(g,2),v)),~
  [SUCC(ij),g,t],[SUCC(ij),g,t]),[SUCC(ij),g,t])
B_2(w_,v):=IF(ELEMENT(w_,1,2)>ELEMENT(w_,3),w_,~
  B_3(ELEMENT(w_,1),ELEMENT(w_,2),v,ELEMENT(w_,3),ELEMENT(ELEMENT(w_,2)`,~
  ELEMENT(w_,1,1)),ELEMENT(ELEMENT(w_,2)`,ELEMENT(w_,1,2))))
B_1(ff,v,t):=ELEMENT(ITERATE(B_2(w_,v),~
  w_,[[1,2],APPEND(ff,[VECTOR(MDEG_AUX(ELEMENT(ff,2,i),v),i,t)]),t]),2,1)
```

```
BUCHBERGER(f,v):=B_1([f,VECTOR(LT(ELEMENT(f,i),v),i,DIMENSION(f))],v,DIMENSION(f))
```

6. ORDERINGS ON $\mathbf{Z}^n$

Definition 1: we call an *ordering* on $\mathbf{Z}^n$ any total ordering compatible with addition in $\mathbf{Z}^n$.

Every monomial ordering $>$ extends to a unique ordering on $\mathbf{Z}^n$. To see this, given $\alpha, \beta \in \mathbf{Z}^n$, let $\gamma(\alpha, \beta)$ be the smallest element (with respect to the well-ordering $>$) of the non-empty set $\{\gamma' \in \mathbf{Z}^n_{\geq 0} | \alpha - \beta + \gamma' \in \mathbf{Z}^n_{\geq 0}\}$. Then we say $\alpha > \beta$ if and only if $\alpha - \beta + \gamma(\alpha, \beta) > \gamma(\alpha, \beta)$ in $\mathbf{Z}^n_{\geq 0}$. Since $\gamma(\alpha + \delta, \beta + \delta) = \gamma(\alpha, \beta)$ for every $\alpha, \beta, \delta \in \mathbf{Z}^n$, this induced ordering is compatible with the addition in $\mathbf{Z}^n$.

Definition 2: a matrix A in $\mathrm{GL}(n, \mathbf{Z})$ induces an ordering $>_A$ on $\mathbf{Z}^n$ by defining

$$\alpha >_A \beta \qquad \text{if and only if} \qquad \alpha A >_{lex} \beta A$$

Examples: the *lex* order is induced by the identity matrix I_n; the *grlex* order, the *graded inverse lex order* (*grevlex*) and the *inverse lex order* (*invlex*) (see Cox et al, 1992 section 2.2) are induced by the matrices

$$A_{grlex} = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix} \quad A_{grevlex} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \cdots & 1 & 0 \\ \vdots & & & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix} \quad A_{invlex} = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ \vdots & & \vdots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}$$

In the following, we shall show that a large class of monomial orderings can be obtained in such a way.

Robbiano (1985 and 1986) has proved that *every* total ordering on $\mathbf{Z}^n$ is induced (in the sense given above) by a *real* nonsingular matrix. In fact, every such ordering extends to a (not necessarily unique) continuous ordering on $\mathbf{R}^n$ (with the euclidean topology). Then it is shown possible to find an orthogonal basis of $\mathbf{R}^n$ whose elements are positive with respect to the ordering. The matrix whose columns are the vectors of the basis in decreasing order induces the ordering on $\mathbf{R}^n$.

The following result, whose easy proof we omit, gives the relation existing between matrices which induce the same ordering.

Proposition 3: two matrices $A, B \in \mathrm{GL}(n, \mathbf{R})$ induce the same ordering on $\mathbf{R}^n$ if and only if they define the same right lateral modulo the (non-normal) subgroup T^+ of upper triangular matrices with positive diagonal. In particular, $A, B \in \mathrm{GL}(n, \mathbf{Z})$ induce the same ordering on $\mathbf{Z}^n$ if and only if $B = AU$, where U is an upper triangular, integer matrix with only 1 on the diagonal.

Definition 3: an ordering $>$ on $\mathbf{Z}^n$ will be called *rational* if there exists a nonsingular rational matrix which induces $>$.

Examples: all the orderings shown above are rational; the following is an example of a non-rational ordering on $\mathbf{Z}^2$: $\alpha > \beta$ if and only if $\sqrt{2}\alpha_1 + \alpha_2 > \sqrt{2}\beta_1 + \beta_2$.

Other rational orderings are *product orders* constructed from two (or more) rational orders (see section 2.4 of Cox et al, 1992): in this case an inducing matrix is the direct sum of the matrices of the given orderings. Another class of rational orderings on $\mathbf{Z}^n$ is given by the *elimination orders* $>_k$ (Bayer and Stillman, 1987): $\alpha >_k \beta$ if and only if $\alpha_1 + \cdots + \alpha_k > \beta_1 + \cdots + \beta_k$, or $\alpha_1 + \cdots + \alpha_k = \beta_1 + \cdots + \beta_k$ and $\alpha >_{grevlex} \beta$. A matrix corresponding to $>_k$ is the following

$$A_{>_k} = \begin{pmatrix} 1 & & & & & & \\ \vdots & & \mathrm{O} & & & A^{k-1} & \\ 1 & & & & & & \\ 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & & & & & & \\ \vdots & & A^{n-k} & & & \mathrm{O} & \\ 0 & & & & & & \end{pmatrix}$$

where A^i denote the square matrix of order i associated to *grevlex*.

Proposition 4: every rational ordering $>$ is induced by a matrix $A \in \mathrm{GL}(n, \mathbf{Z})$.

Proof: let B be a rational matrix inducing $>$. By means of elementary column operations, the transpose matrix B^T can be transformed into its *Hermite form* H, which is a non-negative, lower triangular matrix. Then $H = B^T K$, where $K \in \mathrm{GL}(n, \mathbf{Z})$. Set $U = H^T$ and $A = (K^T)^{-1}$ and get $AU = B$. □

Now we return to monomial orderings. They are characterized by the following condition (see Corollary 2.4.6 in Cox et al, 1992):

Proposition 5: an ordering on $\mathbf{Z}^n$ restricts to a monomial ordering if and only if every non-zero vector in $\mathbf{Z}^n_{\geq 0}$ is positive with respect to the ordering.

Proposition 6: every rational monomial ordering $>$ is induced by a non-negative matrix in $\mathrm{GL}(n, \mathbf{Z})$.

Proof: let $A \in \mathrm{GL}(n, \mathbf{Z})$ a matrix which induces $>$. For every element e_j of the standard basis of $\mathbf{Z}^n$, we get from Proposition 5 that $e_j A >_{lex} 0$. This means that the rows of A are positive with respect to the *lex* order. By adding to every column an integral linear combination of the preceding columns, A can be transformed into a non-negative matrix. □

This result gives an easy method to compute the leading term with respect to any rational monomial ordering. Let $f \in k[x_1, \dots, x_n]$ be a polynomial and $A = (a_{ij}) \in \mathrm{GL}(n, \mathbf{Z})$ a non-negative matrix corresponding to the ordering $>$. Consider the following change of variables

$$x_i = \prod_{j=1}^{n} y_j^{a_{ij}}$$

Then the leading term of $f(x_1, \dots, x_n)$ with respect to $>$ is the monomial obtained by applying the inverse transformation (in general, a rational transformation) to the leading term of $f(y_1, \dots, y_n) \in k[y_1, \dots, y_n]$ with respect to the *lex* order.

Remark: in order to construct Gröbner bases, it is sufficient to consider rational monomial orderings, since any real matrix can be approximated by a rational one.

7. IMPLEMENTATION OF BUCHBERGER'S ALGORITHM: THE RATIONAL CASE

We redefine the functions `LT`, `NF` and `BUCHBERGER` to include the possibility of specifying a monomial ordering. For four orderings, *lex*, *grlex*, *grevlex* and *invlex*, the inducing matrices (see section 6) are given by the function `ORD_MATRIX`. The ordering is chosen by name or by number (from 1 to 4) and stored in the variable `ord`. For other orderings, it is sufficient to provide a corresponding non-negative matrix belonging to $\mathrm{GL}(n, \mathbf{Z})$ as last argument of the functions `LEADING_TERM`, `NF` or `BUCHBERGER` (the function `LT` is used internally by the functions `NF` and `BUCHBERGER`). For elimination orders $>_k$, this matrix is given by the function `EL_ORD_MATRIX(k,n)`.

```
v:=[x,y]
v_:=[y_1,y_2,y_3,y_4,y_5,y_6,y_7,y_8,y_9,y_10]
[ord:=(lex:=1),grlex:=2,grevlex:=3,invlex:=4]
E__(n,i):=ELEMENT(IDENTITY_MATRIX(n),i)
ORD_MATRIX(ord,n):=IF(ord=1,IDENTITY_MATRIX(n),~
  IF(ord=2,APPEND(APPEND([VECTOR(1,i,n-1)],IDENTITY_MATRIX(n-1))`,[E__(n,1)]),~
  IF(ord=3,VECTOR(VECTOR(IF(i+j<n+2,1,0),j,n),i,n),~
  IF(ord=4,VECTOR(E__(n,n-i+1),i,n),?))))
ZERO_MATRIX(m,n):=0*[E__(m,1)]` . [E__(n,1)]
EL_ORD_MATRIX(k,n):=APPEND([VECTOR(IF(i>k,0,1),i,n)],~
  IF(k<n,APPEND(ZERO_MATRIX(k,n-k),ORD_MATRIX(3,n-k))`,[]),~
  IF(k>1,APPEND(ORD_MATRIX(3,k-1),ZERO_MATRIX(n-k+1,k-1))`,[]))`
LOG_V(v):=VECTOR(LOG(ELEMENT(v,i)),i,DIMENSION(v))
EXP_V(v):=VECTOR(EXP(ELEMENT(v,i)),i,DIMENSION(v))
LT_ORD(f,v,v_y):=~
  LIM(LT_LEX(LIM(f,v,EXP_V(ord_m . LOG_V(v_y))),v_y),v_y,EXP_V(ord_minv . LOG_V(v)))
LT(f,v):=IF(ord_=1,LT_LEX(f,v),LT_ORD(f,v,v_y),LT_ORD(f,v,v_y))
DEF_ORD(v,ord):=[v_y:=VECTOR(ELEMENT(v_,i),i,DIMENSION(v)),~
  ord_m:=IF(DIMENSION(ord)>0,ord,?,ORD_MATRIX(ord,DIMENSION(v))),~
  ord_minv:=IF(DIMENSION(ord)>0,ord^(-1),?,ORD_MATRIX(ord,DIMENSION(v))^(-1))]
LEADING_TERM_0(f,v):=LT_ORD(f,v)
LEADING_TERM(f,v,ord):=IF(ord=1,LT_LEX(f,v),LEADING_TERM_0(f,v, DEF_ORD(v,ord)))
NF_0(f,ff,v):=NF_1(f,ff,VECTOR(LT(ELEMENT(ff,i),v),i,DIMENSION(ff)),v)
NF(f,ff,v,ord):=NF_0(f,ff,v,ord_:=ord,DEF_ORD(v,ord))
B_0(f,v):=B_1([f,VECTOR(LT(ELEMENT(f,i),v),i,DIMENSION(f))],v,DIMENSION(f))
BUCHBERGER(f,v,ord):=B_0(f,v,ord_:=ord,DEF_ORD(v,ord))
```

The change of variables is performed by the function LT_ORD by means of the functions EXP_V and LOG_V which map exp and log to the vectors of variables.

The variable ord can be assigned as argument of the functions LEADING_TERM, NF and BUCHBERGER (in this case the ordering is fixed only for that calling of the functions) or it can be used as an option to change the ordering for the following. The same holds for the vector v of ordered variables. The predefined ordering is *lex* order and the predefined variables are (x, y), with x preceeding y.

Examples:

```
[v:=[x,y],ord:=lex]
LEADING_TERM(x*y^2-y^4+2*x)
```

$$x\,y^2$$

```
BUCHBERGER([x*y^2-y^4+2*x,x^2*y^3-y])
```

$$\left[xy^2+2x-y^4, x^2y^3-y, 2x^2y-4xy-y^7+2y^5+y, 2x^2-8x+\frac{y^8}{2}-2y^6+4y^4-\frac{y^2}{2},\right.$$
$$\left.-4x-\frac{y^{10}}{4}+\frac{y^8}{2}-y^6+\frac{9}{4}y^4+\frac{y^2}{2}, -\frac{y^{11}}{8}+\frac{y^5}{8}+\frac{y^3}{2}+\frac{y}{2}\right]$$

```
VECTOR(LEADING_TERM(x*y^2-y^4+2*x,v,ord),ord,1,4)
```

$$\left[xy^2, -y^4, -y^4, -y^4\right]$$

```
BUCHBERGER([x*y^2-y^4+2*x,x^2*y^3-y],v,[[5,2],[2,1]])
```

$$\left[xy^2+2x-y^4, x^2y^3-y, 2x^2y-4xy-y^7+2y^5+y, 2x^3y+xy-y^3, 2x^3+x-y^2\right]$$

8. THE REDUCED GRÖBNER BASIS

Given a Gröbner basis $F = \{f_1, \ldots, f_s\}$, a reduced Gröbner basis G can be obtained by the following algorithm:

```
$G := F$
FOR all $g \in G$ DO
    IF there exists $h \in G$, $h \neq g$, such that LT($h$) divides LT($g$) THEN
        $G := G - \{g\}$
    ELSE
        $g := \mathrm{NF}(g, G - \{g\})$
FOR all $g \in G$ DO
    $g := \frac{g}{\mathrm{LC}(g)}$
```

To implement this algorithm, we need to compute the leading coefficient of a polynomial and to provide a function `DIV_MON` which tests for divisibility of monomials.

```
LC1(ltf,v):=LIM(ltf,v,VECTOR(1,i,DIMENSION(v)))
LC(f,v):=LC1(LT(f,v),v)
DIV_MON1(mdeg_v,i,j):=~
  IF(j>DIMENSION(mdeg_v),1,IF(ELEMENT(mdeg_v,j)<=ELEMENT(mdeg_v,i),0,~
  IF(j+1/=i,DIV_MON1(mdeg_v,i,j+1),DIV_MON1(mdeg_v,i,j+2))))
DIV_MON(mdeg_v,i):=DIV_MON1(mdeg_v,i,IF(i>1,1,2))
DELETE_ELEMENT(v,k):=~
  APPEND(VECTOR(ELEMENT(v,i),i,k-1),VECTOR(ELEMENT(v,j),j,k+1,DIMENSION(v)))
```

(this function comes from *DERIVE*'s utility file `VECTOR.MTH`)

```
EE__(n,m,i,j):=[E__(n,i)]‘ .  [E__(m,j)]
E_(a,i,j,v):=a+EE__(DIMENSION(a),DIMENSION(a‘),i,j)*(v-ELEMENT(a,i,j))
R_2(g,d,i,v):=~
  IF(i>d OR d=1,VECTOR(ELEMENT(g,1,j)/LC1(ELEMENT(g,2,j),v),j,d),~
  IF(DIV_MON(ELEMENT(g,3),i),R_2(DELETE_ELEMENT(g‘,i)‘,d-1,i,v),~
  R_2(E_(g,1,i,NF_1(ELEMENT(g,1,i),DELETE_ELEMENT(ELEMENT(g,1),i),~
  DELETE_ELEMENT(ELEMENT(g,2),i),v,0)),d,i+1,v)))
R_1(ff,d,v):=~
  R_2(APPEND(ff,[VECTOR(MDEG_AUX(ELEMENT(ff,2,i),v),i,d)]),d,1,v)
R_0(f,v):=~
  R_1([f,VECTOR(LT(ELEMENT(f,i),v),i,DIMENSION(f))],DIMENSION(f),v)
REDUCE(f,v,ord):=R_0(f,v,ord_:=ord,DEF_ORD(v,ord))
GROEBNER(f,v,ord):=REDUCE(BUCHBERGER(f,v,ord),v,ord)
```

Examples:

```
REDUCE([x*y^2+2*x-y^4,x^2*y^3-y,2*x^2*y-4*x*y-y^7+2*y^5+y,
  2*x^2-8*x+y^8/2-2*y^6+4*y^4-y^2/2,-4*x-y^10/4+y^8/2-y^6+9*y^4/4+y^2/2,
  -y^11/8+y^5/8+y^3/2+y/2],[x,y],lex)
```

$$\left[x+\frac{y^{10}}{16}-\frac{y^8}{8}+\frac{y^6}{4}-\frac{9}{16}y^4-\frac{y^2}{8},y^{11}-y^5-4y^3-4y \right]$$

```
GROEBNER([x*y^2-y^4+2*x,x^2*y^3-y],[x,y],grlex)
```

$$\left[-x*y^2-2x+y^4,x^2y^3-y,x^3+\frac{x}{2}-\frac{y^2}{2} \right]$$

```
GROEBNER([x^2+y^2+z^2+w^2,x^2+2*y^2-y*z-w^2,x+z^3-w^3],
  [x,y,z,w],grlex)
```

$$\left[x^{2}+yz+2z^{2}+3w^{2},x+z^{3}-w^{3},y^{2}-yz-z^{2}-2w^{2}\right]$$

```
GROEBNER([x^2+y^2+z^2+w^2,x^2+2*y^2-y*z-w^2,x+z^3-w^3],
  [x,y,z,w],EL_ORD_MATRIX(1,4))
```

$$\left[x+z^{3}-w^{3},y^{2}-yz-z^{2}-2w^{2},yz+z^{6}-2w^{3}z^{3}+2z^{2}+w^{6}+3w^{2}\right]$$

REFERENCES

Bayer,D. and Stillman,M. (1987). *A theorem on refining division orders by the reverse lexicographic order.* Duke J.Math., 55, 321-328

Becker,T. and Weispfenning,V. (1993). *Gröbner bases*, Springer-Verlag, New York-Berlin-Heidelberg

Carrà Ferro,G. and Sit,W. (1994). On Term-Orderings and Rankings. In Fischer,K., Loustaunau,P., Shapiro,K., Green,E., Farkas,D. (eds.). *Computational algebra*, Lecture Notes in Pure and Applied Mathematics Vol.151, 31-77.

Cox,D., Little,J., O'Shea,D. (1992). *Ideals, Varieties, and Algorithms*, Springer-Verlag, New York-Berlin-Heidelberg

Robbiano,L. (1985). *Term orderings on the polynomial ring.* Proceedings EUROCAL 1985, LNCS 204, 513-517

Robbiano,L. (1986). *On the theory of graded structures.* J.Symb.Comp., 2, 139-170

BIOGRAPHICAL NOTE

Alessandro Perotti is a researcher of mathematics at the Department of Mathematics of the University of Milan, Italy. His main research area is that of Several Complex Variables, but he is interested also in using technology in teaching and learning mathematics at the undegraduate level. In 1992 he co-authored two books on using *DERIVE* as a teaching tool: Manara,M.P. and A.Perotti, *Algebra lineare e geometria con DERIVE* and Bacchelli,B., Lorenzi,A., Perotti,A., *Analisi matematica con DERIVE*, both published by McGraw-Hill Italia.