The computation required 15 seconds CPU time.

The computations were carried out on the CDC Cyber 76 of the
Rechenzentrum of the Universität zu Köln.

References

[2] E.L. Cohen, The diophantine equation \( x^2 + 11 = 3^k \) and related
    Torino (math.) 11 (1875-76), 928 - 937.
[5] E. Lucas, Théorie des fonctions numériques simplement périodiques,
    equations, EUROCAL 84, Lect. Notes in Computer Sc. 174, 378 - 385,
    Springer Verlag 1984.
[7] A. Schinzel, On two theorems of Gelfond and some of their appli-

TERM ORDERINGS ON THE POLYNOMIAL RING

LORENZO ROSSIANO +

Istituto Matematico dell'Università di Genova
Via L. B. Alberti 4, 16132 Genova Italy

The purpose of this paper is to give an account on some research, which was done
on the graded structures arising in commutative and computer algebra.
The main body of such investigation will appear elsewhere (see [R]), so here I
want to point out mainly one aspect, which is strongly connected with the branch
of computer algebra which deals with polynomial rings. I am referring to the
concept of Gröbner base (G-base), which was introduced by Buchberger (see [S1]
and [S2]) and later studied and developed by many other authors (see the references
given in [S3]), nowadays G-bases are understood to be the technical device which
allows to perform algorithms suitable for the most essential computations in the
polynomial ring. In [R] also a theoretical approach is given, which shows the
strict connection between the ideas and methods of the theory of G-bases and
those of other typical concepts of commutative algebra.

So let me first mention what is the background of the concept of G-base.
Let \( A = k[x_1, \ldots, x_n] \) be the polynomial ring with \( n \) indeterminates over a field
\( k \) and let \( T \) denote the set of terms (i.e. monomials with coefficient 1) in \( A \).

Definition 1. A term ordering on \( A \) is a total ordering \( \prec \) on \( T \) such that
a) \( 1 \prec M \) for every \( M \in T \), \( M \neq 1 \).
b) For every \( M_1, M_2, M \in T \) with \( M_1 \prec M_2 \) then \( M_1 \cdot M \prec M_2 \cdot M \).

Let now \( \phi : T \rightarrow \mathbb{N}^n \) denote the map which associates to every term the \( n \)-uple of
exponents; then of course \( \phi \) is an isomorphism between the multiplicative semigroup
\( T \) and the additive semigroup \( \mathbb{N}^n \). So, after this identification, we can say that
a term ordering on \( A \) is a total ordering \( \prec \) on \( \mathbb{N}^n \), such that \( (\mathbb{N}^n, \prec) \) is a totally
ordered positive semigroup.

+ This work was done while the author was visiting the M.P.I. (Max-Planck-
Institut für Mathematik) in Bonn, during the winter semester 1984-85.
Now, it is clear that if $(S, \prec)$ is a totally ordered semigroup and $G$ denotes the group generated by $S$, then $\prec$ extends uniquely to $G$ in such a way that $(G, \prec)$ becomes a totally ordered group. So we can rephrase the given definition, by saying that a term ordering is a total ordering $\prec$ on $\mathbb{N}^n$ such that $(\mathbb{Z}^n, \prec)$ is a totally ordered group with $\mathbb{N}^n$ positive.

Once we are given a term ordering on $A$, it is clear that every polynomial $f$ in $A$ can be written in a unique way as a finite sum of non-zero monomials with the corresponding terms disposed in an increasing sequence; the biggest one is usually called the maximal term of $f$ and denoted by $M(f)$.

Definition 2. Given a term ordering $\prec$ on $A$, an ideal $I$ of $A$ and a finite subset $\{f_1, \ldots, f_r\}$ of $I$, then $\{f_1, \ldots, f_r\}$ is a Gröbner basis (G-base) of $I$ (with respect to $\prec$) if every element $f$ of $I$ can be written as $f = \sum_{i=1}^{r} a_i f_i$ with $M(f) \geq M(a_i)M(f_i)$ for every $i = 1, \ldots, r$.

This property is easily seen to be equivalent to the following one:

The ideal generated by the maximal monomials of all the elements of $I$ is generated by $\{M(f_1), \ldots, M(f_r)\}$.

This equivalence and other features are investigated from a more general point of view in $[R]$.

Of course G-bases depend on the choice of the term ordering on $A$, so it is quite natural to ask for a classification of all the term orderings on $A$.

Some hints in this direction were given in $[K]$ and $[G]$ and here I am going to give a full answer.

Convention: Henceforth an "ordering $\prec$ on a group $G$" means an "ordering $\prec$ on $G$, such that $(G, \prec)$ is a totally ordered group".

Lemma 1. Every ordering on $\mathbb{Z}^n$ uniquely extends to an ordering on $\mathbb{R}^n$.

Proof. If $a = (a_1, \ldots, a_n) \in \mathbb{R}^n$, let $a = \mathbb{R}^n$ be such that $m^a = (m^1, \ldots, m^n) \in \mathbb{Z}^n$.

Then we say that $a > 0$ if $m^a > 0$.

Let now $\prec$ be an ordering on $\mathbb{R}^n$; we embed $\mathbb{R}^n$ into $\mathbb{R}^n$, on which we consider the usual scalar product (denoted by $\cdot$) and the induced euclidean topology.

Then let $G$ be a $\mathbb{R}$-subvector space of $\mathbb{R}^n$ of dimension $r$ and let us denote by $G^r$ the $\mathbb{R}$-subvector space of $\mathbb{R}^n$ of $\mathbb{R}^n$.

Definition 3. We call $I_G$ the subset of $\mathbb{R}^n$ of all the elements $p \in \mathbb{R}^n$ such that, for every open neighborhood (nnh) $U_p$ of $p$ in $\mathbb{R}^n$, $U_p \cap G^+$ and $U_p \cap G^-$ are non-empty.

Lemma 2. The subset $I_G$ is a subvector space of $\mathbb{R}^n$ of dimension $r - 1$.

Proof. To prove that $I_G$ is a subvector space, we may assume that $G = \mathbb{R}^r$ and $\mathbb{R}^n = \mathbb{R}^r$ and then it is an easy exercise. Let now $\sigma : \mathbb{R}^+ \rightarrow (-1, 1)$ be the map defined by $\sigma(p) = p$ if there exists a nnh $U_p$ of $p$ such that $U_p \cap G^+ = U_p \cap G^-$. It is clear that $\sigma$ is a continuous map and $\sigma(-1, 1)$ with the discrete topology and this excludes the possibility that $\dim I_G < r - 1$, since in that case $G^r - I_G$ would be connected. Now $G$ is a totally ordered group, hence we may choose a base $\{e_1, \ldots, e_r\}$ of $G$ as a $\mathbb{R}$-vectorspace, such that $e_i > 0$, $i = 1, \ldots, r$. But then the set of the linear combinations of the $e_i$'s with coefficients in $\mathbb{R}^+$ is in $G^+$, and this excludes that $\dim I_G < r$.

Definition 4. Let $(G, \prec)$ be as before; then we denote by $U(G)$ the half-line, which is orthogonal to $I_G$ and contained in $\sigma^{-1}(1)$.

Definition 5. Given a vector $v \in \mathbb{R}^n$, we denote by $d(v)$ the dimension of the $\mathbb{R}$-subvector space of $\mathbb{R}^n$ spanned by the coordinates of $v$ and we call it the rational dimension of $v$.

It is clear that $d(v)$ is constant on the set of the nonzero multiples of $v$, in particular it is an invariant of $U(G)$.

Lemma 3. Let $G$, $G^r$ be as before and $v \in \mathbb{R}^r$. Then $d(v) \leq r = \dim G^r$.

Proof. Namely a base $\{v_1, \ldots, v_r\}$ of $G$ as an $\mathbb{R}$-vectorspace can be chosen in such a way that $v_1, \ldots, v_r \in \mathbb{R}^r$: if we write a vector $v \in \mathbb{R}^r$ as $\sum_{i=1}^{r} v_i$ with $\lambda_i \in \mathbb{R}$, it is then clear that the vector space spanned over $\mathbb{R}$ by its coordinates is contained in the vector space spanned by $\{\lambda_1, \ldots, \lambda_r\}$.

Definition 6. On $\mathbb{Z}^n$, $\mathbb{N}^n$, $\mathbb{R}^n$ a total ordering is called lexicographic and denoted by $\leq$ if it is given by the following rule: $v > 0$ if the first nonzero coordinate of $v$ is positive.

A total ordering $\prec$ on $\mathbb{N}^n$ $(\mathbb{N}^n, \preceq)$ is called of lexicographic type if there is an ordered isomorphism between $(\mathbb{N}^n, \prec)$ and $(\mathbb{N}^n, \leq)$ (the same for $\mathbb{R}^n$).
Theorem 4. Given an ordering \(<\) on \(\mathbb{R}^n\), then there exists an integer \(s\) with \(1 \leq s \leq n\), and \(s\) orthogonal vectors \(u_1, \ldots, u_s \in \mathbb{R}^n\) such that \(d(u_1) + \ldots + d(u_s) = n\) and such that the map
\[
\alpha : (\mathbb{R}^n, <) \longrightarrow (\mathbb{R}^s, \text{lex})
\]
\(\alpha(v) = (v \cdot u_1, \ldots, v \cdot u_s)\)
is an injective ordered isomorphism.

Proof. By Lemma 2, we get that \(I = B_{\mathbb{R}}\) is an \((n-1)\)-dimensional \(\mathbb{R}\)-subvector-

space of \(\mathbb{R}^n\), we also get a vector \(u_1 \in U(B_{\mathbb{R}})\), whose rational dimension we denote

by \(d_1\). Then we denote by \(G_1 = B_{\mathbb{R}}^1\), the \(\mathbb{R}\)-subvector space of \(\mathbb{R}^n\) which is defined

by \(G_1 = B_{\mathbb{R}}^1 \cap \mathbb{R}^n\). It is clear that \(\dim G_1 = n-d_1\) and it is also clear that, for a

vector \(v \in \mathbb{R}^n - G_1\) we have \(v > 0\) iff \(v \cdot u_1 > 0\). So now we have to describe what

happens on \(G_1\). Let \((G_1)_R = G_1 \cap \mathbb{R}^n\); we use again Lemma 2 and we get \(I_0\), and

a vector \(u_2 \in U(G_1)\), which is orthogonal to \(u_1\) and whose rational dimension we denote

by \(d_2\). Lemma 3 tells us that \(d_2 \leq n-d_1\). Since the rational dimensions are positive integers, this procedure ends after a finite number of steps and we eventually get \(u_1, \ldots, u_s\), which are orthogonal and such that \(d(u_1) + \ldots + d(u_s) = n\). Moreover, the fact that \(\alpha\) is an injective ordered isomorphism is a direct consequence of the arguments used before.

If \(<\) is an ordering on \(\mathbb{R}^n\), we extend it to \(\mathbb{R}^n\) and we may consider the homomorphism \(\alpha\) of Theorem 4; then we have the following

Definition 7. We denote by \(a(<)\) and we call it the type of \(<\), the number \(s\) which arises in the description of \(\alpha\). We denote by \(d(<)\) and we call it the

partition type of \(<\), the \(s\)-uple \((d(u_1), \ldots, d(u_s))\) which arises in the description of \(\alpha\). Finally, if \(d \in [1, \ldots, n]\), we denote by \(A(d)\) the quotient set \(B(d)/\sim\),

where \(B(d)\) is the set of the vectors \(v \in \mathbb{R}^n\), such that \(d(v) = d\) and \(\sim\) is the

equivalence relation given by \(v \sim v'\) if there exists \(l \in \mathbb{R}\) with \(v' = lv\).

Then the preceding discussion yields the following

Theorem 5. The term orderings \(<\) on \(A = k[x_1, \ldots, x_n]\) are classified by the

following data:

- The type of \(<\), i.e., an integer \(s\), with \(1 \leq s \leq n\).
- The partition type of \(<\), i.e., a partition \((d_1, \ldots, d_s)\) of \(n\).
- An element \((\bar{D}, \ldots, \bar{D})\) of \(A(d_1)x_1 \ldots x_A(d_s)\) such that

\[a(v) = (v \cdot u_1, \ldots, v \cdot u_s)\]
is positive.

Remark. The archimedean orderings are precisely those of type 1. The orderings of lexicographic type (see Definition 6) are those of type \(n\), hence of partition type \((1, \ldots, 1)\).

Remark. If a term ordering is given such that \(d_1 = 1\), then \(u_1\) can be chosen in such a way that \(u_1 = (q_1, \ldots, q_n) \in \mathbb{R}^n\), then, given two terms \(M_1\), \(M_2\), one has
\(M_1 < M_2\) if \(\deg M_1 < \deg M_2\), where the degree is computed after endowing the variables \(x_1, \ldots, x_n\) with the weights \(q_1, \ldots, q_n\) respectively. Of course if \(\deg M_1 = \deg M_2\), then one must look at the other vectors \(u_2, \ldots, u_s\). For instance the usual term ordering on \(A\) is that one given by the following rule: \(M_1 < M_2\) if either \(\deg M_1 < \deg M_2\) (here the variables have degree 1) or \(\deg M_1 = \deg M_2\) and \(M_1 < M_2\) in the lexicographic ordering generated by \(x_1 < \ldots < x_n\). This term ordering turns out to be of lexicographic type and \(u_1 = (1,1,1,\ldots, 1)\), \(u_2 = (n+1,1,\ldots, 1)\), \(u_3 = (0,0,2,1,\ldots, 1)\), \(u_{n-1} = (n,0,0,0,\ldots, 1)\), \(u_n = (0,0,0,\ldots, 1)\).

References


