AN INTRODUCTION
TO THE TANGENT CONE ALGORITHM

Teo MORA
Dipartimento di Matematica
Università
Via L. Alberti 4
I 16132 Genova ITALIE

Gerhard PFISTER
Sektion Mathematik
Humboldt Universität
PF 1297
DDR 1080 Berlin ALLEMAGNE

Carlo TRAVERSO
Dipartimento di Matematica
Università
Via F. Buanorroti 2
I 56100 Pisa ITALIE

In 1965, Buchberger ([BUC1,2]) introduced the notion of Gröbner bases for polynomial ideals and described an algorithm (Buchberger algorithm) to compute them. Since then, it has been widely recognized that Gröbner bases provide a presentation of a polynomial ideal I suitable for the computation of invariants of I and the verification of properties of I.
So it is possible, for instance, to decide if a polynomial is in I, to compute the dimension of I, the relations (syzygies) among a basis of I, algebraic invariants like the Hilbert function, to check if I is prime, to compute its zeroes, to obtain a primary decomposition of I..., so allowing an effective algebraic study of (global) varieties in the affine and projective spaces.

In 1964, Hironaka ([HIR]) introduced a notion of standard bases for ideals in a ring of formal power series (or in the localization of the polynomial ring at the origin). This concept is strictly related to the one of Gröbner basis; actually it is in some sense its dual: namely Gröbner bases are defined with relation to some semigroup ordering on the semigroup of terms of the polynomial ring, which must be a well-ordering, while Hironaka's standard bases were defined in exactly the same way, but with respect to a semigroup ordering whose opposite is a well-ordering.
Since the knowledge of a standard basis of an ideal I allows to reconstruct the variety of the tangents at the origin to the variety defined by I, it could, at least in principle, be used to pursue a local study of varieties at singular points. Actually such a study was pursued (not from an effective point of view) long before the computational applications of Gröbner bases to a global study of varieties and probably inspired some of the results in this direction (cf. [GAL]).
What was lacking was an algorithm to compute a standard basis of an ideal, given any basis of it. In fact, one of the main ingredients of Buchberger algorithm is a "reduction" procedure whose termination is guaranteed because the semigroup ordering which is used is a well-ordering: Hironaka's standard bases requiring an ordering which is not such, if Buchberger algorithm were applied for their computation, it would in general not halt.
An algorithm for standard basis computation (the "tangent cone" algorithm) was given only in 1982 ([MOR1,2]); it essentially consists in a modification of Buchberger's reduction procedure which guarantees termination, while preserving correctness, also if the semigroup ordering is not a well-ordering.

Once a standard basis of a polynomial ideal I is known, the variety T(V) of the tangents at the origin to the variety V defined by I is explicitly given through a Gröbner basis of the ideal defining it.
By the classical method of "associated graded rings", questions about the local behaviour of V can be transformed into questions about the global behaviour of T(V) and the latter can be solved by the Gröbner basis method.
More in general, we can face the following problem:
we are given three affine varieties $V_3 \subset V_2 \subset V_1$ (V_i being defined by the polynomial ideal $I_i \subset k[X_1,...,X_n]$, with I_3 prime) and we are interested in the behaviour of V_2 in a (Zariski)-neighborhood of V_3 inside V_1 (in the situation discussed above V_1 is the whole space, V_3 is the origin, V_2 is V).
We can give the following algebraic description: we consider $B := k[X_1,...,X_n]/I_1$, $p \subset B$ the image of I_3, A the localisation of B at p, I the image of I_2 in A. The ring A "describes" then V_3 as a subvariety of V_1, while I "describes" V_2 in a (Zariski)-neighborhood of V_3 inside V_1.
The method of associated graded rings can be applied to this situation too: there are a polynomial ring $K[Y_1,...,Y_m]$, K a finite extension of k, a homogeneous ideal $H \subset K[Y_1,...,Y_m]$, a homogeneous ideal $in(I) \subset K[Y_1,...,Y_m]/H$, s.t. questions about A can be transformed into questions about $K[Y_1,...,Y_m]/H$ (or about H) and questions about I into questions about in(I).
An application of the tangent cone algorithm ([MOR3]) allows to explicitly present K, to give $H \subset K[Y_1,...,Y_m]$ through a Gröbner basis, and to give in(I) through a Gröbner basis of its preimage in $K[Y_1,...,Y_m]$.
This therefore allows to transform the method of associated graded rings in a computational tool and to effectively solve at least the basic problems in local algebra, s.t. regularity, dimension of A, computation of systems of parameters, deciding if a given element of A lies in I, syzygies of I...

The study of algebraic formal power series is related instead with the study of analytically irreducible branches at the origin of an algebraic variety and comes out naturally when studying singular points of algebraic varieties, for instance in Newton-Puiseux algorithm for determining the analytic branches of a curve at a singular point and more generally when studying analytic components of a complex algebraic variety.
In this context one is again interested in local topological notions like the infinitesimal order of an algebraic series or of an algebraic function defined over some analytical component AC of a variety, the cone of tangents to AC, algebraic invariants of AC. Hironaka's standard bases are tailored to immediately answer to such questions; the tangent cone algorithm can be used to produce a computational model for algebraic series, which allows to compute standard bases of ideals, again by a variant of the tangent cone algorithm.

In this paper we don't propose to discuss at length the applications of the tangent cone algorithm, but just the algorithm itself and the improvements to the original schema which have been proposed over the years, in order to give an update

description of the algorithm, in a version suitable for implementations and (to our present knowledge) optimal and as general as possible.
While this paper is a survey, some results in it are original: all the improved versions of the algorithm have never been published and the published descriptions of the algorithm cover just a subset (not sufficient for some applications) of the semigroup orderings to which it can be applied.

Since the tangent cone algorithm is a variant of Buchberger algorithm, we start our paper with a survey of the Gröbner basis theory and of Buchberger algorithm (§1): since we intend to present implementable versions of the algorithms, we discuss the best variant available, also at the risk to make the presentation less elementary.
Then (§2) we discuss the problems which are met if one extends the algorithm and the underlying theory to orderings which are not well orderings and we develop a theory of standard bases.
In order to have an effective variant of Buchberger algorithm to compute standard bases, one needs to modify Buchbger reduction procedure to this new setting; this point which is the crucial part of the tangent cone algorithm is discussed in §3.
We are then able to describe the tangent cone algorithm itself and to discuss several improvements to the basic computation scheme (§4). After a short discussion on standard bases in formal power series rings (§5), we conclude the paper with a very fast survey of the main applications in local algebra (§6)

1 RECALLS ON GRÖBNER BASES AND BUCHBERGER ALGORITHM

In this introductory section we review the concept and the basic properties of Gröbner bases ([BUC1,2])[1] and of Buchberger's algorithm ([BUC1,3]) for their computation, in the Gebauer-Möller version ([G-M]), which is the most widely implemented.

1.1 Gröbner bases

Let $P := k[X_1,\dots,X_n]$ be a polynomial ring over a field, let $\mathbf{T}$ denote the free commutative semigroup generated by $\{X_1,\dots,X_n\}$, let $<$ be a semigroup total ordering on $\mathbf{T}$.
Then each polynomial $f \in P - \{0\}$ can be written in a unique way as:

$$f = \Sigma_{i=1\dots t}\, c_i\, m_i,\ c_i \in k\text{-}\{0\},\ m_i \in \mathbf{T},\ m_1 > m_2 > \dots > m_t.$$

Denote :

$$T(f) := m_1,\ M(f) := c_1\, m_1,\ lc(f) := c_1;$$

$T(f)$ is the maximal term, $M(f)$ the maximal monomial, $lc(f)$ the leading coefficient in the representation of f.
When we need to specify the ordering $<$ on which the definitions above depend, we will use either the notation $T_<$, $M_<$, or $<_\sigma$, T_σ, M_σ.
If $F \subset P$, denote $M\{F\} := \{M(f) : f \in F - \{0\}\}$, $M(F)$ the ideal generated by $M\{F\}$. Therefore, if I is an ideal, $M(I)$ is the monomial ideal generated by the maximal monomials of the elements in I.
In the rest of the paragraph we will assume $<$ is a well-ordering.

Let I be an ideal in P. In particular I is a subspace of the k-vector space P (of infinite dimension unless $I = \{0\}$).
Let $\mathbf{B} := \{t \in \mathbf{T} : t \notin M(I)\}$ and let $k[\mathbf{B}]$ denote the k-vector space with basis $\mathbf{B}$.

LEMMA 1 1) $I \cap k[\mathbf{B}] = \{0\}$
2) $\forall h \in P$, there are $f \in I$, $g \in k[\mathbf{B}]$ s.t. $h = g + f$.

Proof: 1) let $f \in P - \{0\}$, then $f = \Sigma_{i=1\dots t}\, c_i\, m_i$, $c_i \in k\text{-}\{0\}$, $m_i \in \mathbf{T}$, $m_1 > m_2 > \dots > m_t$; if $f \in I$ then $m_1 = M(f) \in M(I)$, while, if $f \in k[\mathbf{B}]$, $m_1 \in \mathbf{B}$.
2) Let us recursively define sequences of elements of P, $(h_n : n \in \mathbf{N})$, $(f_n : n \in \mathbf{N})$, $(g_n : n \in \mathbf{N})$ as follows:
i) $h_0 := h$, $f_0 := 0$, $g_0 := 0$
ii) if $h_n = 0$ define $h_{n+1} := 0$, $f_n := f_{n-1}$, $g_n := g_{n-1}$
iii) if $h_n \neq 0$ and $M(h_n) \notin M(I)$, define $h_{n+1} := h_n - M(h_n)$, $f_n := f_{n-1}$, $g_n := g_{n-1} + M(h_n)$
iv) otherwise $h_n \neq 0$ and $M(h_n) \in M(I)$. So there is $f \in I$, s.t. $M(h_n) = M(f)$[2]. Define then $h_{n+1} := h_n - f$, $f_n := f_{n-1} + f$, $g_n := g_{n-1}$.
It is immediate that the following properties hold for each n:
$h = h_n + f_n + g_n$
$f_n \in I$, $g_n \in k[\mathbf{B}]$
if $h_n \neq 0$, then $T(h_{n+1}) < T(h_n)$.
Since $<$ is well-ordered, we cannot have an infinite decreasing sequence of terms $T(h_0) > \dots T(h_n) > T(h_{n+1}) > \dots$; therefore there must be n s.t. $h_n = 0$, i.e. $h = f_n + g_n$, with $f_n \in I$ and $g_n \in k[\mathbf{B}]$.

[1] An excellent survey of the concept and of its applications is [BUC4]; for an introduction more on the line of this presentation, cf. [M-M].

[2] Here there is a tricky point, which is usually overlooked, and seems to be the only point in which the requirement that $<$ is a semigroup ordering is actually relevant:

if $c \in k\text{-}\{0\}$, $t \in \mathbf{T}$, $g \in P - \{0\}$, since $<$ is a semigroup ordering, then $M(c\, t\, g) = c\, t\, M(g)$.

Here, since $m \in M(I)$, there are $c \in k$, $t \in \mathbf{T}$, $g \in I$ s.t. $m = c\, t\, M(g)$. But then $m = M(c\, t\, g)$, and $c\, t\, g \in I$.

COROLLARY 1 $\forall h \in P$, there is a unique $g \in k[B]$ s.t. $h - g \in I$. Such a g is called a *canonical form* of h w.r.t. I and denoted $\mathrm{Can}(h,I)$.
Moreover $\mathrm{Can}(h,I) = 0$ iff $h \in I$, $\mathrm{Can}(h_0,I) = \mathrm{Can}(h_1,I)$ iff $h_0 - h_1 \in I$.

The proof of Lemma 1 could be easily turned into an algorithm to compute the canonical form of a polynomial modulo an ideal (and therefore to decide ideal membership), provided that:

given a monomial m, it is possible to decide whether $m \in M(I)$, in which case to find $f \in I$ s.t. $M(f) = m$.

Assume I is given through a basis F s.t. $M(F) = M(I)$; then the above requirement is easily solved: $m \in M(I)$ iff there are $g \in F$, $c \in k - \{0\}$, $t \in T$ s.t. $m = c\ t\ M(g)$; in this case we can then choose $f = c\ t\ g$.
Moreover with such a choice, we obtain a representation of $h - \mathrm{Can}(h,I)$ in terms of F, with nice properties:

$h - \mathrm{Can}(h,I) = \Sigma\, g_i f_i,\ g_i \in P - \{0\},\ f_i \in F,\ T(g_i)\, T(f_i) \leq T(f)$ for every i.

We are then led to the following:

DEFINITION 1 A set $F \subset I - \{0\}$ is called a *Gröbner basis* for the ideal I iff $M\{F\}$ generates the ideal $M(I)$.

Before discussing the computability of Gröbner bases, let us state some of its properties and introduce a notion, *normal form*, weaker than the one of canonical form but which will be crucial later.

DEFINITION 2 Given $f \in P - \{0\}$, $F \subset P - \{0\}$, an element $h \in P$ is called a *normal form* of f w.r.t. F. if

$f - h = \Sigma\, g_i f_i,\ g_i \in P - \{0\},\ f_i \in F$

either $h = 0$ or $M(h) \notin M(F)$.

$NF(f,F)$ will denote the set $\{h \in P : h$ is a normal form of f w.r.t. $F\}$.

We remark that, unlike canonical forms, which are unique and depend just on the ordering <, normal forms are not unique also if F is a Gröbner basis: if h is a normal form of f w.r.t. F, and $\Sigma\, g_i f_i$ is s.t. $T(g_i)\, T(f_i) < T(h)$, then $h + \Sigma\, g_i f_i$ is another normal form of f w.r.t. F.
Some weak uniqueness properties of normal forms (when F is a Gröbner basis) are stated in the following Proposition 2; it shows also that normal forms can be used instead than canonical ones to decide ideal membership.[1]
The following properties of normal forms are obvious and will be used later:

$f \in (F)$ iff $0 \in NF(f,F)$

If $M(f) \notin M(F)$, then $f \in NF(f,F)$.

DEFINITION 3 We say $h \in P-\{0\}$ has a *Gröbner representation* in terms of $F \subset P - \{0\}$ iff it can be represented:

$f = \Sigma\, g_i f_i,\ g_i \in P - \{0\},\ f_i \in F,\ T(g_i)\, T(f_i) \leq T(f)$ for every i

(such a representation will be called a Gröbner representation).

PROPOSITION 1 For each $f \in P - \{0\}$, $F = \{f_1,\ldots, f_t\} \subset P - \{0\}$, there is $h \in P$ s.t.

1) $h \in NF(f,F)$

2) $f - h$ has a Gröbner representation in terms of F.

Proof: 1) Let us recursively define sequences of elements of P, $(h_n : n \in N)$, $(g_{in} : n \in N)$, $i = 1\ldots t$ as follows:

i) $h_0 := f$, $g_{i0} := 0$, $i = 1\ldots t$

ii) if $h_n = 0$ define $h_{n+1} := 0$, $g_{in+1} := g_{in}$, $i = 1\ldots t$

iii) if $h_n \neq 0$ and $M(h_n) \notin M(F)$, define $h_{n+1} := h_n$, $g_{in+1} := g_{in}$, $i = 1\ldots t$

iv) otherwise $h_n \neq 0$ and $M(h_n) \in M(F)$. So there are $c \in k - \{0\}$, $t \in T$, $f_j \in F$, s.t. $M(h_n) = c\ t\ M(f_j)$. Define then $h_{n+1} := h_n - c\ t\ f_j$, $g_{jn+1} := g_{jn} + c\ t\ f_j$, $g_{in+1} := g_{in}$ for $i \neq j$.

It is immediate that the following properties hold for each n:

$f - h_n = \Sigma\, g_{in} f_i$ is a Gröbner representation

if $h_n \neq 0$ and $M(h_n) \in M(F)$, then $T(h_{n+1}) < T(h_n)$.

Since < is well-ordered, we cannot have an infinite decreasing sequence of terms $T(h_0) > \ldots T(h_n) > T(h_{n+1}) > \ldots$; therefore there must be n s.t. either $h_n = 0$ or $M(h_n) \notin M(F)$.
In both cases $f - h_n = \Sigma\, g_{in} f_i \in (F)$, so $h_n \in NF(f,F)$.

THEOREM 1 If $I \subset P$ is an ideal, and $F = \{f_1,\ldots, f_t\} \subset I - \{0\}$, the following conditions are equivalent:

1) F is a Gröbner basis of I

2) $f \in I$ iff f has a Gröbner representation in terms of F

3) for each $f \in P - \{0\}$:

i) if $f \in I$, then $NF(f,F) = \{0\}$

ii) if $f \notin I$, then $NF(f,F) \neq \emptyset$ and $\forall h \in NF(f,F)$, $h \neq 0$.

Proof: 1) $\Rightarrow$ 3) Let $f \in P - \{0\}$. By Proposition 1, f has a normal form w.r.t. F.
There are two cases:

1) $NF(f,F) = \{0\}$.

In this case $f \in (F) \subset I$.

2) there is $h \in NF(f,F) - \{0\}$

[1] One reason for the introduction of normal forms is that they are easier to compute than canonical forms, and still sufficient for deciding ideal membership and ideal congruence. The main reason is however that in the setting of the tangent cone algorithm canonical forms are not available, while normal forms are.

In this case, then $M(h) \notin M(F) = M(I)$, implying $h \notin I$; since $f - h \in (F) \subset I$, then $f \notin I$.
Moreover, if $0 \in NF(f,F)$, then $f \in (F) \subset I$, a contradiction, so $0 \notin NF(f,F)$.

3) $\Rightarrow$ 2) If f has a Gröbner representation in terms of F, then $f \in (F) \subset I$.
For each $f \in P$, by Proposition 1 there is $h \in NF(f,F)$ s.t. $f - h$ has a Gröbner representation in terms of F.
If $f \in I$, then $NF(f,F) = \{0\}$, so $h = 0$ and f has a Gröbner representation in terms of F.

2) $\Rightarrow$ 1) If a polynomial p is in M(I), then it is a sum of monomials in M(I) and so $p = \Sigma_{i=1\ldots s} M(g_i)$, $g_i \in I$. So we have just to show that if $f \in I$, then $M(f) \in M(F)$.
Let $f \in I$, $m = M(f)$, $f = \Sigma\, g_i f_i$ a Gröbner representation in terms of F. Let $I := \{i : T(g_i)\, T(f_i) = T(f)\}$.
Then $m = M(f) = \Sigma_{i \in I} M(g_i)\, M(f_i) \in M(F)$.

PROPOSITION 2 If F is a Gröbner basis for the ideal $I \subset P$, then:

1) let $h \in NF(g,F)$; then:
   - if $h = 0$, then $g \in I$
   - if $h \neq 0$, then $g \notin I$

2) if $h \in NF(g,F)$, $h \neq 0$, then $T(h) = \min\{T(g') : g' - g \in I\}$

3) if $g, g' \in P - I$ are s.t. $g - g' \in I$, then $M(h) = M(h')$ for each $h \in NF(g,F)$ and $h' \in NF(g',F)$.

Proof: 1) If $h = 0$, then $g = g - h \in (F) \subset I$.
If $h \neq 0$, then since $M(h) \notin M(F) = M(I)$, $h \notin I$ and so $g \notin I$.

2) Let g' be s.t. $g' - g \in I$; then $h - g' \in I$ and $M(h - g') \in M(I)$; if $T(h) > T(g')$ then $M(h - g') = M(h) \notin M(F) = M(I)$.

3) The assumptions imply that $h' - g \in I$ and so (by 2) $T(h) \leq T(h')$; in the same way $T(h') \leq T(h)$.
So $T(h) = T(h')$ and therefore either $T(h - h') = T(h)$ and $M(h - h') = M(h) - M(h')$ or $M(h) = M(h')$, $T(h - h') < T(h)$.
The first case cannot occur since $M(h - h') \in M(I)$, $M(h) \notin M(F) = M(I)$.

1.2 Gröbner basis computation

In order to obtain an algorithm to compute Gröbner bases, we need a finite set of tests, s.t. if all are successful the given basis is Gröbner, while if one fails it allows to enlarge the basis.
Theorem 1 gives some hints how to find such a test: F is not a Gröbner basis if and only if there is an element $f \in I$, which has a non-zero normal form h in terms of F; such a normal form h is then an element of I s.t. $M(h) \in M(I) - M(F)$. If we add h to F, $F' := F \cup \{h\}$ is still a subset of I and $M(F) \subset M(F') \subset M(I)$.
Contrariwise, if F is Gröbner, then each element in I has a Gröbner representation in terms of F.
Moreover, the proof of Proposition 1 actually is an algorithm which, given $f \in P$ and $F \subset P$, computes either a Gröbner representation of f in terms of F or a non zero normal form of f w.r.t. F
So, let us assume that for each basis F of I we can compute a finite subset $H = H(F) \subset I$, s.t. F is Gröbner if and only if each element of H has a Gröbner representation in terms of F. We could then apply the following algorithm to compute the Gröbner basis G of an ideal given through a basis F.

```
G := F
H := H(G)
While $H \neq \emptyset$ do
    Choose $h \in H$
    H := H - {h}
    Compute $h' \in NF(h,G)$, s.t. h - h' has a Gröbner representation in terms of G
    If $h' \neq 0$ then
        $G := G \cup \{h'\}$
        H := H(G)
```

Correctness of the algorithm is guaranteed, since, at termination, each element of H(G) has a Gröbner representation, and, by our assumption, this implies that G is Gröbner.
Termination is guaranteed, because any time we enlarge F, we add to it an element h' s.t. $M(h') \in M(I) - M(F)$. By Dickson Lemma[1], after a finite number of steps we must have $M(F) = M(I)$.
So we are left with the problem of finding a finite subset $H = H(F) \subset I$, s.t. F is Gröbner if and only if each element of H has a Gröbner representation in terms of F.

Let $F = \{f_1,\ldots,f_t\}$ be a basis of I; let $f \in I$, $f \neq 0$; since f is in I, it has some representation in terms of F, $f = \Sigma\, g_i f_i$.
Let $t := \max\{T(g_i)\, T(f_i)\}$, $I := \{i : T(g_i)\, T(f_i) = t\}$
Clearly $t \geq T(f)$; if $t = T(f)$, then the given representation is Gröbner..
If $t > T(f)$, we can partition the representation $f = \Sigma\, g_i f_i$ as follows, denoting $R(g_i) := g_i - M(g_i)$:

$$f = \Sigma_{i \in I} M(g_i)\, f_i + \Sigma_{i \in I} R(g_i)\, f_i + \Sigma_{i \notin I}\, g_i f_i$$

where:

$$\Sigma_{i \in I} M(g_i)\, M(f_i) = 0$$
$$T(R(g_i))\, T(f_i) < t \text{ for } i \in I$$
$$T(g_i)\, T(f_i) < t \text{ for } i \notin I$$

[1] In each infinite family M of terms, there is a finite subset M_1 s.t. each term in M is multiple of some term in M_1.

Let $h := \Sigma_{i\in I} M(g_i) f_i$;; if we can find a different representation of h, $h = \Sigma h_i f_i$ with $T(h_i) T(f_i) < t$, then we have a representation of f,

$$f = \Sigma_{i\in I} h_i f_i + \Sigma_{i\in I} R(g_i) f_i + \Sigma_{i\notin I} g_i f_i = \Sigma_{i=1\ldots t} g'_i f_i$$

with $T(f) \le \max\{T(g'_i) T(f_i)\} < t$.

Repeating the same argument on the new representation, we will eventually find either a representation

$$f = \Sigma_{i=1\ldots t} g''_i f_i, \text{ with } \max\{T(g''_i) T(f_i)\} = T(f),$$

i.e. a Gröbner representation; or elements $m_1,\ldots, m_t$ s.t.

i) each m_i is either zero or a monomial,

ii) $T(m_i) T(f_i)$ is a constant $t \in T$ whenever $m_i \ne 0$

iii) $\Sigma m_i M(f_i) = 0$

and moreover $h = \Sigma m_i f_i$ doesn't have another representation $h = \Sigma h_i f_i$ with $T(h_i) T(f_i) < t$.

In particular, since $T(h) < t$, h doesn't have a Gröbner representation in terms of F.

We have therefore proved the following:

LEMMA 2 Let $F = \{f_1,\ldots,f_t\}$ be a basis of I. Let Φ be the set of elements $(m_1,\ldots,m_t) \in P^t$ s.t.

i) each m_i is either zero or a monomial,

ii) $T(m_i) T(f_i)$ is a constant $t \in T$ whenever $m_i \ne 0$

iii) $\Sigma m_i M(f_i) = 0$.

Let $H := \{ \Sigma m_i f_i : (m_1,\ldots,m_t) \in \Phi\}$

If F is not Gröbner, then there is $h \in H$ s.t. for each representation $h = \Sigma h_i f_i$, $\max\{T(h_i) T(f_i)\} \ge \max\{T(m_i) T(f_i)\}$; in particular such an h doesn't have a Gröbner representation in terms of F.

We can therefore restrict our attention to those elements h of I which are obtained taking a relation among the $M(f_i)$'s, $0 = \Sigma m_i M(f_i)$ and substituting f_i to $M(f_i)$. They are still infinitely many, but the set of relations among the $M(f_i)$'s is a module and so it has a finite basis. The aim of the following definitions and results is to show that if we take a finite basis of the relations among the $M(f_i)$'s satisfying some assumptions, and we substitute in each such relation f_i to $M(f_i)$, we obtain a finite set H s.t. if each element of H as a Gröbner representation in terms of F, then F is a Gröbner basis of I. Such a set H can then be used in the algorithm we have outlined above.

Let $f_1,\ldots, f_t \in P - \{0\}$, $F := \{f_1,\ldots,f_t\}$, I the ideal generated by F.

We begin by extending the functions T(-) and M(-) to the module P^t.

Let $\{e_1,\ldots, e_t\}$ denote the canonical basis of P^t [2]; for each $(g_1,\ldots,g_t) = \Sigma g_i e_i \in P^t$ define:

$$T(\Sigma g_i e_i) := \max\{T(g_i) T(f_i)\}$$

$$M(\Sigma g_i e_i) := \Sigma_{i\in I} M(g_i) e_i \text{ where } I := \{i : T(g_i) T(f_i) = T(\Sigma g_i e_i)\}.$$ [3]

If $\Phi \subset P^t$, denote $M\{\Phi\} := \{M(\phi) : \phi \in \Phi - \{0\}\}$, $M(\Phi)$ the submodule of P^t generated by $M\{\Phi\}$.

We say that an element $\phi = \Sigma m_i e_i$ of P^t is *homogeneous* iff for each i s.t. $m_i \ne 0$, then m_i is a monomial and $T(m_i) T(f_i) = T(\phi)$; that a submodule of P^t is *homogeneous* if it is generated by homogeneous elements.

We remark also that:

if ϕ, $\phi_1,\ldots, \phi_s$ are homogeneous elements in P^t and $\phi \in (\phi_1,\ldots, \phi_s)$ then there is a representation

$$\phi = \Sigma c_i m_i \phi_i,\ c_i \in k,\ m_i \in T,\ m_i T(\phi_i) = T(\phi) \text{ for each i with } c_i \ne 0.$$

DEFINITION 4 Given $\phi \in P^t - \{0\}$, $\Phi \subset P^t - \{0\}$, an element $\psi \in P^t$ is called a *normal form* of ϕ w.r.t. Φ if

$\phi - \psi = \Sigma g_i \phi_i$, $g_i \in P - \{0\}$, $\phi_i \in \Phi$

either $\psi = 0$ or $M(\psi) \notin M(\Phi)$.

LEMMA 3 For each $\phi \in P^t - \{0\}$, $\Phi \subset P^t - \{0\}$, there is $\psi \in P^t$, which is a *normal form* of ϕ w.r.t. Φ.

Proof: (*cf.* Prop.1) Let us recursively define sequences of elements of P^t, $(\psi_n : n \in N)$, $(\xi_n : n \in N)$ as follows:

i) $\psi_0 := \phi$, $\xi_0 := 0$

ii) if $\psi_n = 0$ define $\psi_{n+1} := 0$, $\xi_{n+1} := \xi_n$

iii) if $\psi_n \ne 0$ and $M(\psi_n) \notin M(\Phi)$, define $\psi_{n+1} := \psi_n$, $\xi_{n+1} := \xi_n$

iv) otherwise $\psi_n \ne 0$ and $M(\psi_n) \in M(\Phi)$. So there are $c_i \in k-\{0\}$, $m_i \in T$, $\phi_i \in \Phi$, s.t. $M(\psi_n) = \Sigma c_i m_i M(\phi_i)$, and $m_i T(\phi_i) = T(\psi)$ for each i. Define then $\psi_{n+1} := \psi_n - \Sigma c_i m_i \phi_i$, $\xi_{n+1} := \xi_n + \Sigma c_i m_i \phi_i$.

It is immediate that the following properties hold for each n:

$\phi - \psi_n = \xi_n \in (F)$

if $\psi_n \ne 0$ and $M(\psi_n) \in M(\Phi)$, then $T(\psi_{n+1}) < T(\psi_n)$.

Since < is well-ordered, we cannot have an infinite decreasing sequence of terms $T(\psi_0) > \ldots T(\psi_n) > T(\psi_{n+1}) > \ldots$; therefore there must be n s.t. either $\psi_n = 0$ or $M(\psi_n) \notin M(\Phi)$.

In both cases $\phi - \psi_n = \xi_n \in (\Phi)$, so ψ_n is a normal form of ϕ w.r.t. Φ.

[2] i.e. $\Sigma g_i e_i$ is the vector $(g_1,\ldots,g_t)$.

[3] This definitions and the notion of homogeneous elements and modules given below are perfectly natural in the language of graded rings. Since graded rings will disguisedly appear later on too, we have briefly sketched in an Appendix as much of graded ring theory as it is necessary.

Define

$$s : P^t \to P \text{ by } s(\Sigma\, g_i\, e_i) := \Sigma\, g_i\, M(f_i);$$

then the kernel of s

$$\mathrm{Syz}\{M(f_1),\dots,M(f_t)\} := \mathrm{Ker}(s)$$

is the module of syzygies (relations) among $\{M(f_1),\dots,M(f_t)\}$, which is a homogeneous submodule of P^t.
Define $S : P^t \to P$ by $S(\Sigma\, g_i\, e_i) := \Sigma\, g_i\, f_i$ and remark that if u is a homogeneous element in Ker(s), then $T(S(u)) < T(u)$.

If u is a homogeneous element in Ker(s), we say that u *lifts* to $v \in \mathrm{Ker}(S)$ (v is a *lifting* of u) if $M(v) = u$.
In other words v is a lifting of u iff $S(u) = \Sigma\, g_i\, f_i$ with $T(g_i)\, T(f_i) < T(u)$ and $v = u - \Sigma\, g_i\, e_i$.
Remark that:
1) if S(u) has a Gröbner representation, then u has a lifting, while the converse is not necessarily true.
2) Lemma 2 can be restated as follows: if F is not a Gröbner basis of I then there is a homogeneous element $u \in \mathrm{Ker}(s)$ which doesn't have a lifting.

LEMMA 4 Let $f_1,\dots, f_t \in P - \{0\}$, $F := \{f_1,\dots,f_t\}$, I the ideal generated by F. Let s, S be defined as above.
Let U be a basis of Ker(s) consisting of homogeneous elements. Then the following are equivalent:

1) F is a Gröbner basis for I
2) for each $u \in U$, u has a lifting

Proof: 1) ⇒ 2) Let $u \in U$ and let $h = S(u)$. Then $T(h) < T(u)$. So let $\Sigma\, g_i\, f_i$ be a Gröbner representation of h and define $v := u - \Sigma\, g_i\, e_i$. Then $S(v) = S(u) - \Sigma\, g_i\, f_i = h - h = 0$ so $v \in \mathrm{Ker}(S)$.
Moreover $T(g_i)\, T(f_i) \le T(h) < T(u)$, so $u = M(v)$.

2) ⇒ 1) We show that each $h \in I$ has a Gröbner representation.
Since $h \in I$, and F is a basis of I, there is a representation $h = \Sigma_i\, h_i\, f_i$.
Let $\phi := (h_1,\dots,h_t) \in P^t$.
For each $u \in U$, let $\mathrm{lift}(u) \in \mathrm{Ker}(S)$ be a lifting of U; let $V := \{\mathrm{lift}(u) : u \in U\}$.
By Lemma 3, we know that Φ has a normal form $\phi' = (h'_1,\dots,h'_t)$ w.r.t. V.
Then $\phi - \phi' \in \mathrm{Ker}(S)$ so $\Sigma\, h'_i f_i = S(\phi') = S(\phi) = h$ and $T(\phi') = \max\{T(h'_i)\, T(f_i)\} \ge T(h)$.
If $T(\phi') > T(h)$, let $J := \{j : T(h'_j)\, T(f_j) = T(\phi')\}$, then $M(\phi') = \Sigma_{j\in J}\, M(h_j)\, M(f_j) = 0$, i.e. $\Sigma_{j\in J}\, M(h_j)\, e_j$ is a homogeneous element in Ker(s), so $M(\phi') \in (U) = M(V)$, a contradiction since ϕ' is a normal form of ϕ w.r.t. V.

So, in order to compute Gröbner bases, we are left with the problem of explicitly computing some homogeneous basis of Ker(s). One such basis is easy to obtain.
Let $f_1,\dots, f_t \in P - \{0\}$ and denote

$$T(i) := T(f_i)$$
$$T(i,j) := \text{l.c.m.}(T(f_i), T(f_j))$$
$$T(i,j,k) := \text{l.c.m.}(T(f_i), T(f_j), T(f_k))$$
$$\sigma(i,j) := lc(f_i)^{-1}\, T(i,j)/T(i)\, e_i - lc(f_j)^{-1}\, T(i,j)/T(j)\, e_j.$$

A basis of Ker(s) is then given by:

$$U_0 := \{\sigma(i,j) : 1 \le i < j \le t\}.$$[1]

We are then led to the following algorithm to compute a Gröbner basis of an ideal, given through a basis $F = \{f_1,\dots, f_t\}$:

```
G := F
B := { {i,j} : 1 ≤ i < j ≤ t}
While B ≠ Ø do
    Choose {i,j} ∈ B
    B := B - { {i,j} }
    h := S(σ(i,j))
    Compute h' ∈ NF(h,G), s.t. h - h' has a Gröbner representation in terms of G
    If h' ≠ 0 then
        t := t+1
        f_t := h'
        G := G ∪ {f_t}
        B := B ∪ { {i,t} : 1 ≤ i < t}
```

[1] To prove this we have just to show that each homogeneous element in Ker(s) can be represented in terms of U_0 (*cf.* Appendix)
Let u be a homogeneous element of Ker(s); then

$$u = \Sigma_{j\in J}\, c_j\, m_j\, e_j, \text{ with } J \subset \{1,\dots,t\},\ c_j \in k - \{0\},\ m_j \in T,\ m_j\, T(f_j) = T(u),\ \Sigma_{j\in J}\, c_j\, lc(f_j) = 0.$$

Let $j := \max J$, $I := J - \{j\}$ Clearly for each $i \in I$, T(u) is a multiple of T(i,j), $T(u) = m_{ij}\, T(i,j)$ and $m_i = m_{ij}\, T(i,j)/T(i)$, $m_j = m_{ij}\, T(i,j)/T(j)$. Also $c_j = - lc(f_j)^{-1}\, \Sigma_{i\in I}\, c_i\, lc(f_i)$.
So we have

$$\Sigma_{i\in I}\, c_i\, lc(f_i)\, m_{ij}\, \sigma(i,j) = \Sigma_{i\in I}\, c_i\, lc(f_i)\, m_{ij}\, (lc(f_i)^{-1}\, T(i,j)/T(i)\, e_i - lc(f_j)^{-1}\, T(i,j)/T(j)\, e_j) =$$
$$= \Sigma_{i\in I}\, c_i\, m_{ij}\, T(i,j)/T(i)\, e_i - \Sigma_{i\in I}\, c_i\, lc(f_i)\, lc(f_j)^{-1}\, m_{ij}\, T(i,j)/T(j)\, e_j =$$
$$= \Sigma_{i\in I}\, c_i\, m_i\, e_i - lc(f_j)^{-1}\, (\Sigma_{i\in I}\, c_i\, lc(f_i))\, m_j\, e_j = \Sigma_{i\in J}\, c_i\, m_i\, e_i = u.$$

At termination of this algorithm, each $\sigma(i,j)$ has a Gröbner representation in terms of G: in fact if, at some stage, $h' \neq 0$, then $h - h'$ has a Gröbner representation in terms of G, $h - h' = \Sigma\, h_i\, f_i$ and then $h = \Sigma\, h_i\, f_i + h'$ is a Gröbner representation in terms of $G \cup \{h'\}$.

1.3 Buchberger algorithm

A major optimization of the basic version of Buchberger algorithm we have outlined above is obtained by giving criteria to avoid useless computations of normal forms of some $S(\sigma(i,j))$'s. Such a computation can be useless for two different reasons:

1) U_0 is a basis of Ker(s), but usually is by far much larger than a minimal basis. If $U \subset U_0$ is a basis of Ker(s) with less elements, normal form computations, according to Lemma 4, are required just for the elements in U.

2) $\sigma(i,j)$ could be an element in a minimal basis of Ker(s), s.t. however $\sigma(i,j)$ is known to have a lifting by a general theoretical argument.

The second case is covered by the following result in [BUC2]:

LEMMA 5 If $T(i,j) = T(i)\, T(j)$, then $\sigma(i,j)$ has a lifting.

Proof: Denote $R(f) := f - M(f)$, $c := lc(f_i)\, lc(f_j)$. We claim that $\psi := c^{-1} f_j\, e_i - c^{-1} f_i\, e_j$ is a lifting of $\sigma(i,j)$.
In fact $S(\psi) = c^{-1} f_j\, f_i - c^{-1} f_i f_j = 0$, and $\psi = (c^{-1} M(f_j)\, e_i - c^{-1} M(f_i)\, e_j) + (c^{-1} R(f_j)\, e_i - c^{-1} R(f_i)\, e_j)$, where $R(f_j)\, T(i) < T(j)\, T(i) = T(i,j)$ and $R(f_i)\, T(j) < T(i,j)$, while $(c^{-1} M(f_j)\, e_i - c^{-1} M(f_i)\, e_j) = lc(f_i)^{-1}\, T(j)\, e_i - lc(f_j)^{-1}\, T(i)\, e_j = \sigma(i,j)$.

Criteria to detect redundant elements in the basis U_0 have been proposed in [BUC2] and [G-M]; we briefly review without proofs the results of the latter paper:
We say $\sigma(i,k)$ is redundant if either:
i) there is $j < k$ s.t. $T(j,k)$ divides properly $T(i,k)$
ii) or there is $j > k$ s.t. $T(i,j,k) = T(i,k)$, $T(i,j) \neq T(i,k) \neq T(j,k)$

LEMMA 6 1) $\{\sigma(i,j) : 1 \leq i < j \leq t, \sigma(i,j) \text{ is not redundant}\}$ is a homogeneous basis of Ker(s).
2) Let $U \subset U_0$ be a basis of Ker(s), $m \in \mathbf{T}$, $V := \{\sigma(i,t) \in U : T(i,t) = m\}$, j be s.t. $\sigma(j,t) \in V$.
Then $U - V \cup \{\sigma(j,t)\}$ is a homogeneous basis of Ker(s).
Proof: [G-M] Prop. 3.5 and 3.7

LEMMA 7 Let $U \subset \{\sigma(i,j)\ 1 \leq i < j \leq t\text{-}1\}$ be a basis of $Syz\{M(f_1),\ldots, M(f_{t-1})\}$. Then $U \cup \{\sigma(i,t) : 1 \leq i < t\}$ is a basis of $Syz\{M(f_1),\ldots, M(f_t)\}$[1]
Proof: Let u be a homogeneous element in $Syz\{M(f_1),\ldots, M(f_t)\}$, $u = \Sigma_{j\in J}\, c_j\, m_j\, e_j$, with $J \subset \{1,\ldots,t\}$, $c_j \in k - \{0\}$, $m_j \in \mathbf{T}$, $m_j\, T(f_j) = T(u)$, $\Sigma_{j\in J}\, c_j\, lc(f_j) = 0$.
If $t \notin J$, then $u \in Syz\{M(f_1),\ldots, M(f_{t-1})\}$ and it has a representation in terms of U.
If $t \in J$, then there must be $i < t$ s.t. $i \in J$; then $T(i,t)$ divides $T(u)$, $T(u) = m\, T(i,t) = m_i\, T(i) = m_t\, T(t)$. Let $I := J - \{t\}$.
Then $u - c_t\, lc(f_t)\, \sigma(i,t) = \Sigma_{j\in I}\, c_j\, m_j\, e_j + c_t\, m_t e_t - c_t\, lc(f_t)\, lc(f_i)^{-1}\, T(i,t)/T(i)\, e_i + c_t\, T(i,t)/T(t)\, e_t =$
$\Sigma_{j\in I}\, c_j\, m_j\, e_j - c_t\, lc(f_t)\, lc(f_i)^{-1}\, m_i\, e_i \in Syz\{M(f_1),\ldots, M(f_{t-1})\}$.

Let us briefly explain how the results of Lemmata 6 and 7 are to be used in a Gröbner basis algorithm.
At some point we have a basis $U \subset \{\sigma(i,j)\ 1 \leq i < j \leq t\text{-}1\}$ of $Syz\{M(f_1),\ldots, M(f_{t-1})\}$, we obtain a new element f_t and so we are looking for a basis of $Syz\{M(f_1),\ldots, M(f_t)\}$.
By Lemma 7 we know that $U \cup \{\sigma(i,t)\ 1 \leq i < t\}$ is such a basis. We can then use Lemma 6.1 to eliminate redundant elements from it.
First of all, if $i < k < t$ are s.t. $T(i,k,t) = T(i,k)$, $T(i,t) \neq T(i,k) \neq T(k,t)$ then $\sigma(i,k)$ is redundant (*cf.* condition ii), so we discard from U any such element $\sigma(i,k)$, obtaining a subset U_1.
Then (condition i) we can discard from $\{\sigma(i,t)\ 1 \leq i < t\}$ any element $\sigma(i,t)$ s.t. for some j $T(j,t)$ divides properly $T(i,t)$ obtaining a subset V_1.
Then we apply Lemma 6.2): we partition V_1 into subsets $\{\sigma(i,t)\}$ s.t. in each of them $T(i,t)$ is constant and we pick up any element from each subset obtaining a set V_2. In this last operation, since the choice of the element to pick is arbitrary, we can obtain a free bonus if we pick an element (if such is present) $\sigma(i,t)$ with $T(i,t) = T(i)\, T(t)$, since by Lemma 5 there is then no need to compute the normal form of $S(\sigma(i,j))$.
Finally $U_1 \cup V_2$ is the basis of $Syz\{M(f_1),\ldots, M(f_t)\}$ we were looking for.
We formalize this procedure in the following algorithm:

```
$U_0$ := SyzBasis(F,U)
where
    F := $\{f_1,\ldots,f_t\} \subset P - \{0\}$ is an indexed set of non-zero elements in P.
```

[1] There is a notational problem here: $Syz\{M(f_1),\ldots, M(f_{t-1})\}$ is a submodule of P^{t-1} while $Syz\{M(f_1),\ldots, M(f_t)\}$ is a submodule of P^t; if we identify however P^{t-1} with the submodule of P^t generated by $\{e_1,\ldots,e_{t-1}\}$, then $Syz\{M(f_1),\ldots, M(f_{t-1})\}$ is a submodule of $Syz\{M(f_1),\ldots, M(f_t)\}$ and the statement makes sense.
Actually one has $Syz\{M(f_1),\ldots, M(f_{t-1})\} = Syz\{M(f_1),\ldots, M(f_t)\} \cap P^{t-1}$

```
        there is $U'$ s.t. $U \subset U' \subset \{(i,j) : 1 \le i < j \le t-1\}$ s.t.
                1) $\{\sigma(i,j) : (i,j) \in U'\}$ is a basis of $Syz\{M(f_1),\dots,M(f_{t-1})\}$
                2) for each $(i,j) \in U' - U$, $\sigma(i,j)$ has a lifting[2]
        there is $U_0'$ s.t. $U_0 \subset U_0' \subset \{(i,j) : 1 \le i < j \le t\}$ s.t.
                1) $\{\sigma(i,j) : (i,j) \in U_0'\}$ is a basis of $Syz\{M(f_1),\dots,M(f_t)\}$
                2) for each $(i,j) \in U_0' - U_0$, $\sigma(i,j)$ has a lifting
For each $(i,k) \in U$ do
        If $T(i,k) = T(i,k,t)$ and $T(i,t) \ne T(i,k) \ne T(k,t)$ then
                $U := U - \{(i,k)\}$
$V := \{(i,t) : 1 \le i < t\}$
For $i = 1 \dots t-1$ do
        If there is $j$, $1 \le j < t$ s.t. $T(j,t)$ divides properly $T(i,t)$ then
                $V := V - \{(i,t)\}$
Let $T := \{T(i,t) : (i,t) \in V\}$
$V_2 := \emptyset$
For each $\tau \in T$ do
        $V(\tau) := \{(i,t) \in V : T(i,t) = \tau\}$
        If for each $(i,t) \in V(\tau)$, $T(i)\,T(t) \ne T(i,t)$ then
                choose $(i,t) \in V(\tau)$
                $V_2 := V_2 \cup \{(i,t)\}$
$U_0 := U \cup V_2$
```

Before presenting Buchberger algorithm for Gröbner basis computation, we have to present an explicit algorithmic version of Proposition 1. We use the following notation:
if $T(f)$ is a multiple of $T(g)$, $t \in \mathbf{T}$ is s.t. $T(f) = t\,T(g)$, define

$$Red(f,g) := f - lc(f)\,lc(g)^{-1} t\, g.$$

Remark that either $Red(f,g) = 0$ or $T(Red(f,g)) < T(f)$.

```
$h :=$ NF$(g,F)$
where
        $g$ is a non-zero element in $P$
        $F \subset P - \{0\}$ is a finite set.
        $h \in NF(f,F)$ and $g - h$ has a Gröbner representation in terms of $F$.
$h := g$
While $h \ne 0$ and $M(h) \in M(F)$ do
        Choose $f \in F$ s.t. $T(f)$ divides $T(h)$
        $h := Red(h,f)$
```

Correctness of Algorithm **NF** comes directly from the proof of Prop. 1; termination is assured since < is a well-ordering.

```
$G :=$ GröbnerBasis$(F)$
where
        $F := \{f_1,\dots,f_t\} \subset P - \{0\}$ is an indexed set of non-zero elements in $P$.
        $G \subset P - \{0\}$ is a Gröbner basis for the ideal $I := (f_1,\dots,f_t)$
$G := \{f_1\}$
$B := \emptyset$
For $i = 2 \dots t$ do
        $G := G \cup \{f_t\}$
        $B :=$ SyzBasis$(G,B)$
While $B \ne \emptyset$ do
        Choose $(i,j) \in B$
        $B := B - \{(i,j)\}$
        $h := S(\sigma(i,j))$
        $h := NF(h,G)$
        If $h \ne 0$ then
                $t := t + 1$
                $f_t := h$
                $G := G \cup \{f_t\}$
```

[2] This way of describing the algorithm can be confusing, however we are lacking a better one. The point is that at each call of **SyzBasis** a whole basis of $Syz\{M(f_1),\dots,M(f_{t-1})\}$ is not available, since those elements for which the normal form of $S(\sigma(i,j))$ has already been computed or s.t. $T(i,j) = T(i)\,T(j)$ have been discarded.
So we have partitioned the basis U' of $Syz\{M(f_1),\dots,M(f_{t-1})\}$ into the subsets U, consisting of the elements yet to be treated, and $U' - U$ of the discarded elements. The same we have done for the output basis of basis of $Syz\{M(f_1),\dots,M(f_t)\}$, storing only the elements in V which are yet to be tested and discarding those elements for which the test is either already performed or is useless by Lemma 5.

```
        B := SyzBasis(G,B)
```

Correctness of **GröbnerBasis** is an immediate consequence of the preceeding discussion: we explicitly remark that at termination:

1) the $\sigma(i,j)$'s which have been explicitly treated by the algorithm have a Gröbner representation in terms of G.

2) to obtain a basis of $Syz(M(f_1),\ldots,M(f_t))$, we have to add to the $\sigma(i,j)$'s which have been explicitly treated by the algorithm, those $\sigma(i,j)$'s s.t. $T(i)\,T(j) = T(i,j)$, which have a lifting by Lemma 5

3) therefore for such a basis of $Syz(M(f_1),\ldots,M(f_t))$, all its elements have a lifting and G is a Gröbner basis by Lemma 4.

Termination of **GröbnerBasis** is based on Dickson Lemma, since any time we add a new element to the basis we enlarge the ideal M(G).

2 TANGENT CONES, STANDARD BASES AND LOCALIZATIONS

2.1 A counterexample

As we have remarked, termination of **NF** relies on the fact that < is a well-ordering.
If we drop this assumption, we see immediately the existence of examples in which **NF** does not terminate.
Let $P := k[X]$ with $T = \{X^n\}$ ordered so that $X^n < X^m$ iff $m < n$; and let us see what happens if we try $NF(X,\{X - X^2\})$
We have

$h := X,\ f := X - X^2,\ Red(h,f) = X^2$
$h := X^2,\ f := X - X^2,\ Red(h,f) = X^3$
...
$h := X^n,\ f := X - X^2,\ Red(h,f) = X^{n+1}$
...

so that **NF** doesn't actually halt in this instance.
The problem is however related not just to the algorithm but to theory itself.
In fact, let $I \subset P$ be the ideal generated by $\{X\}$ for which clearly $M(I) = (X)$; since $X = M(X - X^2)$ and $X - X^2 \in I$, F is such that:

$F \subset I$ and $M(F) = M(I)$.

Clearly $X \notin (X - X^2)$ so it cannot have a Gröbner representation in terms of F; such a representation would in fact imply that $X \in (F)$.
Finally assume h is a normal form of X w.r.t. F; then $h \neq 0$, otherwise $X \in (F)$, which is false; since $M(h) \notin (X) = M(F)$, necessarily $M(h) = c \in k - \{0\}$. So $h = c + h'$, with $h'(0) = 0$. We have

$$X - c - h'(X) = X - h(X) = g(X)\,(X - X^2)$$

since $X - h \in (X - X^2)$.
Evaluating in 0 we obtain:

$$-c = 0$$

and so a contradiction, proving that X doesn't have normal forms w.r.t. F.
In conclusion, the notions, which, in the well-ordered case, can be used as equivalent definitions of Gröbner bases, are no more equivalent in this context. Moreover there are instances in which normal forms don't exist, and the same is true for canonical forms.

2.2 The cone of tangents to a variety at a point

Before introducing a theory of Gröbner bases (and an algorithm for their computation) in the case of orderings < which are not well-orderings, we intend to give an application of such a theory; this will be of help also to motivate our search for a solution.

Let $f \in P - \{0\}$, then f can be uniquely written as a finite sum of non-zero homogeneous polynomials:

$f = \Sigma_{i=1\ldots t}\, f_i$, f_i homogeneous and non-zero, $deg(f_1) < \ldots < deg(f_i) < deg(f_{i+1}) < \ldots$

To the polynomial f we can associate its *order*, $ord(f) := deg(f_1)$ and its *initial form*, $in(f) := f_1$.
The order of f is the infinitesimal order at the origin of f as an analytic function; its initial form is the lowest order non-zero Taylor approximation of f at the origin.
If $I \subset P = k[X_1,\ldots,X_n]$ is an ideal, we define $in(I) := (in(f) : f \in P)$, the *initial form ideal* of I, to be the homogeneous ideal in P generated by the initial forms of the elements in I. Geometrically, (when the base field k is C) it is the ideal which defines the cone of the tangents at the origin (counted with the correct multiplicity) to the variety in C^n defined by I[1].
It gives therefore a kind of "lowest order approximation" to such variety.
Let now < be an ordering on T s.t.

for $m_1, m_2 \in T$, $deg(m_1) < deg(m_2) \Rightarrow m_1 > m_2$.

The following result holds:

PROPOSITION 3 Let $F \subset I$ be s.t. $M(F) = M(I)$. Then $\{in(f) : f \in F\}$ generates $in(I)$.

[1] To be precise, in order that this geometrical notion makes sense, we should restrict ourselves to radical ideals.

Proof: Since $\forall h \in P$, $M(h) = M(in(h))$, we can easily conclude that both $M(I) = M(in(I))$ and $M(F) = M(in(F))$, so that $M(in(F)) = M(in(I))$.
Now let $<_w$ be the well-ordering which agrees with $<$ on terms of the same degree, but is compatible (instead of anticompatible) with the degree, i.e.

$m_1 <_w m_2$ iff $\deg(m_1) < \deg(m_2)$ or ($\deg(m_1) = \deg(m_2)$ and $m_1 < m_2$)

If f is a homogeneous element of P, $M(f) = M_w(f)$. Therefore $M_w(in(F)) = M(in(F)) = M(in(I)) = M_w(in(I))$.
So $\{in(f) : f \in F\}$ is a Gröbner basis, and therefore a basis, of I.

We have actually proved more, namely:

PROPOSITION 4 Let $F \subset I$ be s.t. $M(F) = M(I)$. Then $\{in(f) : f \in F\}$ is a Gröbner basis of in(I) w.r.t. the well-ordering $<_w$ s.t.

$m_1 <_w m_2$ iff $\deg(m_1) < \deg(m_2)$ or ($\deg(m_1) = \deg(m_2)$ and $m_1 < m_2$).

As a conclusion, the ability of computing "Gröbner bases" w.r.t. orderings $<$ which are not well-orderings implies the ability of computing initial form ideals.
Are normal forms interesting in this context?
Let V be the variety in C^n defined by the radical ideal I. Let $f \in P$; if $g \in P$ is s.t. $f - g \in I$, then f and g define the same polynomial function $f(x_1,\dots,x_n) = g(x_1,\dots,x_n)$ on V. What are the infinitesimal order at the origin and a lowest order non-zero Taylor approximation at the origin of the polynomial function $f(x_1,\dots,x_n)$?

LEMMA 8 Consider the set $R_f := \{g \in P : g - f \in I\}$. Assume there is $g \in R_f$ s.t. $in(g) \notin in(I)$ and let $n := ord(g)$.
Then the following hold:

i) if $h \in R_f$, $ord(h) < n$, then $in(h) \in in(I)$.

ii) if $h \in R_f$, $ord(h) \geq n$, then $ord(h) = n$, $in(g) - in(h) \in in(I)$.

Proof: i) since $ord(h) < ord(g)$, $in(h - g) = in(h)$; since $h - g \in I$, $in(h) = in(h - g) \in in(I)$.

ii) If $ord(h) > n$, then $in(h - g) = in(g) \notin in(I)$; since $h - g \in I$, $in(g) = in(h - g) \in in(I)$, a contradiction.

Then if $ord(h) \geq n$, necessarily $ord(h) = n$, $in(h - g) = in(h) - in(g)$; then, since $h - g \in I$, $in(h) - in(g) = in(h - g) \in in(I)$.

It is then clear that the answer to the questions above is: ord(g) and the residue class of in(g) mod. in(I).
However there are cases in which a g as required by the Lemma doesn't exist.
In fact, slightly modifying our previous example, let $P := C[X,Y]$, $f = X$, I the ideal generated by $X - X^2$, V the variety defined by I, which is the union of the two lines $x = 0$, $x = 1$.
The polynomial function $f(x,y) = x$ vanishes identically in any point of V which is sufficiently near to the origin, so it actually coincides with the polynomial function $g(x,y) = 0$.
This is reflected by the fact that in the set R_f there is no g s.t. $in(g) \notin in(I) = (X)$: in fact if $g - f \in I$, then $g - X = h\,(X - X^2)$ for some polynomial h, so $g = X + h\,(X - X^2) = X\,(1 + h\,(1 - X))$ and in(g) is a multiple of X. However $X \notin I$.

Remark however that the vanishing of the polynomial function x is reflected by the fact that $X = (1 - X)^{-1}\,(X - X^2)$ so X belongs to the ideal generated by $X - X^2$ in any ring containing the inverse of $(1 - X)$; introducing the inverse of $(1 - X)$ makes sense, since "near the origin" $1 - X$ never vanishes so it is an invertible function.
In fact we can actually find a natural solution to our problem by considering the "local" nature of both our problem (infinitesimal orders, lowest order approximations at a point) and of our data (functions defined near a point) and so by carrying on the machinery we have developed to the larger ring of the rational functions which are defined in 0,

$Loc(P) := \{(1+g)^{-1} f : f, g \in P, g(0) = 0\} \subset k(X_1,\dots,X_n)$

where we define, for $h = (1+g)^{-1} f$, and for an ideal $I \subset Loc(P)$:

$in(h) := in(f)$, $ord(h) := ord(f)$, $in(I) := (in(h) : h \in I) \subset P$

preserving the geometrical meaning of these notions.
Also we can define, for $h = (1+g)^{-1} f$, and for an ideal $I \subset Loc(P)$:

$M(h) := M(f)$, $T(h) := T(f)$, $M(I) := (M(h) : h \in I) \subset P$.

As we will establish in the next section, the following holds:

FACT If $I \subset Loc(P)$ is an ideal and $h \in Loc(P)$, then there is $h_0 \in Loc(P)$ s.t.

i) either $h_0 = 0$ or $M(h_0) \notin M(I)$

ii) $h - h_0 \in I$

(i.e. a normal form of h w.r.t. I)

As a consequence we have:

PROPOSITION 5 Let $I \subset Loc(P)$ be an ideal. Let $F \subset I$ be s.t. $M(F) = M(I)$. Let $h \in Loc(P)$.
Let $h_0 \in Loc(P)$ be s.t. $h - h_0 \in I$ and either $h_0 = 0$ or $M(h_0) \notin M(I)$
Then:

i) $\{in(f) : f \in F\}$ generates in(I).

ii) $\{in(f) : f \in F\}$ is a Gröbner basis of in(I) w.r.t. the well-ordering $<_w$.

iii) if $h_0 = 0$, then $h \in I$

iv) if $h_0 \neq 0$, $in(h_0) \notin in(I)$

v) if $h_0 \neq 0$, $g - h \in I$ and $\mathrm{ord}(g) < \mathrm{ord}(h_0)$, then $\mathrm{in}(g) \in \mathrm{in}(I)$.
vi) if $h_0 \neq 0$, $g - h \in I$ and $\mathrm{ord}(g) \geq \mathrm{ord}(h_0)$, then $\mathrm{ord}(g) = \mathrm{ord}(h_0)$, $\mathrm{in}(g) - \mathrm{in}(h_0) \in \mathrm{in}(I)$.

Proof: i) and ii): The proof is the same as for Prop. 4, since $\forall h \in \mathrm{Loc}(P)$, $M(h) = M(\mathrm{in}(h))$.
iii) It is obvious
iv) If $\mathrm{in}(h_0) \in \mathrm{in}(I)$, then $M(h_0) = M(\mathrm{in}(h_0)) \in M(\mathrm{in}(I)) = M(I)$
v) and vi): The proof is the same as for Lemma 8.

As a consequence, the infinitesimal order at the origin of the rational function $h(x_1,\ldots,x_n)$ is $\mathrm{ord}(h_0)$, its lowest order Taylor approximation at the origin is the residue class of $\mathrm{in}(h_0)$ in $P/\mathrm{in}(I)$, which can be canonically represented by $\mathrm{Can}(\mathrm{in}(h_0),\mathrm{in}(I))$.
To go back to the example we are discussing, in $\mathrm{Loc}(P)$ we have $X = (1 - X)^{-1} (X-X^2) \in (X - X^2)$, reflecting the fact that x vanishes identically in any point of V which is sufficiently near to the origin.

Having motivated our interest in extending the Gröbner basis theory to the case of orderings which are not well-orderings, we have yet to justify our choice of the ring $\mathrm{Loc}(P)$; could not a smaller ring R, $P \subset R \subset \mathrm{Loc}(P)$ be sufficient so that:

for each ideal $I \subset R$, for each f, there is g s.t. $f - g \in I$ and either $g = 0$ or $\mathrm{in}(g) \notin \mathrm{in}(I)$?

The answer is no. In fact:

PROPOSITION 6 Let R be a ring s.t. $P \subset R \subset \mathrm{Loc}(P)$ and for each ideal $I \subset R$, for each f, there is g s.t. $f - g \in I$ and either $g = 0$ or $\mathrm{in}(g) \notin \mathrm{in}(I)$.
Then $R = \mathrm{Loc}(P)$.

Proof: We have just to prove that for each $f \in P$ s.t. $f(0) = 0$, $1 - f$ has an inverse in R.
The proof will just generalize the case of $f = X$, $I = (X - X^2)$.
In fact consider the ideal $I = (f - f^2)$ and the element f.
First of all, since $\mathrm{ord}(f) > 0$, we have $\mathrm{ord}(f^2) = 2\,\mathrm{ord}(f) > \mathrm{ord}(f)$, so $\mathrm{in}(f - f^2) = \mathrm{in}(f)$, $\mathrm{in}(I) = (\mathrm{in}(f))$.
If f is not in I, then there are $g \neq 0$, $p \in R$ s.t. $f - g = p\,(f - f^2)$ and $\mathrm{in}(g) \notin \mathrm{in}(I) = (\mathrm{in}(f))$; however, since $g = f\,(1 - p + f) \in (f)$, $\mathrm{in}(g) \in (\mathrm{in}(f))$.
So $f \in I$, $f = p\,(f - f^2)$, and, dividing by f, $1 = p\,(1 - f)$ in R. So p is the inverse in R of $1 - f$.

2.3 A theory of standard bases

From the example at the beginning of the section and the results summarized in Propositions 5 and 6, we immediately realize that a theory of "Gröbner bases" w.r.t. orderings which are not well-orderings cannot be carried on the polynomial ring, but also we got hints that it is perhaps possible to recover it in a localization.
Namely we would like to prove that in such a localization, a generalization of Proposition 1 and Lemma 3 hold, and that they can be used to prove a generalization of Theorem 1.
If such generalizations can be proved and a constructive proof of the existence of normal forms can be given, then we can easily prove that the only thing we have to modify in the Gröbner basis algorithm is just the normal form procedure.
In this section we will assume as a fact, the existence of normal forms in a suitable localization of the polynomial ring and we will show how, under such assumption, Theorem 1 can be stated and proved in a general setting.
The next section will be devoted to prove the existence of normal forms and to derive an algorithm for their computation.

It is known [ROB1] that a semigroup ordering $<$ on $\mathbf{T}$ is, non uniquely, characterized by an array $(\mathbf{u}_1,\ldots,\mathbf{u}_n)$ of vectors $\mathbf{u}_i \in \mathbf{R}^n$ s.t.defining, for $t = X_1^{a_1}\ldots X_n^{a_n} \in \mathbf{T}$, $w_i(t)$ to be the scalar product $\mathbf{u}_i\cdot(a_1,\ldots,a_n)$
then

$t_1 < t_2$ iff there is i with $w_j(t_1) = w_j(t_2)$ for $j < i$, $w_i(t_1) < w_i(t_2)$

We will restrict ourselves to those orderings s.t. there is $r \leq n$ s.t.

$\mathbf{u}_i \in \mathbf{Z}^n$ for $i \leq r$
$\forall\, d_1,\ldots,d_r \in \mathbf{Z}$, $\{t \in \mathbf{T} : w_i(t) = d_i\ i=1\ldots r\}$ doesn't contain any infinite decreasing sequence $t_1 > \ldots > t_s > \ldots$

and we will call any such ordering a *tangent cone ordering*.
The example of a degree anti-compatible ordering as discussed above, i.e. an ordering $<$ s.t.

for $m_1, m_2 \in \mathbf{T}$, $\deg(m_1) < \deg(m_2) \Rightarrow m_1 > m_2$

enters in this class.
In fact consider $\mathbf{u}_1 := (-1,\ldots,-1)$, so that $w_1(t) = -\deg(t)$; it is clear that for each $d \in \mathbf{Z}$, there are just finitely many terms t with $-\deg(t) = d$.

Let $P := k[X_1,\ldots,X_n]$, k a field, and $\mathbf{T}$ be the free commutative semigroup generated by $\{X_1,\ldots,X_n\}$ endowed with a semigroup ordering $<$ satisfying the above condition.
Let $\mathrm{Loc}(P)$ denote the following subring of $k(X_1,\ldots,X_n)$:

$\mathrm{Loc}(P) := \{\, (1+g)^{-1} f \in k(X_1,\ldots,X_n) \text{ s.t } T(g) < 1 \}$.

We can define, for $h = (1+g)^{-1} f$, and for an ideal $I \subset \mathrm{Loc}(P)$:

$M(h) := M(f)$, $T(h) := T(f)$, $M(I) := (M(h) : h \in I) \subset P$.

DEFINITION 5 Given $f \in \mathrm{Loc}(P) - \{0\}$, $F \subset \mathrm{Loc}(P) - \{0\}$, an element $h \in \mathrm{Loc}(P)$ is called a *normal form* of f w.r.t. F if

$f - h = \Sigma\, g_i f_i$, $g_i \in \mathrm{Loc}(P) - \{0\}$, $f_i \in F$
either $h = 0$ or $M(h) \notin M(F)$.

$\mathrm{Nf}(f,F)$ will denote the set $\{h \in \mathrm{Loc}(P)$: h is a normal form of f w.r.t. F$\}$

DEFINITION 6 We say $h \in \mathrm{Loc}(P)-\{0\}$ has a *standard representation* in terms of $F \subset \mathrm{Loc}(P) - \{0\}$ iff it can be represented:

$f = \Sigma\, g_i f_i$, $g_i \in \mathrm{Loc}(P) - \{0\}$, $f_i \in F$, $T(g_i)\, T(f_i) \le T(f)$ for every i

(such a representation will be called a standard representation).

DEFINITION 7 A set $F \subset I - \{0\}$ is called a *standard basis* for the ideal $I \subset \mathrm{Loc}(P)$ iff $M\{F\}$ generates the ideal $M(I)$[1].

We begin by showing some properties of normal forms with respect to a standard set; property 1) shows that they can be used (assuming their existence and computability) to decide ideal membership; properties 2) and 3) are a generalization of Prop. 5, v) and vi).

PROPOSITION 7 Let F be a standard basis for the ideal $I \subset \mathrm{Loc}(P)$, then:

1) let $h \in \mathrm{NF}(g,F)$; then:
 if $h = 0$, then $g \in I$
 if $h \neq 0$, $g \notin I$
2) if $h \in \mathrm{NF}(g,F)$, $h \neq 0$, then $T(h) = \min\{T(g') : g' - g \in I\}$
3) if $g, g' \in \mathrm{Loc}(P) - I$ are s.t. $g - g' \in I$, then $M(h) = M(h')$ for each $h \in \mathrm{NF}(g,F)$ and $h' \in \mathrm{NF}(g',F)$.

Proof: the proof of Prop. 2 applies verbatim.

Our aim now is to prove that for standard bases a characterization analogous to the one provided by Theorem 1 and Lemma 4 still holds, provided a suitable assumption about normal forms holds.

We begin by extending the functions T(-), M(-) to $\mathrm{Loc}(P)^t$. This extension will depend on the arbitrary choice of t terms $\mu_1,\ldots,\mu_t$[2] as follows:

for each $(g_1,\ldots,g_t) = \Sigma\, g_i e_i \in \mathrm{Loc}(P)^t$ define:

$T(\Sigma\, g_i e_i) := \max\{T(g_i)\, \mu_i\}$
$M(\Sigma\, g_i e_i) := \Sigma_{i \in I}\, M(g_i)\, e_i \in P^t$ where $I := \{i : T(g_i)\, \mu_i = T(\Sigma\, g_i e_i)\}$.

If $\Phi \subset \mathrm{Loc}(P)^t$, denote $M\{\Phi\} := \{M(\phi) : \phi \in \Phi - \{0\}\}$, $M(\Phi)$ the submodule of P^t generated by $M\{\Phi\}$.

Clearly the notions of T(-) and M(-) restrict to $P^t \subset \mathrm{Loc}(P)^t$.

As in the first section, we say that an element $\phi = \Sigma\, m_i e_i$ of P^t is *homogeneous* iff for each i s.t. $m_i \neq 0$, then m_i is a monomial and $T(m_i)\, \mu_i = T(\phi)$; that a submodule of P^t is *homogeneous* if it is generated by homogeneous elements; $M(\Phi)$ is clearly a homogeneous submodule of P^t.

DEFINITION 8 We say that *Loc(P) has normal forms with standard representations* iff:

for each $\phi \in \mathrm{Loc}(P)^t - \{0\}$, $\Phi \subset \mathrm{Loc}(P)^t - \{0\}$, there is $\psi \in \mathrm{Loc}(P)^t$, s.t.
 either $\psi = 0$ or $M(\psi) \notin M(\Phi)$.
 $\phi - \psi = \Sigma\, g_i \phi_i$, $g_i \in \mathrm{Loc}(P) - \{0\}$, $\phi_i \in \Phi$, $T(g_i)\, T(\phi_i) \le T(\phi - \psi)$

NOTATION Let $f_1,\ldots, f_t \in \mathrm{Loc}(P) - \{0\}$, $F := \{f_1,\ldots,f_t\}$; let $I \subset \mathrm{Loc}(P)$ be an ideal s.t. $F \subset I$.

Let $\mu_i := T(f_i)$ and let T(-) and M(-) be defined in $\mathrm{Loc}(P)^t$ as above.

Define

$s : P^t \to P$ by $s(\Sigma\, g_i e_i) := \Sigma\, g_i M(f_i)$;

then the kernel of s

$\mathrm{Syz}\{M(f_1),\ldots,M(f_t)\} := \mathrm{Ker}(s)$

is the module of syzygies among $\{M(f_1),\ldots,M(f_t)\}$, which is a homogeneous submodule of P^t.

Define $S : \mathrm{Loc}(P)^t \to \mathrm{Loc}(P)$ by $S(\Sigma\, g_i e_i) := \Sigma\, g_i f_i$ and remark that if u is a homogeneous element in Ker(s), then $T(S(u)) < T(u)$.

If u is a homogeneous element in Ker(s), we say that u *lifts* to $v \in \mathrm{Ker}(S)$ (v is a *lifting* of u) if $M(v) = u$.

[1] The reasons we introduce the term "standard" instead of "Gröbner" are two:

i) there is an historical reason since standard bases (according to definition 7) were introduced for the ring of formal power series by Hironaka in 1964, one year before Buchberger introduced Gröbner bases. An algorithm to compute standard bases in formal power series rings, also under suitable computational assumptions, is still lacking, and the tangent cone algorithm was actually the first algorithm for standard bases computations, in case the input is given by polynomials or rational functions.

ii) while the theory of Gröbner and standard bases is essentially the same, many of the most favorite characterizations of Gröbner bases cannot be generalized to standard bases, namely the rewrite-rule characterization.

So it is perhaps better to restrict the "Gröbner" terminology to the well-ordered cases and the "standard" one to all non well-ordered situations.

[2] In the applications, in analogy with the first section, $\mu_i = T(f_i)$ for some set $\{f_1,\ldots,f_t\} \subset \mathrm{Loc}(P)$.

Let U be a basis of Ker(s) consisting of homogeneous elements.

THEOREM 2 If Loc(P) has normal forms with standard representations[1], the following conditions are equivalent:

1) F is a standard basis of I

2) $f \in I$ iff f has a standard representation in terms of F

3) for each $f \in \mathrm{Loc}(P) - \{0\}$:

i) if $f \in I$, then $NF(f,F) = \{0\}$

ii) if $f \notin I$, then $NF(f,F) \neq \emptyset$ and $\forall h \in NF(f,F)$, $h \neq 0$.

4) F is a basis of I and for each $u \in U$, u has a lifting

Proof: 1) ⇒ 3) Let $f \in \mathrm{Loc}(P) - \{0\}$. By assumption, f has a normal form w.r.t. F.

There are two cases:

1) $NF(f,F) = \{0\}$.

In this case $f \in (F) \subset I$.

2) there is $h \in NF(f,F) - \{0\}$

In this case, then $M(h) \notin M(F) = M(I)$, implying $h \notin I$; since $f - h \in (F) \subset I$, then $f \notin I$.

Moreover, if $0 \in NF(f,F)$, then $f \in (F) \subset I$, a contradiction, so $0 \notin NF(f,F)$.

3) ⇒ 2) If f has a standard representation in terms of F, then $f \in (F) \subset I$.

For each $f \in \mathrm{Loc}(P)$, by assumption, there is $h \in NF(f,F)$ s.t. $f - h$ has a standard representation in terms of F.

If $f \in I$, then $NF(f,F) = \{0\}$, so $h = 0$ and f has a standard representation in terms of F.

2) ⇒ 1) We have just to show that if $f \in I$, then $M(f) \in M(F)$.

Let $f \in I$, $m = M(f)$, $f = \Sigma\, g_i f_i$ a standard representation in terms of F. Let $I := \{i : T(g_i)\, T(f_i) = T(f)\}$.

Then $m = M(f) = \Sigma_{i \in I} M(g_i)\, M(f_i) \in M(F)$.

2) ⇒ 4) Since each $f \in I$ has a standard representation in terms of F, in particular we have $f \in (F)$; so F is a basis of I.

Let $u \in U$ and let $h = S(u)$. Then $T(h) < T(u)$. So let $\Sigma\, g_i f_i$ be a standard representation of h and define $v := u - \Sigma\, g_i e_i$.

Then $S(v) = S(u) - \Sigma\, g_i f_i = h - h = 0$ so $v \in \mathrm{Ker}(S)$.

Moreover $T(g_i)\, T(f_i) \leq T(h) < T(u)$, so $u = M(v)$.

4) ⇒ 2) We show that each $h \in I$ has a standard representation.

Since $h \in I$, and F is a basis of I, there is a representation $h = \Sigma_i h_i f_i$.

Let $\phi := (h_1, \ldots, h_t) \in \mathrm{Loc}(P)^t$.

For each $u \in U$, let $\mathrm{lift}(u) \in \mathrm{Ker}(S)$ be a lifting of U; let $V := \{\mathrm{lift}(u) : u \in U\}$.

By assumption, we know that there is $\phi' = (h'_1, \ldots, h'_t)$ s.t. $\phi - \phi' \in (V)$ and either $\phi' = 0$ or $M(\phi') \notin (U) = M(V)$.

Then $\phi - \phi' \in \mathrm{Ker}(S)$ so $\Sigma\, h'_i f_i = S(\phi') = S(\phi) = h$; therefore $T(\phi') = \max\{T(h'_i)\, T(f_i)\} \geq T(h)$.

If $T(\phi') > T(h)$, let $J := \{j : T(h'_j)\, T(f_j) = T(\phi')\}$, then $M(\phi') = \Sigma_{j \in J} M(h_j)\, M(f_j) = 0$, i.e. $\Sigma_{j \in J} M(h_j)\, e_j$ is a homogeneous element in Ker(s), so $M(\phi') \in (U) = M(V)$, while $M(\phi') \notin M(V)$.

3 NORMAL FORMS AND NORMAL FORM ALGORITHMS IN LOCALIZATIONS

The reader can immediately verify that, if Loc(P) has normal forms with standard representations, then Theorem 2 is sufficient to prove termination and correctness of the algorithm **GröbnerBasis** also for a tangent cone ordering which is not a well-ordering, provided we substitute each call of NF, by a call of some algorithm which, given $f \in \mathrm{Loc}(P)$, $F \subset \mathrm{Loc}(P)$, returns a normal form g of f w.r.t. F, s.t. $g - f$ has a standard representation in terms of F.[2]

So our next step is obliged: we must give a constructive proof of the fact that, for a tangent cone ordering, Loc(P) has normal forms with standard representations.

We will discuss separately the following three cases:

1) normal forms in the polynomial ring for a degree anticompatible ordering

2) normal forms in the polynomial ring for any tangent cone ordering

3) normal forms in a polynomial module for any tangent cone ordering.

The reason is that case 1) is much more easy to describe and it gives an introduction for the more difficult case 2), while case 3) is just needed for the proof of Theorem 2 but is not required in the algorithm, so, unlike the first two cases, its proof is not relevant for the description of the algorithm.

3.1 Normal forms and normal form algorithms: the case of a degree anti-compatible ordering.

Let < be a degree anti-compatible ordering, i.e.

for $m_1, m_2 \in \mathbf{T}$., $\deg(m_1) < \deg(m_2) \Rightarrow m_1 > m_2$

and let $\mathbf{u}_1 := (-1, \ldots, -1)$, so that $w_1(t) = -\deg(t)$.

We will use the notation set up in §2.2.

[1] The reader can verify that in the proof we need normal forms with standard representations only for ring elements, while for module elements one just needs normal forms. We have chosen this formulation, since it is easier to express and (probably) it is equivalent to the exact condition needed. We remark that, to generalize Buchberger and the tangent cone algorithms to modules, one needs a different notion of standard representations for module elements.

[2] Actually we should also give a proof that Buchberger criterion (Lemma 5) holds in this more general setting. Since in our application F consists of polynomials and the proof never makes reference to the ordering, the proof of Lemma 5 can be repeated verbatim.

Since we are mainly interested in an algorithmic proof of the existence of normal forms with standard representations, it is better to start with our trivial example 2.1 and try to understand how to modify the procedure NF in order that it halts at least in that case, by using our new knowledge that in Loc(P), $X = (1 - X)^{-1} (X - X^2)$.

It turns out that we are able to explicitly obtain this representation, if we allow ourselves to reduce not just with elements in the original set F but also with results of previous reductions. In fact we have, then:

$h := X, F := \{X - X^2\}, f := X - X^2, \mathrm{Red}(h,f) = X^2$
$h := X^2, F := \{X - X^2, X\}, f := X, \mathrm{Red}(h,f) = 0$

by which we reconstruct:

$X^2 = X\,X$
$X = 1\,(X - X^2) + X^2 = 1\,(X - X^2) + X\,X$
$X\,(1 - X) = 1\,(X - X^2)$
$X = (1 - X)^{-1}\,(X - X^2).$

Obviously, just allowing ourselves to enlarge the set of reductors is not sufficient to guarantee termination; actually with most of Buchberger algorithm implementations, where the first reductor is always used, we would still have the infinite computation:

$h := X, F := \{X - X^2\}, f := X - X^2, \mathrm{Red}(h,f) = X^2$
$h := X^2, F := \{X - X^2,X\}, f := X - X^2, \mathrm{Red}(h,f) = X^3$
...
$h := X^n, F := \{X - X^2,X,\ldots,X^{n-1}\}, f := X - X^2, \mathrm{Red}(h,f) = X^{n+1}$
...

Assume however that, at some stage, we have to reduce a homogeneous polynomial and we can reduce it using a homogeneous polynomial; the result will be again homogeneous and of the same degree. If from that point on we could always reduce by homogeneous polynomials, we would find a sequence of homogeneous polynomials all of the same degree and whose maximal terms form a decreasing sequence. Since there are just finitely many terms of some fixed degree (or with a fixed value $w_1(t)$), such a sequence should necessarily end either with 0 or with an polynomial which is not further reducible, i.e. whose maximal term is not in the maximal term ideal.

To hope for such luck is nonsense; however, this scenario suggests us a strategy which, non trivially, can be proved to guarantee termination:

at any stage reduce with an element (including the previous reduction results) in order to make the result "as homogeneous as possible".

We formalize this rough idea by introducing the notion of *ecart*, E(f), which actually measures how far a polynomial is from being homogeneous:

if $f \in P - \{0\}$ define

$E(f) := \deg(f) - \mathrm{ord}(f) \in N.$

LEMMA 9 1) If $f, g \in P - \{0\}$, $t \in T$ is s.t. $T(f) = t\,T(g)$, then $E(\mathrm{Red}(f,g)) \leq \max(E(f),E(g))$
2) if, moreover, $E(g) \leq E(f)$ and $E(\mathrm{Red}(f,g)) = E(f)$, then $\mathrm{ord}(\mathrm{Red}(f,g)) = \mathrm{ord}(f)$.

Proof: i) For some $c \in k-\{0\}$, $\mathrm{Red}(f,g) = g - c\,t\,f$; also $\mathrm{ord}(g) = \mathrm{ord}(c\,t\,f)$, $E(c\,t\,f) = E(f)$. So $\mathrm{ord}(\mathrm{Red}(f,g)) \geq \mathrm{ord}(c\,t\,f) = \mathrm{ord}(g) =: d$ and $\deg(\mathrm{Red}(f,g)) \leq \max\{\deg(c\,t\,f), \deg(g)\}$. So $E(\mathrm{Red}(f,g)) \leq \max\{\deg(c\,t\,f), \deg(g)\} - d \leq \max\{E(f), E(g)\}$.

ii) $\mathrm{ord}(f) \leq \mathrm{ord}(\mathrm{Red}(f,g)) = \deg(\mathrm{Red}(f,g)) - E(\mathrm{Red}(f,g)) \leq \deg(f) - E(f) = \mathrm{ord}(f)$.

LEMMA 10 Let $F \subset P - \{0\}$ be a finite set, $g_0 \in P - \{0\}$.

Then there is no infinite sequence $g_0,\ldots,g_i,\ldots$ with $g_i \in P - \{0\}$ s.t., denoting $F_0 := F$, $F_i := F_{i-1} \cup \{g_{i-1}\}$:

1) $\forall\, i \geq 0$, $M(g_i) \in M(F_i)$
2) $\forall\, i \geq 0$, there is $h_i \in F_i$ s.t. $g_{i+1} = \mathrm{Red}(g_i,h_i)$
3) $\forall\, i \geq 0$, if $h'_i \in F_i$ is s.t. $T(h'_i)$ divides $T(g_i)$ then $\max(E(g_i), E(h_i)) \leq \max(E(g_i), E(h'_i))$.

Proof: Assume an infinite sequence $g_0,\ldots,g_i,\ldots$ with $g_i \in P - \{0\}$ be given satisfying 1), 2) and 3).

Since there is just a finite number of terms t having a fixed degree deg(t) and $T(g_i) > T(g_{i+1})$ for each i, the existence of such an infinite sequence implies that the sequence $\mathrm{ord}(g_i)$ is not definitely constant. We want to show that the assumptions imply that $\mathrm{ord}(g_i)$ is a definitely constant sequence, giving a contradiction and proving that no infinite sequence satisfying 1), 2) and 3) exists.

Since, for each α, $E(g_{\alpha+1}) \leq \max(E(g_\alpha)), E(h_\alpha))$, denoting $E := \max\{E(g) : g \in F_1\}$, we can conclude that for each α, $E(g_\alpha) \leq E$.

Define $d_1 := \min\{d \leq E \text{ s.t. } E(g_r) = d \text{ for infinitely many } r\}$.

Then there is an index N_1 s.t. for $r \geq N_1$, $E(g_r) \geq d_1$. By Dickson Lemma there is an index N_2 s.t. if $E(g_r) = d_1$, then $M(g_r)$ is in the ideal generated by $\{M(g_u) : u \leq N_2, E(g_u) \leq d_1\}$. Let $N := \max\{N_1,N_2\}$.

Let $r \geq N$ be s.t. $E(g_r) = d_1$.

Then $r \geq N_1$ implies that $E(g_{r+1}) \geq d_1$; we want to prove that $E(g_{r+1}) = d_1$.

In fact, since $r \geq N_2$ and $E(g_r) = d_1$, there is $h'_r \in F_r$ s.t. $T(h'_r)$ divides $T(g_r)$ and $E(h'_r) \leq d_1$.

So $E(g_{r+1}) \leq \max(E(g_r), E(h_r)) \leq \max(E(g_r), E(h'_r)) = d_1$.

We can therefore conclude that there is an index N' s.t. for $r \geq N'$, $E(g_r) = d_1$, i.e. $E(g_{r+1}) = E(g_r) \geq E(h_r)$.

By Lemma 9.ii) then we can conclude that for $r > N'$, $\mathrm{ord}(g_{r+1}) = \mathrm{ord}(g_r)$, so the sequence $\mathrm{ord}(g_i)$ is definitely constant, giving the desired contradiction.

LEMMA 11 Let $F \subset P - \{0\}$ be a finite set, $g_0 \in P - \{0\}$.
Then there are $g_0,\dots,g_s$ with $g_i \in P$, and $g_i \neq 0$ if $i < s$, s.t., denoting $F_0 := F$, $F_i := F_{i-1} \cup \{g_{i-1}\}$:

1) $\forall\, i,\ 0 \le i < s$, $M(g_i) \in M(F)$
2) $\forall\, i,\ 0 \le i < s$, there is $h_i \in F_i$ s.t. $g_{i+1} = \mathrm{Red}(g_i,h_i)$
3) $\forall\, i,\ 0 \le i < s$, if $h'_i \in F_i$ is s.t. $T(h'_i)$ divides $T(g_i)$ then $\max(E(g_i), E(h_i)) \le \max(E(g_i), E(h'_i))$
4) either $g_s = 0$ or $M(g_s) \notin M(F)$
5) $\forall\, i,\ 0 \le i < s$, $T(g_s) < T(g_i)$ and there are $f_j \in F_i$, $a_{ij} \in \mathrm{Loc}(P)$ and u_i, a unit in $\mathrm{Loc}(P)$, s.t.

$$g_i - u_i\, g_s = \Sigma\, a_{ij}\, f_j \text{ with } T(a_{ij})\, T(f_j) \le T(g_i)$$

<u>Proof</u>: 1), 2), 3) specify how to define recursively a (possibly infinite) sequence $g_0,\dots,g_i,\dots$, while 4) specifies the condition under which the sequence terminates.
Because of Lemma 10, a sequence satisfying 1), 2), 3) is necessarily finite; if its last element g_s doesn't satisfy 4), then $M(g_s) \in M(F_s)$, so a new element g_{s+1} can be added to the sequence.
Therefore, if $g_0,\dots,g_s$ is a maximal sequence satisfying 1), 2), 3) then g_s necessarily satisfies 4).
Hence, we have just to prove 5).
If $i = s-1$, the thesis obviously holds, since, by construction, $g_{s-1} = g_s + c\, t\, h$ with $c \in k - \{0\}$, $t \in T$, $h \in F_{s-1}$ and $T(g_s) < T(g_{s-1}) = t\, T(h)$.
So we can assume it holds for i, i.e.

$$g_i = \Sigma_j\, a_j\, f_j + u_i\, g_s, \text{ with } a_j \in \mathrm{Loc}(P),\ f_j \in F_i,\ u_i \text{ a unit in } \mathrm{Loc}(P),\ T(g_s) < T(g_i),\ T(g_i) \ge T(a_j)\, T(f_j).$$

and prove it for i-1.
We have also $g_i = g_{i-1} - c\, t\, h$ with $c \in k - \{0\}$, $t \in T$, $h \in F_{i-1}$, and $T(g_i) < T(g_{i-1}) = t\, T(h)$.
So $g_{i-1} = g_i + c\, t\, h = \Sigma_j\, a_j\, f_j + c\, t\, h + u_i\, g_s$, with $h \in F_{i-1}$, $f_j \in F_{i-1} \cup \{g_{i-1}\}$.
So, if $J' := \{j : f_j \in F_{i-1}\}$ and $J'' := \{j : f_j = g_{i-1}\}$:

$$g_{i-1} = \Sigma_{j\in J'}\, a_j\, f_j + (\Sigma_{j\in J''}\, a_j)\, g_{i-1} + c\, t\, h + u_i\, g_s,$$
$$(1 - \Sigma_{j\in J''}\, a_j)\, g_{i-1} = \Sigma_{j\in J'}\, a_j\, f_j + c\, t\, h + u_i\, g_s.$$

Also $T(g_{i-1}) = t\, T(h) > T(g_i) \ge T(a_j)\, T(f_j)$ for all j.
So if $j \in J''$, $T(a_j) < 1$ and, denoting $q := \Sigma_{j\in J''}\, a_j$, $T(q) < 1$, $a := 1 - q$ is a unit in $\mathrm{Loc}(P)$.
Therefore $g_{i-1} = \Sigma_{j\in J'}\, a^{-1}\, a_j\, f_j + c\, a^{-1}\, t\, h + u_i\, a^{-1}\, g_s$ is the required representation.

COROLLARY 2 For each $f \in \mathrm{Loc}(P) - \{0\}$, $F \subset \mathrm{Loc}(P) - \{0\}$, there is $h \in \mathrm{Loc}(P)$ s.t.

i) h is a normal form of f w.r.t. F
ii) f - h has a standard representation in terms of F.

<u>Proof</u>: If F is infinite, there is a finite subset $F_1 \subset F$, s.t. $M(F) = M(F_1)$. Clearly if h satisfies the thesis for F_1, it satisfies it for F too. So we can assume F is finite, $F = (f_1,\dots,f_r)$.
There are polynomials h, g, h_i, g_i with $T(g) < 1$, $T(g_i) < 1$, s.t. $f = (1+g)^{-1}\, h$, $f_i = (1+g_i)^{-1} h_i$.
If $p \in \mathrm{Loc}(P)$ is a normal form of h w.r.t. $(h_1,\dots,h_t)$ and $h - p = \Sigma\, a_i\, h_i$, $a_i \in \mathrm{Loc}(P)$ is a standard representation, then

$$f - (1+g)^{-1}\, p = \Sigma\, (1+g)^{-1}\, (1+g_i)\, a_i\, f_i$$

is a standard representation in terms of F and so $(1+g)^{-1}\, p$ is a normal form of f w.r.t. F.
So we are reduced to the case that $f \in P$ and F is a finite subset of P.
The proof in such case is an obvious consequence of Lemma 11.

Clearly, the following modified version of $\mathbf{NF}(g_0,F)$ allows to compute the g_s whose existence is proved in Lemma 11:

```
h := LNF$_0$(g,F)
where
        g is a non-zero element in P
        $F \subset P - \{0\}$ is a finite set.
        there is u a unit in Loc(P), s.t
                u h is a normal form of f w.r.t. F
                f - u h has a standard representation in terms of F
h := g
F' := F
While $h \neq 0$ and $M(h) \in M(F')$ do
        $F'' := \{f \in F' : T(f) \text{ divides } T(h)\}$
        Choose $f \in F''$ s.t. $\max(E(f),E(h)) \le \max(E(f'),E(h))$, $\forall\, f' \in F''$
        $F' := F' \cup \{h\}$
        h := Red(h,f)
```

3.2 Normal forms and normal form algorithms: the polynomial case

First of all, we would like to reinterpret the result in Section 3.1 in the more general context of a tangent cone ordering. We start remarking that if $<$ is an ordering anti-compatible with the degree as in section 2, it is characterized by an array of vectors $(u_1,\dots,u_n)$ where $u_1 = (-1,\dots,-1)$. Then if $f = \Sigma\, c_i\, m_i$, $c_i \in k-\{0\}$, $m_i \in T$, $m_1 > \dots > m_t$, then

$E(f) = deg(f) - ord(f) = w_1(m_1) - w_1(m_t)$.

We could give this definition of ecart in the general case, but we recall that we used the fact that there were just finitely many terms m with the same degree i.e. with $w_1(m)$ constant: in the general case this can be false (e.g. if $\mathbf{u}_1 = (1, 0,...0)$ then each term m which is free of X_1 is s.t. $w_1(m) = 0$). While the result (and the algorithm) above can be applied, with the new definition of ecart, in the more general case:

for each $d \in \mathbf{Z}$, there are just finitely many terms t with $w_1(t) = d$,

if this doesn't hold, we must make use also of the next "degrees" $w_2,..., w_r$.

So we say, for each $j \leq r$:

$f \in P = k[X_1,...,X_n]$ is j-homogeneous of degree $(d_1,...,d_j) \in \mathbf{Z}^j$ iff

$f = \Sigma c_l m_l$, $c_l \in k-\{0\}$, $m_l \in T$ and for each l, for each $i \leq j$, $w_i(m_l) = d_i$.

Clearly:

1) f j-homogeneous of degree $(d_1,...,d_j)$ implies f i-homogeneous of degree $(d_1,...,d_i)$ for $i < j$

2) each polynomial can be written uniquely as a finite sum of j-homogeneous polynomial of different degrees.

Order $\mathbf{Z}^j$ lexicographically and define

$in_j(f)$ to be the j-homogeneous component of highest degree in the decomposition of f

$deg_j(f) := (w_1(M(f)),...,w_j(M(f))$

(remark that for an degree anticompatible ordering $in_1(f)$ is $in(f)$ and $ord(f) = -w_1(M(f))$.

Clearly:

1) $in_j(f) = in_j(in_i(f))$ for $i < j$

2) $M(f) = M(in_j(f))$.

We can now measure "how far a polynomial is from being homogeneous" by the sequence $E_1(f),...,E_r(f)$, defined as follows:

i) f can be written as a finite sum of ρ 1-homogeneous polynomials f_λ of degrees e_λ, $e_1 > ...> e_\rho$. Define $E_1(f) := e_1 - e_\rho \in \mathbf{N}$.

ii) If f is a (j-1)-homogeneous polynomial of degree $(d_1,...,d_{j-1})$, f can be written as a finite sum of ρ j-homogeneous polynomials f_λ of degrees $(d_1,...,d_{j-1},e_\lambda)$, $e_1 > ...> e_\rho$. Define $E_j(f) := e_1 - e_\rho \in \mathbf{N}$. Then for $f \in P$, define $E_j(f) = E_j(in_{j-1}(f))$.

So in practice we are measuring how far f is from being homogeneous w.r.t. w_1, then how far $in_1(f)$ is from being homogeneous w.r.t. w_2, etc.

To give an example, let us consider < to be the converse of the lexicographical ordering on $k[X_1, X_2, X_3]$ with $X_1 > X_2 > X_3$; it is characterized by $\mathbf{u}_1 := (-1,0,0)$, $\mathbf{u}_2 := (0,-1,0)$, $\mathbf{u}_3 := (0,0,-1)$, so $w_i(t) = -deg_{X_i}(t)$ and with respect to this ordering one has:

$1 > X_3 > X_3^2 > ... > X_2 > X_2 X_3 > X_2 X_3^2 > ... > X_2^2 >... > X_1 > X_1 X_3 >... > X_1 X_2 > ... X_1^2 >...$

Consider

$f := X_1^2 + X_1^2 X_3^2 + X_1^2 X_2 X_3 + X_1^2 X_2^2 + X_1^2 X_2^2 X_3^n + X_1^4$

where the monomials are in decreasing order w.r.t. <.

Then

$w_1(X_1^2) = -2 \qquad w_1(X_1^4) = -4 \qquad E_1(f) = 2$

$in_1(f) = X_1^2 + X_1^2 X_3^2 + X_1^2 X_2 X_3 + X_1^2 X_2^2 + X_1^2 X_2^2 X_3^n$

$w_2(X_1^2) = 0 \qquad w_2(X_1^2 X_2^2 X_3^n) = -2 \qquad E_2(f) = 2$

$in_2(f) = X_1^2 + X_1^2 X_3^2$

$w_3(X_1^2) = 0 \qquad w_3(X_1^2 X_3^2) = -2 \qquad E_3(f) = 2$

$in_3(f) = X_1^2$

$M(f) = X_1^2$.

For $f, g \in P - \{0\}$, s.t. $T(f) = t\, T(g)$, for some $t \in \mathbf{T}$, define:

$ind(f,g) := \max\{j: E_j(g) \leq E_j(f)\}$

For notational convenience, we will denote $in_0(f) := f$.

REMARK Let $g, h \in P$ be s.t. $M(g) = c\, t\, M(h)$ for some $t \in \mathbf{T}$, $c \in k-\{0\}$. Let $g' := Red(g,h)$. Then:

1) If j is the minimal index s.t. $in_j(g) = in_j(c\, t\, h)$, so that $in_i(g) = in_i(c\, t\, h)$ for $i > j$, then:

If $i < j$ then $in_i(g) \neq in_i(c\, t\, h)$, $deg_i(g') = deg_i(g) = deg_i(c\, t\, h)$, $in_i(g') = in_i(g) - in_i(c\, t\, h)$, $E_i(g') \leq \max(E_i(g), E_i(h))$.

If $i = j$ then $in_j(g) = in_j(c\, t\, h)$, $deg_j(g') < deg_j(g) = deg_j(c\, t\, h)$, $E_j(g') < \max(E_j(g), E_j(h))$.

If $i > j$, then $in_i(g) = in_i(c\, t\, h)$, $deg_i(g') < deg_i(g) = deg_i(h)$, no relation holds among $E_i(g')$, $E_i(g)$, $E_i(h)$.

2) If $i \leq ind(g,h)$ and $in_{i-1}(g) \neq in_{i-1}(c\, t\, h)$, then $E_i(g') \leq E_i(g)$.

Let's go on with the example above and let

$g := X_1^2 + X_1^2 X_3^2 + X_1^2 X_2 X_3$

for which we have $g = in_1(g)$, $in_2(g) = in_2(f)$, $in_3(g) = in_3(f)$, $E_1(g) = 0$, $E_2(g) = 1$, $E_3(g) = 2$; $ind(f,g) = 3$.

Then $g' := Red(f,g) = f - g = X_1^2 X_2^2 + X_1^2 X_2^2 X_3^n + X_1^4$, so that

$deg_1(g') = deg_1(g) = deg_1(f) = -2$

$in_1(g') = X_1^2 X_2^2 + X_1^2 X_2^2 X_3^n = in_1(f) - in_1(g)$
$E_1(g') = 2 = \max(E_1(f), E_1(g))$
$deg_2(g') = (-2,-2) < deg_2(g) = (-2,0) = deg_2(f)$
$in_2(g') = X_1^2 X_2^2 + X_1^2 X_2^2 X_3^n$
$E_2(g') = 0 < \max(E_2(f), E_2(g))$
$deg_3(g') = (-2,-3,0) < deg_3(g) = (-2,0,0) = deg_3(f)$
$in_3(g') = X_1^2 X_2^2$
$E_3(g') = n$

In the case of a degree-anticompatible ordering, our reduction strategy was to reduce f by a g s.t. either $E(g) \le E(f)$ or $E(g)$ was minimal among all possible choices. We are generalizing that strategy as follows:
when reducing an element g by a set F, we are going to choose $h \in F$ s.t.

```
    for all $h' \in F$ with $T(g)$ multiple of $T(h')$
            $ind(g,h) \le ind(g,h')$
            if $i := ind(g,h) = ind(g,h') < r$, $E_{i+1}(h) \le E_{i+1}(h')$
```

LEMMA 12 Let $F \subset P - \{0\}$ be a finite set, $g_0 \in P - \{0\}$.
Then there is no infinite sequence $g_0,\ldots,g_i,\ldots$ with $g_i \in P - \{0\}$ s.t., denoting $F_0 := F$, $F_i := F_{i-1} \cup \{g_{i-1}\}$:
1) $\forall\, i \ge 0$, $M(g_i) \in M(F_i)$
2) $\forall\, i \ge 0$, there is $h_i \in F_i$ s.t. $g_{i+1} = Red(g_i,h_i)$
3) $\forall\, i \ge 0$, if $h'_i \in F_i$ is s.t. $T(h'_i)$ divides $T(g_i)$ then
$ind(g_i,h_i) \le ind(g_i,h'_i)$
if $\mu := ind(g_i,h_i) = ind(g_i,h'_i) < r$, $E_{\mu+1}(h_i) \le E_{\mu+1}(h'_i)$

Proof: Assume an infinite sequence $g_0,\ldots,g_i,\ldots$ with $g_i \in P - \{0\}$ be given satisfying 1), 2) and 3).
Let, for each α, $c_\alpha \in k-\{0\}$, $m_\alpha \in T$ be s.t. $g_{\alpha+1} = g_\alpha - c_\alpha m_\alpha h_\alpha$.
Since there is just a finite number of terms t having a fixed degree $deg_r(t)$ and $T(g_i) > T(g_{i+1})$ for each i, the existence of such an infinite sequence implies that the sequence $deg_r(g_i)$ is not constant, and so there is a minimal ρ s.t. the sequence $deg_\rho(g_i)$ is not definitely constant. We want to show that the assumptions imply that $deg_\rho(g_i)$ is a definitely constant sequence, giving a contradiction and proving that no infinite sequence satisfying 1), 2) and 3) exists.
The existence of a minimal ρ s.t. the sequence $deg_\rho(g_i)$ is not definitely constant, implies that there is N_0 s.t. $deg_j(g_i)$ is constant for $j < \rho$ and $i \ge N_0$.
For $\alpha \ge N_0$, the following hold:
i) since $deg_j(g_\alpha) = deg_j(g_{\alpha+1})$ for all $j < \rho$, $in_j(g_\alpha) \ne c_\alpha m_\alpha in_j(h_\alpha)$
ii) because of i) and Remark 1), $E_j(g_{\alpha+1}) \le \max(E_j(g_\alpha)), E_j(h_\alpha))$ for all $j \le \rho$
So, for $j \le \rho$, let $E_j := \max\{E_j(g) : g \in F_{N_0+1}\}$; we can conclude that:
for $j \le \rho$, for each $\alpha > N_0$, $E_j(g_\alpha) \le E_j$.
Define $d_\rho := \min\{d \le E_\rho$ s.t. $E_\rho(g_r) = d$ for infinitely many $r \ge N_0\}$.
Also for $j = \rho-1,\ldots,1$ define
$d_j := \min\{d \le E_j$ s.t. $E_i(g_r) = d_i$ for $i > j$, $E_j(g_r) = d$ for infinitely many $r \ge N_0\}$.
Then there is an index N_1 s.t. for $r \ge N_1$:
$E_\rho(g_r) \ge d_\rho$
for $1 \le j < \rho$ if $E_i(g_r) = d_i$ for $i > j$ then $E_j(g_r) \ge d_j$.
Consider the set
$M := \{M(g_r), E_i(g_r) = d_i \text{ for } 1 \le i \le \rho\}$
By Dickson Lemma there is an index N_2 s.t.
if $M(g_r) \in M$ then it is in the ideal generated by $\{M(g_u) : u \le N_2, E_i(g_u) \le d_i \text{ for } 1 \le i \le \rho\}$
So let $N := \max\{N_0,N_1,N_2\}$.
Let $r \ge N$ s.t. $E_i(g_r) = d_i$ for $1 \le i \le \rho$.
Then $r \ge N_1$ implies that either
$E_i(g_{r+1}) = d_i$ for $1 \le i \le \rho$
or there is j, $1 \le j \le \rho$, s.t.
$E_i(g_{r+1}) = E_i(g_r) = d_i$ for $i > j$
$E_j(g_{r+1}) > d_j$
We want to show that the second case cannot occur.
In fact since $r \ge N_2$ and $M(g_r) \in M$, there is $h'_r \in F_r$ s.t. $T(h'_r)$ divides $T(g_r)$ and $E_i(h'_r) \le d_i$ for $i = 1\ldots\rho$.
In particular $j \le \rho \le ind(g_r,h'_r) \le ind(g_r,h_r)$; so, since $in_{j-1}(g_r) = c_r m_r in_{j-1}(h_r)$, then $E_j(g_{r+1}) \le E_j(g_r) \le d_j$, by Remark 2).
We can therefore conclude that there is an index N' s.t. for $r \ge N'$
$E_j(g_r) = d_j$ for $1 \le j \le \rho$.
If $deg_\rho(g_{r+1}) < deg_\rho(g_r)$, then $\rho = \min\{i : in_i(g_r) = c_r m_r in_i(h_r)\}$ (since $in_i(g_r) \ne c_r m_r in(h_r)$ for $i < \rho$) and then $d_\rho = E_\rho(g_{r+1}) < \max\{E_\rho(g_r), E_\rho(h_r)) \le d_\rho$ (the inequality being a consequence of Remark 1), a contradiction.
This implies that $deg_\rho(g_r) = deg_\rho(g_{N'})$ for $r \ge N'$ and gives the desired contradiction.

LEMMA 13 Let $F \subset P - \{0\}$ be a finite set, $g_0 \in P - \{0\}$.
Then there are $g_0,\dots,g_s$ with $g_i \in P$, and $g_i \neq 0$ if $i < s$, s.t., denoting $F_0 := F$, $F_i := F_{i-1} \cup \{g_{i-1}\}$:

1) $\forall\, i$, $0 \leq i < s$, $M(g_i) \in M(F)$
2) $\forall\, i$, $0 \leq i < s$, there is $h_i \in F_i$ s.t. $g_{i+1} = \mathrm{Red}(g_i,h_i)$
3) $\forall\, i$, $0 \leq i < s$, if $h'_i \in F_i$ is s.t. $T(h'_i)$ divides $T(g_i)$ then
   $\mathrm{ind}(g_i,h_i) \leq \mathrm{ind}(g_i,h'_i)$
   if $\mu := \mathrm{ind}(g_i,h_i) = \mathrm{ind}(g_i,h'_i) < r$, $E_{\mu+1}(h_i) \leq E_{\mu+1}(h'_i)$
4) either $g_s = 0$ or $M(g_s) \notin M(F)$
5) $\forall\, i$, $0 \leq i < s$, $T(g_s) < T(g_i)$ and there is u_i, a unit in $\mathrm{Loc}(P)$, s.t.
   $u_i\, g_s$ is a normal form of g_0 w.r.t. F_{i-1}
   $g_i - u_i\, g_s$ has a standard representation in terms of F_{i-1}

Proof: Repeat verbatim the proof of Lemma 11.

COROLLARY 3 For each $f \in \mathrm{Loc}(P) - \{0\}$, $F \subset \mathrm{Loc}(P) - \{0\}$, there is $h \in \mathrm{Loc}(P)$ s.t.

i) h is a normal form of f w.r.t. F
ii) f - h has a standard representation in terms of F.

REMARK Let R be a ring s.t. $P \subset R \subset \mathrm{Loc}(P)$ and for each ideal $I \subset R$, for each f, there is $g \in NF(f,I)$. Then $R = \mathrm{Loc}(P)$ (cf. Prop. 6). So $\mathrm{Loc}(P)$ is the smaller ring available to have standard basis theory and algorithms.
In fact, if $f \in P$ is s.t. $T(f) < 0$, $1 - f$ is invertible: consider the ideal $I = (f - f^2)$ and the element f; since $T(f) < 1$, $T(f^2) < T(f)$, $M(f - f^2) = M(f)$, $M(I) = (M(f))$; let $g \in NF(f,I)$; if $g \neq 0$, then, for some $p \in R$, $f - g = p\,(f - f^2)$, so $M(g) = M(p)\, M(f) \in M(I)$, a contradiction; therefore $f \in I$, $f = p\,(f - f^2)$, for some $p \in R$, and, dividing by f, $1 = p\,(1 - f)$ in R. So p is the inverse in R of $1 - f$.

3.3 Normal forms and normal form algorithms: the module case

PROPOSITION 8 If $<$ is a tangent cone ordering, then $\mathrm{Loc}(P)$ has normal forms with standard representations.
Proof: First of all we need to extend to the module P^t all the relevant notation, as in § 3.2.
We start by extending the notion of j-homogeneous element to P^t; we recall that there are terms $\mu_1,\dots,\mu_t$ s.t. $T(e_i) = \mu_i$.
We say that $\phi = (f_1,\dots,f_t) \in P^t$, is *j-homogeneous* of degree $(d_1,\dots,d_j)$, $j \leq r$, iff:
   for each i, either $f_i = 0$ or $f_i\, \mu_i \in P$ is j-homogeneous of degree $(d_1,\dots,d_j)$.
We can then extend the functions in_j and the notion of *ecart* to P^t as follows:
clearly each $\phi \in P^t$ can be written as a finite sum of j-homogeneous elements ϕ_λ of different degrees $(d_{1\lambda},\dots,d_{j\lambda})$; order $\mathbf{Z}^j$ lexicographically and define:
   $\mathrm{in}_j(\phi)$ to be the j-homogeneous component of highest degree in the decomposition of ϕ
   $\deg_j(\phi) := \deg_j(\mathrm{in}_j(\phi)) = (w_1(T(\phi)),\dots,w_j(T(\phi)))$
   ϕ can be written as a finite sum of ρ 1-homogeneous elements ϕ_λ of degrees$(d_1,\dots,d_{j-1},e_\lambda)$, $e_1 > \dots > e_\rho$; define $E_1(\phi) := e_1 - e_\rho \in \mathbf{N}$.
   for a (j-1)-homogeneous $\phi \in P^t$ of degree $(d_1,\dots,d_{j-1})$, ϕ can be written as a finite sum of ρ j-homogeneous elements ϕ_λ of degrees$(d_1,\dots,d_{j-1},e_\lambda)$, $e_1 > \dots > e_\rho$; define $E_j(\phi) := e_1 - e_\rho \in \mathbf{N}$; then for $\phi \in P^t$, define $E_j(\phi) := E_j(\mathrm{in}_{j-1}(\phi))$.
We need now to define a strategy for reductions, generalizing the one of Lemmata 10 and 12, and reminding that (*cf.* the proof of Lemma 3) "reductions" for modules involve more than one reductor at each step.
So, for $\psi \in P^t$, $\Phi \subset P^t$ define:
   $\Phi(\psi,i) := (M(\phi): \phi \in \Phi \text{ s.t. } E_j(\phi) \leq E_j(\psi) \text{ for } j = 1\dots i)$
Clearly $\Phi(\psi,s) \subset \Phi(\psi,s-1) \subset \dots \subset \Phi(\psi,1)$
For $i = 0\dots s-1$, for $d \in \mathbf{N}$ define
   $\Phi(\psi,i,d) := (M(\phi) : \phi \in \Phi \text{ s.t. } E_j(\phi) \leq E_j(\psi) \text{ for } j = 1\dots i,\ E_i(\phi) \leq d)$
Clearly $\Phi(\psi,i,d) \subset \Phi(\psi,i,d+1) \subset \Phi(\psi,i)$ and $\Phi(\psi,i+1) = \Phi(\psi,i,E_{i+1}(\psi))$.
Let $\psi \in P^t$; if $M(\psi) \in M(\Phi)$ then there is a maximal $j := \mathrm{ind}(\psi,\Phi)$ s.t. $M(\psi) \in \Phi(\psi,j)$. Then (unless $j = r$) there is a minimal $d := E(\psi,\Phi)$ s.t. $M(\psi) \in \Phi(\psi,j,d)$.
An *optimal representation* of $M(\psi)$ in terms of $M(\Phi)$ is then a homogeneous representation $M(\psi) = \Sigma\, c_\alpha\, m_\alpha\, M(\phi_\alpha)$ with $c_\alpha \in k$, $m_\alpha \in \mathbf{T}$, $\phi_\alpha \in \Phi(\psi,j,d)$ with $j = \mathrm{ind}(\psi,\Phi)$, $d = E(\psi,\Phi)$, $m_\alpha\, T(\phi_\alpha) = T(\psi)$.
We remark the two following facts:
Let $\psi \in P^t$, $\Phi \subset P^t$, $M(\psi) = \Sigma\, c_\alpha\, m_\alpha\, M(\phi_\alpha)$ be an optimal representation in terms of $M(\Phi)$, $\psi_1 := \psi - \Sigma\, c_\alpha\, m_\alpha\, \phi_\alpha$.
Then:
1) If j is the minimal index s.t. $in_j(\psi) = \Sigma\, c_\alpha\, m_\alpha\, in_j(\phi_\alpha)$, so that $in_i(\psi) = \Sigma\, c_\alpha\, m_\alpha\, in_i(\phi_\alpha)$ for $i > j$, then:
If $i < j$ then $in_i(\psi) \neq \Sigma\, c_\alpha\, m_\alpha\, in_i(\phi_\alpha)$, $deg_i(\psi_1) = deg_i(\psi) = deg_i(\Sigma\, c_\alpha\, m_\alpha\, \phi_\alpha)$, $in_i(\psi_1) = in_i(\psi) - \Sigma\, c_\alpha\, m_\alpha\, in_i(\phi_\alpha)$, $E_i(\psi_1) \leq max(E_i(\psi), E_i(\phi_\alpha))$.
If $i = j$ then $in_j(\psi) = \Sigma\, c_\alpha\, m_\alpha\, in_j(\phi_\alpha)$, $deg_j(\psi_1) < deg_j(\psi) = deg_j(\Sigma\, c_\alpha\, m_\alpha\, \phi_\alpha)$, $E_j(\psi_1) < max(E_j(\psi), E_j(\phi_\alpha))$
2) If $i \leq ind(\psi,\Phi)$ and $in_{i-1}(\psi) \neq \Sigma\, c_\alpha\, m_\alpha\, in_{i-1}(\phi_\alpha)$, then $E_i(\psi_1) \leq E_i(\psi)$ (again denoting $in_0(\phi) := \phi$).

We can now turn to prove the proposition.

First of all we remark that, by the same argument of the proof of Corollaries 2 and 3, we can restrict to prove:

for each $\phi \in P^t - \{0\}$, Φ *a finite set in* $P^t - \{0\}$, *there is* $\psi \in P^t$, *s.t.*

either $\psi = 0$ *or* $M(\psi) \notin M(\Phi)$.

$\phi - \psi = \Sigma\, g_i\, \phi_i$, $g_i \in Loc(P) - \{0\}$, $\phi_i \in \Phi$, $T(g_i)\, T(\phi_i) \le T(\phi - \psi)$

The thesis derives then by the following two claims:

CLAIM 1 Let $\Phi \subset P^t - \{0\}$ *be a finite set,* $\psi_0 \in P^t - \{0\}$

Then there is no infinite sequence $\psi_0,\dots,\psi_i,\dots$ *with* $\psi_i \in P^t - \{0\}$ *s.t., denoting* $\Phi_0 := \Phi$, $\Phi_i := \Phi_{i-1} \cup \{\psi_{i-1}\}$:

1) $\forall\, i \ge 0$, $M(\psi_i) \in M(\Phi_i)$

2) $\forall\, i \ge 0$, *there are* $c_{i\alpha} \in k$, $m_{i\alpha} \in T$, $\phi_{i\alpha} \in \Phi_i$ *s.t.* $M(\psi_i) = \Sigma\, c_{i\alpha}\, m_{i\alpha}\, M(\phi_{i\alpha})$ *is an optimal representation,* $\psi_{i+1} = \psi_i - \Sigma\, c_{i\alpha}\, m_{i\alpha}\, \phi_{i\alpha}$

CLAIM 2 Let $\Phi \subset P^t - \{0\}$ *be a finite set,* $\psi_0 \in P^t - \{0\}$.

If $\psi_0,\dots,\psi_s$ *with* $\psi_i \in P^t$, $\psi_i \ne 0$ *for* $i < s$, *are s.t., denoting* $\Phi_0 := \Phi$, $\Phi_i := \Phi_{i-1} \cup \{\psi_{i-1}\}$:

1) $\forall\, i, 0 \le i < s$, $M(\psi_i) \in M(\Phi)$

2) $\forall\, i, 0 \le i < s$, *there are* $c_{i\alpha} \in k$, $m_{i\alpha} \in T$, $\phi_{i\alpha} \in \Phi_i$ *s.t.* $M(\psi_i) = \Sigma\, c_{i\alpha}\, m_{i\alpha}\, M(\phi_{i\alpha})$ *is an optimal representation,* $\psi_{i+1} = \psi_i - \Sigma\, c_{i\alpha}\, m_{i\alpha}\, \phi_{i\alpha}$

3) either $\psi_s = 0$ *or* $M(\psi_s) \notin M(\Phi)$

then:

4) $\forall\, i, 0 \le i < s$, *there are* $q_{i\alpha} \in Loc(P)$, u_i, *a unit in* $Loc(P)$, *s.t.*

$\psi_i - u_i\, \psi_s = \Sigma\, q_{i\alpha}\, \phi_{i\alpha}$ *with* $\phi_{i\alpha} \in F_i$, $T(q_{i\alpha})\, T(\phi_{i\alpha}) \le T(\psi_i - u_i\, \psi_s)$

Derivation of the thesis by the claims: 1) and 2) specify how to define recursively a (possibly infinite) sequence $\psi_0,\dots,\psi_i,\dots$; because of Claim 1), such a sequence is necessarily finite and then a maximal sequence $\psi_0,\dots,\psi_i,\dots,\psi_s$ satisfies 3) too. Because of 3) and Claim 2), then $u_0\, \psi_s$ satisfies the thesis.

Proof of Claim 1: Assume an infinite sequence $\psi_0,\dots,\psi_i,\dots$ with $\psi_i \in P^t - \{0\}$ be given satisfying 1), 2).

Since there is just a finite number of terms t s.t. $deg_r(t)$ assumes any fixed value, and $T(\psi_i) > T(\psi_{i+1})$ for each i, the existence of such an infinite sequence implies that there is a minimal ρ s.t. the sequence $deg_\rho(\psi_i)$ is not definitely constant. We want to show that the assumptions imply that $deg_\rho(\psi_i)$ is a definitely constant sequence, giving a contradiction and proving that no infinite sequence satisfying 1), 2) exists.

The existence of a minimal ρ s.t. the sequence $deg_\rho(\psi_i)$ is not definitely constant, implies that there is N_0 s.t. $deg_j(\psi_i)$ is constant for $j < \rho$ and $i \ge N_0$.

For $i \ge N_0$, the following hold:

i) since $deg_j(\psi_i) = deg_j(\psi_{i+1})$ for all $j < \rho$, $in_j(\psi_i) \ne \Sigma\, c_{i\alpha}\, m_{i\alpha}\, in_j(\phi_{i\alpha})$

ii) because of i) and of remark 1) above, $E_j(\psi_{i+1}) \le \max(E_j(\psi_i)), E_j(\phi_{i\alpha}))$ for all $j \le \rho$

So, for $j \le \rho$, let $E_j := \max\{E_j(\psi) : \psi \in \Phi_{N_0+1}\}$; we can conclude that:

for $j \le \rho$, for each $i > N_0$, $E_j(\psi_i) \le E_j$.

Define $d_\rho := \min\{d \le E_\rho$ s.t. $E_\rho(\psi_r) = d$ for infinitely many $r \ge N_0\}$.

Also for $j = \rho-1,\dots,1$ define

$d_j := \min\{d \le E_j$ s.t. $E_i(\psi_r) = d_i$ for $i > j$, $E_j(\psi_r) = d$ for infinitely many $r \ge N_0\}$.

Then there is an index N_1 s.t. for $r \ge N_1$:

$E_\rho(\psi_r) \ge d_\rho$

for $1 \le j < \rho$ if $E_i(\psi_r) = d_i$ for $i > j$ then $E_j(\psi_r) \ge d_j$.

Consider the set

$\mathbf{M} := \{M(\psi_r), E_i(\psi_r) = d_i$ for $1 \le i \le \rho\}$

By noetherianity there is an index N_2 s.t.

if $M(\psi_r) \in \mathbf{M}$ then it is in the submodule of P^t generated by $\{M(\psi_u) : u \le N_2, E_i(\psi_u) \le d_i$ for $1 \le i \le \rho\}$

So let $N := \max\{N_0, N_1, N_2\}$.

Let $r \ge N$ be s.t. $E_i(\psi_r) = d_i$ for $1 \le i \le \rho$.

Then $r \ge N_1$ implies that either

$E_i(\psi_{r+1}) = d_i$ for $1 \le i \le \rho$

or there is j, $1 \le j \le \rho$, s.t.

$E_i(\psi_{r+1}) = E_i(\psi_r) = d_i$ for $i > j$

$E_j(\psi_{r+1}) > d_j$

We want to show that the second case cannot occur.

In fact since $r \ge N_2$ and $M(\psi_r) \in \mathbf{M}$, then $M(\psi_r) \in \Phi_{N_2}(\psi_r, \rho) = \{M(\psi) \in \Phi_{N_2} : E_j(\psi) \le E_j(\psi_r)$ for $j \le \rho\}$.

So $ind(\psi_r, \Phi_r) \ge \rho \ge j$. Therefore $E_j(\psi_{r+1}) \le E_j(\psi_r) \le d_j$, by remark 2).

We can therefore conclude that there is an index N' s.t. for $r \ge N'$

$E_j(\psi_r) = d_j$ for $1 \le j \le \rho$.

If $deg_\rho(\psi_{r+1}) < deg_\rho(\psi_r)$, then $\rho = \min\{i : in_i(\psi_r) = \Sigma\, c_{r\alpha}\, m_{r\alpha}\, in_i(\phi_{r\alpha})\}$ (since $in_i(\psi_r) \ne \Sigma\, c_{r\alpha}\, m_{r\alpha}\, in_i(\phi_{r\alpha})$ for $i < \rho$) and then $d_\rho = E_\rho(\psi_{r+1}) < \max\{E_\rho(\psi_r), E_\rho(\phi_{r\alpha})) \le d_\rho$ (the inequality being a consequence of remark 1)), a contradiction.

This implies that $deg_\rho(\psi_r) = deg_\rho(\psi_{N'})$ for $r \ge N'$ and gives the desired contradiction.

Proof of Claim 2: If i = s-1, the thesis obviously holds, since, by construction, $\psi_{s-1} = \psi_s + \Sigma\, c_{s-1\alpha}\, m_{s-1\alpha}\, \phi_{s-1\alpha}$

with $\phi_{s-1\alpha} \in \Phi_{s-1}$ and $T(\psi_s) < T(\psi_{s-1}) = m_{s-1\alpha}\, T(\phi_{s-1\alpha})\ \forall\alpha$.
So we can assume it holds for i, i.e.

$\psi_i = \Sigma\, q_{i\alpha}\, \phi_{i\alpha} + u_i\, \psi_s$ with $q_{i\alpha} \in$ Loc(P), $\phi_{i\alpha} \in \Phi_i$, u_i a unit in Loc(P), $T(\psi_s) < T(\psi_i)$, $T(q_{i\alpha})\, T(\phi_{i\alpha}) \leq T(\psi_i)$

and prove it for i-1.
We have also $\psi_i = \psi_{i-1} - \Sigma\, c_{i-1\alpha}\, m_{i-1\alpha}\, \phi_{i-1\alpha}$ with $c_{i-1\alpha} \in k - \{0\}$, $m_{i-1\alpha} \in T$, $\phi_{i-1\alpha} \in \Phi_{i-1}$, and $T(\psi_i) < T(\psi_{i-1}) = m_{i-1\alpha}\, T(\phi_{i-1\alpha})\ \forall\alpha$.
So $\psi_{i-1} = \psi_i + \Sigma\, c_{i-1\alpha}\, m_{i-1\alpha}\, \phi_{i-1\alpha} = \Sigma\, q_{i\alpha}\, \phi_{i\alpha} + \Sigma\, c_{i-1\alpha}\, m_{i-1\alpha}\, \phi_{i-1\alpha} + u_i\, \psi_s$, with $\phi_{i-1\alpha} \in \Phi_{i-1}$, $\phi_{i\alpha} \in \Phi_{i-1} \cup \{\psi_{i-1}\}$.
So, if $J' := \{\alpha : \phi_{i\alpha} \in \Phi_{i-1}\}$ and $J'' := \{\alpha : \phi_{i\alpha} = \psi_{i-1}\}$:

$\psi_{i-1} = \Sigma_{\alpha\in J'}\, q_{i\alpha}\, \phi_{i\alpha} + (\Sigma_{\alpha\in J''}\, q_{i\alpha})\, \psi_{i-1} + \Sigma\, c_{i-1\alpha}\, m_{i-1\alpha}\, \phi_{i-1\alpha} + u_i\, \psi_s$

$(1 - \Sigma_{\alpha\in J''}\, q_{i\alpha})\, \psi_{i-1} = \Sigma_{\alpha\in J'}\, q_{i\alpha}\, \phi_{i\alpha} + \Sigma\, c_{i-1\alpha}\, m_{i-1\alpha}\, \phi_{i-1\alpha} + u_i\, \psi_s$.

Also $T(\psi_{i-1}) = m_{i-1\alpha}\, M(\phi_{i-1\alpha}) > T(\psi_i) \geq T(q_{i\alpha})\, T(\phi_{i\alpha})$ for all α.
So if $\alpha \in J''$, $T(q_{i\alpha}) < 1$ and, denoting $q := \Sigma_{\alpha\in J''}\, q_{i\alpha}$, $T(q) < 1$, $u := 1 - q$ is a unit in Loc(P).
Therefore $\psi_{i-1} = \Sigma_{\alpha\in J'}\, u^{-1}\, q_{i\alpha}\, \phi_{i\alpha} + \Sigma\, c_{i-1\alpha}\, u^{-1}\, m_{i-1\alpha}\, \phi_{i-1\alpha} + u^{-1}\, u_i\, \psi_s$ is the required representation.

4 THE TANGENT CONE ALGORITHM

4.1 The tangent cone algorithm: basic version

From the results of the previous section and of §2.3, correctness and termination of the following algorithms **LNF(g,F)** and **StandardBasis(F)** (whose subroutine SyzBasis(F,U) is the same as in §1.3) follow easily, when < is a tangent cone ordering:

```
h := LNF(g,F)
where
        g is a non-zero element in P
        $F \subset P - \{0\}$ is a finite set.
        there is u a unit in Loc(P) s.t.
                u h is a normal form of f w.r.t. F
                f - u h has a standard representation in terms of F
h := g
F' := F
While $h \neq 0$ and $M(h) \in M(F')$ do
        F" := $\{f \in F' : T(f)$ divides $T(h)\}$
        Choose $f \in F''$ s.t. $\mu := ind(f,h) \geq ind(f',h)\ \forall f' \in F''$ and $E_{\mu+1}(f) \leq E_{\mu+1}(f')\ \forall f' \in F''$, $ind(f',h) = \mu$
        F' := $F \cup \{h\}$
        h := Red(h,f)
```

```
G := StandardBasis(F)
where
        $F := \{f_1,\dots,f_t\} \subset P - \{0\}$ is an indexed set of non-zero elements in P.
        $G \subset P - \{0\}$ is a standard basis for the ideal $I := (f_1,\dots,f_t)$
G := $\{f_1\}$
B := $\emptyset$
For i = 2...t do
        G := $G \cup \{f_t\}$
        B := SyzBasis(G,B)
While $B \neq \emptyset$ do
        Choose $(i,j) \in B$
        B := $B - \{(i,j)\}$
        h := $S(\sigma(i,j))$
        h := LNF(h,G)
        If $h \neq 0$ then
                t := t + 1
                $f_t$ := h
                G := $G \cup \{f_t\}$
                B := SyzBasis(G,B)
```

We just remark that **LNF₀** can be used instead of **LNF**, anytime for each $d \in \mathbf{Z}$, there are just finitely terms t with $w_1(t) = d$.

EXAMPLE We give here an example of the algorithm:
Let P := Q[X,Y,Z] and let < be the ordering on **T**, associated to the following array of vectors:

(-1,-1,-1), (0,0,-1), (0,-1,0).

We explicitly remark that this is a degree anti-compatible ordering, so the easier notion of ecart introduced in 3.1 can be used.

For such ordering we have:

$$1 > X > Y > Z > X^2 > XY > Y^2 > XZ > YZ > Z^2 > \ldots$$

Let:

$f_1 := XZ - YZ - Y^2Z \qquad T(f_1) = XZ \qquad E(f_1) = 1$

$f_2 := XZ - YZ + Y^2Z \qquad T(f_2) = XZ \qquad E(f_2) = 1$

$f_3 := Z + Y^2Z \qquad T(f_3) = Z \qquad E(f_3) = 2$

We want to compute a standard basis of $I = (f_1, f_2, f_3)$.

Since a minimal homogeneous basis of $\mathrm{Syz}(M(f_1), M(f_2), M(f_3))$ is $\{\sigma(1,2), \sigma(1,3)\}$, we start with:

$h_1 := S(\sigma(1,2)) = f_1 - f_2 = -2Y^2Z \qquad T(h_1) = Y^2Z \qquad E(h_1) = 0$

$h_2 := \mathrm{Red}(h_1, f_3) = h_1 + 2\,Y^2 f_3 = 2Y^4Z \qquad T(h_2) = Y^4Z \qquad E(h_2) = 0$

We can now reduce h_2 with h_1 (actually we must since $E(h_1) = 0 < E(f_3)$) and we get:

$\mathrm{Red}(h_2, h_1) = h_2 + Y^2 h_1 = 0.$

We can then reconstruct a standard representation of h_1 as follows:

$h_1 = -2\,Y^2 f_3 + h_2$

$h_2 = -Y^2 h_1$

so $h_1 = -2\,Y^2 f_3 - Y^2 h_1$, $h_1 = -2\,(1 + Y^2)^{-1}\,Y^2 f_3$ (*cf.* the reduction of X by $\{X-X^2\}$).

Then we go on with:

$h_3 := S(\sigma(1,3)) = f_1 - X f_3 = -YZ - Y^2Z - XY^2Z \qquad T(h_3) = YZ \qquad E(h_3) = 2$

$h_4 := \mathrm{Red}(h_3, f_3) = h_3 + Y f_3 = -Y^2Z - XY^2Z + Y^3Z \qquad T(h_4) = Y^2Z \qquad E(h_4) = 1$

We can now reduce either with f_3 or h_3; choosing f_3 we obtain:

$h_5 := \mathrm{Red}(h_4, f_3) = h_4 + Y^2 f_3 = -XY^2Z + Y^3Z + Y^4Z \qquad T(h_5) = XY^2Z \qquad E(h_5) = 1$

so the next reduction can be done either with f_1, f_2 or h_4 but not with f_3; we choose f_2, obtaining:

$h_6 := \mathrm{Red}(h_5, f_1) = h_5 + Y^2 f_2 = 2Y^4Z \qquad T(h_6) = Y^4Z \qquad E(h_6) = 0$

The next reduction can be performed with h_4, not with f_3 or h_3, since $E(h_6) < E(h_4) < E(f_3) = E(h_3)$; we get:

$h_7 := \mathrm{Red}(h_6, h_4) = h_6 + 2\,Y^2 h_4 = -2\,XY^4Z + 2Y^5Z \qquad T(h_7) = XY^4Z \qquad E(h_7) = 1$

For the next reduction we can choose f_1, f_2, h_4, h_5 or h_6; choosing h_6 we get:

$h_8 := \mathrm{Red}(h_7, h_8) = h_7 + X\,h_6 = 2\,Y^5Z$

and then:

$\mathrm{Red}(h_8, h_6) = h_8 - Y\,h_6 = 0.$

From this we reconstruct a standard representation as follows:

$h_3 = -Y f_3 + h_4$

$h_4 = -Y^2 f_3 + h_5$

$h_5 = -Y^2 f_2 + h_6$

$h_6 = -2\,Y^2 h_4 + h_7$

$h_7 = -X h_6 + h_8$

$h_8 = Y h_6$

so

$h_6 = -2\,Y^2 h_4 - X h_6 + Y h_6$

$h_6 = -2\,(1 + X - Y)^{-1}\,Y^2 h_4$

$h_4 = -Y^2 f_3 - Y^2 f_2 + h_6 = -Y^2 f_3 - Y^2 f_2 - 2\,(1 + X - Y)^{-1}\,Y^2 h_4$

so

$(1 + X - Y)\,h_4 + 2\,Y^2 h_4 = (-Y^2 - XY^2 + Y^3)\,f_3 + (-Y^2 - XY^2 + Y^3)\,f_2$

and

$h_4 = (1 + X - Y + 2\,Y^2)^{-1}\,(-Y^2 - XY^2 + Y^3)\,f_3 + (1 + X - Y + 2\,Y^2)^{-1}\,(-Y^2 - XY^2 + Y^3)\,f_2$

$h_3 = -Y f_3 + (1 + X - Y + 2\,Y^2)^{-1}\,(-Y^2 - XY^2 + Y^3)\,f_3 + (1 + X - Y + 2\,Y^2)^{-1}\,(-Y^2 - XY^2 + Y^3)\,f_2 =$

$= (1 + X - Y + 2\,Y^2)^{-1}\,(-Y - XY - XY^2 - Y^3)\,f_3 + (1 + X - Y + 2\,Y^2)^{-1}\,(-Y^2 - XY^2 + Y^3)\,f_2$

So the original basis is a standard basis; after eliminating elements corresponding to redundant generators of $M(I) = (Z)$, we are left with the standard basis $\{f_3\}$; in fact, visual inspection would have been sufficient to remark that, in Loc(P), $I = (Z)$.

4.2 Improvements to the tangent cone algorithm: enlarging the set of simplifiers

The only difference between Buchberger algorithm and the tangent cone algorithm as presented above is in the subroutine for normal form computation and the difference can be easily explained stating the set of simplifiers used in NF is fixed and global (being the current basis G), while the one used in LNF is variable (new elements being added during the computation) and local (the added elements are forgot at termination).

We can clearly improve the performance of LNF if we globalize the set of simplifiers, i.e. if we use also simplifiers produced by previous calls of LNF; that's because in the enlarged set, there being more elements, there are more chances to find a simplifier f s.t., say, $E_j(f) \le E_j(h)$ for all j.

To avoid storage of too many simplifiers, we can drop out those simplifiers which are clearly redundant: if f, g are s.t. T(f) divides T(g) and $E_j(f) \le E_j(g)$ for all j, any time g can be used to reduce h, f can be used instead.

We are then lead to the following formal definition of simplifiers:

DEFINITION 9 $H \subset P$ is a set of simplifiers for $F \subset P$ iff $\forall h \in H$, h has a standard representation in terms of F

and to the formalization of the discussion above in the statement of the following properties of sets of simplifiers, where we say that h_1 makes h redundant if

$T(h_1)$ divides properly $T(h)$ and $E_j(h_1) \le E_j(h)$ $\forall j$:

LEMMA 14 Let $F \subset P - \{0\}$ be a finite set, let $H \subset P - \{0\}$ be a finite set of simplifiers for F. Let $H_1 := \{h \in H$: there is no $h' \in H$, s.t. $T(h')$ divides properly $T(h)$ and $E_j(h') \le E_j(h)$ $\forall j\}$. Let $f \in P - \{0\}$. Then:

1) $f \in P - \{0\}$ has a standard representation in terms of F iff f has a standard representation in terms of H.

2) H_1 is a set of simplifiers for F (called a *minimal set of simplifiers*)

3) If $h \in H - H_1$, there is $h_1 \in H_1$ which makes h redundant.

4) If $h \in H$ is s.t. $T(h)$ divides $T(f)$ and $\forall$ $h' \in H$ s.t. $T(h')$ divides $T(f)$

$ind(f,h) \ge ind(f,h')$

if $\mu := ind(f,h) = ind(f,h') < r$ then $E_{\mu+1}(h) \le E_{\mu+1}(h')$

then there is $h_1 \in H_1$ s.t. $T(h_1)$ divides $T(f)$ and $\forall$ $h' \in H$ s.t. $T(h')$ divides $T(f)$

$ind(f,h_1) \ge ind(f,h')$

if $\nu := ind(f,h_1) = ind(f,h') < r$ then $E_{\nu+1}(h_1) \le E_{\nu+1}(h')$

Proof: 1) Let $g = \Sigma_i q_i h_i$, $q_i \in Loc(P)$, $h_i \in H$ be a standard representation in terms of H. For each h_i let $h_i = \Sigma_j q_{ij} f_j$, $q_{ij} \in Loc(P)$, $f_j \in F$ be a standard representation in terms of F. Then $g = \Sigma_{i,j} q_i q_{ij} f_j$ is a standard representation in terms of F.

2) and 3) are trivial

4) Either $h \in H_1$, and there is nothing to prove, or $h \notin H_1$, and there is $h_1 \in H_1$ which makes h redundant. Then $T(h_1)$ divides $T(f)$; for $j \le \mu$, $E_j(h_1) \le E_j(h) \le E_j(f)$, so $\nu \ge \mu$ and (by the maximality of μ) $\nu = \mu$. Moreover $E_{\mu+1}(h_1) \le E_{\mu+1}(h) \le E_{\mu+1}(h_1)$.

So $\forall$ $h' \in H$ s.t. $T(h')$ divides $T(f)$:

$ind(f,h_1) = ind(f,h) \ge ind(f,h')$

if $ind(f,h') = \nu = \mu$ then $E_{\mu+1}(h_1) = E_{\mu+1}(h) \le E_{\mu+1}(h')$.

This leads immediately to the following version of the tangent cone and the normal form algorithms:

```
$H_1$ := Simp(H,h)
where
    H is a minimal set of simplifiers for some set F
    $h \in P$
    $H_1$ is a minimal set of simplifiers for $F \cup \{h\}$
$H_1 := \emptyset$
Repeat
    Choose $f \in H$
    $H := H - \{f\}$
    If h doesn't make f redundant then
        $H_1 := H_1 \cup \{f\}$
until f makes h redundant or $H = \emptyset$
If f makes h redundant then
    $H_1 := H_1 \cup H$
else
    $H_1 := H_1 \cup \{h\}$
```

```
$(h,H_1)$ := SimpLNF(g,F,H)
where
    g is a non-zero element in P
    $F \subset P - \{0\}$ is a finite set
    H is a minimal set of simplifiers for F
    there is u a unit in Loc(P) s.t.
        u h is a normal form of f w.r.t. F
        f - u h has a standard representation in terms of F
    $H_1$ is a minimal set of simplifiers for $F \cup \{h\}$
h := g
$H_1$ := H
While $h \neq 0$ and $M(h) \in M(H_1)$ do
    $H_2 := \{f \in H_1 : T(f) \text{ divides } T(h)\}$
    Choose $f \in H_2$ s.t. $\mu := ind(f,h) \ge ind(f',h)\ \forall f' \in H_2$ and $E_{\mu+1}(f) \le E_{\mu+1}(f')\ \forall f' \in H_2, ind(f',h) = \mu$
    $H_1$ := Simp($H_1$,h)
    h := Red(h,f)
```

```
G := SimpStandardBasis(F)
where
        $F := \{f_1,...,f_t\} \subset P - \{0\}$ is an indexed set of non-zero elements in P.
        $G \subset P - \{0\}$ is a standard basis for the ideal $I := (f_1,...,f_t)$
$G := \{f_1\}$
$H := \{f_1\}$
$B := \emptyset$
For i = 2...t do
        $G := G \cup \{f_i\}$
        B := SyzBasis(G,B)
        $H :=$ Simp$(H,f_i)$
While $B \neq \emptyset$ do
        Choose $(i,j) \in B$
        $B := B - \{(i,j)\}$
        $h := S(\sigma(i,j))$
        (h,H) := SimpLNF(h,H)
        If $h \neq 0$ then
                $t := t + 1$
                $f_t := h$
                $G := G \cup \{f_t\}$
                B := SyzBasis(G,B)
                $H :=$ Simp$(H,f_t)$
```

EXAMPLE Let us now compute the previous example with **SimpStandardBasis**:
Again we have $B = \{(1,2), (1,3)\}$; from $\{f_1, f_2, f_3\}$ we return the minimal set of simplifiers $H = \{f_2, f_3\}$; then we start with:

$h_1 := S(\sigma(1,2)) = f_1 - f_2 = -2Y^2Z$ $T(h_1) = Y^2Z$ $E(h_1) = 0$

We add h_1 to the set of simplifiers since its ecart is less than the one of its divisor f_3, $H = \{f_2, f_3, h_1\}$

$h_2 := \mathrm{Red}(h_1, f_3) = h_1 + 2Y^2 f_3 = 2Y^4Z$ $T(h_2) = Y^4Z$ $E(h_2) = 0$

We don't add h_2 to H (since $E(h_1) < E(h_2)$) and we go on with:

$\mathrm{Red}(h_2, h_1) = h_2 + Y^2 h_1 = 0.$

Then we go on with:

$h_3 := S(\sigma(1,3)) = f_1 - X f_3 = -YZ - Y^2Z - XY^2Z$ $T(h_3) = YZ$ $E(h_3) = 2$

$h_4 := \mathrm{Red}(h_3, f_3) = h_3 + Y f_3 = -Y^2Z - XY^2Z + Y^3Z$ $T(h_4) = Y^2Z$ $E(h_4) = 1$

The computation differs now from the previous one because of the presence of h_1 in H; we get the shorter reduction sequence:

$h_9 := \mathrm{Red}(h_4, h_1) = h_4 - 1/2\, h_1 = -XY^2Z + Y^3Z$ $T(h_9) = XY^2Z$ $E(h_9) = 0$

$h_{10} := \mathrm{Red}(h_9, h_1) = h_9 - 1/2\, X h_1 = Y^3 Z$ $T(h_{10}) = Y^3Z$ $E(h_{10}) = 0$

$\mathrm{Red}(h_{10}, h_1) = h_{10} + 1/2\, Y h_1 = 0$

producing the standard representation:

$h_3 = -Y f_3 + h_4$
$h_4 = 1/2\, h_1 + h_9$
$h_9 = 1/2\, X h_1 + h_{10}$
$h_{10} = -1/2\, Y h_1$

so

$h_4 = 1/2\,(1 + X - Y)\, h_1$

and substituting the standard representation of h_1, $h_1 = -2(1 + Y^2)^{-1} Y^2 f_3$:

$h_4 = -(1 + Y^2)^{-1} (Y^2 + XY^2 - Y^3) f_3.$

So, having saved results of previous reductions has shortened the computation; we remark however that **SimpStandardBasis** is clearly very dependent on the ordering in which reductions are performed; if we had chosen to compute $S(\sigma(1,3))$ before $S(\sigma(1,2))$, the computation would have been more or less the same than for **StandardBasis**.

4.3 Improvements to the tangent cone algorithm: early termination tests

Let us assume that the set F is s.t. there are only finitely many terms not belonging to M(F). This happens when F is a standard (or Gröbner) basis of a 0-dimensional ideal I (those ideals which have only finitely many zeroes), and occurs in the applications of the tangent cone algorithm related to the study of isolated singularities (*cf.* § 6.2).
If this occurs there is a term t s.t. $t_1 \in M(F)\ \forall\, t_1 < t$[1].
So, if f is s.t. $T(f) < t$, then $NF(f,F) = \{0\}$; in fact, if $g \neq 0$ is a normal form of f, then $T(g) \leq T(f) < t$, implying $M(g) \in M(F)$, while, by definition of normal form, $M(g) \notin M(F)$.

[1] This fact is absolutely of no help for Gröbner bases; in fact 1 is then the minimal term and either $1 \in M(F)$, I is the whole ring, and, detecting that, the algorithm is forced to terminate; or $t = 1$, and the remarks above don't help at all.

Therefore, if there is a term t s.t. $t_1 \in M(F)\ \forall\ t_1 < t$, and in the computation of the normal form of $f \in P$ w.r.t. F, we obtain $h \in P$ s.t. $T(h) < t$, we can conclude that $NF(f,F) = \{0\}$ and we can force an immediate termination of the normal form computation.

Also, if $T(i,j) \leq t$, then $T(S(\sigma(i,j)) < t$, and we know that the normal form of $S(\sigma(i,j)$ is necessarily 0[1].

With this in mind, we need therefore:

1) to recognize if there are only finitely many terms not belonging to M(F)

2) to find the minimal term $t \notin M(F)$ s.t. $t_1 \in M(F)\ \forall\ t_1 < t$.

The first problem is easy to solve, because of the following well-known fact:

REMARK There are only finitely many terms not belonging to M(F) iff for each i, $X_i^{\delta_i} \in M(F)$ for some δ_i

A solution to the second problem which is both efficient and holding for the general case seems difficult to obtain, so we restrict our discussion to those orderings s.t.

$X_i < 1$ for each i

where an efficient solution can be achieved and which covers the orderings used in the known applications (study of isolated singularities) in which one can expect to work with a 0-dim. ideal.

Let $M = \{m_1,\dots,m_t\} \subset P - \{0\}$ be a finite set of monomials, **M** the ideal generated by M. Assume that for each i there is δ_i s.t. $X_i^{\delta_i} \in$ **M**.

Define:

Comp(M) := $\{t \in \mathbf{T} : t \notin \mathbf{M}\}$, the complementary of the ideal generated by M

MinComp(M) to be the minimal term $t \notin \mathbf{M}$ s.t. $t_1 \in \mathbf{M}\ \forall\ t_1 < t$ (the minimal term in the complementary of the ideal generated by M)

Corners(M) := $\{t \notin \mathbf{M} : X_i t \in \mathbf{M}\ \forall i\}$, which is the set of the elements of Comp(M) which are maximal for the divisibility property[2].

LEMMA 15 1) MinComp(M) $\in$ Corners(M).

2) Corners(M) := $\{t \in$ Comp(M) : t doesn't properly divide t' $\forall t' \in$ Comp(M)$\}$

Proof: 1) By definition t := MinComp(M) $\notin$ **M**. Since t is the minimal element in Comp(M) and $X_i < 1$, then $X_i t < t$, so $X_i t \in \mathbf{M}\ \forall i$.

2) is obvious

So we obtain MinComp(M) if we are able to compute Corners(M). To compute the latter, we propose an "incremental" algorithm, which, just with small adjustments, given Corners(M), allows to compute Corners(M_1) for $M_1 = M \cup \{m\}$, together with an obvious computation of Corners(M) for $M = \{X_1^{\delta_1},\dots,X_n^{\delta_n}\}$

It is based on the following result, where $\mathbf{M_1}$ denotes the ideal generated by M_1, and on the following operations on terms t, m, where m is multiple of X_i:

let α be the exponent of X_i in t, $\beta = \gamma + 1 > 0$ the exponent of X_i in m, $\gamma := \min(\alpha, \beta-1)$; denote by $\lambda_i(t,m)$ the term which is obtained from t substituting X_i^α with X_i^γ, i.e. $\lambda_i(t,m) = t / X_i^{\alpha-\gamma}$;

remark that if m divides t (as in the following application), then $\gamma = \beta-1$.

LEMMA 16 If t, m $\in$ **T**, either:

i) m doesn't divide X_i t for all variables X_i

ii) m doesn't divide t and divides X_i t for just one variable X_i

iii) m divides t

Proof: We have just to show that if m divides both X_i t and X_j t, $i \neq j$, then it divides t. But this is immediate since then t divides G.C.D.(X_i t, X_j t) = t.

LEMMA 17 1) If $M = \{X_1^{\delta_1},\dots,X_n^{\delta_n}\}$ then Corners(M) = $\{X_1^{\delta_1-1}\dots X_n^{\delta_n-1}\}$

2) Corners(M_1) $\subset$ {t $\in$ Corners(M) : t is not multiple of m} $\cup$ {$\lambda_i(t,m)$: t $\in$ Corners(M), t multiple of m, i s.t. X_i divides m}

[1] We have never discussed the strategies which can be applied for the various Choose commands in the algorithm.

Both for Gröbner bases and for standard bases, a sensible choice for the next pair $(i,j) \in B$ is to choose (i,j) s.t. T(i,j) is not properly divided by any other $T(\alpha,\beta)$.

For Gröbner bases, this is usually implemented by choosing (i,j) s.t. T(i,j) is minimal according to < (if m properly divides m', then m < m').

In the case of an ordering s.t. $X_i < 1\ \forall i$, if m divides m' then m > m', so the corresponding choice is to choose (i,j) s.t. T(i,j) is maximal according to <. For such an ordering and with this strategy, if at some stage (i,j) is chosen with $T(i,j) \leq t$, then for each $(\alpha,\beta) \in B$, $T(\alpha,\beta) \leq t$; therefore immediate termination of the algorithm can be forced.

For a discussion of good strategies for Choose commands in Buchberger algorithm, cf. [T-D]

[2] If terms are represented as points in an integral lattice (the coordinates being given by the exponent vectors), a monomial ideal looks like a stair. The elements of Corners(M) are exactly the concave corners of the complementary of M.

3) If Γ is s.t. $\mathrm{Corners}(M) \subset \Gamma \subset \mathrm{Comp}(M)$, then $\mathrm{Corners}(M) = \{t \in \Gamma : t$ doesn't properly divide $t'\ \forall t' \in \Gamma\}$

Proof: 1) Let $t := X_1^{\delta_1 -1} \ldots X_n^{\delta_n -1}$. Then clearly $t \notin M$. If t_1 doesn't divide t, then t_1 is multiple of $X_i\, t$ for some i, so it is multiple of $X_i^{\delta_i}$.

2) Let $t \in \mathrm{Corners}(M_1)$; then $X_i\, t \in M_1$ for each i. Since $t \notin M_1$, so that m doesn't divide t, we have two cases:

i) m doesn't divide $X_i\, t$ for all variables X_i: in this case $X_i\, t \in M$ for each i, $t \in \mathrm{Corners}(M)$.

ii) m divides $X_i\, t$ for just one variable X_i: in this case $X_j\, t \in M$ for all $j \neq i$. So if $t_1 \in \mathrm{Corners}(M)$ is a multiple of t, necessarily $t_1 = X_i^{\delta}\, t$. Denote γ the exponent of X_i in t, $\beta > 0$ the exponent of X_i in m, $\alpha = \delta + \gamma$ the exponent of X_i in t_1. Then $\gamma = \min(\alpha, \beta-1)$, i.e. $t = \lambda_i(t_1,m)$

3) Denote by $\Gamma_0 := \{t \in \Gamma : t$ doesn't properly divide $t'\ \forall t' \in \Gamma\}$. Then $\mathrm{Corners}(M) \subset \Gamma_0$, since its elements don't divide properly any element of Comp(M), and a fortiori of Γ.
If $t \in \Gamma_0$, then it doesn't properly divide any element of Γ, and so any element of Corners(M).
Since each element of Comp(M) divides some element of Corners(M), we can conclude that t doesn't properly divide any element of Comp(M), so by Lemma 15.2) it is in Corners(M).

We have then the following algorithm to compute $\mathrm{Corners}(M_1)$ from Corners(M):

```
for each $t \in \mathrm{Corners}(M)$, insert in $\mathrm{Corners}(M_1)$:
    t itself if m doesn't divide t,
    $\lambda_i(t,m)$ for all i s.t. $X_i$ divides m, otherwise;
remove those elements which divide some other element.
```

Example Let (writing the vector of exponents instead of the terms) $m_1 := (3,0,0)$, $m_2 := (0,4,0)$, $m_3 := (0,0,5)$, $m_4 := (2,2,2)$, $m_5 := (1,0,4)$, $m_6 := (0,2,3)$.
Then

$\mathrm{Corners}(\{m_1, m_2, m_3\}) = \{(2,3,4)\}$

$\{\lambda_i((2,3,4), m_4) : i = 1\ldots3\} = \{(1,3,4), (2,1,4), (2,3,1)\}$

$\mathrm{Corners}(\{m_1, m_2, m_3, m_4\}) = \{(1,3,4), (2,1,4), (2,3,1)\}$

$\{\lambda_i((1,3,4), m_5) : i = 1,3\} \cup \{\lambda_i((2,1,4), m_5) : i = 1,3\} \cup \{(2,3,1)\} =$
$= \{(0,3,4), (1,3,3), (0,1,4), (2,1,3), (2,3,1)\}$

$\mathrm{Corners}(\{m_1, m_2, m_3, m_4, m_5\}) = \{(0,3,4), (1,3,3), (2,1,3), (2,3,1)\}$

$\{\lambda_i((0,3,4), m_6) : i = 2,3\} \cup \{\lambda_i((1,3,3), m_6) : i = 2,3\} \cup \{(0,1,4), (2,1,3), (2,3,1)\} =$
$= \{(0,1,4), (0,3,2), (1,1,3), (1,3,2), (0,1,4), (2,1,3), (2,3,1)\}$

$\mathrm{Corners}(\{m_1, m_2, m_3, m_4, m_5, m_6\}) = \{(0,1,4), (1,3,2), (2,1,3), (2,3,1)\}$

```
C' := Corners(C,m)
where
    C = Corners(M) for some monomial set M
    $m \in T$
    $C' = \mathrm{Corners}(M \cup \{m\})$
$C' = \varnothing$
While $C \neq \varnothing$ do
    Choose $t \in C$
    $C := C - \{t\}$
    If m divides t then
        $C' := C' \cup \{\lambda_i(t,m) : i$ s.t. $X_i$ divides $m\}$
    else
        $C' := C' \cup \{t\}$
$C' := \{t \in C' : t$ doesn' t divide properly any $t' \in C'\}$
```

```
C := InitCorners(G)
where
    G is a set of polynomials s.t. $\{M(f) : f \in G\}$ contains a pure power of each variable
    C = Corners(M(F))
$M := \{M(f) : f \in G : M(f)$ is not multiple of $M(f')$ for some $f' \in G\}$
$M_1 := \{m \in M : m$ is a pure power of a variable$\}$
$M_2 := M - M_1$
Compute t to be the product of the elements in $M_1$
$C := \{t/(X_1 \ldots X_n)\}$
For $m \in M_2$ do
    C := Corners(C,m)
```

We can now describe a normal form and a standard basis algorithm with the Early Termination and the Simplifier improvements: to consider the situation in which t doesn't exist we enlarge T by adding a symbol $-\infty$, which we assume to be less than any element of T; we list in X the indexes i s.t. no pure power of X_i is in M(G).

```
$(h,H_1) := $ ET-S-LNF$(g,F,H,t)$
where
        $g$ is a non-zero element in $P$
        $F \subset P - \{0\}$ is a finite set
        $H$ is a minimal set of simplifiers for $F$
        $t \in T \cup \{-\infty\}$ is s.t. for each $t' < t$, $t' \in M(F)$
        there is $u$ a unit in $Loc(P)$ s.t.
                $u\ h$ is a normal form of $f$ w.r.t. $F$
                $f - u\ h$ has a standard representation in terms of $F$
        $H_1$ is a minimal set of simplifiers for $F \cup \{h\}$
$h := g$
$H_1 := H$
While $h \neq 0$ and $M(h) \in M(H_1)$ and $M(h) \geq t$ do
        $H_2 := \{f \in H_1 : T(f) \text{ divides } T(h)\}$
        Choose $f \in H_2$ s.t. $\mu := ind(f,h) \geq ind(f',h)\ \forall f' \in H_2$ and $E_{\mu+1}(f) \leq E_{\mu+1}(f')\ \forall f' \in H_2, ind(f',h) = \mu$ [1]
        $H_1 :=$ Simp$(H_1,h)$
        $h := Red(h,f)$
If $M(h) < t$ then
        $h := 0$
```

```
$G :=$ ET-S-StandardBasis$(F)$
where
        $F := \{f_1,\ldots,f_t\} \subset P - \{0\}$ is an indexed set of non-zero elements in $P$.
        $G \subset P - \{0\}$ is a standard basis for the ideal $I := (f_1,\ldots,f_t)$
$G := \{f_1\}$
$H := \{f_1\}$
$B := \emptyset$
$X := \{1,\ldots,n\}$
$MinComp := -\infty$
For $i = 2\ldots t$ do
        $G := G \cup \{f_i\}$
        $B :=$ SyzBasis$(G,B)$
        $H :=$ Simp$(H,f_i)$
        If $M(f_i)$ is a pure power of $X_j$ then
                $X := X - \{j\}$
If $X = \emptyset$ then
        $C :=$ InitCorners$(G)$
        $MinComp := \min\{t : t \in C\}$
While $B \neq \emptyset$ do
        Choose $(i,j) \in B$
        $B := B - \{(i,j)\}$
        If $T(i,j) \geq t$ then
                $h := S(\sigma(i,j))$
                $(h,H) :=$ SimpLNF$(h,H)$
                If $h \neq 0$ then
                        $t := t + 1$
                        $f_t := h$
                        $G := G \cup \{f_t\}$
                        $B :=$ SyzBasis$(G,B)$
                        $H :=$ Simp$(H,f_t)$
                        If $MinComp \neq -\infty$ then
                                $C :=$ Corners$(C,M(f_t))$
                                $MinComp := \min\{t : t \in C\}$
                        else $(X \neq \emptyset)$
                                If $M(f_t)$ is a pure power of $X_j$ then
                                        $X := X - \{j\}$
                                        If $X = \emptyset$ then
                                                $C :=$ InitCorners$(F)$
                                                $MinComp := \min\{t : t \in C\}$
```

If $<$ is an ordering on T, the variables can be divided in two classes and renamed, denoting by
$\{Z_1,\ldots,Z_m\}$ the set of variables s.t. $Z_i > 1$
$\{Y_1,\ldots,Y_d\}$ the set of variables s.t. $Y_j < 1$;

[1]

each term $m \in T$ is then the product $m = m_Z m_Y$ of a term m_Z in the Z's only and of a term m_Y in the Y's only
While we have presented the theory of standard bases and the algorithms in a general setting, the orderings for which we know interesting applications fall in four classes:

i) $X_i > 1$ for each i, which is covered by Buchberger algorithm, where early terminations tests are impossible

ii) $X_i < 1$ for each i, which is covered by the algorithm above (tangent cone computation, isolated singularity theory)

iii) $m < m'$ iff $m_Y < m'_Y$ or ($m_Y = m'_Y$ and $m_Z < m'_Z$) (computations in local rings and in algebraic series rings)

iv) $m < m'$ iff $m_Z < m'_Z$ or ($m_Z = m'_Z$ and $m_Y < m'_Y$) (elimination in algebraic series rings).

The following results allow to obtain an Early Termination algorithm to these two cases too:

LEMMA 18 1) In case iii), if for each Y_i, M contains a pure power of Y_i, then there is m s.t. $\forall$ $t < m$, $m \in M$, and MinComp(M)) = min{Corners(M_0)}, where $M_0 = \{m \in M \text{ s.t. } m_Z = 1\}$

2) In case iv), if for each Y_i, M contains a pure power of Y_i, then there is m s.t. $\forall$ $t < m$, $m \in M$, and m = min{Corners(M_0)}, where $M_0 = \{m \in M \text{ s.t. } m_Z = 1\}$

Proof: 1) Let $m = m_Y$ = min{Corners(M_0)}. If $t = t_Y t_Z < m$, then $t_Y < m_Y$; since the restriction of < on the terms in the Y's only is an ordering in class ii), by the argument above we know there is $m' = m'_Y \in M_0$ which divides t_Y and so t. Since $m \notin M_0 \subset M$, then m = MinComp(M))

2) Let m_Y = min{Corners(M_0)}. If $t = t_Y t_Z < m$, then $t_Z \leq m_Z = 1$, so $t_Z = 1$ and $t = t_Y < m_Y$; since the restriction of < on the terms in the Y's only is an ordering in class ii), by the argument above we know there is $m' = m'_Y \in M_0$ which divides $t_Y = t$. Again $m \notin M$, so m = MinComp(M)).

4.4 The tangent cone algorithm: the lazy version

Practical experience with Buchberger algorithm shows instances in which several normal form reductions performed at some stage are time and space consuming, while, if postponed until some specific new element is added to the current basis, all of them become very fast.
Clearly, one could, still preserving correctness, postpone the reduction to normal form of some element, in the hope that this occurs. One good reason why this has never been tried (at least in documented form), is that it could as well be that the postponed reduction is exactly the one giving the element of the basis which is needed in order that the other reductions become fast.

Let us fix now our attention to an ordering s.t. $X_i < 1$ for each i. In this case, the fact that < is not a well-ordering, which, as we have seen, is cause of troubles, has however a very desirable effect.
In fact while for a well-ordering, if m divides m_1 then necessarily $m \leq m_1$, for such an ordering:

if m divides m_1 then necessarily $m \geq m_1$.

As a consequence, if we postpone the reduction to normal form of some polynomial h, we know that its normal form will never be used in the reduction to normal form of some other element g, until we obtain an intermediate reduction g' s.t. $T(g') \geq T(h)$.
If we pursue this idea to the utmost consequence, we realize that after *a single step of reduction*, it is convenient to interrupt the normal form computation, add the partial result to some *queue* containing all partial results of interrupted computations, pick that element h of the queue s.t. T(h) is maximal, and restart the normal form reduction of it (just one step, of course!).

To formalize this, we have to think of Buchberger and the tangent cone algorithms, as they were processing *queues* of elements, by means of *elementary operations* involving other *lists* of elements.
In the versions we have described up to now:

the *lists* are the one consisting of the *basis* elements and the one consisting of the *simplifiers* (they coincide in Buchberger algorithm)

the *queues* are the one consisting of the *pairs* (i,j) still to treated, and the one consisting of the single element, the *simplificand*, to undergo a normal form computation.

The *elementary operations* are:

for an element (i,j) from the pair queue: compute $S(\sigma(i,j))$; add the output to the (void) simplificand queue

for an element (the only one) from the simplificand queue: compute its normal form (and upgrade the simplifier list); if the output is not zero, upgrade the basis list and the pair queue.

The second operation is not so elementary, but it becomes so if we unwind the normal form computation in its components, as follows:

for an element from the simplificand queue which can be reduced: compute one reduction step and upgrade the simplifier list; add the output to the simplificand queue

for an element from the simplificand queue which cannot be reduced: upgrade the simplifier and the basis list; upgrade the pair queue.

Before writing down the algorithm consequent to the unwinding above, we need to remark that, from the discussion above, we have seen that the obvious strategy for choosing an element from a queue is, *when $X_i < 1$ for each i*, to take the simplificand h s.t. T(h) is maximal and the pair (i,j) s.t. T(i,j) is maximal.

This is not a good strategy, whenever the assumption of the ordering is not satisfied[1]. So we need to find a sensible strategy.
We use the following:

NOTATION Let H be a set of polynomials; let $H_1 := \{h_1 \in H : T(h_1)$ is not multiple of $T(h)\ \forall\ h \in H, h \neq h_1\}$; let $h_1 \in H_1$ be s.t. $T(h_1) \geq T(h)\ \forall h \in H_1$. Denote $h_1 =: opt(H)$ (the optimal choice in H as we are going to prove).
Let $\{f_1,\ldots,f_t\}$ be a set of polynomials; let $B \subset \{(i,j) : 1 \leq i < j \leq t\}$; let $B_1 := \{(i,j) \in B : T(i,j)$ is not multiple of $T(\alpha,\beta)\ \forall\ (\alpha,\beta) \in B, (\alpha,\beta) \neq (i,j)\}$; let $(i,j) \in B_1$ be s.t. $T(i,j) \geq T(\alpha,\beta)\ \forall\ (\alpha,\beta) \in B_1$. Denote $(i,j) =: opt(B)$, $T(opt(B)) := T(i,j)$.

LEMMA 19 1) If $T(opt(B)) \leq T(opt(H))$, then
$\forall\ h' \in H, h' \neq h$, $T(opt(H))$ is not divisible by $T(h')$
$\forall\ (\alpha,\beta) \in B$, $T(opt(H))$ is not divisible by $T(S(\sigma(\alpha,\beta)))$

```
G := LazyStandardBasis(F)
where
    $F := \{f_1,\ldots,f_t\} \subset P - \{0\}$ is an indexed set of non-zero elements in P.
    $G \subset P - \{0\}$ is a standard basis for the ideal $I := (f_1,\ldots,f_t)$
BasisList := $\{f_1\}$
SimpList := $\{f_1\}$
PairQueue := $\emptyset$
For i = 2...t do
    BasisList := BasisList $\cup$ $\{f_i\}$
    PairQueue := SyzBasis(BasisList,PairQueue)
    SimpList := Simp(SimpList,$f_i$)
SimpQueue := $\emptyset$
While PairQueue $\cup$ SimpQueue $\neq \emptyset$ do
    (i,j) := Opt(PairQueue)
    h := Opt(SimpList)
    If T(i,j) > T(h) then
        PairOperation((i,j))
    else
        if M(h) $\in$ M(BasisList) then
            BasisElementOperation(h)
        else
            SimplificandOperation(h)
G := BasisList
```

where we have:

```
PairOperation((i,j))
h := S($\sigma$(i,j))
PairQueue := PairQueue - {(i,j)}
If h $\neq$ 0 then
    SimpQueue := SimpQueue $\cup$ {h}
```

```
BasisElementOperation(h)
t := t + 1
$f_t$ := h
BasisList := BasisList $\cup$ $\{f_t\}$
SimpList := Simp(SimpList, $f_t$)
BasisQueue := SyzBasis(BasisList, BasisQueue)
SimpQueue := SimpQueue - $\{f_t\}$
```

```
SimplificandOperation(h)
H := {f $\in$ SimpList : T(f) divides T(h)}
Choose f $\in$ H s.t. $\mu$ := ind(f,h) $\geq$ ind(f',h) $\forall$ f' $\in$ H and $E_{\mu+1}(f) \leq E_{\mu+1}(f')$ $\forall$ f' $\in$ H, ind(f',h) = $\mu$
SimpList := Simp(SimpList,h)
SimpQueue := SimpQueue - {h}
h := Red(h,f)
If h $\neq$ 0 then
    SimpQueue := SimpQueue $\cup$ {h}
```

We leave to the reader how to introduce early termination tests in this version too.

[1] Actually for Gröbner basis computation, it would give a strategy which is unanimously considered by the experts as the worst possible strategy.

We remark however that in the case the ideal is (known in advance to be) 0-dimensional and we use an ordering s.t.

for each term t, for each infinite decreasing sequence of terms $t_1 > t_2 > \ldots > t_s > \ldots$ there is s s.t. $t > t_s$

we can generalize **SimplificandOperation** allowing in its second line any choice, not only one governed by the ecart. The line becomes simply:

Choose $f \in H$

This comes back to a form of Buchberger algorithm.

The proof that the early termination test is successful after a finite number of computations, relies heavily on the property of the ordering: in fact the maximal terms of the elements which undergo **SimplificandOperation** form a decreasing sequence; so if a pure power of a variable is the maximal term of a basis element, it must appear after finitely many computations; when all pure powers have been found, there can be just finitely many applications of **SimplificandOperation**(h) with $T(h) \geq$ MinComp.

EXAMPLE Let us go back of our previous example. We remarked that **SimpStandardBasis** is dependent on the ordering in which reductions are performed; clearly **LazyStandardBasis** instead is not dependent on that:

We start with:

BasisList = $\{f_1, f_2, f_3\}$ SimpList = $\{f_2, f_3\}$ PairQueue = $\{(1,2),(1,3)\}$ SimpQueue = $\emptyset$

Then we apply **PairOperation** to (1,2):

$h_1 := S(\sigma(1,2)) = f_1 - f_2 = -2Y^2Z$ $T(h_1) = Y^2Z$ $E(h_1) = 0$

BasisList = $\{f_1, f_2, f_3\}$ SimpList = $\{f_2, f_3\}$ PairQueue = $\{(1,3)\}$ SimpQueue = $\{h_1\}$

and since $T(1,3) > T(h_1)$, we apply again **PairOperation** to (1,3):

$h_3 := S(\sigma(1,3)) = f_1 - X f_3 = -YZ - Y^2Z - XY^2Z$ $T(h_3) = YZ$ $E(h_3) = 2$

BasisList = $\{f_1, f_2, f_3\}$ SimpList = $\{f_2, f_3\}$ PairQueue = $\emptyset$ SimpQueue = $\{h_1, h_3\}$

Since $T(h_3) > T(h_1)$, we next apply **SimplificandOperation** to h_3:

$h_4 := \mathrm{Red}(h_3, f_3) = h_3 + Y f_3 = -Y^2Z - XY^2Z + Y^3Z$ $T(h_4) = Y^2Z$ $E(h_4) = 1$

BasisList = $\{f_1, f_2, f_3\}$ SimpList = $\{f_2, f_3\}$ PairQueue = $\emptyset$ SimpQueue = $\{h_1, h_4\}$

Then we apply **SimplificandOperation** to h_1:

$h_2 := \mathrm{Red}(h_1, f_3) = h_1 + 2\,Y^2 f_3 = 2Y^4Z$ $T(h_2) = Y^4Z$ $E(h_2) = 0$

BasisList = $\{f_1, f_2, f_3\}$ SimpList = $\{f_2, f_3, h_1\}$ PairQueue = $\emptyset$ SimpQueue = $\{h_2, h_4\}$

then to h_2:

$\mathrm{Red}(h_2, h_1) = h_2 + Y^2 h_1 = 0.$

and to h_4:

$h_9 := \mathrm{Red}(h_4, h_1) = h_4 - 1/2\, h_1 = -XY^2Z + Y^3Z$ $T(h_9) = XY^2Z$ $E(h_9) = 0$

$h_{10} := \mathrm{Red}(h_9, h_1) = h_9 - 1/2\, X h_1 = -Y^3 Z$ $T(h_{10}) = Y^3Z$ $E(h_{10}) = 0$

$\mathrm{Red}(h_{10}, h_1) = h_{10} + 1/2\, Y h_1 = 0$

4.5 A detailed example

The example above was actually chosen mainly to compare the different performance of the three versions; a less trivial example, where the three versions behave more or less identically, but which gives a fuller flavour of an actual tangent cone computation is the following (the ring and the ordering being the same as above); we describe just the computation performed by the lazy version:

We consider the ideal $I := (f_1, f_2, f_3, f_4)$ where:

$f_1 = X^2Z^2 - Y^6$ $E(f_1) = 2$ $T(f_1) = X^2Z^2$

$f_2 = XYZ^2 + Y^4Z - X^5Z - X^4Y^3$ $E(f_2) = 3$ $T(f_2) = XYZ^2$

$f_3 = XZ - Y^3 + X^2Z - XY^3$ $E(f_3) = 2$ $T(f_3) = XZ$

$f_4 = YZ + XYZ - X^4 - X^5$ $E(f_4) = 3$ $T(f_4) = YZ$

We compute a minimal homogeneous basis of $\mathrm{Syz}\{M(f_1),\ldots,M(f_4)\}$ and discard redundant simplifiers from the original basis, obtaining:

BasisList = $\{f_1, f_2, f_3, f_4\}$ SimpList = $\{f_3, f_4\}$

PairQueue = $\{(1,3), (2,3), (3,4)\}$ SimpQueue = $\emptyset$.

Since $T(3,4)$ is maximal among all choices, we apply **PairOperation** to (3,4):

$h_1 := S(\sigma(3,4)) = Y f_3 - X f_4 = -Y^4 + X^5 - XY^4 + X^6$ $E(h_1) = 2$ $T(h_1) = Y^4$

BasisList = $\{f_1, f_2, f_3, f_4\}$ SimpList = $\{f_3, f_4\}$

PairQueue = $\{(1,3), (2,3)\}$ SimpQueue = $\{h_1\}$.

Since $T(h_1) > T(1,3) > T(2,3)$, and $M(h_1) \notin M(F)$, we next apply **BasisElementOperation** to $f_5 := h_1$:

BasisList = $\{f_1, f_2, f_3, f_4, f_5\}$ SimpList = $\{f_3, f_4, f_5\}$

PairQueue = $\{(1,3), (2,3), (4,5)\}$ SimpQueue = $\emptyset$,

since $\{\sigma(1,3), \sigma(2,3), \sigma(3,4), \sigma(3,5), \sigma(4,5)\}$ is a minimal homogeneous basis of $\mathrm{Syz}\{M(f_1),\ldots,M(f_5)\}$ and $T(3,5) = T(3)T(5)$.

Then, applying **PairOperation** to (1,3):

$h_2 := S(\sigma(1,3)) = f_1 - XZ f_3 = XY^3Z - X^3Z^2 - Y^6 + X^2Y^3Z$ $E(h_2) = 1$ $T(h_2) = XY^3Z$

BasisList = $\{f_1, f_2, f_3, f_4, f_5\}$ SimpList = $\{f_3, f_4, f_5\}$

PairQueue = $\{(2,4), (4,5)\}$ SimpQueue = $\{h_2\}$

Since $T(h_2) \geq T(2,3) > T(4,5)$ we next apply **SimplificandOperation** to h_2:

$h_3 := Red(h_2,f_3) = h_2 - Y^3 f_3 = -X^3Z^2 + XY^6$ $E(h_3) = 2$ $T(h_3) = X^3Z^2$

BasisList = $\{f_1, f_2, f_3, f_4, f_5\}$ SimpList = $\{f_3, f_4, f_5, h_2\}$

PairQueue = $\{(2,4), (4,5)\}$ SimpQueue = $\{h_3\}$

adding h_2 to the simplifier list since $E(h_2) < E(f_3) = E(f_4)$.

Then, applying **PairOperation** to (2,3):

$h_4 := S(\sigma(2,3)) = f_2 - YZ f_3 = 2 Y^4Z - X^2YZ^2 - X^5Z + XY^4Z - X^4Y^3$ $E(h_4) = 2$ $T(h_4) = Y^4Z$

BasisList = $\{f_1, f_2, f_3, f_4, f_5\}$ SimpList = $\{f_3, f_4, f_5, h_2\}$

PairQueue = $\{(4,5)\}$ SimpQueue = $\{h_3,h_4\}$

We have $T(h_4) = T(4,5) > T(h_3)$, so we now apply **SimplificandOperation** to h_4:

$h_5 := h_4 + 2\,Z f_5 =$

$= -X^2YZ^2 + X^5Z - XY^4Z - X^4Y^3 + 2\,X^6Z$ $E(h_5) = 2$ $T(h_5) = X^2YZ^2$

BasisList = $\{f_1, f_2, f_3, f_4, f_5\}$ SimpList = $\{f_3, f_4, f_5, h_2\}$

PairQueue = $\{(4,5)\}$ SimpQueue = $\{h_3,h_5\}$

Applying **PairOperation** to (4,5):

$h_6 := S(\sigma(4,5)) = Y^3 f_4 + Z f_5 = X^5Z - X^4Y^3 + X^6Z - X^5Y^3$ $E(h_6) = 2$ $T(h_6) = X^5Z$

BasisList = $\{f_1, f_2, f_3, f_4, f_5\}$ SimpList = $\{f_3, f_4, f_5, h_2\}$

PairQueue = $\emptyset$ SimpQueue = $\{h_3, h_5, h_6\}$

Applying **SimplificandOperation** to h_3:

$h_7 := Red(h_3,f_3) = h_3 + X^2Z f_3 = -X^2Y^3Z + X^4Z^2 + XY^6 - X^3Y^3Z$ $E(h_7) = 1$ $T(h_7) = X^2Y^3Z$

BasisList = $\{f_1, f_2, f_3, f_4, f_5\}$ SimpList = $\{f_3, f_4, f_5, h_2\}$

PairQueue = $\emptyset$ SimpQueue = $\{h_5, h_6,h_7\}$

Applying **SimplificandOperation** to h_5:

$h_8 := Red(h_5, f_3) = h_5 + XYZ f_3 =$

$= X^5Z - 2\,XY^4Z + X^3YZ^2 - X^4Y^3 + 2\,X^6Z - X^2Y^4Z$ $E(h_8) = 1$ $T(h_8) = X^5Z$

BasisList = $\{f_1, f_2, f_3, f_4, f_5\}$ SimpList = $\{f_3, f_4, f_5, h_2\}$

PairQueue = $\emptyset$ SimpQueue = $\{h_8, h_6,h_7\}$

We now choose h_8 since $T(h_8) = T(h_6)$ but $E(h_8) < E(h_6)$; applying **SimplificandOperation** to it:

$h_9 := Red(h_8, f_3) = h_8 - X^4 f_3 = -2XY^4Z + X^3YZ^2 + X^6Z - X^2Y^4Z + X^5Y^3$

$E(h_9) = 2$ $T(h_9) = XY^4Z$

BasisList = $\{f_1, f_2, f_3, f_4, f_5\}$ SimpList = $\{f_3, f_4, f_5, h_2, h_8\}$

PairQueue = $\emptyset$ SimpQueue = $\{h_6, h_7, h_9\}$

Then, applying **SimplificandOperation** to h_6:

$Red(h_6,f_3) = h_6 - X^4 f_3 = 0;$

to h_7:

$Red(h_7, h_2) = h_7 + X h_2 = 0;$

and to h_9:

$h_{10} := Red(h_9, f_5) = h_9 - 2\,XZ f_5 = X^3YZ^2 - X^6Z + X^2Y^4Z + X^5Y^3 - 2\,X^7Z$

$E(h_{10}) = 2$ $T(h_{10}) = X^3YZ^2$

BasisList = $\{f_1, f_2, f_3, f_4, f_5\}$ SimpList = $\{f_3, f_4, f_5, h_2, h_8\}$

PairQueue = $\emptyset$ SimpQueue = $\{h_{10}\}$

$h_{11} := Red(h_{10}, f_3) = h_{10} - X^2YZ f_3 =$

$= -X^6Z + 2\,X^2Y^4Z - X^4YZ^2 + X^5Y^3 - 2\,X^7Z + X^3Y^4Z$ $E(h_{11}) = 1$ $T(h_{11}) = X^6Z$

$Red(h_{11}, h_8) = h_{11} + X h_8 = 0$

We can now reconstruct the standard representations as follows:

$f_1 = XZ f_3 + h_2$

$h_2 = Y^3 f_3 + h_3$

$h_3 = -X^2Z f_3 + h_7$

$h_7 = -X h_2$

so

$h_2 = (Y^3 - X^2Z) f_3 - X h_2$

$h_2 = (1 + X)^{-1} (Y^3 - X^2Z) f_3$

$f_1 = (XZ + (1 + X)^{-1} (Y^3 - X^2Z)) f_3 = (1 + X)^{-1} (XZ + Y^3) f_3$

$f_2 = YZ f_3 + h_4$

$h_4 = -2\,Z f_5 + h_5$

$h_5 = -XYZ f_3 + h_8$

$h_8 = X^4 f_3 + h_9$

$h_9 = 2\,XZ\,f_5 + h_{10}$
$h_{10} = X^2YZ\,f_3 + h_{11}$
$h_{11} = -X\,h_8$

so

$$h_8 = (X^4 + X^2YZ)\,f_3 + 2\,XZ\,f_5 - X\,h_8$$
$$h_8 = (1+X)^{-1}\,(X^4 + X^2YZ)\,f_3 + 2\,(1+X)^{-1}\,XZ\,f_5$$
$$\begin{aligned} f_2 = (YZ - XYZ)\,f_3 - 2\,Z\,f_5 + h_8 = \\ = ((YZ - XYZ) + (1+X)^{-1}\,(X^4 + X^2YZ))\,f_3 + 2\,(-Z + (1+X)^{-1}\,XZ)\,f_5 = \\ = (YZ + X^4)\,(1+X)^{-1}\,f_3 -2\,(1+X)^{-1}\,Z\,f_5. \end{aligned}$$

$$h_6 = X^4\,f_3$$

A standard basis of I is, after removing redundant elements, (f_3, f_4, f_5).
We now remark that denoting:

$g_1 := XZ - Y^3$
$g_2 := YZ - X^4$
$g_3 := -Y^4 + X^5$

we have $f_1 = (XZ + Y^3)\,g_1$, $f_2 = (XZ + Y^3)\,g_2$, $f_3 = (1 + X)\,g_1$, $f_4 = (1 + X)\,g_2$, so in Loc(P), $I = (g_1, g_2, g_3)$
It is immediate to verify that (g_1, g_2, g_3) is a standard basis of J; moreover we remark that $f_5 = (1 + X)\,g_3$ and that the standard representations obtained for f_1 and f_2 can be read:

$f_1 = (XZ + Y^3)\,g_1$
$f_2 = (YZ + X^4)\,g_1 -2\,Z\,g_3$

4.6 Implementations

There are at our knowledge the following available implementations of the tangent cone algorithm:

- a MODULA 2 version running on ATARI and on IBM-PCs, realized by G. Pfister and H. Schoenemann and essentially implementing **SimpStandardBasis**: Buchberger algorithm, a version of the tangent cone algorithm for modules and specific applications for singularity theory are part of the system;
- a SAC 2 version, realised in Kaiserslautern by M. Zimnol [ZIM]
- the lazy version is included in the AlPI system (a MU-LISP system for Gröbner basis computations, running on IBM-PCs) by C. Traverso.

The algorithm is also under implementation in the CoCoA system (a Pascal system for Gröbner basis and commutative algebra computations, running on MacIntosh), designed by A. Giovini and G.Niesi (Genova).
Tangent cone computations can moreover be performed on any system containing Buchberger algorithm by means of Lazard's Homogeneization technique ([LAZ])

5 STANDARD BASES IN FORMAL POWER SERIES RINGS

Standard bases were originally introduced in the ring of formal power series by Hironaka [HIR]; we will devote here a very short discussion to the subject.
For the whole paragraph, the ordering < on T will satisfy the condition:

$1 > X_i$ for each i

which is equivalent to:

for each $m \in \mathbf{T}$, $m \leq 1$.

In some instances we will restrict our discussion to those orderings s.t.

$w_1(X_i) < 0$ for each i

but we will not require that $w_1(X_i) \in \mathbf{Z}$[1].
Because of the restriction on the ordering, for each formal power series $f = \Sigma_{t \in T}\, c(t)\, t$, $c(t) \in k$,

$T(f) := \max_<\{t : c(t) \neq 0\}$
$M(f) := c(T(f))\, T(f)$

are well-defined.
The definitions can then be extended to the modules $k[[X_1,\dots,X_n]]^t$.
Generalizing our definitions for polynomials and elements in the localization we can then speak of

M(F), the ideal in $k[X_1,\dots,X_n]$ generated by $\{M(f) : f \in F\}$

for each $F \subset k[[X_1,\dots,X_n]]$ and we can extend the various notions related to standard bases to any ring R s.t. $k[X_1,\dots,X_n] \subset R \subset k[[X_1,\dots,X_n]]$:

DEFINITION 10 Given $f \in R - \{0\}$, $F \subset R - \{0\}$:
an element $h \in R$ is called a *normal form* of f w.r.t. F if

$f - h = \Sigma\, g_i\, f_i$, $g_i \in R - \{0\}$, $f_i \in F$
either $h = 0$ or $M(h) \notin M(F)$.

[1] Clearly if $w_1(X_i) \in \mathbf{R}$, the resulting ordering could be not computable; we will implicitly assume suitable restrictions when discussing algorithms.

NF(f,F) will denote the set $\{h \in R$: h is a normal form of f w.r.t. F$\}$

f has a *standard representation* in terms of F iff it can be represented:

$f = \Sigma g_i f_i, g_i \in R - \{0\}, f_i \in F, T(g_i) T(f_i) \leq T(f)$ for every i

(such a representation will be called a standard representation).

$F \subset I - \{0\}$ is called a *standard basis* for the ideal $I \subset R$ iff $M\{F\}$ generates the ideal M(I).

R *has normal forms with standard representations* iff:

for each $\phi \in R^t - \{0\}, \Phi \subset R^t - \{0\}$, there is $\psi \in R^t$, s.t.

either $\psi = 0$ or $M(\psi) \notin M(\Phi)$.

$\phi - \psi = \Sigma g_i \phi_i, g_i \in R - \{0\}, \phi_i \in \Phi, T(g_i) T(\phi_i) \leq T(\phi - \psi)$.

The basic result in this context is Hironaka's Division Theorem:

PROPOSITION 9 Let $R = k[[X_1,...,X_n]]$. For each $f \in R - \{0\}, F \subset R - \{0\}$, there is $g \in R$, s.t.

either $g = 0$ or $g = \Sigma_{t\in T}$ c(t) t, with c(t) = 0 if $t \in M(F)$.

$f - g = \Sigma g_i f_i, g_i \in R - \{0\}, f_i \in F, T(g_i) T(f_i) \leq T(f - g)$

Proof: For an ordering s.t. $w_1(X_i) < 0$ for each i, *cf.* [HIR], [GAL]. The restriction on the ordering has been removed in [BEC1].

COROLLARY 4 $k[[X_1,..., X_n]]$ has canonical forms w.r.t. ideals, i.e.

for each $h \in k[[X_1,..., X_n]]$ there is a unique $g \in k[[X_1,...,X_n]]$ s.t. $h - g \in I$ and no term appearing in the development of g is in M(I).

By a suitable generalization of Prop. 9 to modules, one can prove that $k[[X_1,..., X_n]]$ has normal forms with standard representations; as a consequence the conditions of Theorem 2 give equivalent characterizations for standard bases in $k[[X_1,...,X_n]]$; for a proof one can consult [GAL] with the restriction $w_1(X_i) < 0$ for each i, [BEC1] and [BEC2] for the general case.

Since one performs computations in subrings of $k[[X_1,...,X_n]]$ which are finite extensions of $k[X_1,...,X_n]$, it could be interesting to have Theorem 2 for the general case of a ring R s.t. $k[X_1,...,X_n] \subset R \subset k[[X_1,...,X_n]]$:

PROPOSITION 10 Assume:

for each ideal $I \subset R$, for each $f \in R$, f has a normal form w.r.t. I

and let F be a standard basis for the ideal $I \subset R$. Then:

1) let $h \in NF(g,F)$; then:

if $h = 0$, then $g \in I$

if $h \neq 0$, $g \notin I$

2) if $h \in NF(g,F)$, $h \neq 0$, then $T(h) = \min\{T(g') : g' - g \in I\}$

3) if $g, g' \in R - I$ are s.t. $g - g' \in I$, then $M(h) = M(h')$ for each $h \in NF(g,F)$ and $h' \in NF(g',F)$.

Proof: The proof of Prop. 7 applies verbatim.

NOTATION Let $f_1,..., f_t \in R - \{0\}, F := \{f_1,...,f_t\}$; let $I \subset R$ be an ideal s.t. $F \subset I$.

Let T(-) and M(-) be defined in R^t, so that $T(e_i) = T(f_i)$.

Define

$s : P^t \to P$ by $s(\Sigma g_i e_i) := \Sigma g_i M(f_i)$;

so that the kernel of s

$Syz\{M(f_1),...,M(f_t)\} := Ker(s)$

is the module of syzygies among $\{M(f_1),...,M(f_t)\}$.

Define $S : R^t \to R$ by $S(\Sigma g_i e_i) := \Sigma g_i f_i$.

If u is a homogeneous element in Ker(s), we say that u *lifts* to $v \in Ker(S)$ (v is a *lifting* of u) if $M(v) = u$.

Let U be a basis of Ker(s) consisting of homogeneous elements.

THEOREM 3 If R has normal forms with standard representations[1], the following conditions are equivalent:

1) F is a standard basis of I

2) $f \in I$ iff f has a standard representation in terms of F

3) for each $f \in R - \{0\}$:

i) if $f \in I$, then $NF(f,F) = \{0\}$

ii) if $f \notin I$, then $NF(f,F) \neq \emptyset$ and $\forall h \in NF(f,F)$, $h \neq 0$.

4) F is a basis of I and for each $u \in U$, u has a lifting

Proof: The proof of Theorem 2 applies verbatim.

No much is known about standard basis computations in formal power series rings: we will discuss briefly in the next section the case of algebraic formal power series.

Here we remark only the following:

[1] Standard representations for module elements are not necessary; cf. the note to Theorem 2.

assume a 0-dimensional ideal $I \subset k[[X_1,\dots,X_n]]$ is given through a basis F, and one is interested to compute a standard basis of I, w.r.t. some ordering $<$ s.t. $w_1(X_i) < 0$ for each i (these being exactly those orderings s.t. $X_i < 1\ \forall i$ and satisfying the assumption introduced at the end of §4.4).
Assume also that for each element of F it is possible to compute any truncated expansion, i.e.

for each $f \in F$, for each $t \in T$, it is possible to compute $g \in k[X_1,\dots,X_n]$ s.t. $T(f - g) < t$.

Then, since the modified version of the lazy algorithm with early termination for 0-dimensional ideals (discussed at the end of §4.4) doesn't make any more reference to the notion of ecart (which is not generalizable to power series), one can apply it to compute a standard basis of I w.r.t. $<$.
Of course the operations on standard bases must be "lazy", i.e. the value of a coefficient should be computed only when it is used in the computation of the leading term and equality tests should (and can) be avoided. The early termination test, being bound to succeed after a finite number of steps, allows then to compute a standard basis of I.

6. APPLICATIONS[2]

6.1 J-adic topologies in local rings

We have discussed in §2.2 the computation of the tangent cone to a variety at the origin. Its generalization in commutative algebra is the following:
Let R be a commutative ring (noetherian and with identity), $J \subset R$ be an ideal s.t. $\cap J^n = (0)$.
Then J induces a topology, the J-adic topology, on R, to which the graded ring $gr_J(R) := \oplus J^n / J^{n+1}$ is associated.
For each $a \in R - \{0\}$, there is n s.t. $a \in J^n - J^{n+1}$. We can then define $v_J(a) := n$, $in_J(a) \in gr_J(Q)$ to be the residue class of a mod. J^{n+1}. We define also $in_J(0) := 0$.
To each ideal $I \subset R$, the homogeneous ideal $in_J(I) := (in_J(a) : a \in I) \subset gr_J(Q)$ is associated.
A *J-standard basis* of I is a finite set $\{g_1,\dots, g_s\} \subset I$ s.t. $in_J(I) = (in_J(g_1),\dots, in_J(g_s))$[3].
It is a classical technique in commutative algebra to study properties of the J-adic topology on R by studying related properties of $gr_J(Q)$ (cf. [Z-S], Ch. VIII)
We will use the following standard notations:

$R_{1+J} := \{(1+g)^{-1} f : f \in R, g \in J\}$

$R_J := \{g^{-1} f : f \in R, g \notin J\}$, whenever J is prime and contains all zero-divisors of R

and remark that if J is moreover maximal then $R_{1+J} = R_J$.

In the tangent cone case we have: $R = k[X_1,\dots,X_n] = P$ or $R = Loc(P)$, $J := (X_1,\dots,X_n)$, $gr_J(R) = P$, $v_J(a) := ord(a)$, $in_J(a) := in(a)$, $in_J(I) := in(I)$.
The same techniques based on standard basis computations can be generalized to other J-adic topologies. We will restrict here to discuss the case in which R is the localization at a prime ideal of a coordinate ring and J is its maximal ideal.

Our computational tool will be however related to the $(X_1,\dots,X_i)$-topology on $k[X_1,\dots,X_n]$:
let $P := k[Z_1,\dots,Z_m, Y_1,\dots,Y_s]$, let $\wp := (Y_1,\dots,Y_s) \subset P$; remark that $gr_{\wp}(P) \cong P$, graded by $deg_Y : P \to N$, where $deg_Y(Z_i) = 0$, $deg_Y(Y_j) = 1$.
We impose an ordering $<$ on the semigroup of terms of P s.t.

1) $w_1(Z_i) = 0$, $w_1(Y_j) = -1$

2) $Z_i > 1$ for each i;

such an ordering is a tangent cone ordering (of the third class in the partial classification before lemma 18). Let $<_w$ be the total semigroup well-ordering on the semigroup of terms of P defined by:

$m <_w n$ iff $deg_Y(m) < deg_Y(n)$ or ($deg_Y(m) = deg_Y(n)$ and $m < n$).

Remark that under $<$, for $f \in P$ one has $T(f) < 1$ iff $f \in \wp$, so that $Loc(P) = P_{1+\wp}$.

LEMMA 20 If G is a standard basis for $I \subset P$ w.r.t. $<$, then it is a $\wp$-standard basis for I and $\{in_{\wp}(f) : f \in G\}$ is a Gröbner basis for $in_{\wp}(I)$ w.r.t. $<_w$.

We now turn to the following situation:
let $A := k[Z_1,\dots,Z_m]$; let $H \subset J \subset A$ be two ideals, with $H := (h_1,\dots, h_t)$, $J := (f_1,\dots,f_s)$. Let $Q := A/H$, $\pi : A \to Q$ the canonical projection, $L := \pi(J)$. Remark that, since $\cap J^n = (0)$, one has $\cap L^n = (0)$.
Let us moreover assume that J is maximal and contains all associated primes to H; this is equivalent to the fact that L is maximal and contains all zero-divisors of Q; it is easy to verify $L^* := L\, Q_L$ is the maximal ideal of Q_L.
Let P, $\wp$, $<$ as above and define $q : P \to Q$ by $q(Z_i) = \pi(Z_i)$, $q(Y_j) = \pi(f_j)$, so that

$Ker(q) = (h_1,\dots, h_t, f_1 - Y_1,\dots,f_s - Y_s) =: \mathfrak{I}$.

Remark that q induces a surjective morphism (which we will still denote by q) q: $Loc(P) = P_{1+\wp} \to Q_{1+L}$, whose kernel is $Loc(\mathfrak{I}) := \mathfrak{I}\, Loc(P)$, so that $P_{1+\wp}/Loc(\mathfrak{I}) \cong Q_{1+L} = Q_L$ and $q(\wp) = L^*$.
Since

$gr_{L^*}(Q_L) \cong gr_{\wp}(P) / in_{\wp}(\mathfrak{I}) \cong P / in_{\wp}(\mathfrak{I})$,

[2] We give here only a brief sketch, with no proofs, of the main applications in local algebra, and we refer the reader for details and proofs to [MOR4].

[3] For a theory unifying and generalizing Gröbner bases, standard bases, J-standard bases, one can consult [ROB2]

after a standard basis G of $\mathfrak{S}$ w.r.t. $<$ is computed, because of Lemma 20 and Lemma 1:

1) $gr_{L^*}(Q_L)$ is explicitly given as a polynomial ring modulo a homogeneous ideal, which is given through a Gröbner basis.

2) $P / in_{\wp}(\mathfrak{S})$ is isomorphic as a k-vector space to the k-vector space $k[\mathbf{B}]$, with basis $\mathbf{B} := \{t \in \mathbf{T} - M(\mathfrak{S})\}$, this allows, by canonical Gröbner basis techniques, to define a ring structure on $k[\mathbf{B}]$ isomorphic to $gr_{L^*}(Q_L)$ and therefore a projection $\Pi: P \to k[\mathbf{B}]$. It is immediate to see that the isomorphism between $gr_{L^*}(Q_L)$ and $k[\mathbf{B}]$ is degree preserving if we just assign to each $b \in \mathbf{B}$ its degree $deg_Y(b)$ in P.

Then:

PROPOSITION 11 Let $a \in A - \{0\} \subset P$ and let us compute $b \in P$ and a unit u s.t. u^{-1} b is a normal form of a w.r.t. G. Let $I \supset \mathfrak{S}$ be an ideal in P, $F \subset P$ a standard basis for I Loc(P) w.r.t. $<$.

Then:

$v_{L^*}(\pi(a)) = v_{\wp}(b) = -w_{<}(M(b)).$

$in_{L^*}(\pi(a)) = \Pi(in_{\wp}(b))$

$\{q(f) : f \in F\}$ is a L^*-standard basis of $q(I)$.

so that we are able to obtain in an explicit computational way, the relevant informations about the L^*-adic topology of Q_L.

We can now turn to the following more general case:

let $A := k[Z_1,\dots,Z_m]$; let $H \subset J \subset A$ be two ideals, with J maximal and containing all associated primes to H; let $Q := A/H$, $\pi : A \to Q$ the canonical projection, $L := \pi(J)$. Then L is prime and contains all zero-divisors of Q; let us consider Q_L and $L^* := L\, Q_L$ the maximal ideal of Q_L. We want to study the L^*-topology of Q_L.

The reason is that the prime ideals of Q_L canonically correspond to those prime ideals of A which contain H and are contained in J; so (at least if H is radical) they describe those irreducible algebraic varieties contained in the variety V defined by H and passing through the subvariety W defined by J.

The notions related to the L^*-adic topology are then, in a very rough sense, a generalization of the concepts involving the "infinitesimal order" in a "neighborhood" of W, for "germs of rational functions" over the topological space Spec(A) of all prime ideals (irreducible algebraic varieties) of A with the Zariski topology.

To do this we just show that considering only maximal ideals is no restriction: in fact let us consider a maximal subset of variables $\{Z_{i_1},\dots,Z_{i_d}\}$ s.t. $J \cap k[Z_{i_1},\dots,Z_{i_d}] = (0)$ (such a set can be computed by Gröbner basis techniques) and let us relabel our variables denoting Z_{i_j} by U_j and $V_1,\dots, V_r$ the remaining ones.

LEMMA 21 Denote $A^0 := k(U_1,\dots,U_d)[V_1,\dots,V_r]$, $J^0 := J\, A^0$, $H^0 := H\, A^0$, $Q^0 := A^0/H^0$, $\pi^0 : A^0 \to Q^0$ the canonical projection, $L^0 := \pi^0(J^0)$. Then:

1) J^0 is a maximal ideal, L^0 is a maximal ideal

2) $(Q^0)_{L^0} \approx Q_L$.

6.2 Isolated singularities

The tangent cone algorithm and its generalization to modules[1] has been applied in [L-P] and [P-S] to the study of isolated singularities.

Let C be a variety in C^n with an isolated singularity at the origin; two important invariants of the singularity are the Milnor number μ and the Tjurina number τ of the singularity, the first being a topological invariant and the second an analytic invariant of the singularity.

In case C is a complete intersection variety with an isolated singularity, both numbers have an easy characterization as dimensions of C-vector spaces; namely let C be a complete intersection variety in C^n with an isolated singularity at the origin; in particular C is given by equations $f_1 = \dots = f_m = 0$, where $f_i \in C[X_1,\dots,X_n]$[2], $f(0) = 0$.

Let I_μ be the ideal in $C[[X_1,\dots,X_n]]$ generated by the maximal minors of the Jacobian matrix of $f_1,\dots, f_m$; I_τ the ideal in $C[[X_1,\dots,X_n]]$ generated by the maximal minors of the Jacobian matrix of $f_1,\dots, f_m$ and by $f_1,\dots,f_m$.

Since 0 is an isolated singularity of C, both ideals are 0-dimensional so that $C[[X_1,\dots,X_n]]/I_\mu$ and $C[[X_1,\dots,X_n]]/I_\tau$ are finitely dimensional C-vector spaces.

It is possible then to characterize the Milnor and Tjurina numbers of C by:

$\mu := \dim_C C[[X_1,\dots,X_n]]/I_\mu$

$\tau := \dim_C C[[X_1,\dots,X_n]]/I_\tau.$

Because of the following easy:

[1] We have not discussed such a generalization. We only remark that the notion of M(-) we have given for theoretical purposes is not to be used in such a generalization, since then normal form reduction would involve linear algebra. To achieve a better generalization, one needs a suitable notion of "monomial" in P^s: it turns out that monomials must be defined to be elements m e_i with m a monomial in P. Then a tangent cone algorithm for modules is obtained by generalizing the ideal case, in the same way as Buchberger algorithm has been generalized (cf. [BAY], [M-M], [C-T])

[2] Actually one should require the f_i to be convergent power series; the (non essential) restriction is due to computability reasons.

LEMMA 22 Let $\{f_1,\ldots,f_t\} \in k[X_1,\ldots,X_n] =: P$, denote by I the ideal they generate in $k[X_1,\ldots,X_n]$, by J the ideal they generate in $k[[X_1,\ldots,X_n]]$, by $\mathrm{Loc}(I) := I\,\mathrm{Loc}(P)$. If J is a 0-dimensional ideal, then:

$\dim_k k[[X_1,\ldots,X_n]]/J = \dim_k \mathrm{Loc}(P)/\mathrm{Loc}(I) = \dim_k P/M_<(I)$

where < is any total semigroup ordering on T s.t. $w_<(X_i) < 0$ for each i

both μ and τ can be computed easily by means of the tangent cone algorithm.

Other invariants (related to the Poincaré complex of the singularity) for isolated singularities can be described in terms of the finite dimension as C-vector spaces of modules $C[[X_1,\ldots,X_n]]^r/U$, U a submodule explicitly given through a basis.

Since an analogue of the result above holds for modules, such invariants have been extensively computed (using a generalization to modules of the tangent cone algorithm) and used to derive theoretical results ([L-P],[P-S]) on isolated singularities of curves in C^2 and complete intersection curves in C^3.

6.3 Standard bases in algebraic series rings

In the recent paper [AMR], a computational model for algebraic formal power series has been proposed which relies on the symbolic codification of the series by means of the Implicit Function Theorem introduced in [ALR], and on the tangent cone algorithm.

For a ring B s.t. $k[Z_1,\ldots,Z_r] \subset B \subset k[[Z_1,\ldots,Z_r]]$, denote $B_{loc} := \{f\,g^{-1} : f, g \in B, g \text{ invertible in } k[[Z_1,\ldots,Z_r]]\}$, and remark that for $B = k[Z_1,\ldots,Z_r]$, and for each ordering < s.t. $m \leq 1\ \forall m$, $B_{loc} = \mathrm{Loc}(B)$.

Let k be a computable field; $k[[X_1,\ldots,X_n]]_{alg}$ denotes the ring of algebraic formal power series.

Let us fix an ordering < on the semigroup T generated by the X_i's s.t.

$w_1(X_i) \in Z$, $w_1(X_i) < 0\ \forall i$.

Let us consider polynomials $F_1,\ldots, F_r \in k[X_1,\ldots,X_n, Y_1,\ldots,Y_r]$ vanishing at the origin and s.t. the Jacobian of the F_i's with respect to the Y_j's at the origin is a lower triangular non singular matrix. Under this assumption, by the Implicit Function Theorem, there are unique $f_1,\ldots, f_r \in k[[X_1,\ldots,X_n]]_{alg}$ s.t. $f_j(0) = 0\ \forall j$, and $F_i(X,f_1,\ldots,f_r) = 0\ \forall i$.

DEFINITION 11 $(F_1,\ldots, F_r)$ is called a locally smooth system (LSS) defining $f_1,\ldots, f_r \in k[[X_1,\ldots,X_n]]_{alg}$ if:

the Jacobian of the F_i's with respect to the Y_j's at the origin is a lower triangular non singular matrix.

$f_1,\ldots, f_r$ are the unique solutions of $F_1 = 0,\ldots, F_r = 0$ which vanish at the origin.

Given the LSS $\mathbf{F} := (F_1,\ldots,F_r)$ defining $f_1,\ldots, f_r$, let $P := k[X_1, \ldots, X_n, Y_1, \ldots, Y_r]$, $k[\underline{X},\mathbf{F}]_{loc} := k[X_1, \ldots, X_n, f_1,\ldots, f_r]_{loc} \subset k[[X_1,\ldots,X_n]]_{alg}$. To compute in it, we consider the evaluation map $\sigma_F : \mathrm{Loc}(P) \rightarrow k[\underline{X},\mathbf{F}]_{loc}$ defined by $\sigma_F(Y_i) = f_i$, for which $\mathrm{Ker}(\sigma_F) = (F_1,\ldots,F_r)\,\mathrm{Loc}(P)$, so that $k[\underline{X},\mathbf{F}]_{loc} \cong \mathrm{Loc}(P)/(F_1,\ldots,F_r)$.

If an algebraic series g is given by assigning a polynomial $G(X_1,\ldots,X_n,T)$ s.t. $G(X_1,\ldots,X_n,g) = 0$ and an algorithm to compute any truncation of g, it is possible to compute a LSS $\mathbf{F}$ s.t. $g \in k[\underline{X},\mathbf{F}]_{loc}$.

It is possible to show that, for suitable orderings $<_u$ on P which restricts to < on $\mathbf{T}$, a locally smooth system $(F_1,\ldots,F_r)$ is a standard basis in Loc(P) for the ideal it generates and $M_u(F_1,\ldots,F_r) = (Y_1,\ldots,Y_r)$; therefore, by normal form computations with the tangent cone algorithm it is possible to modify the LSS defining the f_i's so that it satisfies the following assumptions, for an explicitly obtained ordering $<_\sigma$, which restricts to < on T:

1) $\mathbf{F} = (F_1,\ldots,F_r)$ is a LSS for $f_1,\ldots,f_r$

2) $f_i \neq 0\ \forall i$

3) $F_i = Y_i\,(1+Q_i) - R_i$ with $Q_i, R_i \in (X,Y)$, $R_i \in k[X,Y_1,\ldots,Y_{i-1},Y_{i+1},\ldots,Y_r]$ and $M(R_i) = M(f_i)$

4) $\{F_1,\ldots,F_r\}$ is a standard basis for the ideal it generates in $K[X,Y]_{loc}$ w.r.t. $<_\sigma$.

Such an F is called a *standard locally smooth system* (SLSS).

By applying the tangent cone algorithm w.r.t. $<_\sigma$ in Loc(P), given $G_0,\ldots,G_s \in \mathrm{Loc}(P)$ and denoting $g_i := \sigma(G_i)\forall i$, it is then possible:

1) to compute $H \in \mathrm{Loc}(P)$ which is a normal form of G_0 w.r.t. $\{F_1,\ldots,F_r\}$; such an H is s.t. $H = 0$ iff $g_0 = 0$ and, if $H \neq 0$ then $\sigma(H) = g_0$, $M_\sigma(H) \in k[X_1,\ldots,X_n]$, $M_\sigma(H) = M(g_0)$ and is called a *representation* of g_0

2) therefore to decide whether $g_0 = 0$, and, if $g_0 \neq 0$, to compute $T(g_0)$ and $M(g_0)$

3) to compute a representation of a normal form of g_0 w.r.t. $\{g_1,\ldots,g_s\}$

4) to compute $H_1,\ldots,H_t$ s.t. H_i is a representation of $h_i := \sigma(H_i)$ and $\{h_1,\ldots,h_t\}$ is a standard basis for $(g_1,\ldots,g_s)$ w.r.t. <.

It is also possible to prove that the conditions of Theorem 3 are equivalent for $R = k[\underline{X},\mathbf{F}]_{loc}$ and $R = k[[X_1,\ldots,X_n]]_{alg}$.

In the same context, a different application of the tangent cone algorithm, together with effective algorithms for classical results on algebraic series (Weierstrass Division Theorem and Noether Normalization Lemma) can be applied to effectively perform elimination theory for ideals in $k[[X_1,\dots,X_n]]_{alg}$:

PROPOSITION 12 Let $P := k[Z_1,\dots,Z_m]$, $<_0$ a tangent cone ordering on the semigroup T generated by $\{Z_1,\dots,Z_m\}$.
Let $R := Loc(P)[Y_1,\dots,Y_s]$. Let I be an ideal in R given through a basis $\{f_1,\dots,f_t\}$.
It is possible to compute a basis of $I \cap Loc(P)$.
Proof: Let T be the semigroup of terms in P, and impose a tangent cone ordering $<$ on the semigroup of terms of $Q := k[Z_1,\dots,Z_m,Y_1,\dots,Y_s]$ s.t.

$w_1(T_i) = 1$, $w_1(Z_j) = 0$

the restriction of $<$ to T is $<_0$.

Remark that $<$ is an ordering of the fourth class in the partial classification after Lemma 18 and that $Loc(Q) = R$.
Remark also that for a term m, $m \in T$ iff $w_1(m) = 0$ and that if $m' < m \in T$, then $m' \in T$.
Therefore if for $g \in Q$, $M(g) \in T$, then $g \in k[Z_1,\dots,Z_n]$
Since $<$ is a tangent cone ordering, we can compute a standard basis G for I w.r.t. $<$.
Then we claim that $G \cap Loc(P)$ is a standard basis for $I \cap Loc(P)$ w.r.t. $<$.
In fact if $f \in I \cap Loc(P)$, then $M(f) = M_0(f) \in P$; so there is $g \in G$ s.t. $M(g) = M_0(g)$ divides $M(f)$.
But then $M(g) \in T$ and $g \in G \cap Loc(P)$.

COROLLARY 5 Let $f_1,\dots, f_r \in k[[X_1,\dots,X_n]]_{alg}$ be given (w.l.o.g. by a local smooth system). Let $I \subset k[[X_1,\dots,X_n]]_{alg}$ be the ideal generated by them.
It is possible to compute a linear change of coordinates C on $k[[X_1,\dots,X_n]]_{alg}$, a L.S.S. H defining series in $k[[X_1,\dots,X_i]]_{alg}$, a basis of an ideal $I^* \subset k[X_1,\dots,X_i,H]_{loc}$ s.t.

$$I^*\, k[[X_1,\dots,X_i]]_{alg} = C(I)\, k[[X_1,\dots,X_n]]_{alg} \cap k[[X_1,\dots,X_i]]_{alg}$$

Sketch of proof: The techniques of [AMR] allow to explicitly compute C, H and a basis of an ideal $J \subset k[X_1,\dots,X_i,H]_{loc}[X_{i+1},\dots X_n]$ s.t. $I^* = J \cap k[X_1,\dots,X_i,H]_{loc}$.
Denoting by $P := k[X_1,\dots,X_i,Y_1,\dots Y_r]$ and by σ both the evaluation map σ_H and its polynomial extension $Loc(P)[X_{i+1},\dots X_n] \rightarrow k[[X_1,\dots,X_n]]_{alg}$, by the result above applied to $\sigma^{-1}(J) \subset Loc(P)[X_{i+1},\dots X_n]$ one obtains $J^* = \sigma^{-1}(J) \cap Loc(P)$, so that $I^* = \sigma(J^*)$.

APPENDIX: GRADED RINGS

The polynomial ring is the basic example of a graded ring: each polynomial is uniquely represented as the sum of homogeneous components of different degrees, and since the natural numbers are an ordered semigroup:

1) a notion of degree can be defined for any non-zero polynomial f, to be the degree of the non-zero homogeneous component of highest degree in the representation of f

2) these notion of degree satisfies the well-known rules:

$\deg(f+g) \le \max(\deg(f),\deg(g))$

$\deg(f\,g) \le \deg(f) + \deg(g)$.

More in general, let us consider an ordered (additive) semigroup Γ. We say a ring G is a Γ-graded ring if there are subgroups $G(\gamma)$ for $\gamma \in \Gamma$ s.t.

for each $g \in G$, g can be uniquely represented $g = \Sigma_{\gamma\in\Gamma}\, g_\gamma$, $g_\gamma \in G(\gamma)$, only finitely many of them not zero.

Then one can define $\deg(g) := \max\{\gamma \in \Gamma : g_\gamma \neq 0\}$, which satisfies the rules above; the non-zero elements of $G(\gamma)$ are called the *homogeneous* elements of degree γ.

Gröbner basis theory is an instance of a different graded ring structure over the polynomial ring: here Γ is the (multiplicative) semigroup T, homogeneous elements of degree $t \in T$ are the monomials c t, $c \in k$, T(f) is then the degree of f, while M(f) is the highest degree non-zero homogeneous component in the representation of f.

In graded rings an important role is played by *homogeneous* ideals.
An ideal I is called *homogeneous* if it satisfies the following equivalent conditions:

1) I is generated by homogeneous elements

2) if $g = \Sigma_{\gamma\in\Gamma}\, g_\gamma \in I$, then each homogeneous component $g_\gamma \in I$.

If g is homogeneous of degree γ and it is in a homogeneous ideal I generated by homogeneous element g_i of degree γ_i, then it has a *homogeneous* representation

$g = \Sigma f_i g_i$, $f_i = 0$ or f_i homogeneous, $\deg(g) = \deg(f_i) + \deg(g_i)$.

Homogeneous ideals in the T-graduation of the polynomial ring are exactly the monomial ideals.

Graduations can be extended to modules of a Γ-graded ring G; we will just mention the easiest case of a finite free module G^t.
If we assign arbitrarily a degree $\gamma_i \in \Gamma$ to each element e_i of the canonical basis $(e_1,\dots, e_t)$, we can define homogeneous elements in G^t:

$\Sigma g_i e_i$ is homogeneous of degree γ if $\forall i$ $g_i = 0$ or g_i is homogeneous and $\deg(g_i) + \gamma_i = \gamma$.

Then homogeneous elements of a fixed degree form a subgroup of G^t, each element of G^t is uniquely represented as a finite sum of non-zero homogeneous elements of different degree, one defines the degree of $\phi \in G^t$ to be the maximum of the degrees of its non-zero homogeneous components, which satisfies:

$$\deg(\phi+\psi) \le \max(\deg(\phi),\deg(\psi)) \text{ for } \phi,\psi \in G^t$$
$$\deg(g\ \phi) \le \deg(g) + \deg(\phi) \text{ for } g \in G,\ \phi \in G^t.$$

A submodule Φ of G^t is called *homogeneous* if it satisfies the equivalent conditions:

1) Φ is generated by homogeneous elements
2) if $\phi \in \Phi$, then each homogeneous component in the representation of g is in Φ.

If $\phi \in G^t$ is homogeneous of degree γ and it is in a homogeneous submodule Φ generated by homogeneous element ϕ_i of degree γ_i, then it has a *homogeneous* representation

$$\phi = \Sigma\ g_i\ \phi_i,\ g_i = 0 \text{ or } g_i \in G \text{ homogeneous and } \deg(\phi) = \deg(g_i) + \deg(\phi_i).$$

REFERENCES

[ALR] M.E. ALONSO, I. LUENGO, M. RAIMONDO, An Algorithm on Quasi-Ordinary Polynomials, Proc. AAECC 6, *Lect. N. Comp. Sci.* 357 (1989), 59-73

[AMR] M.E. ALONSO, T. MORA, M. RAIMONDO, Computing with algebraic series, , *Proc. ISSAC 89*, ACM (1989), 101-111

[BAY] D. BAYER The division algorithm and the Hilbert scheme, *Ph. D. Thesis*, Harvard (1982)

[BEC1] T. BECKER, Standard bases and some computations in rings of power series, *J. Symb. Comp.*, to appear

[BEC2] T. BECKER, Stability and Buchbger criterion for standard bases in power series rings, Preprint, Univ. Passau (1989)

[BUC1] B. BUCHBERGER, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, *Ph. D. Thesis*, Innsbruck Univ. (1965)

[BUC2] B. BUCHBERGER, Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems, *Aeq. Math.* 4 (1970), 374-383

[BUC3] B. BUCHBERGER, A criterion for detecting unnecessary reductions in the construction of Gröbner bases, Proc. EUROSAM 79, *Lect. N. Comp. Sci.* 72 (1979), 3-21

[BUC4] B. BUCHBERGER, Gröbner bases: an algorithmic method in polynomial ideal theory, in N.K. BOSE *Recent trends in multidimensional systems theory*, Reidel (1985)

[C-T] P. CONTI, C. TRAVERSO, Computing the conductor of an integral extension, Proc. AAECC 7, *Disc. Appl. Math.*, to appear

[GAL] A. GALLIGO, A propos du theoreme de preparation de Weierstrass, *Lect. N. Math.* 409 (1974), 543-579

[G-M] R. GEBAUER, H.M. MÖLLER, On an installation of Buchberger's algorithm, *J. Symb. Comp.* 6 (1988), 141-152

[HIR] H. HIRONAKA, Resolution of singularities of an algebraic variety over a field of characteristic zero, *Ann. Math.* 79 (1964), 109-326

[LAZ] D.LAZARD, Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations, Proc. EUROCAL 83, *Lect. N. Comp. Sci. 162* (1983), 146-156

[L-P] I. LUENGO, G. PFISTER Normal forms and moduli spaces of curve singularities with semigroup <2 p, 2 q, 2 p q + d>, *Preprint Univ. Compl. Madrid* (1988)

[M-M] H.M. MÖLLER, F. MORA, New constructive methods in classical ideal theory, *J. Alg.* 100 (1986), 138-178

[MOR1] F. MORA An algorithm to compute the equations of tangent cones, Proc. EUROCAM 82, *Lect. N. Comp. Sci.* 144 (1982), 158-165

[MOR2] F. MORA, A constructive characterization of standard bases, *Boll. U.M.I.* D 2 (1983), 41-50

[MOR3] F. MORA, An algorithmic approach to local rings, Proc. EUROCAL 85, *Lect. N. Comp. Sci.* 204 (1985), 518-525

[MOR4] T. MORA, La queste del saint $Gr_a(A_L)$: a computational approach to local algebra, Proc. AAECC 7, *Disc. Appl. Math.*, to appear

[P-S] G. PFISTER, H. SCHÖNEMANN, Singularities with exact Poincaré complex but not quasihomogeneous, *Preprint* 147, Humboldt Univ., Dept. Math. (1988)

[ROB1] L. ROBBIANO, Term orderings on the polynomial ring, Proc. EUROCAL 85, *Lect. N. Comp. Sci.* 204 (1985), 513- 517

[ROB2] L. ROBBIANO, On the theory of graded structures, *J. Symb. Comp.*, 2 (1986), 139-170

[T-D] C. TRAVERSO, L. DONATI, Experimenting the Gröbner basis algorithm with the AlPI system, *Proc. ISSAC 89*, ACM (1989), 192-198

[Z-S] O. ZARISKI, P. SAMUEL, *Commutative Algebra*, Van Nostrand (1958)

[ZIM] M. ZIMNOL, Beispiele Algebraischer Reduktionsstrukturen, *Diplomarbeit*, Univ. Kaiserslautern (1987)