

Gröbner bases and algebraic geometry

Gert-Martin Greuel and Gerhard Pfister

Universität Kaiserslautern, Fachbereich Mathematik

Contents

Preface	1
1 Introduction by simple questions	2
2 Standard bases	7
2.1 Monomial orderings and associated rings	7
2.2 Standard bases and normal forms	10
2.3 Syzygies and free resolutions	16
3 Applications	20
3.1 The normalization	20
3.2 Singularities	22
3.3 Deformations	25
References	33

Preface

After the notion of Gröbner bases and an algorithm for constructing them was introduced by Buchberger [Bu1, Bu2] algebraic geometers have used Gröbner bases as the main computational tool for many years, either to prove a theorem or to disprove a conjecture or just to experiment with examples in order to obtain a feeling about the structure of an algebraic variety. Nontrivial problems coming either from logic, mathematics or applications usually lead to nontrivial Gröbner basis computations, which is the reason why several improvements have been provided by many people and have been implemented in general purpose systems like Axiom, Maple, Mathematica, Reduce, etc., and systems specialized for use in algebraic geometry and commutative algebra like CoCoA, Macaulay and Singular.

The present paper starts with an introduction to some concepts of algebraic geometry which should be understood by people with (almost) no knowledge in this field.

In the second chapter we introduce standard bases (generalization of Gröbner bases to non-well-orderings), which are needed for applications to local algebraic geometry (singularity theory), and a method for computing syzygies and free resolutions.

The last chapter describes a new algorithm for computing the normalization of a reduced affine ring and gives an elementary introduction to singularity theory. Then we describe algorithms, using standard bases, to compute infinitesimal deformations and obstructions, which are basic for the deformation theory of isolated singularities.

It is impossible to list all papers where Gröbner bases have been used in local and global algebraic geometry, and even more impossible to give an overview about these contributions. We have, therefore, included only references to papers mentioned in this tutorial paper. The interested reader will find many more in the other contributions of this volume and in the literature cited there.

1 Introduction by simple questions

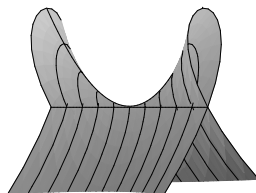
The basic problem of algebraic geometry can be formulated as a very simple question: “What is the structure of the set of solutions of finitely many polynomial equations in finitely many indeterminates?”

That is, we try to understand the set of points $x = (x_1, \dots, x_n) \in K^n$ satisfying

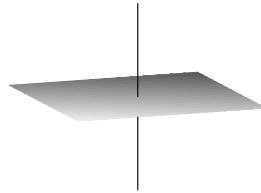
$$\begin{aligned} f_1(x_1, \dots, x_n) &= 0, \\ &\vdots \\ f_k(x_1, \dots, x_n) &= 0, \end{aligned}$$

where K is a field and f_1, \dots, f_k are elements of the polynomial ring $K[x] = K[x_1, \dots, x_n]$. The solution set of f_1, \dots, f_k is called the algebraic set, or algebraic variety of f_1, \dots, f_k and is denoted by $V(f_1, \dots, f_k)$.

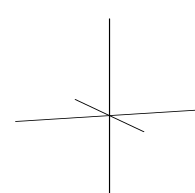
Here are three simple examples, which will be used to illustrate some of our subsequent questions:



1) the hypersurface
 $V(x^2 + y^3 - t^2y^2)$



2) the variety
 $V(xz, yz)$



3) the variety
 $V(xy, xz, yz)$

The simple question, however, does not have an easy answer at all. On the contrary, the mathematical discipline algebraic geometry, which provides

tools for possible answers, belongs with its long history to one of the highly developed branches of mathematics, which has created deep and quite sophisticated theories in geometry as well as in algebra. It has been estimated, as Kunz states in the introduction to his book on commutative algebra and algebraic geometry [Ku], that one can teach a course on algebraic geometry for 200 terms without repetition.

Of course, *understanding* is relative to the status of the theory but also to the cultural, economical and technical status of the society. Nowadays, faced by the technical revolution through computers, understanding requires, more and more, a computational approach to a problem, if possible. This is evident in algebraic geometry, as one can see, for instance, from recent textbooks (for example, [CLO], [St]). It is also evident that the majority of computational tools developed for algebraic geometry is based on Gröbner basis techniques.

Of course, any linear combination $f = \sum a_i f_i$, $a_i \in K[x]$, vanishes on $V = V(f_1, \dots, f_k)$ and V is equal to the solutions of all $f \in I = \langle f_1, \dots, f_k \rangle_{K[x]}$, the ideal generated by f_1, \dots, f_k in $K[x]$. Even the radical of I ,

$$\sqrt{I} = \{f \in K[x] \mid \exists d, f^d \in I\}$$

has the same solution set and, by the Hilbert Nullstellensatz, there is the following tight relation between ideals of $K[x]$ and algebraic sets, provided the field K is algebraically closed:

For any variety $V \subset K^n$ let $I(V) = \{f \in K[x] \mid f(x) = 0 \forall x \in V\}$ the ideal of V , then

$$V = V(J) \Rightarrow I(V) = \sqrt{J}.$$

The converse is trivially true.

This theorem is the reason why the couple algebra and geometry married and produced so many wonderful theorems. Using this ideal–variety correspondence, we may formulate several geometric question and their algebraic counterparts.

One word about the role of the field K . Algebraic geometers usually draw real pictures, think about it as complex varieties and perform computations over some finite field. This attitude is justified by successful practice.

From the geometric point of view, the field K is, however, extremely important. Algebraic geometry over \mathbb{R} , for instance, is much more complicated and by far not as complete as over \mathbb{C} .

The following **questions and problems** together with those mentioned in Buchberger's article [Bu4] belong to the very basic ones in algebraic geometry. They are also quite natural and are motivated already from the above examples. Note that for these examples, the answers are more or less obvious from the figures but, nevertheless, they require a mathematical proof which is usually given by algebra. The answers given by algebra however coincide with our geometric intuition only in the case of an algebraically closed field.

- Is $V(I)$ irreducible or may it be decomposed into several algebraic varieties? If so, find its irreducible components. Algebraically this means to compute a primary decomposition of I or of \sqrt{I} , the latter means to compute the associated prime ideals of I .

The first example is irreducible, the second has two components (one of dimension 2 and one of dimension 1), while the third example has three components (all of dimension 1).

- A natural question to ask is "How independent are the generators f_1, \dots, f_k of I ?" that is, we ask for all relations

$$(r_1, \dots, r_k) \in K[x]^r, \text{ such that } \sum r_i f_i = 0.$$

These relations form a submodule of $K[x]^r$, which is called the *syzygy module* of I and is denoted by $\text{syz}(I)$. It is the kernel of the $K[x]$ -linear map

$$K[x]^k \longrightarrow K[x], (r_1, \dots, r_k) \mapsto \sum r_i f_i.$$

- More generally, we may ask for generators of the kernel of a $K[x]$ -linear map $K[x]^r \rightarrow K[x]^s$, or, in other words, for solutions of a system of linear equations over $K[x]$.

A direct geometric interpretation of syzygies is not so clear, but there are instances where properties of syzygies have important geometric consequences (cf. [Sch2]).

In example 1 we have $\text{syz}(I) = 0$, in example 2, $\text{syz}(I) = \langle (-y, x) \rangle \subset K[x]^2$ and in example 3, $\text{syz}(I) = \langle (-z, y - 0), (-z, 0, x) \rangle \subset K[x]^3$.

- A more geometric question is the following. Let $V(I) = V(I_1) \cup V(I_2)$ be a union of not necessarily irreducible varieties and let us assume that $V(I)$ and $V(I_1)$ are known. How can we describe $V(I_2)$? Algebraically, we want to compute generators for I_2 if we know those of I and I_1 . This amounts to finding generators for the ideal quotient

$$I : I_1 = \{f \in K[x] \mid fI_1 \subset I\}.$$

Geometrically, $V(I : I_1)$ is the smallest variety containing $V(I) \setminus V(I_1)$, which is the (Zariski) closure of $V(I) \setminus V(I_1)$.

In example 2 we have $\langle xz, yz \rangle : \langle x, y \rangle = z$ and in example 3 $\langle xy, xz, yz \rangle : \langle x, y \rangle = \langle z, xy \rangle$, which gives, in both cases, equations for the complement of the z -axis $x = y = 0$.

- Geometrically important is the projection of a variety $V(I) \subset K^n$ into a linear subspace K^{n-r} . Given generators f_1, \dots, f_k of I , we want to find

generators for the (closure of the) image of $V(I)$ in $K^{n-r} = \{x \mid x_1 = \dots = x_r = 0\}$. The image is defined by the ideal $I \cap K[x_{r+1}, \dots, x_n]$ and finding generators for this intersection is known as eliminating x_1, \dots, x_r from f_1, \dots, f_k .

Projecting the three varieties above to the (x, y) plane is, in the first two cases, surjective and in the third case it gives the two coordinate axes in the (x, y) plane. This corresponds to the fact that the intersection with $K[x, y]$ of the first two ideals is 0, while the last one is xy .

- Another problem is related to the Riemann removable theorem, which states that a function on a complex manifold, which is holomorphic and bounded outside a subvariety of codimension 1, is actually holomorphic everywhere. This is well-known for open subsets of \mathbb{C} , but in higher dimension there exists a second removable theorem, which states that a function, which is holomorphic outside a subvariety of codimension 2 (no assumption on boundedness), is holomorphic everywhere.

For singular complex varieties this is not true in general, but those for which the two removable theorems hold are called *normal*. Moreover, each reduced variety has a normalization and there is a morphism with finite fibres from the normalization to the variety, which is an isomorphism outside the singular locus.

The problem is, given a variety $V(I) \subset K^n$, find a normal variety $V(J) \subset K^m$ and a polynomial map $K^m \rightarrow K^n$ inducing the normalization map $V(J) \rightarrow V(I)$.

The problem can be reduced to irreducible varieties (but need not be, as we shall see) and then the equivalent algebraic problem is to find the normalization of $K[x_1, \dots, x_n]/I$, that is the integral closure of $K[x]/I$ in the quotient field of $K[x]/I$ and present this ring as an affine ring $K[x_1, \dots, x_m]/J$ for some m and J .

In the above examples it can be shown that the normalization of all three varieties are smooth, the last two are the disjoint union of the (smooth) components. The corresponding rings are $K[x_1, x_2]$, $K[x_1, x_2] \oplus K[x_3]$, $K[x_1] \oplus K[x_2] \oplus K[x_3]$.

- The significance of *singularities* appears not only in the normalization problem. The study of singularities is also called *local algebraic geometry* and belongs to the basic tasks of algebraic geometry. Nowadays, singularity theory is a whole subject on its own.

A singularity of a variety is a point which has no neighbourhood in which the Jacobian matrix of the generators has constant rank.

In the first example the whole x -axis is singular, in the two other examples only the origin.

One task is to compute generators for the ideal of the singular locus, which is itself a variety. This is just done by computing subdeterminants of the Jacobian matrix, if there are no components of different dimensions. In general, however, we need ideal quotients.

In the above examples, the singular locus is given by $\langle x, y \rangle$, $\langle x, y, z \rangle$ and $\langle x, y, z \rangle$, respectively.

- *Studying a variety $V(I)$, $I = (f_1, \dots, f_k)$, locally at a singular point, say the origin of K^n , means studying the ideal $IK[x]_{(x)}$ generated by I in the local ring*

$$K[x]_{(x)} = \left\{ \frac{f}{g} \mid f, g \in K[x], g \notin \langle x_1, \dots, x_n \rangle \right\}.$$

In this local ring the polynomials g with $g(0) \neq 0$ are units and $K[x]$ is a subring of $K[x]_{(x)}$.

Now all the problems we considered above can be formulated for ideals in $K[x]_{(x)}$ and modules over $K[x]_{(x)}$ instead of $K[x]$.

The geometric problems should be interpreted as concerning properties of the variety in a neighbourhood of the given point.

It should not be a surprise to say that all the above problems have algorithmic and computational solutions, which use, at some place, Gröbner basis methods. Moreover, algorithms for most of these have been implemented quite efficiently, in several computer algebra systems, such as CoCoA [CNR], Macaulay [GS] and SINGULAR [GPS]. The most complicated problem by far is the primary decomposition, the latest achievement is the normalization, both being implemented in SINGULAR.

At first glance, it seems that computation in the localization $K[x]_{(x)}$ requires computation with rational functions. It is an important fact that this is not necessary, but that basically the same algorithms which were developed for $K[x]$ can be used for $K[x]_{(x)}$. This is achieved by the choice of a special ordering on the monomials of $K[x]$ where, loosely speaking, the monomials of lower degree are considered to be bigger.

However, such orderings are no longer well-orderings and the classical Buchberger algorithm would not terminate. Mora discovered [Mo] that a different normal form algorithm, or, equivalently, a different division with remainders, leads to termination. Thus, Buchberger's algorithm with Mora's normal form is able to compute in $K[x]_{(x)}$ without denominators.

Several algorithms for $K[x]$ use elimination of (some auxiliary extra) variables. But variables to be eliminated have, necessarily, to be well-ordered. Hence, to be able to apply the full power of Gröbner basis methods also for the local ring $K[x]_{(x)}$, we need mixed orders, where the monomial ordering

restricted to some variables is not a well-ordering, while restricted to other variables it is. In [GP] the authors described a modification of Mora's normal form, which terminates for mixed ordering and, more generally, for any monomial ordering which is compatible with the natural semigroup structure.

The corresponding modification of Buchberger's algorithm with this general normal form computes, in the case of a well-ordering (which we also call global ordering) *Gröbner bases* while, in the case of a local ordering (which was called tangent cone ordering by Mora), it computes so-called *standard bases*, which enjoy similar nice properties as Gröbner bases. We follow a suggestion by Mora and call bases computed by the general algorithm, standard bases, whilst, following the tradition of the last 33 years, reserving the name Gröbner basis for the established case of well-orderings.

2 Standard bases

Let K be a field and $K[x] = K[x_1, \dots, x_n]$ be the polynomial ring in n variables over K .

2.1 Monomial orderings and associated rings

Definition 2.1. A **monomial ordering** on $K[x]$ is a total order on the set of monomials $\{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ satisfying

$$x^\alpha > x^\beta \Rightarrow x^{\alpha+\gamma} > x^{\beta+\gamma} \text{ for all } \alpha, \beta, \gamma \in \mathbb{N}^n.$$

We call a monomial ordering $>$ a **global** (respectively **local**, respectively **mixed**) ordering if $x_i > 1$ for all i (respectively $x_i < 1$ for all i , respectively if there exist i, j so that $x_i > 1$ and $x_j < 1$).

This notion is justified by the associated ring to be defined later. Note that $>$ is global if and only if $>$ is a well-ordering.

Definition 2.2. Any $f \in K[x] \setminus \{0\}$ can be written uniquely as

$$f = cx^\alpha + f'$$

with $c \in K \setminus \{0\}$ and $\alpha > \alpha'$ for any non-zero term $c'x^{\alpha'}$ of f' . We set

$$\begin{aligned} \text{lm}(f) &= x^\alpha, & \text{the leading monomial of } f, \\ \text{lc}(f) &= c, & \text{the leading coefficient of } f. \end{aligned}$$

For a subset $G \subset K[x]$ we define the **leading ideal** of G as

$$L(G) = \langle \text{lm}(g) \mid g \in G \setminus \{0\} \rangle_{K[x]},$$

the ideal generated by $\{\text{lm}(g) \mid g \in G \setminus \{0\}\}$ in $K[x]$.

Typical global orderings are the **lexicographical ordering lp** ($x^\alpha >_{lp} x^\beta : \Leftrightarrow$ the first non-zero entry of $\alpha - \beta$ is positive) and the **degree reverse lexicographical ordering dp** ($x^\alpha >_{dp} x^\beta : \Leftrightarrow \deg x^\alpha > \deg x^\beta$ or $\deg x^\alpha = \deg x^\beta$ and the last non-zero entry of $\alpha - \beta$ is negative), typical local orderings are the **negative lexicographical ordering ls** ($x^\alpha >_{ls} x^\beta : \Leftrightarrow$ the first non-zero entry of $\alpha - \beta$ is negative) and the **negative degree reverse lexicographical ordering ds** ($x^\alpha >_{ds} x^\beta : \Leftrightarrow \deg x^\alpha < \deg x^\beta$ or $\deg x^\alpha = \deg x^\beta$ and the last non-zero entry of $\alpha - \beta$ is negative). In the abbreviations lp, dp, ls, ds the p refers to a polynomial ring and the s to a series ring (cf. Definition 2.3).

For practical purposes, as well as for certain theoretical arguments, it is important to extend the definitions of dp, respectively ds, to weighted degree orderings, where the variables have positive, respectively negative, weights.

Given monomial orderings $>_1$ on $K[x_1, \dots, x_n]$ and $>_2$ on $K[y_1, \dots, y_m]$, we define the **product ordering** or **block ordering** $> = (>_1, >_2)$ on $K[x, y]$ by $x^\alpha y^\beta > x^\gamma y^\delta : \Leftrightarrow x^\alpha >_1 x^\gamma$ or $x^\alpha = x^\gamma$ and $y^\beta >_2 y^\delta$.

Definition 2.3. For a given monomial ordering $>$ define the multiplicatively closed set

$$S_{>} := \{u \in K[x] \setminus \{0\} \mid \text{lm}(u) = 1\}$$

and the K -algebra

$$\text{Loc } K[x] := S_{>}^{-1} K[x] = \left\{ \frac{f}{u} \mid f \in K[x], u \in S_{>} \right\},$$

the localization (ring of fractions) of $K[x]$ with respect to $S_{>}$.

We call $\text{Loc } K[x]$ also the **ring associated to $K[x]$ and $>$** .

Remark 2.1. 1) $K[x] \subset \text{Loc } K[x] \subset K[x]_{(x)}$ where $K[x]_{(x)}$ denotes the localization of $K[x]$ with respect to the maximal ideal (x_1, \dots, x_n) . $\text{Loc } K[x]$ is Noetherian, it is $K[x]$ -flat and $K[x]_{(x)}$ is $\text{Loc } K[x]$ -flat.

- 2) $\text{Loc } K[x] = K[x]$ if and only if $>$ is global and $\text{Loc } K[x] = K[x]_{(x)}$ if and only if $>$ is local (which justifies the names).

Mixed orderings occur as a product ordering of two orderings with one global and the other local. Many constructions with Gröbner bases in $K[x]$ use a set of auxiliary variables which have to be eliminated later. If one wants to perform such constructions in $K[x]_{(x)}$, the auxiliary variables must be bigger than 1, hence, mixed orderings occur naturally in this context.

- 3) The product ordering on $K[x, y] = K[x_1, \dots, x_n, y_1, \dots, y_m]$ with $>_1$ global on $K[x]$ and $>_2$ arbitrary on $K[y]$ is an **elimination ordering**

for x_1, \dots, x_n on $K[x, y]$, that is, for $g \in K[x, y]$ and $\text{lm}(g) \in K[y]$ we have $g \in K[y]$. It is easy to see that for an arbitrary monomial ordering $>$ to be an elimination ordering for x_1, \dots, x_r it is necessary that $x_i > 1$ for $i = 1, \dots, r$. For example, let $>_1$ be global on $K[x]$ and $>_2$ local on $K[y]$, then the product ordering $> = (>_1, >_2)$ on $K[x, y]$ satisfies $S_{>} = K^* + (y)K[y]$, hence

$$\text{Loc } K[x, y] = (K[y]_{(y)})[x].$$

Note that lm and lc have natural **extensions to the localization**. For $f \in \text{Loc } K[x]$ there exists $u \in S_{>}$, $\text{lc}(u) = 1$, such that $uf \in K[x]$ and we define

$$\text{lm}(f) := \text{lm}(uf), \quad \text{lc}(f) := \text{lc}(uf).$$

Since

$$\begin{aligned} \text{lm}(fg) &= \text{lm}(f) \text{lm}(g) \text{ and} \\ \text{lc}(fg) &= \text{lc}(f)\text{lc}(g) \end{aligned}$$

this definition is independent of the choice of u . Moreover, for a subset $G \subset \text{Loc } K[x]$ set

$$L(G) = \langle \text{lm}(g) \mid g \in G \setminus \{0\} \rangle_{K[x]} \subset K[x]$$

and call it the **leading ideal** of G . Note also that $u \in \text{Loc } K[x] \setminus \{0\}$ is a unit in $\text{Loc } K[x]$ if and only if $\text{lm}(u) = 1$, that is, if $u \in S_{>}$.

For our intended applications of standard bases, but also for an elegant proof of Buchberger's standard basis criterion, we have to extend the notion of monomial orderings to the free module $K[x]^r = \sum_{i=1, \dots, r} K[x]e_i$ where

$$e_i = (0, \dots, 1, \dots, 0) \in K[x]^r$$

denotes the i -th canonical basis vector of $K[x]^r$. We call

$$x^\alpha e_i = (0, \dots, x^\alpha, \dots, 0) \in K[x]^r$$

a **monomial (involving component i)**.

Definition 2.4. Let $>$ be a monomial ordering on $K[x]$. A **monomial ordering** or a **module ordering** on $K[x]^r$ is a total ordering $>_m$ on the set of monomials $\{x^\alpha e_i \mid \alpha \in \mathbb{N}^n, i = 1, \dots, r\}$ satisfying

$$\begin{aligned} x^\alpha e_i >_m x^\beta e_j &\Rightarrow x^{\alpha+\gamma} e_i >_m x^{\beta+\gamma} e_j, \\ x^\alpha > x^\beta &\Rightarrow x^\alpha e_i >_m x^\beta e_i, \end{aligned}$$

for all $\alpha, \beta, \gamma \in \mathbb{N}^n$, $i, j = 1, \dots, r$.

Two module orderings are of particular practical interest:

$$x^\alpha e_i > x^\beta e_j \Leftrightarrow i > j \text{ or } i = j \text{ and } x^\alpha > x^\beta,$$

giving priority to the components and

$$x^\alpha e_i > x^\beta e_j \Leftrightarrow x^\alpha > x^\beta \text{ or } x^\alpha = x^\beta \text{ and } i > j,$$

which gives priority to the monomials in $K[x]$.

Note that, by the second condition, each component of $K[x]^r$ carries the ordering of $K[x]$. Hence, $>_m$ is a well-ordering on $K[x]^r$ if and only if $>$ is a well-ordering on $K[x]$. We call $>_m$ **global** respectively **local** respectively **mixed**, if this holds for $>$ respectively.

Now we fix a module ordering $>_m$ and denote it also with $>$. Since any $f \in K[x]^r \setminus \{0\}$ can be written uniquely as

$$f = cx^\alpha e_i + f'$$

with $c \in K \setminus \{0\}$ and $x^\alpha e_i > x^{\alpha'} e_j$ for any non-zero term $c'x^{\alpha'} e_j$ of f' we can define as before

$$\begin{aligned} \text{lm}(f) &= x^\alpha e_i, \\ \text{lc}(f) &= c \end{aligned}$$

and call it the **leading monomial** respectively the **leading coefficient** of f . Moreover, for $G \subset K[x]^r$ we call

$$L(G) = \langle \text{lm}(g) \mid g \in G \setminus \{0\} \rangle_{K[x]} \subset K[x]^r$$

the **leading submodule** of G .

As from $K[x]$ to $\text{Loc } K[x]$ these definitions carry over naturally from $K[x]^r$ to $(\text{Loc } K[x])^r$.

We say that $x^\alpha e_i$ is divisible by $x^\beta e_j$ if $i = j$ and $x^\beta \mid x^\alpha$. For any set of monomials $G \subset K[x]^r$ and any monomial $x^\alpha e_i$, we have

$$x^\alpha e_i \notin \langle G \rangle_{K[x]} \Leftrightarrow x^\alpha e_i \text{ is not divisible by any element of } G.$$

2.2 Standard bases and normal forms

Let $>$ be a fixed monomial ordering on $K[x]$. In order to have a short notation, we write

$$R := \text{Loc } K[x] = S_{>}^{-1} K[x]$$

to denote the localization of $K[x]$ with respect to $>$.

We define the notion of standard basis respectively Gröbner basis and give an algorithm to compute such a basis. In the case of a well-ordering this is Buchberger's [Bu1], [Bu2], [Bu3], [Bu4] celebrated algorithm, in the general case it is a variation of Mora's tangent cone algorithm [Mo], first published in [Geta], [GP], [Gra]. We like to stress that it is important to work consequently with the ring R and not with $K[x]$, even if the input is polynomial.

Definition 2.5.

- 1) Let $I \subset R^r$ be a submodule. A finite set $G \subset I$ is called a **standard basis** of I if and only if $L(G) = L(I)$, that is, for any $f \in I \setminus \{0\}$ there exists a $g \in G$ satisfying $\text{lm}(g) \mid \text{lm}(f)$.
- 2) If the ordering is a well-ordering, then a standard basis G is called a **Gröbner basis**. In this case $R = K[x]$ and, hence, $G \subset I \subset K[x]^r$.

With the above notation, we follow the suggestion of [MPT], reserving the name Gröbner basis exclusively for well-orderings.

A set $G \subset R^r$ is called **interreduced** if $0 \notin G$ and if $\text{lm}(g) \notin L(G \setminus \{g\})$.

Note that any standard basis can be made interreduced by deleting successively those g with $\text{lm}(g) \mid \text{lm}(h)$ for some $h \in G \setminus \{g\}$. An interreduced standard basis is also called **minimal**.

For $f \in K[x]^r$ and $G \subset K[x]^r$ we say that f is **reduced with respect to G** if no monomial of f is contained in $L(G)$. If $>$ is not a well-ordering, we extend this to $f \in R^r$ and $G \subset R^r$ by saying that f is (completely) reduced with respect to G if there exist $u_f \in S_{>}$, and for each $g \in G$, $u_g \in S_{>}$ such that $u_f f, u_g g \in K[x]^r$ and $u_f f$ is reduced with respect to $\{u_g g \mid g \in G\}$.

A set $G \subset R^r$ is called **reduced** if $0 \notin G$ and if each $g \in G$ is reduced with respect to $G \setminus \{g\}$ and if, moreover, $g - \text{lc}(g) \text{lm}(g)$ is reduced with respect to G . For $>$ a well-ordering this just means that for each $g \in G \subset K[x]^r$, $\text{lm}(g)$ does not divide any monomial of any element of $G \setminus \{g\}$.

We shall see later that reduced Gröbner bases do always exist, but reduced standard bases, in general, do not.

Definition 2.6. Let \mathcal{G} denote the set of all finite and ordered subsets $G \subset R^r$.

- 1) A map

$$\text{NF} : R^r \times \mathcal{G} \rightarrow R^r, (f, G) \mapsto \text{NF}(f|G),$$

is called a **normal form** on R^r if, for all f and G ,

- (i) $\text{NF}(f|G) \neq 0 \Rightarrow \text{lm}(\text{NF}(f|G)) \notin L(G)$,
- (ii) $f - \text{NF}(f|G) \in \langle G \rangle_R$.

NF is called a **reduced normal form** if, moreover, $\text{NF}(f, G)$ is reduced with respect to G . NF is called a **weak normal form** if, instead of (ii), only the condition (ii') holds:

(ii') for each $f \in R^r$ and each $G \in \mathcal{G}$ there exists a unit $u \in R$, so that $uf - \text{NF}(f|G) \in \langle G \rangle_R$.

2) Let $G = \{g_1, \dots, g_s\} \in \mathcal{G}$. A representation of $f \in \langle G \rangle_R$,

$$f = \sum_{i=1}^s a_i g_i, \quad a_i \in R,$$

satisfying $\text{lm}(f) \geq \text{lm}(a_i g_i)$, whenever both sides are defined, is called a **standard representation** of f (with respect to G).

Remark 2.2. The reason for introducing weak normal forms is twofold. On the one hand, they are usually more easy to compute and as good as normal forms for practical applications. On the other hand, and more seriously, normal forms may not exist, while weak normal forms do. For example, it is easy to see that $f = x \in R = K[x]_{(x)}$ (with ls) does not have a normal form with respect to $G = \{x - x^2\}$. On the other hand, since $(1 - x)f = x - x^2$ and $1 - x$ a unit in R , f is a weak normal form of itself with respect to G .

$\text{NF}(f|G)$ is by no means unique. For applications (weak) normal forms are most useful if G is a standard basis of $\langle G \rangle_R$. We shall demonstrate this with a first application, which follows immediately from the definitions.

Lemma 2.1. *Let $I \subset R^r$ be a submodule, $G \subset I$ a standard basis of I and $\text{NF}(-|G)$ a weak normal form on R^r with respect to G .*

- 1) For any $f \in R^r$ we have $f \in I \Leftrightarrow \text{NF}(f|G) = 0$.
- 2) If $J \subset R^r$ is a submodule with $I \subset J$, then $L(I) = L(J)$ implies $I = J$.
- 3) $I = \langle G \rangle_R$, that is, G generates I as R -module.
- 4) If $\text{NF}(-|G)$ is a reduced normal form, then it is unique.

For describing Buchberger's normal form algorithm, we need the notion of an s -polynomial.

Definition 2.7. Let $f, g \in R^r \setminus \{0\}$ with $\text{lm}(f) = x^\alpha e_i$ and $\text{lm}(g) = x^\beta e_j$, respectively. Let

$$\gamma := \text{lcm}(\alpha, \beta) := (\max(\alpha_1, \beta_1), \dots, \max(\alpha_n, \beta_n))$$

be the **least common multiple** of x^α and x^β and define the **s-polynomial** of f and g to be

$$\text{spoly}(f, g) := \begin{cases} x^{\gamma-\alpha}f - \frac{\text{lc}(f)}{\text{lc}(g)}x^{\gamma-\beta}g, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

If $\text{lm}(g) \mid \text{lm}(f)$, say $\text{lm}(g) = x^\beta e_i$, $\text{lm}(f) = x^\alpha e_j$, then the s -polynomial is especially simple,

$$\text{spoly}(f, g) = f - \frac{c(f)}{c(g)}x^{\alpha-\beta}g,$$

and $\text{lm}(\text{spoly}(f, g)) < \text{lm}(g)$. For the normal form algorithm, the s -polynomial will only be used in this form, while for the standard basis algorithm we need it in the general form above. In order to be able to use the same expression in both algorithms, we prefer the definition of spoly above and not the more symmetric form $\text{lc}(g)x^{\gamma-\alpha}f - \text{lc}(f)x^{\gamma-\beta}g$. Both are, of course, equivalent, since our ground ring K is a field.

Algorithm 2.1. Assume that $>$ is a well-ordering on $K[x]^r$.

NFBUCHBERGER($f \mid G$)

Input: $f \in K[x]^r$, $G \in \mathcal{G}$.

Output: $h \in K[x]^r$, a normal form of f with respect to G .

- $h = f$;
- while ($h \neq 0$ and $G_h = \{g \in G \mid \text{lm}(g) \mid \text{lm}(h)\} \neq \emptyset$)
 choose any $g \in G_h$;
 $h = \text{spoly}(h, g)$;
- return h ;

For termination and correctness see [Bu4]. Note that each specific choice of “any” gives a different normal form function.

It is easy to extend NFBuchberger to a reduced normal form.

The idea of many standard basis algorithms may be formalized as follows:

Algorithm 2.2. Let $>$ be any monomial ordering on R^r and assume that a weak normal form algorithm NF on R^r is given.

STANDARD(G, NF)

Input: $G \in \mathcal{G}$

Output: $S \in \mathcal{G}$ such that S is a standard basis of the submodule $I = \langle G \rangle_R \subset R^r$

- $S = G$;
- $P = \{(f, g) \mid f, g \in S\} \subset S \times S$
- while ($P \neq \emptyset$)
 - choose $(f, g) \in P$;
 - $P = P \setminus \{(f, g)\}$;
 - $h = \text{NF}(\text{spoly}(f, g) \mid S)$;
 - If ($h \neq 0$)
 - $P = P \cup \{(h, f) \mid f \in S\}$;
 - $S = S \cup h$;
- return S ;

To see termination of STANDARD, note that if $h \neq 0$ then $\text{lm}(h) \notin L(S)$ by property 1) of NF. Hence, we obtain a strictly increasing sequence of monomial submodules of $K[x]^r$, which becomes stationary by Dickson's lemma or by the Noetherian property of $K[x]$. That is, after finitely many steps, we always have $\text{NF}(\text{spoly}(f, g) \mid S) = 0$ for $(f, g) \in P$ and, after some finite time, the pairset P will become empty.

Correctness follows from applying Buchberger's fundamental standard basis criterion below.

Theorem 2.1. [*Buchberger's criterion*] *Let $I \subset R^r$ be a submodule and $G = \{g_1, \dots, g_s\}$ be a subset of I . Let $\text{NF}(- \mid G)$ be a weak normal form on R^r with respect to G , satisfying: for each $f \in R^r$ there exists a unit u such that $uf - \text{NF}(f \mid G)$ has a standard representation with respect to G .*

Then the following are equivalent

- 1) G is a standard basis of I ,
- 2) $\text{NF}(f \mid G) = 0$ for all $f \in I$,
- 3) each $f \in I$ has a standard representation with respect to G ,
- 4) G generates I and $\text{NF}(\text{spoly}(g_i, g_j) \mid G) = 0$ for $i, j = 1, \dots, s$.

The implications 1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 4) are easy.

The implication 4) \Rightarrow 1) is the important criterion which allows the checking and construction of standard bases in finitely many steps. The proof is most easily done by using syzygies and is, therefore, postponed to the next section (Theorem 2.2).

We present now a general normal form algorithm, which works for any monomial ordering. It is basically due to Mora [Mo], with a different notion of ecart, as given in [Geta], [GP]).

Before doing this, let us first analyze Buchberger's algorithm in the case of a local ordering.

The standard example is in one variable x , with $x < 1$, $f = x$ and $G = \{g = x - x^2\}$. We obtain

$$x - \left(\sum_{i=0}^{\infty} x^i \right) (x - x^2) = 0$$

in $K[[x]]$, which is checked to be true, since $\sum x^i = \frac{1}{1-x}$ in $K[[x]]$. However, this is not a normal form in our sense, since $\sum x^i \notin R$.

Mora's idea was to allow more elements for reduction in order to create a standard expression of the form

$$uf = \sum_{i=1}^s a_i g_i + \text{NF}(f|G),$$

with u a unit, $a_i \in K[x]$ and $\text{NF}(f|G) \in K[x]^r$ in the case when the input data f and $G = \{g_1, \dots, g_s\}$ are *polynomial*. In the above example he arrives at an expression

$$(1-x)x = x - x^2$$

instead of $x = \left(\sum_{i=0}^{\infty} x^i \right) (x - x^2)$.

Definition 2.8. For a monomial $x^\alpha e_i \in K[x]^r$ set $\deg x^\alpha e_i = \deg x^\alpha = \alpha_1 + \dots + \alpha_n$. For $f \in K[x]^r \setminus \{0\}$, let $\deg f$ be the maximal degree of all monomials occurring in f . We define the **ecart** of f as

$$\text{ecart}(f) = \deg f - \deg \text{lm}(f).$$

For a homogeneous $f = \sum f_i e_i$ (all components f_i are homogeneous polynomials of the same degree), we have $\text{ecart}(f) = 0$.

Algorithm 2.3. Let $>$ be any monomial ordering on $K[x]^r$, $R = S_{>}^{-1}K[x]$. $\text{NFMORA}(f|G)$

Input: $f \in K[x]^r$, $G = \{g_1, \dots, g_s\} \subset K[x]^r$

Output: $h \in K[x]^r$ a weak normal form of f with respect to G . Moreover, there exists a standard representation $uf - h = \sum_{i=1}^s a_i g_i$ with $a_i \in K[x]$, $u \in S_{>}$.

- $h = f$;
- $T = G$,

- while($h \neq 0$ and $T_h = \{g \in T \mid \text{lm}(g) \mid \text{lm}(h)\} \neq \emptyset$)
 - choose $g \in T_h$ with $\text{ecart}(g)$ minimal;
 - if ($\text{ecart}(g) > \text{ecart}(h)$)
 - $T = T \cup \{h\}$;
 - $h = \text{spoly}(h, g)$;
- return h ;

If the input is homogeneous, then the ecart is always 0 and NFMORA is equal to NFBUCHBERGER. If $>$ is a well-ordering, then $\text{lm}(g) \mid \text{lm}(h)$ implies that $\text{lm}(g) \leq \text{lm}(h)$, hence $T = G$ during the algorithm. Thus, NFMora is the same as NFBuchberger, but with a special selection strategy for the elements from G .

For termination and correctness see [GP].

It is clear that, with a little extra storage, the algorithm does also return $u \in S_{>}$.

Algorithm 2.4. Let $>$ be any monomial ordering on $K[x]^r$, $R = S_{>}^{-1}K[x]$.

STANDARD BASIS(G)

Input: $G = \{g_1, \dots, g_s\} \subset K[x]^r$

Output: $S = \{h_1, \dots, h_t\} \subset K[x]^r$ such that S is a standard basis of $I = \langle G \rangle_R \subset R^r$.

- $S = \text{Standard}(G, \text{NFMora})$;
- return S ;

2.3 Syzygies and free resolutions

Let K be a field and $>$ a monomial ordering on $K[x]^r$. Again R denotes the localization of $K[x]$ with respect to $S_{>}$.

We shall give a method, using standard bases, to compute syzygies and, more generally, free resolutions of finitely generated R -modules. Syzygies and free resolutions are very important objects and basic ingredients for many constructions in homological algebra and algebraic geometry. On the other hand, the use of syzygies gives a very elegant way to prove Buchberger's criterion for a standard basis. Moreover, a close inspection of the syzygies of the generators of an ideal allows detection of useless pairs during a computation of a standard basis (cf. [MM], [Ei]). Our presentation follows partly that of Schreyer [Sch1], [Sch2], cf. also [Ei]. The generalization to arbitrary monomial orderings was first formulated and proved in [Getal] and [GP].

A **syzygy** or a **relation** between k elements $f_1, \dots, f_k \in R^r = \bigoplus_{i=1}^r Re_i$ is a k -tuple $(g_1, \dots, g_k) \in R^k$ satisfying

$$\sum_{i=1}^k g_i f_i = 0.$$

The set of all syzygies between f_1, \dots, f_k is a submodule of R^k . Indeed, it is the kernel of the ring homomorphism

$$\begin{aligned} \varphi_1 : F_1 := \bigoplus_{i=1}^k R\varepsilon_i &\longrightarrow F_0 := \bigoplus_{i=1}^r Re_i, \\ \varepsilon_i &\longmapsto f_i, \end{aligned}$$

where e_i respectively ε_i denote the canonical bases of R^r respectively R^k . φ_1 surjects onto $I = \langle f_1, \dots, f_k \rangle_R$ and

$$\text{syz } I = \text{Ker } \varphi_1$$

is called the **module of syzygies** of I with respect to the generators f_1, \dots, f_k .

We shall now define a monomial ordering on F_1 , which behaves perfectly well with respect to standard bases. This was first introduced and used by Schreyer [Sch1].

Set

$$\begin{aligned} x^\alpha \varepsilon_i > x^\beta \varepsilon_j &\Leftrightarrow \text{lm}(x^\alpha f_i) > \text{lm}(x^\beta f_j) \text{ or} \\ &\text{lm}(x^\alpha f_i) = \text{lm}(x^\beta f_j) \text{ and } i < j. \end{aligned}$$

The left-hand side $>$ is the new ordering on F_1 and the right-hand side $>$ is the ordering on F_0 . In order to distinguish them, we occasionally call them $>_1$ respectively $>_0$. $>_0$ and $>_1$ induce the same ordering on R . We call the ordering $>_1$ the Schreyer ordering. Note that it depends on f_1, \dots, f_k .

Now we are going to prove Buchberger's criterion, stating that $G = \{f_1, \dots, f_k\}$ is a standard basis of I , if, for all $i < j$, $\text{NF}(\text{spoly}(f_i, f_j)|G) = 0$. The proof uses syzygies and is basically due to Schreyer [Sch1], [Sch2], although our generalization (to general monomial orderings) seems to be simpler. It gives, at the same time, a proof of Schreyer's result that the syzygies derived from a standard representation of $\text{spoly}(f_i, f_j)$ form a standard basis of $\text{syz } I$ for the Schreyer ordering.

We introduce some notations. For each $i < j$ such that f_i and f_j have leading term in the same component, say $\text{lm}(f_i) = x^{\alpha_i} e_\nu$, $\text{lm}(f_j) = x^{\alpha_j} e_\nu$, define the monomial

$$m_{ji} := x^{\gamma - \alpha_i} \in K[x],$$

where $\gamma = \text{lcm}(\alpha_i, \alpha_j)$. If $c_i = \text{lc}(f_i)$ and $c_j = \text{lc}(f_j)$ then

$$m_{ji} f_i - \frac{c_i}{c_j} m_{ij} f_j = \text{spoly}(f_i, f_j).$$

Assume now that for $i < j$

$$\text{NF}(\text{spoly}(f_i, f_j)|G) = 0,$$

for some weak normal form NF on R^r .

Then we have a standard representation

$$m_{ji}f_i - \frac{c_i}{c_j}m_{ij}f_j = \sum_{\nu=1}^k a_{\nu}^{(ij)}f_{\nu}, \quad a_{\nu}^{(ij)} \in R.$$

Define for $i < j$ such that $\text{lm}(f_i)$ and $\text{lm}(f_j)$ involve the same component

$$s_{ij} = m_{ji}\varepsilon_i - \frac{c_i}{c_j}m_{ij}\varepsilon_j - \sum_{\nu} a_{\nu}^{(ij)}\varepsilon_{\nu}.$$

Then $s_{ij} \in \text{syz } I$ and it is easy to see that

Lemma 2.2. $\text{lm}(s_{ij}) = m_{ji}\varepsilon_i$.

Theorem 2.2. Let $G = \{g_1, \dots, g_s\}$ be a set of generators of $I \subset R^r$ satisfying, for some weak normal form NF on R^r ,

$$NF(\text{spoly}(g_i, g_j) \mid G) = 0, \quad i < j,$$

then the following holds:

- 1) G is a standard basis of I .
- 2) $\{s_{ij}\}$ is a standard basis of $\text{syz } I$ with respect to the Schreyer ordering. In particular, $\{s_{ij}\}$ generates $\text{syz } I$.

Proof. We give a proof of 1) and 2) at the time time.

Take any $f \in I$ and a preimage $g \in F_1$ of f ,

$$g = \sum_{i=1}^s a_i\varepsilon_i, \quad f = \varphi(g) = \sum_{i=1}^s a_i g_i.$$

This is possible as G generates I .

In case 1), we assume $f \neq 0$, in case 2) $f = 0$.

Consider a standard representation of $g - h$,

$$g = \sum a_{ij}s_{ij} + h, \quad a_{ij} \in R,$$

where $h = \sum h_j\varepsilon_j \in F_1$ is a normal form of g with respect to $\{s_{ij}\}$ for some weak normal form on F_1 (we need only know that it exists). We have, if $h \neq 0$,

$$\text{lm}(h) = \text{lm}(h_{\nu}) \cdot \varepsilon_{\nu} \text{ for some } \nu$$

and $\text{lm}(h) \notin L(\{s_{ij}\}) = \langle \{m_{ji}\varepsilon_i\} \rangle$ by Lemma 2.2. This shows

$$m_{j\nu} \nmid \text{lm}(h_{\nu}) \text{ for all } j.$$

Since $g - h \in \langle \{s_{ij}\} \rangle \subset \text{syz } I$, we obtain

$$f = \varphi(g) = \varphi(h) = \sum h_j g_j.$$

Assume that for some $j \neq \nu$, $\text{lm}(h_j g_j) = \text{lm}(h_\nu g_\nu)$. Then $\text{lm}(h_\nu g_\nu)$ is divisible by $\text{lm}(g_\nu)$ and by $\text{lm}(g_j)$ and hence, by

$$\text{lm}(g_\nu) \text{lm}(g_j) / \gcd(\text{lm}(g_\nu), \text{lm}(g_j)) = \text{lm}(g_\nu) m_{j\nu}.$$

This contradicts $m_{j\nu} \nmid \text{lm}(h_\nu)$.

In case 1) we obtain $\text{lm}(f) = \text{lm}(h_\nu g_\nu) \in L(G)$, in case 2) it shows that $h \neq 0$ leads to a contradiction. In case 1) G is a standard basis by definition and in case 2) $\{s_{ij}\}$ is a standard basis by Theorem 2.1, 2) \Rightarrow 1), which was already proved. \square

We shall now see, as an application, that the Hilbert syzygy theorem holds for the rings $R = S_{>}^{-1}K[x]$, stating that each finitely generated R -module has a free resolution of length at most n , the number of variables.

Lemma 2.3. *Let $G = \{g_1, \dots, g_s\}$ be a standard basis of $I \subset R^r$, ordered in such a way that the following holds: if $i < j$ and $\text{lm}(g_i) = x^{\alpha_i} e_\nu$, $\text{lm}(g_j) = x^{\alpha_j} e_\nu$ for some ν , then $\alpha_i \geq \alpha_j$ lexicographically. Let s_{ij} denote the syzygies defined above. Suppose that $\text{lm}(g_1), \dots, \text{lm}(g_s)$ do not depend on the variables x_1, \dots, x_k . Then the $\text{lm}(s_{ij})$, taken with respect to the Schreyer ordering, do not depend on x_1, \dots, x_{k+1} .*

Proof. Given s_{ij} , then $i < j$ and $\text{lm}(g_i)$ and $\text{lm}(g_j)$ involve the same component, say e_ν . By assumption $\text{lm}(g_i) = x^{\alpha_i} e_\nu$, $\text{lm}(g_j) = x^{\alpha_j} e_\nu$ satisfy $\alpha_i = (0, \dots, \alpha_{i,k+1}, \dots)$ $\alpha_j = (0, \dots, \alpha_{j,k+1}, \dots)$ with $\alpha_{i,k+1} \geq \alpha_{j,k+1}$. Therefore, $\text{lm}(s_{ij}) = m_{ji} e_i$, $m_{ji} = x^{\text{lcm}(\alpha_i, \alpha_j) - \alpha_i}$, does not depend on x_{k+1} . \square

Applying the lemma successively to the higher syzygy modules, we obtain (cf. [GP] for a detailed proof):

Theorem 2.3. *Let $>$ be any monomial ordering on $K[x] = K[x_1, \dots, x_n]$ and $R = S_{>}^{-1}K[x]$ be the associated ring. Then any finitely generated R -module M has a free resolution*

$$0 \longrightarrow F_m \longrightarrow F_{m-1} \longrightarrow \dots \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

F_i free R -modules, of length $m \leq n$. In particular, R is a regular ring.

It is clear that the methods of this section provide an algorithm to compute (non-minimal) free resolutions. This algorithm has been implemented in SINGULAR.

3 Applications

3.1 The normalization

Here we describe an algorithm which goes back to Grauert and Remmert [GR] and was proposed by T. de Jong ([J]). There are also algorithms by Gianni, Trager ([GT]) and Vasconcelos ([V]).

The algorithm is based on the following criterion for normality:

Proposition 3.1. *Let R be a Noetherian reduced ring and J be a radical ideal containing a non-zero divisor such that the zero set of J , $V(J)$ contains the non-normal locus of $\text{Spec}(R)$. Then R is normal if and only if $R = \text{Hom}_R(J, J)$.*

Remark 3.1. Let J, R be as in the proposition and x a non-zero divisor, then

$$1) \quad xJ : J = x \cdot \text{Hom}_R(J, J)$$

and, consequently,

$$2) \quad R = \text{Hom}_R(J, J) \text{ if and only if } xJ : J \subseteq \langle x \rangle.$$

3) Let $u_0 = x, u_1, \dots, u_s$ be generators of $xJ : J$. Because of the fact that $\text{Hom}_R(J, J)$ is a ring we have $\frac{s(s+1)}{2}$ relations $\frac{u_i}{x} \cdot \frac{u_j}{x} = \sum_{k=0}^s \xi_k^{ij} \frac{u_k}{x}$, $s \geq i \geq j \geq 1$, $\xi_k^{ij} \in R$ in $\frac{1}{x}(xJ : J)$, which, together with the linear relations, the syzygies, between u_0, \dots, u_s define the ring structure of $\text{Hom}_R(J, J)$:

$$\begin{array}{ccc} R[T_1, \dots, T_s] & \twoheadrightarrow & \text{Hom}_R(J, J) \\ T_i & \rightsquigarrow & \frac{u_i}{x}. \end{array}$$

The kernel of this map is the ideal generated by the $T_i T_j - \sum_{k=0}^s \xi_k^{ij} T_k$,

where $T_0 = 1$, and $\sum_{k=0}^s \eta_k T_k$ such that $\sum_{k=0}^s \eta_k u_k = 0$.

Algorithm 3.1.

`NORMAL(I)`

Input: a radical ideal $I \subseteq K[x_1, \dots, x_n]$,

Output: s polynomial rings R_1, \dots, R_s and s prime ideals $I_1 \subset R_1, \dots, I_s \subset R_s$ and s maps $\pi_i : R \rightarrow R_j$, such that the induced map $\pi : K[x_1, \dots, x_n]/I \rightarrow R_1/I_1 \times \dots \times R_s/I_s$ is the normalization of $K[x_1, \dots, x_n]/I$

- Result = \emptyset ;

- compute idempotents of $K[x_1, \dots, x_n]/I$;
Assume $K[x_1, \dots, x_n]/I = K[x_1, \dots, x_n]/I_1 \times \dots \times K[x_1, \dots, x_n]/I_s$.
- For $i = 1$ to s do
 - compute $J = \text{singular locus of } I_i$
 - choose $f \in J \setminus I_i$ and compute $I_i : f$ to check whether f is a zero divisor
 - if $I_i : f \not\supseteq I_i$ then
Result = Result \cup NORMAL($\sqrt{I_i, f}$) \cup NORMAL($I_i : f$)
 - else
 $J = \sqrt{I_i, f}$
 $H = fJ : J$
 if $H = \langle f \rangle$
 Result = Result \cup $\{K[x_1, \dots, x_n], I_i, \text{id}\}$
 else
 assume $H = fJ : J = \langle f, u_1, \dots, u_s \rangle$
 then compute an ideal $L \subseteq K[x_1, \dots, x_n, T_1, \dots, T_s]$ such
 that
 $K[x_1, \dots, x_n, T_1, \dots, T_s]/L \xrightarrow{\sim} \text{Hom}(J, J), T_i \rightsquigarrow \frac{u_i}{f}$
 let $\varphi : K[x_1, \dots, x_n] \rightarrow K[x_1, \dots, x_n, T_1, \dots, T_s]$ be the inclusion.
 $S = \text{normal}(L)$;
 compose the maps of S with φ ;
 Result = Result $\cup S$;
- return Result

It remains to give an algorithm to compute the idempotents.

We shall explain this for the case when the input ideal I is (weighted) homogeneous with strictly positive weight.

An idempotent e , that is, $e^2 - e \in I$ has to be homogeneous of degree 0, will, therefore, not occur in the first step. It can, however, occur after one normalization loop in $\text{Hom}(J, J) \simeq K[x_1, \dots, x_n, T_1, \dots, T_s]/L$ because some of the generators may have the same degree.

Let $T \subseteq \{T_1, \dots, T_s\}$ be the subset of variables of degree 0.

Then $L \cap K[T]$ is zero-dimensional because $T_j^2 - \sum \xi_k^{jj} T_k \in L \cap K[T]$ for all $T_j \in T$ (the weights are ≥ 0 and, therefore, $\xi_k^{jj} \in K, T_k \in T$).

For this situation there is an easy algorithm:

Algorithm 3.2.
IDEMPOTENTS(I)

Input: $I \subseteq K[x_1, \dots, x_n]$ a (weighted) homogeneous radical ideal, $\deg(x_i) = 0$ for $i \leq k$, $\deg(x_i) > 0$ for $i > k$, $I \cap K[x_1, \dots, x_k]$ 0-dimensional.

Output: ideals I_1, \dots, I_s such that

$$K[x_1, \dots, x_n]/I = K[x_1, \dots, x_n]/I_1 \times \cdots \times K[x_1, \dots, x_n]/I_s$$

and $I \cap K[x_1, \dots, x_k] = \bigcap (I_v \cap K[x_1, \dots, x_k])$ is the prime decomposition

- Result = \emptyset ;
- compute $J = I \cap K[x_1, \dots, x_k]$;
- compute $J = P_1 \cap \cdots \cap P_s$ the (0-dimensional) prime decomposition;
- For $i = 1$ to s do
 - choose $g_i \neq 0$ in $\bigcap_{v \neq i} P_v$;
 - Result = Result $\cup \{I : g_i\}$;
- return Result;

3.2 Singularities

The basic concepts and ideas of singularity theory are best explained over the field \mathbb{C} of complex numbers, although, algebraically, most invariants make sense over arbitrary fields.

Let $U \subset \mathbb{C}^n$ be an open subset in the usual Euclidian topology, and f_1, \dots, f_k holomorphic (complex analytic) functions on U , then we may consider

$$V = V(f_1, \dots, f_k) = \{x \in U \mid f_1(x) = \cdots = f_k(x) = 0\},$$

the complex analytic sub-variety defined by f_1, \dots, f_k in U .

In practice, f_1, \dots, f_k will be polynomials, but singularity theory is interested only in the behaviour of $V(f_1, \dots, f_k)$ in an arbitrary small neighbourhood of some point $p \in V$, that is, the **germ** of V at p , which is denoted by (V, p) . Algebraically, this means that we are not interested in the ideal generated by f_1, \dots, f_k in the polynomial ring $\mathbb{C}[x_1, \dots, x_n]$ but in the ideal I generated by f_1, \dots, f_k in the convergent power series ring $\mathbb{C}\{x_1 - p_1, \dots, x_n - p_n\} = \mathbb{C}\{x - p\}$.

For arbitrary fields K , where the notion of convergence does not make sense, we consider instead the formal power series ring $K[[x]] = K[[x_1, \dots, x_n]]$

and ideals I generated by formal power series (in practice polynomials) $f_1, \dots, f_k \in K[[x]]$. In order to have a uniform notation, we write

$$K\langle x \rangle = K\langle x_1, \dots, x_n \rangle$$

to denote both $K[[x]]$ and $K\{x\} = K\{x_1, \dots, x_n\}$ if K is a complete valued field (for example, $K = \mathbb{C}$).

The ring $\mathcal{O}_{V,p} = \mathbb{C}\{x - p\}/I$ (respectively $K\langle x \rangle/I$) is called the **analytic local ring** of the singularity (V, p) .

If f_1, \dots, f_k are polynomials, we may also consider the corresponding **algebraic local ring** $K[x]_{(x-p)}/\langle f_1, \dots, f_k \rangle$, where $K[x]_{(x-p)}$ is the localization of $K[x]$ in the maximal ideal $\langle x_1 - p_1, \dots, x_n - p_n \rangle$. Indeed in this ring we are able to compute standard bases (cf. Section 1).

As in the affine case, we have the Hilbert Nullstellensatz (also called the Hilbert–Rückert Nullstellensatz), stating that

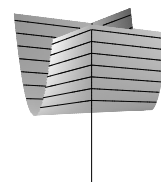
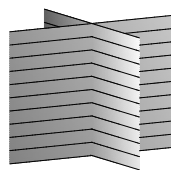
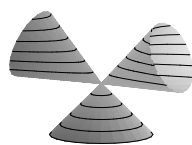
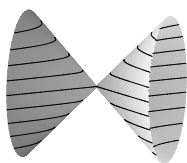
$$\sqrt{I} = I(V, p) := \{f \in \mathbb{C}\{x - p\} \mid f|_{(V,p)} = 0\}$$

for $I \subset \mathbb{C}\{x - p\}$ and (V, p) the complex analytic germ defined by I .

A **(complex) singularity** is, by definition, nothing but a complex analytic germ (V, p) (together with its analytic local ring $\mathbb{C}\{x - p\}/I$). (V, p) is called **non-singular** or **regular** or **smooth** if $\mathbb{C}\{x_1 - p_1, \dots, x_n - p_n\}/I$ is isomorphic (as local ring) to a power series ring $\mathbb{C}\{y_1, \dots, y_d\}$ (respectively $K\langle x_1, \dots, x_n \rangle/I \cong K\langle y_1, \dots, y_d \rangle$). By the implicit function theorem, this is equivalent to the fact that I has a system of generators g_1, \dots, g_{n-d} such that the Jacobian matrix of g_1, \dots, g_{n-d} has rank $n - d$ in some neighbourhood of p . (V, p) is called an **isolated singularity** if there is a neighbourhood $W \subset \mathbb{C}^n$ of p such that $W \cap (V \setminus \{p\})$ is regular everywhere.

Isolated Singularities

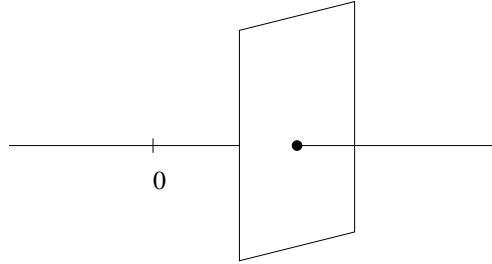
Non-isolated singularities



$$A_1 : x^2 - y^2 + z^2 = 0 \quad D_4 : z^3 - zx^2 + y^2 = 0 \quad A_\infty : x^2 - y^2 = 0 \quad D_\infty : y^2 - zx^2 = 0$$

The **dimension** of the singularity (V, p) is, by definition, the Krull dimension of the analytic local ring $\mathcal{O}_{V,p} = K\langle x \rangle/I$, which is the same as the Krull dimension of the algebraic local ring $K[x]_{(x-p)}/I$ if $I = \langle f_1, \dots, f_k \rangle$ is generated by polynomials, which follows easily from the theory of dimensions by Hilbert–Samuel series. Using this fact, we can compute $\dim(V, p)$ by computing a standard basis of the ideal $\langle f_1, \dots, f_k \rangle_{\text{Loc } K[x]}$ with respect to any *local* monomial ordering on $K[x]$. The dimension is equal to the dimension of the corresponding monomial ideal (which is a combinatorial problem).

It is important to compute a standard basis with respect to a local ordering. For example, the leading ideal of $\langle yx - y, zx - z \rangle$, with respect to dp , is $\langle xy, xz \rangle$ (hence of dimension 2), but, with respect to ds , it is $\langle y, z \rangle$ (hence of dimension 1). Geometrically, this means that the dimension of the affine variety $V = V(yx - y, zx - z)$ is 2 but the dimension of the singularity $(V, 0)$ (that is, the dimension of V at the point 0) is 1:



$$V : y(x - 1) = z(x - 1) = 0, \dim(V, 0) = 1$$

Another basic invariant is the **multiplicity** $\text{mt}(V, p)$ of the singularity (V, p) . If (V, p) is reduced, that is, $I = \sqrt{I}$, then $\text{mt}(V, p)$ has a nice geometric interpretation: it is the number of intersection points of a sufficiently small representative $V \subset \mathbb{C}^n$ of (V, p) with a general $(n - d)$ -dimensional plane in \mathbb{C}^n close to p (but not through p). If (V, p) is a **hypersurface singularity**, that is, $I = \langle f \rangle$ is a principal ideal in $\mathbb{C}\{x - p\}$, then $\text{mt}(V, p)$ is the smallest degree in the Taylor expansion of f in p .

Algebraically, $\text{mt}(V, p)$ is the Hilbert–Samuel multiplicity of the ideal $\langle x_1 - p_1, \dots, x_n - p_n \rangle$ in the analytic or in the algebraic local ring of (V, p) .

As before the Hilbert-Samuel function of the ideal defining V coincides with the Hilbert-Samuel function of the leading ideal of a standard basis with respect to a local degree ordering.

One of the most important invariants of an isolated hypersurface singularity (V, p) given by $I = \langle f \rangle \subset K\langle x \rangle$ is the **Milnor number**

$$\mu(f) := \dim_K K\langle x \rangle / \langle f_{x_1}, \dots, f_{x_n} \rangle$$

($\text{char}(K) = 0$) where f_{x_i} denotes the partial derivative of f with respect to x_i .

For $K = \mathbb{C}$, μ is even a topological invariant and has the following topological meaning, due to Milnor [Mil]. For $f \in \mathbb{C}\{x_1, \dots, x_n\}$ defining an isolated singularity at 0, let

$$V_t = B_\varepsilon(0) \cap f^{-1}(t),$$

$0 < |t| \ll 1$ and $B_\varepsilon(0)$ a small ball of radius ε around 0, then V_t (the “Milnor fibre of f ”) has the homotopy type of a 1-point union of $\mu(f)$ $(n - 1)$ -dimensional spheres. In particular, $\mu(f) = \dim_{\mathbb{C}} H_n(V_t, \mathbb{C})$.

Algorithm 3.3. (Assume $\text{char}(K) = 0$).
MILNOR(f)

Input: $f \in K[x_1, \dots, x_n]$

Output: $\mu(f)$

- compute a standard basis $\{g_1, \dots, g_s\}$ of $\langle f_{x_1}, \dots, f_{x_n} \rangle_{\text{Loc } K[x]}$ with respect to any *local monomial ordering* on $K[x]$;
- the number of monomials of $K[x]$ not in $\langle \text{lm}(g_1), \dots, \text{lm}(g_s) \rangle$ is equal to $\mu(f)$;

The correctness of this algorithm follows from [GP, 3.7].

Similarly, we can compute the **Tjurina number** ($\text{char}(K) \geq 0$)

$$\tau(f) = \dim_K K\langle x \rangle / \langle f, f_{x_1}, \dots, f_{x_n} \rangle.$$

This number plays an important role in the deformation theory of the singularity defined by f and will be considered in the next section.

There is an interesting conjecture, due to Zariski, stating that the multiplicity of a complex hypersurface singularity is a topological invariant. This conjecture is still open. For a formulation, using the Milnor number, and for a partial positive answer (which was prompted by computer experiments using SINGULAR with local standard bases) see [GP].

3.3 Deformations

Let $(V, 0) \subset (\mathbb{C}^n, 0)$ be a singularity given by convergent power series f_1, \dots, f_k , converging in a neighbourhood U of $0 \in \mathbb{C}^n$. The idea of deformation theory is to perturb the defining functions, that is to consider functions $F_1(t, x), \dots, F_k(t, x)$ with $F_i(0, x) = f_i(x)$, where t are small parameters of a parameter space S . For $t \in S$ the functions $f_{i,t}(x) = F_i(t, x)$ define a complex analytic set

$$V_t = V(f_{1,t}, \dots, f_{k,t}) \subset U$$

which, for t close to 0, may be considered to be a small deformation of $V = V_0$. It may be hoped that V_t is simpler than V_0 but still contains enough information about V . For this hope to be fulfilled, it is, however, necessary to restrict the possible perturbations of the equations to flat perturbations, which are called deformations.

The formal definition is as follows: a **deformation** of the singularity $(V, 0)$ over a complex analytic germ $(S, 0)$ consists of a cartesian diagram

$$\begin{array}{ccc} (V, 0) & \xrightarrow{i} & (\mathcal{U}, 0) = \{(t, x) \in S \times U \mid F_1(t, x) = \dots = F_k(t, x) = 0\} \\ \downarrow & & \downarrow \phi \\ \{0\} & \in & (S, 0) \end{array}$$

such that ϕ , which is the restriction of the second projection, is flat, that is, $\mathcal{O}_{\mathcal{U},0}$ is, via ϕ^* , a flat $\mathcal{O}_{S,0}$ -module.

Grothendieck's criterion of flatness states that ϕ is **flat** if and only if any relation between the f_i , say $\sum r_i(x)f_i(x) = 0$, lifts to a relation $\sum R_i(t,x)F_i(t,x) = 0$, where $R_i(x,0) = r_i(x)$, between the F_i . Equivalently, for any generator (r_1, \dots, r_k) of $\text{syz}(\langle f_1, \dots, f_k \rangle)$ there exists an element $(R_1, \dots, R_k) \in \text{syz}(\langle F_1, \dots, F_k \rangle)$ satisfying $R_i(0,x) = r_i(x)$.

The notion of flatness is not easy to explain geometrically. It has, however, important geometric consequences. For example, the fibres of a flat morphism have all the same dimension. Topologists would call a flat morphism perhaps transversal. In any case, the intuitive meaning is that the fibres of a flat morphism vary in some sense continuously with the parameter.

By a theorem of Grauert [Gr] (see also Schlessinger [Sch1] for the formal case), every isolated singularity admits a semi-universal or mini-versal deformation $\phi : (\mathcal{U}, 0) \rightarrow (S, 0)$ of $(V, 0)$, which, in some sense, contains the information upon all possible deformations.

By a power series Ansatz it is possible to compute the mini-versal deformation up to a given order. In general, the algorithm will, however, not stop. The existence of such an algorithm follows from the work of Laudal [La]. This algorithm has been implemented in SINGULAR by Martin.

We are not going to describe this algorithm here but just mention that for an isolated hypersurface singularity $f(x_1, \dots, x_n)$ the semi-universal deformation is given by

$$F(t, x) = f(x) + \sum_{j=1}^{\tau} t_j g_j(x),$$

where $1 = g_1, g_2, \dots, g_{\tau}$ represent a basis of the Tjurina algebra

$$K\langle x \rangle / \langle f, f_{x_1}, \dots, f_{x_n} \rangle,$$

τ being the Tjurina number.

Instead we describe algorithms to compute the modules $T_{V,0}^1$ respectively $T_{V,0}^2$ of first order deformations of $(V, 0)$ respectively of obstructions, which are the first objects one likes to know about the semi-universal deformation.

We switch now to an algebraic setting where deformations are described on the algebra level.

Since the infinitesimal deformation theory of an affine algebra and an analytic algebra is pretty much the same (cf. [Ar]), we use from now on the same notation $K\langle x_1, \dots, x_n \rangle$ for the polynomial ring over the field K as well as for power series ring over K .

Let $I = \langle f_1, \dots, f_k \rangle \subset K\langle x \rangle = K\langle x_1, \dots, x_n \rangle$ be an ideal and let $R = K\langle x \rangle / I$.

An **embedded deformation of \mathbf{R}** over an analytic algebra $A = K\langle t \rangle / J = K\langle t_1, \dots, t_m \rangle / J$ is given by

$$F_i(t, x) = f_i(x) + \sum_{j=1}^m t_j g_j^i(t, x) \in A\langle x \rangle$$

satisfying that every relation (syzygy) between the f_i ,

$$(r_1, \dots, r_k) \in K\langle x \rangle^k, \quad \sum_{i=1}^k r_i(x) f_i(x) = 0,$$

lifts to a relation between the F_i ,

$$(R_1, \dots, R_k) \in A\langle x \rangle^k, \quad \sum R_i(t, x) F_i(t, x) = 0,$$

$$R_i(0, x) = r_i(x).$$

By definition, F_1, \dots, F_k and F'_1, \dots, F'_k define the same embedded deformation, if they generate the same ideal.

Setting

$$R_A = A\langle x \rangle / \langle F_1, \dots, F_k \rangle$$

we obtain a commutative cartesian diagram

$$\begin{array}{ccc} R & \leftarrow & R_A \\ \uparrow & & \uparrow \varphi \\ K & \leftarrow & A \end{array}$$

with φ flat, which is called a **deformation of \mathbf{R} over \mathbf{A}** (and which is just the algebraic translation of the geometric definition). Two deformations $A \rightarrow R_A$ and $A \rightarrow R'_A$ of R over A are called **isomorphic** if there is an A -isomorphism $R_A \cong R'_A$ compatible with the given isomorphisms to the “special fibre”,

$$R_A / \langle t \rangle \cong R \cong R'_A / \langle t \rangle,$$

where $\langle t \rangle = \langle t_1, \dots, t_m \rangle$. It is not difficult to see that every deformation of R is isomorphic to an embedded deformation.

We like to stress the fact that the base algebras A for deformations have to be local analytic K -algebras with $K \xrightarrow{\cong} A/\mathfrak{m}$, \mathfrak{m} the maximal ideal of A , even if R is affine.

Infinitesimal deformations

Let $K[\varepsilon] = K\langle \varepsilon \rangle / \langle \varepsilon^2 \rangle$ denote the two-dimensional analytic algebra $K + K\varepsilon$, $\varepsilon^2 = 0$ (the space $\text{Spec}(K[\varepsilon])$ may be considered as a “thick” point, that is, a point together with a tangent direction). An (embedded) deformation of R over $K[\varepsilon]$ is called an **infinitesimal (embedded) deformation**.

Proposition 3.2.

- 1) The R -module of infinitesimal embedded deformations is isomorphic to the normal module

$$N_R = \text{Hom}_R(I/I^2, R).$$

- 2) The R -module of isomorphism classes of infinitesimal deformations of R is isomorphic to T_R^1 , where \mathbf{T}_R^1 is defined by the exact sequence

$$\Theta \otimes_{K\langle x \rangle} R \xrightarrow{\alpha} N_R \longrightarrow T_R^1 \longrightarrow 0.$$

Here, $\Theta = \text{Der}_K K\langle x \rangle = \bigoplus_{i=1}^n K\langle x \rangle \frac{\partial}{\partial x_i}$ and the map α sends the derivation $\frac{\partial}{\partial x_i}$ to the homomorphism sending h to $\frac{\partial h}{\partial x_i}$.

For the proof we refer to [Schl2].

Remarks:

- 1) Schlessinger's theorem [Schl1] states that R admits a formal semi-universal deformation $B \longrightarrow R_B = B\langle x \rangle / \langle F_1, \dots, F_k \rangle$ over a complete local K -algebra B if and only if $\dim_K T_R^1 < \infty$.

This assumption is fulfilled in the affine case $R = K[x_1, \dots, x_n]/I$ if the affine variety $V(I)$ has only isolated singularities (necessarily finitely many) or in the analytic case $R = K\langle x_1, \dots, x_n \rangle / I$ if the singularity $(V(I), 0)$ has an isolated singularity.

- 2) In the complex analytic case with $R = \mathbb{C}\{x_1, \dots, x_n\}/I$ and $\dim_{\mathbb{C}} T_R^1 < \infty$, R admits even a convergent complex analytic semi-universal deformation with base algebra $B = \mathbb{C}\{t_1, \dots, t_m\}/J$ and total algebra $R_B = \mathbb{C}\{t_1, \dots, t_m, x_1, \dots, x_n\}/\langle F_1, \dots, F_k \rangle$.

The proof of the convergence is quite difficult and was given by Grauert in 1972 [Gr] and it was in this paper that he proved the "division theorem by an ideal". In our language, he introduced the notion of standard bases and proved the existence of normal forms for complex analytic convergent power series. An equivalent theorem had already been proved before in 1964 by Hironaka in his famous resolution paper ([Hi]). It is interesting to notice that the analog of Gröbner bases in power series rings was invented for proving deep theoretical results. The proofs were, however, not constructive and did not contain Buchberger's criterion.

- 3) It follows from Grothendieck's definition of tangent spaces that, if a semi-universal deformation $B \longrightarrow R_B$ of R exists, then T_R^1 is isomorphic to the Zariski tangent space to $\text{Spec } B$ at the maximal ideal of B .

This shows, with t_1, \dots, t_m a K -basis of T_R^{1*} , that $B \cong K\langle T_R^1 \rangle / J \cong K\langle t_1, \dots, t_m \rangle / J$ for some ideal of J . Hence, the base algebra B of the semi-universal deformation of R is defined by analytic relations between the elements t_1, \dots, t_m of a K -basis of the dual of T_R^1 and these relations generate J .

To compute T_R^1 , let $0 \leftarrow R \leftarrow K\langle x \rangle \leftarrow K\langle x \rangle^k \xleftarrow{r} K\langle x \rangle^\ell$ be a representation of R , then, applying $\text{Hom}_{K\langle x \rangle}(-, R)$ to the sequence

$$0 \leftarrow R \leftarrow K\langle x \rangle \leftarrow K\langle x \rangle^k \xleftarrow{r} K\langle x \rangle^\ell,$$

we obtain $N_R = \ker(R^k \xrightarrow{r^t} R^\ell)$.

Now choose a resolution of N_R

$$\begin{array}{ccccc} R^k & \xleftarrow{s_1} & R^s & \xleftarrow{s_2} & R^t \\ \Downarrow & & \searrow & & \\ & & N_R & & \end{array}$$

The canonical map $\pi : R^n \simeq \Theta_{K\langle x \rangle} \otimes R \longrightarrow N_R$ is induced by the map $j : R^n \longrightarrow R^k$ defined by the Jacobian matrix $\left(\frac{\partial f_i}{\partial x_j} \right)_{\substack{i \leq k \\ j \leq n}}$. We can lift j to a map $lj : R^n \longrightarrow R^s$ such that $s_1 \circ lj = j$ because j induces the map π .

$$\begin{array}{ccccccc} R^l & \xleftarrow{r^t} & R^k & \xleftarrow{s_1} & R^s & \xleftarrow{s_2} & R^t \\ & & \uparrow & \swarrow & \nearrow & & \\ & & N_R & & & & \\ & & \uparrow \pi & & \nearrow lj & & \\ & & R^n & & & & \end{array}$$

Now $T_R^1 = N_R / \text{Im}(\pi) \simeq R^s / \text{Im}(s_2) + \text{Im}(lj)$ gives the required representation

$$0 \leftarrow T_R^1 \leftarrow R^s \xleftarrow{s_2 \oplus lj} R^t \oplus R^n.$$

Algorithm 3.4.
T1(I)

Input: an ideal $I = \langle f_1, \dots, f_k \rangle \subseteq K\langle x \rangle$,

Output: a matrix $M \in M_{a,b}(K\langle x \rangle)$ which defines a representation

$$T_{K\langle x \rangle / I}^1 \leftarrow K\langle x \rangle^a \xleftarrow{M} K\langle x \rangle^b$$

- compute $r = \text{syz}(I)$ the matrix of the syzygies of f_1, \dots, f_k ;
- compute the Jacobian matrix $j = \left(\frac{\partial f_i}{\partial x_j} \right)$;
- compute in $K\langle x \rangle/I$ a representation of the kernel of the transposed matrix r^t of r :

$$(K\langle x \rangle/I)^k \xleftarrow{s_1} (K\langle x \rangle/I)^s \xleftarrow{s_2} (K\langle x \rangle/I)^t;$$

- lift the Jacobian matrix j to a $s \times n$ -matrix lj such that $s_1 \cdot lj = j$;
- concatenate lj and s_2 to obtain the matrix $t1 = lj, s_2$;
- choose a matrix $M_0 \in M_{s, n+t}(K\langle x \rangle)$ such that $M_0 \bmod I = t1$;
- choose a matrix $L \in M_{s, k \cdot s}$ (corresponding to $IK\langle x \rangle^s$), such that

$$0 \leftarrow (K\langle x \rangle/I)^s \leftarrow K\langle x \rangle^s \xleftarrow{L} K\langle x \rangle^{k \cdot s}$$

is exact;

- concatenate M_0 and L to obtain $M = M_0, L$;
- return M

Obstructions

The construction of a semi-universal deformation of R , in case T_R^1 is finite dimensional, starts with the preceding remark 3): we start with the infinitesimal deformations of first order, that is, with elements of T_R^1 , and try to lift these to second order. This is not always possible, there are obstructions against lifting. That is, a lifting to second order is possible if and only if the corresponding obstruction is zero. Assuming that the obstruction is zero, we choose a lifting to second order (which is not unique) and try to lift this to third order. Again there are obstructions, but if these are zero, the lifting is possible and we can continue. In any case, the obstructions yield formal power series in $K[[t_1, \dots, f_n]]$, t_1, \dots, t_n a K -basis of T_R^{1*} , and if J denotes the ideal generated by them, $B = K[[t_1, \dots, t_m]]/J$ will be the base algebra of the formal semi-universal deformation of R .

The following proposition describes the module of obstructions to lift a deformation from an Artinian algebra to an infinitesimally bigger one, where we may think of starting with $A = K\langle t_1, \dots, t_n \rangle / \langle t_1, \dots, t_n \rangle^2$.

For this, let $R = K\langle x \rangle/I$ and consider a presentation of $I = \langle f_1, \dots, f_k \rangle$,

$$0 \leftarrow I \xleftarrow{\alpha} K\langle x \rangle^k \xleftarrow{\beta} K\langle x \rangle^\ell$$

with $\alpha(e_i) = f_i$ and $\text{syz}(I) = \ker(\alpha) = \text{im}(\beta)$ is the module of relations of f_1, \dots, f_k , which contains the module of **Koszul relations**,

$$\text{Kos} = \langle f_i e_j - f_j e_i \mid 1 \leq i < j \leq k \rangle.$$

Set $\text{Rel} = K\langle x \rangle^\ell / \ker(\beta)$ which is isomorphic to $\text{syz}(I)$ and $\text{Rel}_0 = \beta^{-1}(\text{Kos})$. We define the module \mathbf{T}_R^2 by the exact sequence

$$\text{Hom}_R(R^k, R) \xrightarrow{\beta^*} \text{Hom}_R(\text{Rel} / \text{Rel}_0, R) \longrightarrow T_R^2 \longrightarrow 0.$$

Proposition 3.3.

1) Let $A' \twoheadrightarrow A$ be a surjection of Artinian local K -algebras with kernel an ideal J satisfying $J^2 = 0$. There is an obstruction map

$$\text{ob}: \text{Def}_R(A) \longrightarrow T_R^2 \otimes_K J$$

satisfying: a deformation $A \twoheadrightarrow R_A$ of R admits a lifting $A' \twoheadrightarrow R_{A'}$,

$$\begin{array}{ccc} R_A & \leftarrow & R_{A'} \\ \uparrow & \square & \uparrow \\ A & \leftarrow & A', \end{array}$$

if and only if $\text{ob}([A \twoheadrightarrow R_A]) = 0$ ($[A \twoheadrightarrow R_A]$ denotes the deformation class of $A \twoheadrightarrow R_A$).

2) If T_R^1 is finite dimensional over K and if $T_R^2 = 0$, then the semi-universal deformation $B \twoheadrightarrow R_B$ of R has a smooth base space, that is B is a free analytic algebra $K\langle t_1, \dots, t_m \rangle$ for some $m \geq 0$.

For the computation of T_R^2 we choose, as before, a representation

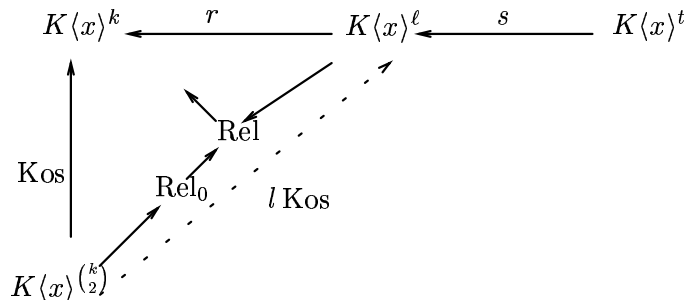
$$0 \longleftarrow R \longleftarrow K\langle x \rangle \xleftarrow{r} K\langle x \rangle^k \xleftarrow{s} K\langle x \rangle^\ell \xleftarrow{t} K\langle x \rangle^t.$$

Then $\text{Rel} = \text{syz}(I) = \text{Im}(r)$ and Rel_0 is the submodule of Rel generated by the $\binom{k}{2}$ Koszul relations Kos .

Now $\text{Rel} / \text{Rel}_0 \twoheadrightarrow R^k$ is the induced map defined by the following diagram

$$\begin{array}{ccccc} IK\langle x \rangle^k & \hookrightarrow & K\langle x \rangle^k & \longrightarrow & R^k \\ \cup \downarrow & & \cup \downarrow & & \uparrow \\ \text{Rel}_0 & \hookrightarrow & \text{Rel} & \longrightarrow & \text{Rel} / \text{Rel}_0. \end{array}$$

To obtain a representation of $\text{Rel} / \text{Rel}_0$ we lift the Koszul relations to $K\langle x \rangle^\ell$:



Then $\text{Rel} / \text{Rel}_0 \simeq K\langle x \rangle^\ell / \text{Im}(s) + \text{Im}(\ell \text{Kos})$ and if we denote by $s\ell$ the $\ell \times (t + \binom{k}{2})$ -matrix s , ℓKos :

$$0 \longleftarrow \text{Rel} / \text{Rel}_0 \longleftarrow K\langle x \rangle^\ell \xleftarrow{s\ell} K\langle x \rangle^{t_1}, \quad t_1 = t + \binom{k}{2},$$

is a representation of $\text{Rel} / \text{Rel}_0$.

Now we are interested in a representation of T_R^2 which is just

$$\text{coker}(\text{Hom}_R(R^k, R) \longrightarrow \text{Hom}_R(\text{Rel} / \text{Rel}_0, R)).$$

We dualize the representation of $\text{Rel} / \text{Rel}_0$ and obtain

$$\begin{array}{ccccc} 0 \rightarrow \text{Hom}_{K\langle x \rangle}(\text{Rel} / \text{Rel}_0, R) & \rightarrow & \text{Hom}_{K\langle x \rangle}(K\langle x \rangle^\ell, R) & \xrightarrow{s\ell^t} & \text{Hom}_{K\langle x \rangle}(K\langle x \rangle^{t_1}, R) \\ & & \parallel & & \parallel \\ & & \text{Hom}_R(\text{Rel} / \text{Rel}_0, R) & & \text{Hom}_R(R^\ell, R) & & \text{Hom}_R(R^{t_1}, R), \end{array}$$

that is, $\text{Hom}_R(\text{Rel} / \text{Rel}_0, R) = \ker(s\ell^t)$.

Now we take a representation of $\text{Hom}_R(\text{Rel} / \text{Rel}_0, R)$

$$\begin{array}{ccccc} R^{t_1} & \xleftarrow{s\ell^t} & R^\ell & & \xleftarrow{r_1} & R^{\ell_1} & \xleftarrow{r_2} & R^{\ell_2} \\ & & \cup & & & \swarrow & & \\ & & \text{Hom}_R(\text{Rel} / \text{Rel}_0, R) & & & & & \end{array}$$

The map $R^k \simeq \text{Hom}_R(R^k, R) \longrightarrow \text{Hom}_R(\text{Rel} / \text{Rel}_0, R)$ is defined by $r^t : R^k \longrightarrow R^\ell$. We can lift this map to a map $\ell r t : R^k \longrightarrow R^{\ell_1}$ such that $r_1 \circ \ell r t = r^t$.

$$\begin{array}{ccccc} R^\ell & \xleftarrow{r_1} & R^{\ell_1} & \xleftarrow{r_2} & R^{\ell_2} \\ & \swarrow & \uparrow & \searrow & \\ & r^t & \text{Hom}(\text{Rel} / \text{Rel}_0, R) & \ell r t & \\ & \swarrow & \uparrow & \searrow & \\ & & R^k & & \end{array}$$

Then $T_R^2 = \text{coker}(R^k \longrightarrow \text{Hom}(\text{Rel} / \text{Rel}_0, R)) \simeq R^{\ell_1} / \text{Im}(r_2) + \text{Im}(\ell r t)$ gives the required representation

$$0 \longleftarrow T_R^2 \longleftarrow R^{\ell_1} \xleftarrow{r_2 \oplus \ell r t} R^{\ell_2} \oplus R^k.$$

We obtain the following algorithm:

Algorithm 3.5.

$T_2(I)$

Input: an ideal $I = \langle f_1, \dots, f_k \rangle \subseteq K\langle x \rangle$

Output: a matrix $M \in M_{a,b}(K\langle x \rangle)$ which defines a representation

$$T_{K\langle x \rangle / I}^2 \longleftarrow K\langle x \rangle^a \xrightarrow{M} K\langle x \rangle^b$$

- compute $r = \text{syz}(I) \in M_{k,\ell}(K\langle x \rangle)$, the matrix of the syzygies of f_1, \dots, f_k and $s = \text{syz}(\text{syz}(I)) \in M_{\ell,t}(K\langle x \rangle)$ to obtain a representation of $K\langle x \rangle/I$;
- compute the matrix $\text{Kos} \in M_{k,\binom{k}{2}}$, the Koszul matrix of the relations of f_1, \dots, f_k ;
- lift Kos to a matrix $\ell \text{Kos} \in M_{\ell,\binom{k}{2}}$ such that $r \cdot \ell \text{Kos} = \text{Kos}$;
- concatenate ℓKos and s to obtain the matrix $s\ell = \ell \text{Kos}$, $s \in M_{\ell,\binom{k}{2}+t}$;
- compute in $K\langle x \rangle/I$ a representation of the kernel $\ker(s\ell^t)$ given by matrices r_1 and r_2 ($r_1 = \text{syz}(s\ell^t) \in M_{\ell,\ell_1}(K\langle x \rangle/I)$, $r_2 = \text{syz}(r_1) \in M_{\ell_1,\ell_2}(K\langle x \rangle/I)$);
- lift the matrix r_2 to a matrix $\ell r_2 \in M_{\ell_1,k}(K\langle x \rangle/I)$ such that $r_1 \cdot \ell r_2 = r_2$;
- concatenate ℓr_2 and r_1 to obtain $t_2 = \ell r_2$, $r_1 \in M_{\ell_1,k+\ell_2}(K\langle x \rangle/I)$;
- choose a matrix $M_0 \in M_{\ell_1,k+\ell_2}(K\langle x \rangle)$ such that $M_0 \bmod I = t_2$;
- choose a matrix $L \in M_{\ell_1,k \cdot \ell_1}$ (corresponding to $IK\langle x \rangle^{\ell_1}$) such that

$$0 \leftarrow (K\langle x \rangle/I)^{\ell_1} \leftarrow K\langle x \rangle^{\ell_1} \xleftarrow{L} K\langle x \rangle^{k \cdot \ell_1}$$

is exact;

- concatenate M_0 and L to obtain $M = M_0, L$;
- return M .

References

- [Ar] Artin, M.: Lectures on deformations of singularities. Tata Institute, Bombay (1976).
- [Bu1] Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD Thesis, University of Innsbruck, Austria (1965).
- [Bu2] Buchberger, B.: Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. In: Aequ. Math. **4**, 374-383 (1970).
- [Bu3] Buchberger, B.: Gröbner bases: an algorithmic method in polynomial ideal theory. In: Recent trends in multidimensional system theory, N.B. Bose, ed., Reidel (1985).

- [Bu4] Buchberger, B.: Introduction to Gröbner bases. This volume.
- [BWe] Becker, T.; Weispfennig, V.: Gröbner Bases, A Computational Approach to commutative Algebra. Graduate Texts in Mathematics 141, Springer 1993.
- [CLO] Cox, D.; Little, J.; O’Shea, D.: Ideals, Varieties and Algorithms. Springer Verlag (1992).
- [CNR] Capani, A.; Niesi, G.; Robbiano, L.: Some Features of CoCoA 3. Moldova Journal of Computer Science. To appear.
- [Ei] Eisenbud, D: Commutative Algebra with a view toward Algebraic Geometry. Springer 1995.
- [ERS] Eisenbud, D.; Riemenschneider, O.; Schreyer, F.-O.: Resolutions of Cohen-Macaulay Algebras. Math Ann. **257** (1981).
- [Getal] Grassmann, H.; Greuel, G.-M.; Martin, B.; Neumann, W.; Pfister, G.; Pohl, W.; Schönemann, H.; Siebert, T.: Standard bases, syzygies and their implementation in SINGULAR. In: Beiträge zur angewandten Analysis und Informatik, Shaker, Aachen, 69-96, 1994.
- [GP] Greuel, G.-M.; Pfister, G.: Advances and improvements in the theory of standard bases and syzygies. Arch. Math. **66**, 163–1796 (1996).
- [GPS] Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR Reference Manual, Reports On Computer Algebra Number 12, May 1997, Centre for Computer Algebra, University of Kaiserslautern from www.mathematik.uni-kl.de/zca/Singular.
- [GR] Grauert, H.; Remmert, R.: Analytische Stellenalgebren. Springer 1971.
- [Gr] Grauert, H.: Über die Deformation isolierter Singularitäten analytischer Mengen. Invent. Math. **15**, 171–198 (1972).
- [Gra] Gräbe, H.-G.: The tangent cone algorithm and homogeneization. J. Pure Appl. Alg. 97, 303–312 (1994).
- [GS] Grayson, D.; Stillmann, M.: A computer software system designed to support research in commutative algebra and algebraic geometry. Available from math.uiuc.edu.
- [GT] Gianni, P.; Trager, B.: Integral closure of noetherian rings. Preprint, to appear.

- [Hi] Hironaka, H.: Resolution of singularities of an algebraic variety over a field of characteristic zero. *Ann. of Math.* **79**, 109–326 (1994).
- [J] de Jong, T.: An algorithm for computing the integral closure. Preprint, Saarland University, Saarbrücken.
- [Ku] Kunz, E.: Einführung in die kommutative Algebra und algebraische Geometrie. Vieweg (1980).
- [La] Laudal, O.A.: Formal Moduli of Algebraic Structures. LNM **754**, Springer (1979).
- [Mil] Milnor, J.: Singular Points of Complex Hypersurfaces. *Ann. of Math. Studies* 61, Princeton (1968).
- [Mo] Mora, T.: An algorithm to compute the equations of tangent cones. *Proc. EUROCAM 82, Lecture Notes in Comput. Sci.* (1982).
- [MM] Möller, H.M.; Mora, T.: Computational aspects of reduction strategies to construct resolutions of monomial ideals. *Proc. AAEECC 2, Lecture Notes in Comput. Sci.* **228** (1986).
- [MPT] Mora, T.; Pfister, G.; Traverso, C.: An introduction to the tangent cone algorithm. In: *Issues in non-linear geometry and robotics*, JAI Press (1992).
- [Sch1] Schreyer, F.-O.: Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrass'schen Divisionssatz. Diplomarbeit, Hamburg (1980).
- [Sch2] Schreyer, F.-O.: A standard basis approach to syzygies of canonical curves. *J. reine angew. Math.* **421**, 83–123 (1991).
- [Sch3] Schreyer, F.-O.: Syzygies of canonical curves and special linear series. *Math. Ann.* **275** (1986).
- [Schl1] Schlessinger, M.: Functors of Artin rings. *Trans. AMS* **130**, 208–222, (1968).
- [Schl2] Schlessinger, M.: On rigid singularities. *Rice. Univ. Stud.* **59**, 147–162 (1973).
- [St] Sturmfels, B.: *Algorithms in Invariant Theory*. Springer Verlag (1993).
- [V] Vasconcelos, W.: Computing the integral closure of an affine domain. *Proc. AMS* **113** (3), 633–638 (1991).