Algorithmic Ideal Theory

Gert-Martin Greuel
Universität Kaiserslautern
Fachbereich Mathematik

Gerhard Pfister
Universität Kaiserslautern
Fachbereich Mathematik

DMV–Seminar (Oktober 1997)

Contents

Preface **2**

0 Introduction by simple questions **3**

1 Standard bases **10**

1.1 Monomial orderings and associated rings 10

1.2 Standard bases and normal forms 15

1.3 Syzygies and free resolutions 25

2 Primary decomposition **31**

2.1 The theory 31

2.2 The algorithms 35

2.2.1 Computation of the radical 37

2.2.2 Computation of the equidimensional part of an ideal 40

2.2.3 Zerodimensional primary decomposition 43

2.2.4 Higher dimensional primary decomposition 47

2.2.5 The normalization 51

3 Applications to Singularity Theory **55**

3.1 Basic concepts and invariants 55

3.2 Deformations 59

References **72**

Preface

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. Non–trivial mathematical problems usually lead to non–trivial Gröbner basis computations, which is the reason why several improvements and efficient implementations have been provided by algebraic geometers (for example, the systems 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.

In the third chapter several algorithms for primary decomposition of polynomial ideals are presented, together with a discussion of improvements and preferable choices. We also describe a newly invented algorithm for computing the normalization of a reduced affine ring.

The last chapter gives an elementary introduction to singularity theory and then describes 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 basis 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 a few references to papers which contain interesting applications and which are not 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.

0 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?"

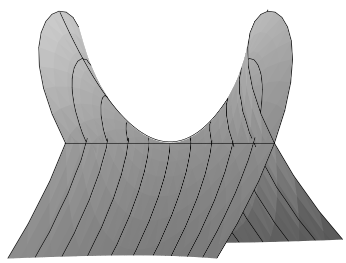
That is, we try to understand the set of points $x = (x_1, \ldots, x_n) \in K^n$ satisfying

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

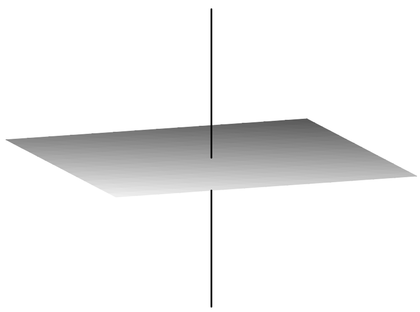
where K is a field and $f_1, \ldots, f_k$ are elements of the polynomial ring $K[x] = K[x_1, \ldots, x_n]$. The solution set of $f_1, \ldots, f_k$ is called the algebraic set, or algebraic variety of $f_1, \ldots, f_k$ and is denoted by $V(f_1, \ldots, f_k)$.

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

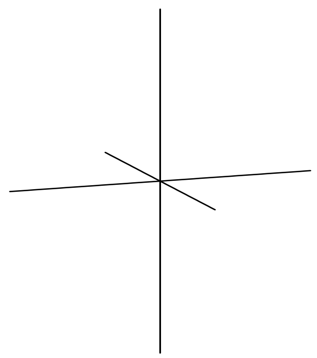
1) The hypersurface (a variety defined by one equation) $V(x^2 + y^3 - t^2y^2)$:



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, 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, one can see this already in recent textbooks (for example, [CLO], [St], [V3]).

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 $V = V(f_1, \ldots, f_k)$ and V is equal to the solutions of all $f \in I = \langle f_1, \ldots, f_k \rangle_{K[x]}$, the ideal generated by $f_1, \ldots, f_k$ 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. Fortunately, Gröbner basis theory is completely independent of the field, although the result of a computation may very well depend on the field.

From the geometric point of view, the field K is, however, extremely important. Algebraic geometry over $\mathbb{R}$, for instance, is is much more complicated and by far not as complete as over $\mathbb{C}$. To avoid such "rationality questions", we should like to change our definition of variety slightly and define

$$V(f_1, \ldots, f_k) = \{x \in \overline{K}^n | f_1(x) = \cdots = f_k(x) = 0\}$$

for $f_1, \ldots, f_k \in K[x]$, $x = (x_1, \ldots, x_n)$, and where $\overline{K}$ is an algebraic closure of the field K.

The following **questions and problems** 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).

- *What is the dimension of the variety $V(I)$, or, what is the Krull dimension of the quotient ring $K[x]/I$?*

  Following tradition in computer algebra, we denote this dimension by $\dim(I)$ and call it the dimension of I. The dimension of a variety is the maximum dimension of its components.

  In the first two examples, the dimension is 2, in the third example it is 1.

- *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).

- *Instead of decomposing a variety, we may wish to compute equations for the union $V(I_1) \cup V(I_2)$. Algebraically this means to find generators for the intersection $I_1 \cap I_2$.*

In example 3, for instance, we have given the generators xy, xz, yz for the intersection $\langle x, y\rangle \cap \langle y, z\rangle \cap \langle x, z\rangle$.

- *A simpler problem is to decide whether a given polynomial f vanishes on $V(I)$, or, algebraically, whether f is in $\sqrt{I}$. Even simpler is the question whether f is an element of I.*

- *Given generators for an ideal I, we may ask for another set of polynomials describing the same variety $V(I)$. For instance, we may ask for a minimal set of generators of I or, more complicatedly, for a set of generators for $\sqrt{I}$, the radical of I.*

  In the above examples, $I = \sqrt{I}$, and the given set of generators is minimal.

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

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

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

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

- *More generally, we may ask for generators of the kernel of a $K[x]$–linear map $K[x]^r \to K[x]^s$, 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 $\operatorname{syz}(I) = 0$, in example 2, $\operatorname{syz}(I) = \langle(-y, x)\rangle \subset K[x]^2$ and in example 3, $\operatorname{syz}(I) = \langle(-z, y - 0),\ (-z, 0, x)\rangle \subset K[x]^3$.

- *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*

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

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

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

  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 $K^m \to K^n$ inducing the normalization map $V(J) \to V(I)$.

  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 $K[x_1, \ldots, x_n]/I$, 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 $K[x_1, \ldots, x_m]/J$ 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 $V(I)$, $I = (f_1, \ldots, f_k)$, 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*

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

  In this local ring the polynomials g with $g(0) \neq 0$ are units and $K[x]$ is a sub-ring 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 bases 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 semi-group 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.

1 Standard bases

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

1.1 Monomial orderings and associated rings

Definition 1.1. A **monomial ordering** on $K[x]$ is a total order on the set of monomials $\{x^\alpha | \alpha \in \mathbb{N}^n\}$ 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 $>$ **global** (respectively **local**, respectively **mixed**) 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.

We often identify the set of monomials with $\mathbb{N}^n$ and write $\alpha > \beta$ if $x^\alpha > x^\beta$. By [Ro] there exists a (non–unique) matrix $A \in GL(n, \mathbb{R})$ such that $\alpha > \beta$ if and only if $A \cdot \alpha$ is bigger than $A \cdot \beta$ with respect to the lexicographical ordering on $\mathbb{R}^n$. We say then that $>$ is given by A.

Remark 1.1. On $\mathbb{N}^n$ we have the **natural partial ordering** $\geq_{\text{nat}}$ ($\alpha \geq_{\text{nat}} \beta$ iff $\alpha - \beta \in \mathbb{N}^n$, that is if $x^\beta | x^\alpha$).

The following are equivalent:

(i) $>$ is global,

(ii) if $>$ is given by a matrix A, then the first non–zero entry of each column of A is positive,

(iii) $>$ refines the natural partial ordering, that is

$$\alpha \geq_{\text{nat}} \beta, \alpha \neq \beta \Rightarrow x^\alpha > x^\beta,$$

(iv) $>$ is a well–ordering.

The implication (iii) $\Rightarrow$ (iv) follows from Dickson's lemma, saying that every subset of $\mathbb{N}^n$ has, at most, finitely many minimal elements with respect to $\geq_{\text{nat}}$.

Definition 1.2. Any $f \in K[x] \smallsetminus \{0\}$ can be written uniquely as

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

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

$\mathrm{lm}(f)$	$= x^\alpha$,	the **leading monomial** of f,
$\mathrm{lc}(f)$	$= c$,	the **leading coefficient** of f.
$\exp(f)$	$= \alpha$,	the **leading exponent** of f.

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

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

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

In the following examples, we define important orderings and accompany this with a polynomial f written as a sum of monomials in decreasing order (hence, the leading monomial is first) and a matrix A describing the ordering for three variables.

Example 1.1.
Typical global orderings are the **lexicographical ordering lp** ($x^\alpha >_{\mathrm{lp}} x^\beta :\Leftrightarrow$ the first non–zero entry of $\alpha - \beta$ is positive) and the

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$f = x^4 + x^3z + x^2y^2 + yz^4 + z^5$, $\exp(f) = (4,0,0)$. **degree reverse lexicographical ordering dp** ($x^\alpha >_{\mathrm{dp}} x^\beta :\Leftrightarrow \deg x^\alpha > \deg x^\beta$ or $\deg x^\alpha = \deg x^\beta$ and the last non–zero entry of $\alpha - \beta$ is negative), typical local orderings are the

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix},$$

$f = yz^4 + z^5 + x^4 + x^2y^2 + x^3z$, $\exp(f) = (0,1,4)$. **negative lexicographical ordering ls** ($x^\alpha >_{\mathrm{ls}} x^\beta :\Leftrightarrow$ the first non–zero entry of $\alpha - \beta$ is negative) and the

$$A = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$f = z^5 + yz^4 + x^2y^2 + x^3z + x^4$, $\exp(f) = (0,0,5)$. **negative degree reverse lexicographical ordering ds** ($x^\alpha >_{\mathrm{ds}} x^\beta :\Leftrightarrow \deg x^\alpha < \deg x^\beta$ 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

$$A = \begin{pmatrix} -1 & -1 & -1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$$

$f = x^4 + x^2y^2 + x^3z + yz^4 + z^5$, $\exp(f) = (4,0,0)$.

p refers to a polynomial ring and the s to a series ring (cf. Definition 1.3).

In the above examples lp and dp are global, while ls and ds are local (the p refers to a polynomial ring and s to a series ring, cf. Definition 1.1).

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.

For any n–tuple of real numbers $w = (w_1, \ldots, w_n)$ we define the **weighted degree** of a monomial x^α to be

$$w\text{–}\deg x^\alpha = \langle w, \alpha \rangle = w_1\alpha_1 + \cdots + w_n\alpha_n.$$

Hence, for $w = (1, \ldots, 1)$, $w\text{–}\deg x^\alpha = \deg x^\alpha$.

Let $w_1, \ldots, w_n$ be strictly positive, then the **weighted degree reverse lexicographical ordering** $\mathbf{wp(w_1, \ldots, w_n)}$ (respectively the **negative weighted degree reverse lexicographical ordering** $\mathbf{ws(w_1, \ldots, w_n)}$) are defined as dp (respectively ds) but with deg replaced by w–deg.

$$A = \begin{pmatrix} w_1 & w_2 & w_3 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix} \text{ respectively } A = \begin{pmatrix} -w_1 & -w_2 & -w_3 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$$

wp$(5,3,4)$: $f = x^4 + z^5 + x^3z + yz^4 + x^2y^2$, $\exp(f) = (4,0,0)$,
ws$(5,5,4)$: $f = x^3z + x^4 + x^2y^2 + z^5 + yz^4$, $\exp(f) = (3,0,1)$.
wp is global and ws is local.

Given two monomial orderings $>_1$ on $K[x_1, \ldots, x_n]$ and $>_2$ on $K[y_1, \ldots, y_m]$, 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 $y^\beta >_2 y^\delta$.

$$A = \left(\begin{array}{c|c} A_1 & \\ \hline & A_2 \end{array}\right),$$

if $>_1$ is given by A_1 and $>_2$ by A_2.

(dp(1), ls(2)) : $x^4 + x^3z + x^2y^2 + z^5 + yz^4$, $\exp(f) = (4,0,0)$.
(ds(1), lp(2)) : $x^2y^2 + x^3z + x^4 + yz^4 + z^5$, $\exp(f) = (2,2,0)$.

Remark 1.2. The leading monomial function has the following basic property ($f, g \in K[x] \setminus \{0\}$):

$\mathrm{lm}(gf) = \mathrm{lm}(g)\,\mathrm{lm}(f)$,
$\mathrm{lm}(g+f) \le \max(\mathrm{lm}(f), \mathrm{lm}(g))$ with inequality
if and only if $\mathrm{lm}(g) = \mathrm{lm}(f)$ and $\mathrm{lc}(f) = -\mathrm{lc}(g)$.

This implies that

$$S_> = \{u \in K[x] \setminus \{0\} | \operatorname{lm}(u) = 1\}$$

is a multiplicatively closed subset of $K[x]$.

The localization of $K[x]$ with respect to $S_>$ plays an important role for local and mixed orderings.

Definition 1.3. For a given monomial ordering $>$ define the multiplicatively closed set

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

and the K–algebra

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

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

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

Remark 1.3. 1) $K[x] \subset \operatorname{Loc} K[x] \subset K[x]_{(x)}$ where $K[x]_{(x)}$ denotes the localization of $K[x]$ with respect to the maximal ideal $(x_1, \ldots, x_n)$. $\operatorname{Loc} K[x]$ is Noetherian, it is $K[x]$–flat and $K[x]_{(x)}$ is $\operatorname{Loc} K[x]$–flat.

2) $\operatorname{Loc} K[x] = K[x]$ if and only if $>$ is global and $\operatorname{Loc} K[x] = K[x]_{(x)}$ 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 $K[x, y] = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ with $>_1$ global on $K[x]$ and $>_2$ arbitrary on $K[y]$ is an **elimination ordering** for $x_1, \ldots, x_n$ on $K[x, y]$, that is, for $g \in K[x, y]$ and $\operatorname{lm}(g) \in K[y]$ we have $g \in K[y]$. It is easy to see that for an arbitrary monomial ordering $>$ to be an elimination ordering for $x_1, \ldots, x_r$ it is necessary that $x_i > 1$ for $i = 1, \ldots, r$. 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

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

4) The product ordering is not commutative, that is, if $>_1$ and $>_2$ are as in 1) and we define the product ordering $>= (>_2, >_1)$ on $K[y,x]$ by changing variables, then $S_> = K * +(y)K[y,x]$ and

$$\operatorname{Loc} K[x] = S_>^{-1} K[y,x] \supsetneqq (K[y]_{(y)})[x]$$

since $\frac{1}{1+xy}$, for instance, is in the first but not in the latter.

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

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

Since

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

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

$$L(G) = \langle \operatorname{lm}(g) | g \in G \smallsetminus \{0\}\rangle_{K[x]} \subset K[x]$$

and call it the **leading ideal** of G. Note also that $u \in \operatorname{Loc} K[x] \smallsetminus \{0\}$ is a unit in $\operatorname{Loc} K[x]$ if and only if $\operatorname{lm}(u) = 1$, 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 $K[x]^r = \sum\limits_{i=1,\dots,r} K[x]e_i$ 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 1.4. 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 $\{x^\alpha e_i | \alpha \in \mathbb{N}^n, i = 1, \dots, r\}$ satisfying

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

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

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

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

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

the **leading submodule** of G.

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

Note that the set of monomials of $K[x]^r$ may be identified with $\mathbb{N}^n \times E^r \subset \mathbb{N}^n \times \mathbb{N}^r = \mathbb{N}^{n+r}$, $E^r = \{e_1, \ldots, e_r\}$ and here e_i is considered as an element of $\mathbb{N}^r$. The natural partial order on $\mathbb{N}^{n+r}$ induces a partial order $\geq_{\mathrm{nat}}$ on the set of monomials, which is given by

$$\begin{aligned} x^\alpha e_i \leq_{\mathrm{nat}} x^\alpha e_j \quad &\Leftrightarrow \quad i = j \text{ and } x^\alpha | x^\beta \\ &\Leftrightarrow: \quad x^\alpha e_i | x^\beta e_j. \end{aligned}$$

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

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

Hence, Dickson's lemma for $\mathbb{N}^m$ (m arbitrary) is equivalent to the statement that any monomial submodule of $K[x]^r$ (r arbitrary) is finitely generated.

1.2 Standard bases and normal forms

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

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

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] celebrated algorithm, in the general case it is a variation of Mora's tangent cone algorithm [Mo], first published in [Getal], [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 1.5.

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 $f \in I \smallsetminus \{0\}$ there exists a $g \in G$ satisfying $\operatorname{lm}(g) | \operatorname{lm}(f)$.
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 **inter-reduced** if $0 \notin G$ and if $\operatorname{lm}(g) \notin L(G \smallsetminus \{g\})$.

Note that any standard basis can be made inter-reduced by deleting successively those g with $\operatorname{lm}(g) | \operatorname{lm}(h)$ for some $h \in G \smallsetminus \{g\}$. An inter-reduced 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 $\{u_g g | g \in G\}$.

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

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

Definition 1.6. Let $\mathcal{G}$ denote the set of all finite and ordered subsets $G \subset R^r$.

1) A map

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

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

(i) $\mathrm{NF}(f|G) \neq 0 \Rightarrow \mathrm{lm}\big(\mathrm{NF}(f|G)\big) \notin L(G)$,

(ii) $f - \mathrm{NF}(f|G) \in \langle G\rangle_R$.

NF is called a **reduced normal form** if, moreover, $\mathrm{NF}(f, G)$ 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 $uf - \mathrm{NF}(f|G) \in \langle G\rangle_R$.

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

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

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

Remark 1.4. 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.

$\mathrm{NF}(f|G)$ 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 1.1. *Let $I \subset R^r$ be a submodule, $G \subset I$ a standard basis of I and $\mathrm{NF}(-|G)$ a weak normal form on R^r with respect to G.*

1) For any $f \in R^r$ we have $f \in I \Leftrightarrow \mathrm{NF}(f|G) = 0$.

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 $\mathrm{NF}(-|G)$ is a reduced normal form, then it is unique.

Proof. 1) If $\mathrm{NF}(f|G) = 0$ then $uf \in I$ and, hence, $f \in I$. If $\mathrm{NF}(f|G) \neq 0$, then $\mathrm{lm}\big(\mathrm{NF}(f|G)\big) \notin L(G) = L(I)$, hence $\mathrm{NF}(f|G) \notin I$, which implies $f \notin I$.

2) Let $f \in J$ and assume $\mathrm{NF}(f|G) \neq 0$. Then $\mathrm{lm}\big(\mathrm{NF}(f|G)\big) \notin L[G] = L(I) = L(J)$, a contradiction since $\mathrm{NF}(f|G) \in J$. Hence, $f \in I$ by 1).

3) Follows from 2).

4) Let $f \in R^r$ and assume that h, h' are two reduced normal forms of f with respect to G. Then

$$h - h' \in \langle G \rangle_R = I.$$

If $h - h' \neq 0$, then $\mathrm{lm}(h - h') \in L(I) = L(G)$, a contradiction, since $\mathrm{lm}(h - h')$ is a monomial of either h or h'.

□

Remark 1.5. The above properties are well–known for Gröbner bases with $R = K[x]$. For local, or mixed, orderings it is quite important to work consequently with R instead of $K[x]$. We give an example showing that none of the above properties 1) – 3) hold for $K[x]$, if they make sense, that is, if the input data are polynomial.

Let $f_1 = x^{10} - y^2x^9$, $f_2 = y^8 - x^2y^7$, $f_3 = x^{10}y^7$ and consider $>_s$ on $K[x, y]$. Then $R = K[x, y]_{(x,y)}$, $(1 - xy)f_3 = y^7 f_1 + x^9 y f_2$ and we set

$$\begin{aligned} I &= (f_1, f_2)R = (f_1, f_2, f_3)R, \\ I' &= (f_1, f_2)K[x, y] \\ J' &= (f_1, f_2, f_3)K[x, y], \\ G &= \{f_1, f_2\}. \end{aligned}$$

Then G is a reduced standard basis of I (since we must multiply f_1 at least with y^7 and f_2 with x^{10} to produce new monomials, but then the resulting monomials are already in $L(G)$). If $\mathrm{NF}(-, G)$ is any (weak) normal form on R, then $\mathrm{NF}(f_3|G) = 0$, since $f_3 \in I$. Hence, we have

$\mathrm{NF}(f_3|G) = 0$ but $f_3 \notin I'$,
$G \subset J'$ but $\langle G \rangle_{K[x]} \neq J'$,
$I' \subset J$, $L(I') = L(J')$ but $I' \neq J'$.

Note that J' is even (x, y)–primary.

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

Definition 1.7. Let $f, g \in R^r \smallsetminus \{0\}$ with $\mathrm{lm}(f) = x^\alpha e_i$ and $\mathrm{lm}(f) = x^\beta e_j$, respectively. Let

$$\gamma := \mathrm{lcm}(\alpha, \beta) := \big(\max(\alpha_1, \beta_1), \ldots, \max(\alpha_n, \beta_n)\big)$$

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

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

which is called the **s–polynomial** of f and g.

Of course, $\operatorname{spoly}(f,g) \in R^r$ is only a polynomial if $r = 1$ and $f, g \in K[x]$.

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

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

and $\operatorname{lm}\big(\operatorname{spoly}(f,g)\big) < \operatorname{lm}(g)$. 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 $\operatorname{lc}(g) x^{\gamma-\alpha} f - \operatorname{lc}(f) x^{\gamma-\beta} g$. Both are, of course, equivalent, since our ground ring K is a field.

Algorithm 1.1.
Assume that $>$ is a well–ordering on $K[x]^r$.

NFBuchberger$(f|G)$

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 $G_h = \{g \in G \mid \operatorname{lm}(g) \mid \operatorname{lm}(h)\} \neq \emptyset$)
  choose any $g \in G_h$;
  $h = \operatorname{spoly}(h, g)$;
- return h;

For termination and correctness see [Bu3]. Note that each specific choice of "any" gives a different normal form function. The algorithm terminates, since in the i–th step of the while loop we create ($h_0 := f$) a spoly

$$\begin{aligned} &h_i = h_{i-1} - m_i g_i, \\ &\operatorname{lm}(h_{i-1}) = \operatorname{lm}(m_i g_i) > \operatorname{lm}(h_i) \end{aligned}$$

where m_i is a term (monomial times coefficient) and $g_i \in G$ (allowing repetitions).

Since $>$ is a well–ordering, $\{\mathrm{lm}(h_i)\}$ has a minimum, which is reached at some step m. Back substitution gives an expression ($h = h_m$)

$$h = f - \sum_{i=1}^{m-1} m_i g_i,$$

satisfying $\mathrm{lm}(f) = \mathrm{lm}(m-1g_1) > \mathrm{lm}(m_i g_i) > \mathrm{lm}(h_m)$.

Moreover, by construction, $\mathrm{lm}(h) \notin L(G)$. This proves correctness, independently of the specific choice of "any" in the while loop

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

Algorithm 1.2.
Assume that $>$ is a well–ordering on $K[x]^r$.

REDNFBUCHBEGER

Input: $f \in K[x]^r$, $G \in \mathcal{G}$
Output: $h \in K[x]^r$, a reduced normal form of f with regard to G

$h := 0,\ g = f,$
WHILE $(g \neq 0)$
  $g =$ NFBuchberger $(g|G)$,
  $h = h + \mathrm{lc}(g)\,\mathrm{lm}(g)$;
  $g = g - \mathrm{lc}(g)\,\mathrm{lm}(g)$;

Since the "tail" $g - \mathrm{lc}(g)\,\mathrm{lm}(g)$ of g has strictly smaller leading term than g, the algorithm terminates, since $>$ is a well–ordering. Correctness follows from the correctness of NFBuchberger.

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

Algorithm 1.3.
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 $I = \langle G \rangle_R \subset R^r$

- $S = G$;
- $P = \{(f,g)|f,g \in S\} \subset S \times S$
- while $(P \neq \emptyset)$
  choose $(f,g) \in P$;
  $P = P \setminus \{(f,g)\}$;

$h = \mathrm{NF}\big(\mathrm{spoly}(f,g)|S\big)$;
If $(h \neq 0)$
  $P = P \cup \{(h,f)|f \in S\}$;
  $S = S \cup h$;

- return S;

Remark 1.6. If NF is a reduced normal form and if G is reduced, then S is a reduced standard basis. If G is not reduced, we may apply NF afterward to $(f, S - \{f\})$ for all $f \in S$ in order to obtain a reduced standard basis.

To see termination of STANDARD, note that if $h \neq 0$ then $\mathrm{lm}(h) \notin L(S)$ 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 Noether property of $K[x]$. That is, after finitely many steps, we always have $\mathrm{NF}\big(\mathrm{spoly}(f,g)|S)\big) = 0$ for $(f,g) \in P$ and, after some finite time, the pair-set P will become empty.

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

Theorem 1.1 (Buchberger's criterion). *Let $I \subset R^r$ be a submodule and $G = \{g_1, \ldots, g_s\} \subset I$. Let $NF(-|G)$ 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 $uf - \mathrm{NF}(f|G)$ has a standard representation with respect to G.*

Then the following are equivalent

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

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

Proof. Let us first prove the equivalence of 1) – 3), which is easy. The implication 1) $\Rightarrow$ 2) follows from Lemma 1.1, 2) $\Rightarrow$ 3) is trivial.

Assuming 3), we see that $\mathrm{lm}(f)$ must occur as the leading monomials of $a_i g_i$ for some i. This implies that $\mathrm{lm}(g_i) | \mathrm{lm}(f)$, whence 1).

To see 3) $\Rightarrow$ 4), note that $h = \mathrm{NF}\big(\mathrm{spoly}(f_i, f_j)|G\big) \in I$ and, hence, by 3), if $h \neq 0$, $\mathrm{lm}(h) \in L(G)$ by 3), a contradiction to property (ii) of NF. Generation was shown in Lemma 1.1.

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 1.2). $\square$

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 [Getal], [GP]).

Before doing this, let us first analyze Buchberger's algorithm in the case of a local ordering. We may assume that in $K[x,y]$ we have $x_1,\ldots,x_n < 1$, $y_1,\ldots,y_m > 1 (m \geq 0)$. Look at the sequence $m_i = c_i x^{\alpha_i} y^{\beta_i}$ of terms constructed in the algorithm.

If $\deg_x(m_i) = \deg(x^{\alpha_i})$ and, hence, since $>$ induces a well–ordering on $K[y]$ the algorithm stops after finitely many steps.

If $\deg_x(m_i)$ is unbounded, then, for each fixed factor x^{α_i}, there can only be finitely many cofactors y^{β_j} and, hence, $\sum m_i$ converges in the (x)–adic topology, that is, $\sum m_i \in (K[y])[[x]]$. If $G = \{g_1,\ldots,g_s\}$ we may gather the coefficients m_j of any g_i, obtaining thus an expression

$$h = f - \sum_{i=1}^{s} a_i g_i,\ h, a_i \in K[y][[x]],$$

which holds in $K[y][[x]]$. This is not a normal form in our sense since, in general, $a_i,\ h \notin R$.

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

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

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

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

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

Definition 1.8. For a monomial $x^\alpha e_i \in K[x]^r$ set $\deg x^\alpha e_i = \deg x^\alpha = \alpha_1 + \cdots + \alpha_n$. 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

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

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

If $w = (w_1, \dots, w_s)$ is any tuple of positive real numbers, we can define the **weighted ecart** by $e_w(f) = w\text{–deg } f - w\text{–deg } \text{lm}(f)$ with $w\text{–deg } x^\alpha = w - 1\alpha_1 + \cdots + w_n\alpha_n$. In the following normal form NFMora, we may always take e_w instead of e, the algorithm works as well. Gräbe noticed [Gra] that, for certain examples, the algorithm can become much faster for a good choice of w.

More generally, let f^h denote the homogenization of f with respect to a new variable t (such that all components of f are homogeneous of the same degree). Define on $K[t, x]$ an ordering by the matrix

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix}$$

where A is a matrix defining the ordering on $K[x]$. This defines a well–ordering on $K[t, x]$. Extend it to $K[t, x]^r$ by

$$t^\alpha x^\gamma e_i > t^\beta x^\delta e_j \Leftrightarrow \deg(t^\alpha x^\gamma) > \deg[t^\beta x^\delta) \text{ or } x^\gamma e_i > x^\delta e_j.$$

Then we have for $f \in K[x]^r$

$$\text{lm}(f^h) = t^{\text{ecart}(f)}\,\text{lm}(f),$$

in particular, $\text{ecart}(f) = \deg_t \text{lm}(f^h)$.

Algorithm 1.4.
Let $>$ be any monomial ordering on $K[x]^r$, $R = S_>^{-1}K[x]$.

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 $T_h = \{g \in T | \text{lm}(g) | \text{lm}(h)\} \neq \emptyset$)
  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 $\mathrm{lm}(g) | \mathrm{lm}(h)$ implies that $\mathrm{lm}(g) \leq \mathrm{lm}(h)$, hence $T = G$ during the algorithm. Thus, NFMora is the same as NFBuchberger, but with a special selection strategy for the elements from G.

Termination is most easily seen by using homogenization: start with $h = f^h$ and $T = G^h$. The WHILE loop looks as follows:

WHILE ($h \neq 0$ and $T' = \{g \in T | \mathrm{lm}(g) | t^\alpha \mathrm{lm}(h)$ for some $\alpha\} \neq 0$)
    choose $G \in T'$ with α minimal;
    IF ($\alpha > 0$)
        $T = T \cup h$;
    $h = \mathrm{spoly}(h, g)$;
    $h = (h|_{t=1})^h$;
$h|_{t=\underline{1}}$;

By Dickson's lemma $L(T_\nu)$ becomes stable for $\nu \geq N$, where T_ν denotes the set T after the ν–th step of the WHILE loop. The next h, therefore, satisfies $\mathrm{lm}(h) \subset L(T_N) = L(T)$, whence, $\mathrm{lm}(g) | \mathrm{lm}(h)$ for some $g \in T$ and $\alpha = 0$. That is, T_ν itself becomes stable for $\nu \geq N$ and the algorithm continues with fixed T. Then it terminates, since $>$ is a well–ordering on $K[t,x]^r$.

To see correctness, consider the ν–th step in the WHILE loop. There we create (with $h_0 = f$) a spoly

$$\begin{aligned} h_\nu &= h_{\nu-1} - m_\nu g'_\nu, \\ \mathrm{lm}(h_{\nu-1}) &= \mathrm{lm}(m_\nu g'_\nu) > \mathrm{lm}(h_\nu), \end{aligned}$$

where m_ν is a term and for g_ν we have two possibilities:

a) $g'_\nu = g_i \in G$ for some i, or

b) $g'_\nu \in \{h_0, h_1, \ldots, h_{\nu-2}\} \subset T \setminus G$.

Suppose, by induction, that we have, after step $\nu - 1$, constructed a standard representation $(u_0 = 1, h_0 = f)$

$$u_{\nu-1} f = \sum_{i=1}^{s} a_i^{(\nu-1)} g_i + h_{\nu-1},\ u^{(\nu-1)} \in S_>.$$

In case b), we substitute $h_{\nu-1}$ by $h_\nu + m_\nu h_j$ with $j < \nu - 1$. y induction, we know

$$h_j = \sum_i a_i^{(j)} g_i - u_j f,\ u_j \in S_>$$

hence,

$$(u_{\nu-1} - m_\nu u_j)f = \sum_i a_i^{(\nu)} g_i + h_\nu.$$

Since $\mathrm{lm}(m_\nu h_j) = \mathrm{lm}(h_{\nu-1}) < \mathrm{lm}(h_j)$ we get $\mathrm{lm}(m_\nu) < 1$ and $u_\nu = u_{\nu-1} - m_\nu u_j \in S_>$.

By construction $\mathrm{lm}(h) \notin L(G)$, hence, the result.

For termination and correctness see [GP].

It is clear that, with a little extra storage, the algorithm does also return $u \in S_>$. Moreover, with quite a bit of bookkeeping one obtains the a_i. However, u is usually not needed and the a_i can be computed, as we shall see, more easily with the standard basis algorithm itself.

Algorithm 1.5.
Let $>$ be any monomial ordering on $K[x]^r$, $R = S_>^{-1}K[x]$.

STANDARD BASIS(G)

Input: $G = \{g_1, \ldots, g_s\} \subset K[x]^r$
Output: $S = \{h_1, \ldots, h_t\} \subset K[x]^r$ such that S is a standard basis of $I = \langle G \rangle_R \subset R^r$.

- $S = $ Standard(G,NFMora);
- return S;

1.3 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], [Schl2], 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 $f_1, \ldots, f_k \in R^r = \bigoplus_{i=1}^r Re_i$ is a k–tuple $(g_1, \ldots, g_k) \in R^k$ 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

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

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

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

is called the **module of syzygies** of I with respect to the generators $f_1, \dots, f_k$. It can be shown that the isomorphism class of $\operatorname{syz} I$ as R–module does only depend on the isomorphism class of I, in particular, it is independent of the set of generators.

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

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

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 $i < j$, $\operatorname{NF}\big(\operatorname{spoly}(f_i, f_j)|G\big) = 0$. We give an elegant proof by using syzygies, which is different from Schreyer's [Sch1], [Sch2] original one (cf. also [Ei]), although the basic ideas are due to Schreyer. Our proof gives,

The proof uses syzygies and is basically due to Schreyer [Sch1], [Schl2], 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 $\operatorname{spoly}(f_i, f_j)$ form a standard basis of $\operatorname{syz} I$ 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 $\operatorname{lm}(f_i) = x^{\alpha_i} e_\nu$, $\operatorname{lm}(f_j) = x^{\alpha_j} e_\nu$, define the monomial

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

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

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

Assume now that for $i < j$

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

for some weak normal form NF on R^r.

Then we have a standard representation

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

Define for $i < j$ such that $\mathrm{lm}(f_i)$ and $\mathrm{lm}(f_j)$ 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 $s_{ij} \in \mathrm{syz}\, I$ and it is easy to see that

Lemma 1.2. $\mathrm{lm}(s_{ij}) = m_{ji}\varepsilon_i$.

Proof. This follows, since $L(m_{ij}f_j) = L(m_{ji}f_i)$, hence $L(m_{ji}\varepsilon_i) > L(m_{ij}\varepsilon_j)$ by definition of $>_1$, since $i < j$. From the defining property of a standard representation we obtain

$$\begin{aligned}\mathrm{lm}(a_\nu^{(ij)}f_\nu) &\le \mathrm{lm}(m_{ji}f_i - \frac{c_i}{c_j}m_{ij}f_j)\\ &< \mathrm{lm}(f_{ji}f_i)\end{aligned}$$

and hence the claim. □

Theorem 1.2. *Let $G = \{g_1, \ldots, g_s\}$ be a set of generators of $I \subset R^r$ satisfying, for some weak normal form NF on R^r,*

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

then the following holds:

1) *G is a standard basis of I.*

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

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,

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

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 $g - h$,

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

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 $h \neq 0$,

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

and $\mathrm{lm}(h) \notin L(\{s_{ij}\}) = \langle \{m_{ji}\varepsilon_i\}\rangle$ by Lemma 1.2. This shows

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

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

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

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

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

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

In case 1) we obtain $\mathrm{lm}(f) = \mathrm{lm}(h_\nu g_\nu) \in L(G)$, 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 1.1, 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 1.3. *Let $G = \{g_1, \ldots, g_s\}$ be a pairwise different minimal (inter-reduced) standard basis of $I \subset R^r = \sum\limits_{i=1}^{r} Re_i$ such that $\mathrm{lm}(g_i) \in \{e_1, \ldots, e_r\}$. Let J denote the set of indices j such that $e_j \notin \{\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s)\}$. Then*

$$I = \bigoplus_{i=1}^{s} Rg_i,\quad R^r/I \cong \bigoplus_{j\in J} Re_j.$$

Proof. The set $G \cup \{e_j | j \in J\}$ is R–linear independent, since the leading terms are. This shows that both sums above are direct. For $f \in R^r$ consider a standard representation

$$f = \sum_{i=1}^{s} a_i g_i + h,\ \mathrm{lm}(h) \notin L(G).$$

This implies $h \in \sum\limits_{j\in J} Re_j$, and hence the result. $\square$

Lemma 1.4. *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 $\mathrm{lm}(g_i) = x^{\alpha_i} e_\nu$, $\mathrm{lm}(g_j) = x^{\alpha_j} e_\nu$ for some ν, then $\alpha_i \geq \alpha_j$ lexicographically. Let s_{ij} denote the syzygies defined above. Suppose that $\mathrm{lm}(g_1), \dots, \mathrm{lm}(g_s)$ do not depend on the variables $x_1, \dots, x_k$. Then the $\mathrm{lm}(s_{ij})$, 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 $\mathrm{lm}(g_i)$ and $\mathrm{lm}(g_j)$ involve the same component, say e_ν. By assumption $\mathrm{lm}(g_i) = x^{\alpha_i} e_\nu$, $\mathrm{lm}(g_j) = x^{\alpha_j} e_\nu$ 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, $\mathrm{lm}(s_{ij}) = m_{ji} e_i$, $m_{ji} = x^{\mathrm{lcm}(\alpha_i, \alpha_j) - \alpha_i}$, 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 1.3. *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.

Proof. Since R is Noetherian, M has a presentation

$$0 \longrightarrow I \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

with $F_0 = \sum_{i=1}^{r_0} R e_i$, and I finitely generated. Let $G = \{g_1, \dots, g_s\}$ be a standard basis of I and assume that the $\mathrm{lm}(g_i)$ do not depend on the variables $x_1, \dots, x_k$, $k \geq 0$. By Theorem 1.2, the syzygies s_{ij} generate $\mathrm{syz}\, I$, are a standard basis of $\mathrm{syz}\, I$ and by Lemma 1.4 we may assume that $\mathrm{lm}(s_{ij})$ do not depend on $x_1, \dots, x_{k+1}$. Hence, we obtain an exact sequence

$$0 \longrightarrow \mathrm{Ker}\, \varphi_1 = \mathrm{syz}\, I \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow M \longrightarrow 0$$

$F_1 = \sum_{i=1}^{s} R\varepsilon_i$, $\varphi_1(\varepsilon_i) = g_i$, with $\mathrm{syz}\, I$ satisfying analogous properties as I. We can, therefore, construct by induction an exact sequence

$$0 \longrightarrow \mathrm{Ker}\, \varphi_{n-k} \longrightarrow F_{n-k} \xrightarrow{\varphi_{n-k}} F_{n-k+1} \longrightarrow \dots \xrightarrow{\varphi_2} F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

with F_i free of rank r_i and $\mathrm{Ker}\, \varphi_{n-k}$ given by a standard basis $\{s_{ij}^{(n-k)}\}$ such that none of the variables appear in $\mathrm{lm}(s_{ij}^{(n-k)})$. By Lemma 1.3, $F_{n-k} / \mathrm{Ker}\, \varphi_{n-k}$ is free, and replacing F_{n-k} by $F_{n-k} / \mathrm{Ker}\, \varphi_{n-k}$ we obtained the desired free resolution. By Serre's criterion [Mat, 19.2], R is regular. $\square$

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.

Algorithm 1.6.
Let $>$ be any monomial ordering on $K[x_1,\dots,x_n]^r$, $R = S_>^{-1}K[x]$.

SRESOLUTION

Input: A matrix $G = (g_1,\dots,g_t)$, $g_1,\dots,g_t \in K[x]^r$ a standard basis of $I = \langle G\rangle_R \subset R^r$.
Output: A set of matrices A_i of size (r_{i-1}, r_i), $i = 1,\dots,n$ such that

$$0 \longleftarrow R^r/I \longleftarrow R^{r_0} \longleftarrow \cdots \longleftarrow R^{r_{i-1}} \xleftarrow{A_i} R^{r_i} \longleftarrow \dots$$

is a resolution.

- $A_1 = (g_1,\dots,g_t)$.
- For $i < j$ compute a standard representation of $\mathrm{spoly}(g_i, g_j) = \sum_{v=1}^{k} a_v^{(ij)} g_r$
  $s_{ij} := m_{ij}\varepsilon_i - \frac{c_i}{c_j} m_{ij}\varepsilon_j - \sum_v^{(ij)} \varepsilon_v$.
- $A_2 = (s_{12},\dots,s_{t-1},t)$.
- Change the monomial ordering to the Schreyer ordering with respect to $g_1,\dots,g_t$.
- result $= \{A_1\} \cup$ SResolution (A_2).
- return result.

`Etwas zur Berechnung von Ext und annExt als Anwendung`

2 Primary decomposition

2.1 The theory

Let R be a Noetherian ring.

Definition 2.1. An ideal $I \subseteq R$ is a prime ideal if $I \subsetneqq R$ and $ab \in I$, $a \notin I$ implies $b \in I$ for all $a, b \in R$.

Example 2.1.

1) Let M be a maximal ideal of R, then M is prime.

2) Let R be factorial (for instance, $K[x_1, \ldots, x_n]$ for a field K or $K = \mathbb{Z}$). If $f \in R$ is irreducible, then (f) is prime.

3) $(x_{i_1}, \ldots, x_{i_k}) \subseteq K[x_1, \ldots, x_n]$, K a field, is prime.

4) Let $I \subseteq R$ be an ideal, $P \supseteq I$ a prime ideal, then $\bar{P} = \{\bar{f} | f| \in P\} \subseteq R/I$ is prime.

The proof of 1) – 4) is simple and we leave it to the reader.

Definition 2.2. An ideal $I \subseteq R$ is a primary ideal, if $I \subsetneqq R$ and $ab \in I$, $a \notin I$ implies $b^m \in I$ for some m, $a, b \in R$.

Example 2.2.

1) The power of a maximal ideal is primary.

2) In a factorial ring, the ideal generated by the power of an irreducible element is primary.

3) Let $R = K[x, y, z]/(xy - z^2)$, K a field, then $P = (x, z)$ is a prime ideal but P^2 is not primary.

4) The image of a primary ideal of R in R/I is primary.

Remark: Let $Q \subseteq R$ be a prime (respectively primary) ideal. Let $A \cdot B \subseteq Q$ and $A \not\subseteq Q$ for two ideals $A, B \subseteq R$, then B (respectively B^s for some s) is contained in Q.

Definition 2.3. Let $I \subseteq R$ be an ideal, the radical of I is defined by

$$\sqrt{I} = \{f | f \in R,\ f^m \in I \text{ for some } m\}.$$

We leave it to the reader to prove that $\sqrt{I}$ is an ideal.

Lemma 2.1. *Let $Q \subseteq R$ be primary, then $\sqrt{Q}$ is prime.*

Proof. Let $ab \in \sqrt{Q}$ and $a \notin \sqrt{Q}$ then $(ab)^m \in Q$ for some m, but $a^m \notin Q$. This implies $(b^m)^s \in Q$ for some s and, therefore, $b \in \sqrt{Q}$. $\square$

Remark: Example 2.2 3) shows that there are ideals Q with $\sqrt{Q}$ being prime but Q not being primary. Such ideals are called pseudo primary. Equidimensional pseudo primary ideals are primary.

Definition 2.4. Let $I \subseteq R$ be an ideal, the set of associated primes $\operatorname{Ass}(I)$ is defined by

$$\begin{aligned}\operatorname{Ass}(I) &= \{P \mid P \text{ prime}, P = \operatorname{Ann}(\bar{b}),\ \bar{b} \in R/I\}\\ &= \{P \mid P \text{ prime}, P = I : b\}.\end{aligned}$$

Example 2.3.

1) Let $Q \subseteq R$ be primary, then $\operatorname{Ass}(Q) = \{\sqrt{Q}\}$.

2) Let $I = (x^2, xy) \subseteq K[x, y]$, K a field, then $= Ass(I) = \{(x),\ (x, y)\}$.

3) $I = (x^2, xy)$ is pseudo primary, $\sqrt{I} = (x)$.

Proof.

1) Let $P = Q : b$ be prime, then $Q \subseteq P$ implies $\sqrt{Q} \subseteq \sqrt{P} = P$. On the other hand, $b \notin Q$ implies $P^m \subseteq Q$ for some m and, therefore, $P \subseteq \sqrt{Q}$.

2) $I : x = (x, y)$ and $I : y = (x)$. $\square$

Definition 2.5. Let $P, Q \in \operatorname{Ass}(I)$ and $P \subsetneqq Q$, then Q is an embedded prime ideal of I. $\operatorname{Minass}(I) := \{P \in \operatorname{Ass}(I) \mid P \text{ is not an embedded prime ideal}\}$. For $P \in \operatorname{Ass}(I)$ let $C(I, P) = \{Q \mid Q \in \operatorname{Ass}(I),\ Q \subseteq P\}$.

Example 2.4.

1) (x, y) is an embedded prime ideal of I.

2) $\operatorname{Minass}(I) = \{(x)\}$.

3) $C\big(I, (x, y)\big) = \operatorname{Ass}(I)$, $C\big(I, (x)\big) = \operatorname{Minass}(I)$.

Definition 2.6. Let $I = Q_1 \cap \cdots \cap Q_r$, Q_i primary. The decomposition is redundant, if there is an i such that $I = Q_1 \cap \ldots, \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_r$. If the decomposition is not redundant, it is called irredundant.

A decomposition of I into an intersection of primary ideals is called minimal, if the number of necessary primary ideals is minimal between all possible decompositions.

Example 2.5. Let $I = (x^2, xy)$.

1) $I = (x) \cap (x,y)^2$ is minimal.

2) Minimal implies irredundant.

3) $I = (x) \cap (x,y)^2 \cap (x,y)$ is redundant.

4) The decomposition $(x,y)^2 = (x^2, y) \cap (x, y^2)$ is irredundant, but not minimal.

Now we are prepared to prove the following main theorem of this chapter:

Theorem 2.1. *Let $I \subseteq R$ be an ideal, then there exists a minimal decomposition $I = Q_1 \cap \dots \cap Q_r$ of I as an intersection of primary ideals $Q_1, \dots, Q_r$ and $r = \# \operatorname{Ass}(I)$. Furthermore, $\operatorname{Ass}(I) = \{\sqrt{Q_1}, \dots, \sqrt{Q_r}\}$ and if $C(I,P) = \{\sqrt{Q_{i_1}}, \dots, \sqrt{Q_{i_s}}\}$ for some $P \in \operatorname{Ass}(I)$, then also $Q_{i_1} \cap \dots \cap Q_{i_s}$ is independent on the choice of a minimal decomposition.*

Proof. To prove the existence of a minimal decomposition, it is sufficient to prove that any ideal is the intersection of finitely many primary ideals. Assume that this is not true, and let $\mathcal{X} = \{J/J \subseteq R$ be an ideal which is not an intersection of finitely many primary ideals $\}$.

We shall use Zorn's lemma to prove that $\mathcal{X}$ has a maximal element. To do this we have to prove that for every ascending chain $\dots \subseteq J_i \subseteq J_{i+1} \subseteq \dots$ of ideals of $\mathcal{X}$, also $\cup J_j \in \mathcal{X}$.

Because R is noetherian, such a chain stabilizes and $\cup J_i = J_k$ for some k, that is, $\cup J_i \in \mathcal{X}$ and the assumptions of Zorn's lemma are satisfied.

Now let $J \in \mathcal{X}$ be a maximal element. Being in $\mathcal{X}$ the ideal I cannot be primary itself and we can choose $a, b \in R$ such that $a \cdot b \in J$, $a \notin J$ and $b^n \notin J$ for all n.

Now the ascending chain $\dots \subseteq (J : b^m) \subseteq (J : b^{m+1}) \subseteq \dots$ stabilizes and we obtain an n such that $J : b^n = J : b^{n+1}$. We shall prove later that, under this condition,

$$J = (J : b^n) \cap (J, b^n).$$

But $J \subsetneqq J : b^n$ and $J \subsetneqq (J, b^n)$ because of the choice of b, therefore, $(J : b^n)$, $(J, b^n) \notin \mathcal{X}$ and, consequently, intersections of finitely many primary ideals. This holds, therefore, for J, too, and gives a contradiction to the assumption that $\mathcal{X} \neq \emptyset$.

Now we shall prove that $\sqrt{Q_i} \neq \sqrt{Q_j}$ if $i \neq j$. Assume $\sqrt{Q_i} = \sqrt{Q_j}$ for some i, j and $i \neq j$. Then $\sqrt{Q_i \cap Q_j} = \sqrt{Q_i} \cap \sqrt{Q_j} = \sqrt{Q_i}$. We shall see that $Q_i \cap Q_j$ is, again, a primary ideal. Let $ab \in Q_i \cap Q_j$ and $a \notin Q_i \cap Q_j$ (we may assume $a \notin Q_i$), then $b^m \in Q_i$ for some m. This implies $b \in \sqrt{Q_i} = \sqrt{Q_j}$ and, therefore, $b^s \in Q_j$ for some s, especially $b^{m \cdot s} \in Q_i \cap Q_j$, which proves that $Q_i \cap Q_j$ is primary. But this is a contradiction to the minimality of the decomposition:
$I = Q_1 \cap \dots \cap Q_{i-1} \cap (Q_i \cap Q_j) \cap Q_{i+1} \cap \dots \cap Q_{j-1} \cap Q_{j+1} \cap \dots \cap Q_r$ is a decomposition of length $r - 1$.

We proved that the $\{\sqrt{Q_i}\}$ is a set of pairwise different prime ideals.

To continue, we need the following lemma:

Lemma 2.2. *Let $I = A \cap Q$, $A \not\subset Q$ and Q primary, then there is a $d \in R$ such that $I : d = \sqrt{Q}$. We shall prove the lemma later.*

We choose $d_1, \dots, d_r \in R$ such that $I : d_i = \sqrt{Q_i}$. This implies $\{\sqrt{Q_1}, \dots, \sqrt{Q_r}\} \subseteq \mathrm{Ass}(I)$. Let $P \in \mathrm{Ass}(I)$, $P = I : b$ for some b, then

$$\begin{aligned} P = I : b &= (Q_1 : b) \cap \dots \cap (Q_r : b) \\ &= \sqrt{Q_1 : b} \cap \dots \cap \sqrt{Q_r : b} \text{ because of } P = \sqrt{P}. \end{aligned}$$

If $b \in Q_i$ then $\sqrt{Q_i : b} = R$, if $b \notin Q_i$ then $\sqrt{Q_i : b} = \sqrt{Q_i}$ and we obtain

$$P = \sqrt{Q_{i_1}} \cap \dots \cap \sqrt{Q_{i_s}}, \text{ for } \{i_1, \dots, i_s\}$$

being the set of indices with $b \notin Q_{ij}$.

In particular, we have

$$P \subseteq \sqrt{Q_{i_j}} \qquad j = 1, \dots, s$$

and

$$\sqrt{Q_{i_1}} \cdot \ldots \cdot \sqrt{Q_{i_s}} \subseteq P.$$

This implies that $P = \sqrt{Q_{i_k}}$ for some k and we proved $\mathrm{Ass}(I) = \{\sqrt{Q_1}, \dots, \sqrt{Q_r}\}$.

Finally, let $P \in \mathrm{Ass}(I)$ and $C(I, P) = \{\sqrt{Q_{i_1}}, \dots, \sqrt{Q_{i_s}}\}$, then it is easy to see that

$$IR_P \cap R = Q_{i_1} \cap \dots \cap Q_{i_s},$$

which proves the rest of the theorem. □

Proof of Lemma 2.2. We choose $d_0 \in A$, $d_0 \notin Q$ and obtain

$$I : d_0 = Q : d_0.$$

If $Q : d_0$ is already prime, the lemma is proved with $d = d_0$. Otherwise, let $Q_1 = Q : d_0$ and we choose $d_1 \in \sqrt{Q_1} = \sqrt{Q}$, $d_i \notin Q_1$. In this way, we assume Q_i, d_{i-1} are already defined and $Q_i \subsetneqq \sqrt{Q_i} = \sqrt{Q}$, then we choose $d_i \in \sqrt{Q} \setminus Q_i$ and define Q_{i+1} by $Q_i : d_i$.

We have $Q_i \subsetneqq Q_{i+1}$: namely, there is a minimal $t \geq 2$ such that $d_i^t \in Q_i$, then $d_i^{t-1} \in Q_{i+1}$ and $d_i^{t-1} \notin Q_i$. The ascending chain $Q \subsetneqq Q_1 \subsetneqq Q_2 \subseteq \dots \subseteq Q_i \subseteq \dots$ has to stabilize. Therefore, there is a k such that

$$Q_k : d_k = \sqrt{Q}.$$

This proves the lemma with $d = d_0 \cdot \ldots \cdot d_k$. □

Remark: The two different minimal decompositions $(x) \cap (x, y)^2 = (x) \cap (x^2, y)$ show that we cannot obtain uniqueness for the primary ideals in a minimal decomposition.

During the proof of the theorem, we promised to prove the following lemma:

Lemma 2.3. *Let $I \subseteq R$ be an ideal and assume $I : b = I : b^2$ for some $b \in R$, then $I = (I : b) \cap (I, b)$.*

Proof. Let $f \in (I : b) \cap (I, b)$, $f = m + rb$, $m \in I$, and $bf \in I$. Then $b \cdot m + rb^2 \in I$ and, therefore, $rb^2 \in I$. This implies $r \in I : b^2 = I : b$ and, therefore, $f \in I$, which means $(I : b) \cap (I, b) \subseteq I$. The other inclusion is obvious. □

Corollary 2.1. *Let I be pseudo primary and assume that $\operatorname{Ass}(I) = \operatorname{Min\,ass}(I)$ then I is primary.*

Proof. Let $I = Q_1 \cap \cdots \cap Q_r$. Because all associated primes are minimal we have $\sqrt{Q_i} \not\subset \sqrt{Q_j}$ for $i \neq j$. $\sqrt{I} = \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_r}$ is prime implies, therefore, $r = 1$. □

2.2 The algorithms

In this section, let $R = K[x_1, \ldots, x_n]$ and $I \subseteq R$ be an ideal.

The aim is to explain how to compute several decompositions of I, its radical $\sqrt{I}$ and the normalization of the factoring R/I. Our main tools are Gröbner bases (for well–orderings) but all algorithms involving just these carry over to $\operatorname{Loc} K[x_1, \ldots, x_n]$ for arbitrary monomial orderings. For primary decomposition we need, in addition, multivariate polynomial factorization. Almost all algorithms of this chapter are implemented in SINGULAR.

Let $I = \bigcap_{i=1}^{r} Q_i$ be a minimal primary decomposition (that is, r is minimal) and denote by $P_i = \sqrt{Q_i}$ the associated prime ideals. We are interested in solving the following problems:

(1) For $v \geq \operatorname{codim}(I)$, compute $E_v(I) := \bigcap_{\operatorname{codim}(Q_i)=v} Q_i$ the equidimensional part of I of codimension v (if $\operatorname{codim}(Q_i) \neq v$ for all i let $E_v(I) = R$).

(1') To solve a weaker problem, compute equidimensional ideals I_v such that $\sqrt{I_v} = \sqrt{E_v(I)}$.

(2) Compute $\operatorname{Ass}(I) = \{P_1, \ldots, P_r\}$ and $\operatorname{minAss}(I) = \{P_i \in \operatorname{Ass}(I) \mid P_i \subsetneqq Pj$ for $i \neq j\}$.

(3) Compute the radical $\sqrt{I} = \bigcap_{i=1}^{r} P_i = \bigcap_{P \in \min \operatorname{Ass}(I)} P$ and the equidimensional radical $\sqrt[\text{equi}]{I} = \sqrt{E_d(I)}$, $d = \operatorname{codim}(I)$.

(4) Compute, for I radical, the normalization of R/I, that is the integral closure of R/I in its quotient ring $Q(R/I)$.

(5) Compute a minimal primary decomposition of I.

There are some basic tools for the solution of these problems.

Lemma 2.4 (splitting tools).

1) If $I : f = I : f^2$ for some $f \in R$, then $I = (I : f) \cap (I, f)$.

2) Let $f \cdot g \in I$ and $\langle f, g\rangle = R$, then $I = (I, f) \cap (I, g)$.

3) Let $f \cdot g \in I$, then $\sqrt{I} = \sqrt{I, f} \cap \sqrt{I, g}$.

4) Let $f^n \in I$, then $\sqrt{I} = \sqrt{I, f}$.

5) Let J be an ideal, then $\sqrt{I} = \sqrt{I : J} \cap \sqrt{I + J} = \sqrt{I : J} \cap \sqrt{I : (I : J)}$.

Proof. 1) is just Lemma 2.3, 2), 3) and 4) are obvious. To prove 5), let $P \in \operatorname{minAss}(I : J)$. If $P \notin \operatorname{minAss}(I)$, there is a $Q \in \operatorname{minAss}(I)$ and $P \supsetneqq Q$. This implies $I : J \not\subset Q$ and, therefore, $I : (I : J) \subseteq Q$. If $P \in \operatorname{minAss}\big(I : (I : J)\big)$ and $P \notin \operatorname{minAss}(I)$ there is a $Q \in \operatorname{minAss}(I)$ and $P \supsetneqq Q$. This implies $Q \supseteq I : J$, because $Q \not\supset I : J$ would imply $I : (I : J) \subset Q$. This proves $\sqrt{I} = \sqrt{I : J} \cap \sqrt{I : (I : J)}$. Now $I + J \subset I : (I : J)$, which proves $\sqrt{I} = \sqrt{I : I} \cap \sqrt{I + J}$. ☐

Remark 2.1. Our experience shows that during all algorithms one should use Lemma 2.4 to split the ideal as often as possible.

Lemma 2.5. *Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal and $S = \{g_1, \ldots, g_s\}$, $g_i \in K[x_1, \ldots, x_n]$ be a Gröbner basis of $IK(x_1, \ldots, x_k)[x_{k+1}, \ldots, x_n]$. Let $h = \operatorname{lcm}\big(\operatorname{lc}(g_1), \ldots, \operatorname{lc}(g_s)\big)$ then*

1) $IK(x_1, \ldots, x_k)[x_{k+1}, \ldots, x_n] \cap K[x_1, \ldots, x_n] = (I : h^\infty)$.

2) Let $(I : h^\infty) = I : h^N$, then $I = (I : h^N) \cap (I, h^N)$.

3) Assume $IK(x_1, \ldots, x_k)[x_{k+1}, \ldots, x_n] = \sqrt{IK(x_1, \ldots, x_k)[x_{k+1}, \ldots, x_n]}$ then $\sqrt{I} = (I : h^\infty) \cap \sqrt{(I, h)}$.

Proof. Obviously $(I : h^\infty) \subseteq IK(x_1, \ldots, x_k)[x_{k+1}, \ldots, x_n]$.
Let $f \in IK(x_1, \ldots, x_k)[x_{k+1}, \ldots, x_n] \cap K[x_1, \ldots, x_n]$, S being a Gröbner basis implies $\operatorname{NF}(f|S) = 0$ in $K(x_1, \ldots, x_k)[x_{k+1}, \ldots, x_n]$. But the algorithm of the normal form requires only dividing by the leading coefficients $\operatorname{lc}(g_i)$ of the g_i. This implies $f = \sum_{i=1}^{s} \xi_i g_i$ and $\xi_i \in K[x_1, \ldots, x_n]_h$ and, therefore, $h^N \xi_i \in K[x_1, \ldots, x_n]$ for some h, which proves 1).

2) ist just Lemma 2.3.

To prove 3), we choose an N such that $I : h^\infty = I : h^N$. We know (by 2)) $I = (I : h^N) \cap (I, h^N)$.

This implies $\sqrt{I} = \sqrt{I : h^N} \cap \sqrt{I, h^N}$.

Now $\sqrt{I, h^N} = \sqrt{I, h}$ and by assumption $\sqrt{(I : h^\infty)} = (I : h^\infty)$ proves the proposition. $\square$

2.2.1 Computation of the radical

We shall describe two different approaches to compute the radical of an ideal. Another approach is due to Becker and Wörmann, which we shall not treat here ([BW]).

We start with an algorithm, which, in its main part, is due to Krick and Loger ([KL]).

Proposition 2.1. *Let $I \subseteq K[x_1, \ldots, x_n]$ be a zero–dimensional ideal and $P_i(x_i) \in K[x_i] \cap I$ polynomials of minimal degree $i = 1, \ldots, n$, $L_i(x_i)$ the square free part of P_i then $\sqrt{I} = I + \langle L_1, \ldots, L_n \rangle$.*

Proof. $K[x_1, \ldots, x_n]/\langle L_1, \ldots, L_n \rangle \simeq K[x_1]/L_1 \otimes_K \cdots \otimes_K K[x_m]/L_1$ is semisimple, because $K[x_i]/L_i$ is a direct sum of fields (square freeness of L_i). Then $K[x_1, \ldots, x_n]/I + \langle L_1, \ldots, L_n \rangle$ is semisimple and contains, therefore, no nilpotent elements. This implies that $\sqrt{I} \subseteq \sqrt{I + \langle L_1, \ldots, L_n \rangle} = I + \langle L_1, \ldots, L_n \rangle \subseteq \sqrt{I}$. $\square$

Algorithm 2.1.
RADICAL (I)

Input: an ideal I,
Output: $\sqrt{I}$:

- Result $= \langle 1 \rangle$;
- choose any admissible term–ordering $<$;
- use the factorizing Gröbner basis algorithm to compute ideals $I_1, \ldots, I_k$ and Gröbner bases $G^{(1)}, \ldots, G^{(i)}$ such that $\sqrt{I} = \cap \sqrt{I_k}$. Let $\mathfrak{m} = \{I_1, \ldots, I_k\}$;
- For $I \in \mathfrak{m}$ do
  - compute $\Gamma = \{u^{(1)}, \ldots, u^{(\ell)}\}$, $u^{(i)} \subseteq \{x_1, \ldots, x_n\} = x$, $\#u^{(i)} = \dim(I)$ and $L(I) \cap K[u^{(i)}] = (0)$, the maximal independent set of the leading ideal $L(I)$ of I (this is a combinatorical problem);
  - start with the ideals Result $= (1)$ and $W = I$;

- for $i = 1$ to s do
  compute $S^{(i)}$, a Gröbner basis of W with respect to a block–ordering $<_i$ having the property that if $x_a \in u^{(i)}$, $x_b \notin u^{(i)}$, then $x_a < x_b$
  (notice that $WK(u^{(i)})[x \smallsetminus u^{(i)}]$ is zerodimensional and $S^{(i)}$ is a Gröbner basis of this ideal with respect to $<_i$ restricted to $x \smallsetminus u^{(i)}$);
- using linear algebra and the Gröbner basis $S^{(i)}$, compute for all $x_a \in x \smallsetminus u^{(i)}$ $P_a(x_a)$ such that $\big(P_a(x_a)\big) = WK(u^{(i)})[x \smallsetminus u^{(i)}] \cap K(u^{(i)})[x_a]$;
- compute the square free L_a part of P_a;
- compute a Gröbner basis $T^{(i)}$ of $WK(u^{(i)})[x \smallsetminus u^{(i)}] + \langle\{L_a | x_a \in x \smallsetminus u^{(i)}\}\rangle$ such that the elements of $T^{(i)}$ are polynomials in $K[x_1, \dots, x_n]$;
- compute $h^{(i)} \in K[u^{(i)}]$, the least common multiple of the leading coefficients of the elements in $T^{(i)}$;
- compute in $K[x_1, \dots, x_n]$ $(\langle T^{(i)}\rangle : h^{(i)})^\infty = J^{(i)}$;
- Result = Result $\cap J^{(i)}$;
- $W = (W, h^{(i)})$;
  (if this is done for $i = 1, \dots, s$, then Result = equidimensional radical of I if $\dim W < \dim I$).
- Result = Result $\cap$ radical (W);

• return Result

A quite different approach is due to Eisenbud, Huneke and Vasconcelos ([EHV]).

We fix a field K of characteristic 0, or characteristic p, sufficiently large.

Let $A = K[x_1, \dots, x_n]/I$ be a K–algebra of finite type. We denote by $J_a(A)$ the a–th fitting ideal of $\Omega_{A|K}$, the module of Kähler differentials and by $J_a(I)$ its pull–back in $K[x_1, \dots, x_n]$.

$J_a(A)$ is compatible with localizations and base change.

Note that if $I = \langle f_1, \dots, f_m\rangle$, then $J_a(I) = I +$ the ideal generated by the $(n-a)$–minors of the Jacobian matrix $\left(\frac{\partial f_i}{\partial x_j}\right)$.

The idea of the algorithm goes back to the following theorem of Scheja and Storch ([SS]).

Theorem 2.2. *Let A be a local Artinian K–algebra with maximal ideal $\mathcal{M}_A$, then A is a complete intersection if and only if $(0) : J_0(A) = \mathcal{M}_A$.*

For $A = K[x_1, \dots, x_n]/I$ the result can be formulated as follows:

Let $I \subseteq K[x_1, \dots, x_n]$ be a $(x_1, \dots, x_n)$–primary ideal, then I is a complete intersection if and only if $I : J_0(I) = (x_1, \dots, x_n)$.

Corollary 2.2. *Let $I \subseteq K[x_1, \ldots, x_n]$ be a complete intersection of dimension d, then $\sqrt{I} = I : J_d(I)$.*

Corollary 2.3. *Let I be equidimensional of codimension m and $f_1, \ldots, f_m \in I$ a regular sequence. If $I_0 = \langle f_1, \ldots, f_m \rangle$, then*

$$\sqrt{I} = \sqrt{I_0} : (\sqrt{I_0} : I).$$

Proof. Because of $I_0 \subseteq I$ equidimensional, we have $\sqrt{I_0} = \sqrt{I} \cap L$ and $\sqrt{I_0} : I = L : I = L$ and $\sqrt{I_0} : L = \sqrt{I} : L = \sqrt{I}$. □

Remark 2.2. Let $I = I_1 \cap I_2$ and I_1 the equidimensional part of I intersected with the embedded components corresponding to the equidimensional part, I_2 the part of higher codimension. Then $I_2 = I : \sqrt{I_1}^N$, where N has the property that $I : \sqrt{I_1}^N = I : \sqrt{I_1}^{N+1}$.

We obtain the following algorithms:

Algorithm 2.2.
EquiRadical(I)

Input: an ideal I
Output: the radical of the equidimensional part of I

- compute a Gröbner basis of I and the codimension $d = \operatorname{codim}(I)$;
- choose a regular sequence $f_1, \ldots, f_d$ in I (try the first d elements of a set of minimal generators of I, if this does not work, choose d elements as a generic linear combination of the generators of I with coefficients in K);
- compute the Jacobian ideal $J_0 = J_{n-d}(I_0)$ of $I_0 = \langle f_1, \ldots, f_d \rangle$ and then compute $\sqrt{I_0} = I_0 : J_0$;
- compute $\sqrt{I_0} : (\sqrt{I_0} : I) =: I_1$ (this is the radical of the equidimensional part);
- Return I_1

Algorithm 2.3.
Radical(I)

Input: an ideal I
Output: the radical of I

- $I_1 =$ EquiRadical (I);
- compute N such that $I : I_1^N = I : I_1^{N+1}$;
- return $I_1 \cap$ Radical ($I : I_1^N$)

2.2.2 Computation of the equidimensional part of an ideal

Again we present two different approaches. The first approach is used in several papers ([GTZ], [KL], ...) and is based on Proposition 2.5:

Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal of dimension d and $u \subseteq \{x_1, \ldots, x_n\} =: x$ be a maximal independent set, that is, $I \cap K[u] = (0)$ and $\#u = d$. Let $<$ be a block–ordering for u and $x \smallsetminus u$, such that elements of $x \smallsetminus u$ are always greater than elements of u.

Let G be a Gröbner basis of I with respect to $<$. G, considered as polynomials in $K(u)[x \smallsetminus u]$, is still a Gröbner basis of $IK[u)[x \smallsetminus u]$, which is zero–dimensional. Let $h \in K[u]$ be the least common multiple of the leading coefficients of G in $K(u)[x \smallsetminus u]$, then $IK(u)[x \smallsetminus u] \cap K[x] = I : h^\infty$ is equidimensional of dimension d and $I = (I : h^N) \cap (I, h^N)$ if $I : h^\infty = I : h^N$.

This is the basis of the following algorithm:

The algorithm (input an ideal I of codimension d, output the equidimensional part $E_d(I)$ of I and an ideal W of codimension $> d$ such that $I = E_d(I) \cap W$):

Algorithm 2.4.
EQUIDIMENSIONAL (I)

Input: an ideal I of codimension d
Output: the equidimensional part $E_d(I)$ of I and an ideal W of codimension $> d$ such that $I = E_d(I) \cap W$.

- choose any admissible term–ordering $<$;
- compute S, a Gröbner basis of I with respect to $<$;
- compute $d = \dim(I)$ and $\Gamma = \{u^{(1)}, \ldots, u^{(\ell)}\}$, $u^{(i)} \subseteq \{x_1, \ldots, x_n\} = x$, $\#u^{(i)} = d$ and $L(I) \cap K[u^{(i)}] = (0)$, the maximal independent set of the leading ideal $L(I)$ of I;
- start with the ideals Result $= (1)$ and $W = I$;
- for $i = 1$ to S do
  - compute $S^{(i)}$, a Gröbner basis of W with respect to a block–ordering $<_i$, having the property such that if $x_a \in u^{(i)}$, $x_b \notin u^{(i)}$, then $x_a < x_b$; ($S^{(i)}$ is a Gröbner basis of $WK(u^{(i)})[x \smallsetminus u^{(i)}]$)
  - choose $T^{(i)}$, a subset of $S^{(i)}$, which is a minimal Gröbner basis of $WK(u^{(i)})[x \smallsetminus u^{(i)}]$ and compute $h^{(i)} \in K[u^{(i)}]$ the least common multiple of the leading coefficients of the elements in $T^{(i)}$;
  - compute in $K[x_1, \ldots, x_n]$, $(\langle T^{(i)} \rangle : h^{(i)\infty}) = J^{(i)}$;

- Result = Result $\cap J^{(i)}$;
- $W = (W, h^{(i)})$, if $\dim(W) < \dim(I)$
  return {Result, W}.

- Result = Result $\cap$ Equidimensional $(W)[1]$;
  return {Result, Equidimensional $(W)[2]$}.

Proposition 2.2. *Let $I \subseteq K[x_1, \ldots, x_n] =: R$ be an ideal of codimension d and denote by $E_j(I)$ the equidimensional part of I of codimension j, then*

1) $E_d(I) = ann\mathrm{Ext}^d_R(R/I, R)$.

2) If $I_0 \subseteq I$ is a complete intersection, then $E_d(I) = I_0 : (I_0 : I)$.

3) For $\ell \geq d$

$$\sqrt{E_\ell(I)} = \sqrt{E_\ell\big(ann(\mathrm{Ext}^\ell_R(R/I, R))\big)}.$$

Proof. To prove 2), we use the following property of zero–dimensional complete intersections (cf. [SS]):

Let A be a local complete intersection Artinian ring. Let $I \subseteq A$ be an ideal, then $(0) : \big((0) : I\big) = I$.

The reason for this property is the non–degenerate symmetric bilinear form σ, defined by the socle S (the determinant of the Jacobian matrix of the complete intersection):

Extend a fixed socle element s to a K–base of A. Define $\sigma(a, b)$ = coefficient of $a \cdot b$ of s written in terms of the base. Then $(0) : I = I^\perp = \{x \in A | \sigma(x, I) = 0\}$ and $(I^\perp)^\perp = I$.

Now it is not difficult to see that always $I \subseteq I_0 : (I_0 : I)$. It is sufficient to prove that $I_P = \big(I_0 : (I_0 : I)\big)_P$ for all associated prime ideals of codimension d of I because $\sqrt{E_d(I)} = \sqrt{I_0 : (I_0 : I)}$ (I_0 has, as complete intersection of codimension d, all associated primes of I of codimension d as associated primes, $I_0 : I$ has, as associated primes, the complement of $\mathrm{Ass}(I_0)$). Now we may consider $(R/I_0)_P =: A$, but here $(0) : \big((0) : IA\big) = IA$ holds, which proves 2).

To prove 1), we use the following standard formula ([M, p. 140]):

Let B be a noetherian ring, M, N B–modules, $x \in B$ B–regular und M–regular and $xN = 0$, then $\mathrm{Ext}^{n+1}_B(N, M) \simeq \mathrm{Ext}^n_{B/xB}(N, M/xM)$.

Applying this d times to our situation we obtain:

$$\mathrm{Ext}^d_R(R/I, R) \simeq \mathrm{Hom}_{R/I_0}(R/I, R/I_0),$$

$I_0 \subseteq I$ as in 2) a complete intersection of codimension d

$$\mathrm{Hom}_{R/I_0}(R/I, R/I_0) \simeq (I_0 : I)/I_0.$$

This implies that

$$\mathrm{ann}\,\mathrm{Ext}^d_R(R/I, R) = I_0 : (I_0 : I).$$

Now, using 2), $E_d(I) = \mathrm{ann}\mathrm{Ext}^d_R(R/I, R)$.

To prove 3), let P be a prime of codimension ℓ and $S = R_P$. Assume that $P \supseteq I$. Consider the exact sequence

$$0 \longrightarrow (0 : P^\infty) \longrightarrow S/I \longrightarrow F \longrightarrow 0.$$

Then, by construction, $\mathrm{Hom}_S(S/P, F) = 0$ and, therefore, depth $(F) > 0$. Using the formulae of Auslander and Buchsbaum (projdim(F)+ depth(F) = depth$(S) = \ell$), we obtain $\mathrm{Ext}^\ell_S(F, S) = 0$. From the long exact sequence

$$\ldots \longrightarrow \mathrm{Ext}^\ell_S(F, S) \longrightarrow \mathrm{Ext}^\ell_S(S/I, S) \longrightarrow \mathrm{Ext}^\ell_S\big((0 : P^\infty), S\big) \longrightarrow 0$$

we obtain $\mathrm{Ext}^\ell_S(S/I, S) \cong \mathrm{Ext}^\ell_S((0 : P^\infty), S)$ and especially $\mathrm{ann}(\mathrm{Ext}^\ell_S(S/I, S)) = \mathrm{ann}(\mathrm{Ext}^\ell_S((0 : P^\infty), S))$. Now $(0 : P^\infty)$ is of finite length and S is regular; this implies $\mathrm{Ext}^\ell_s(\mathrm{Ext}^\ell_S((0 : P^\infty), S), S) = (0 : P^\infty)$ (dualizing the free resolution of $(0 : P^\infty)$ gives a free resolution of $\mathrm{Ext}^\ell_S((0 : P^\infty), S)$ because $\mathrm{Ext}^j_S((0 : P^\infty), S) = 0$ for $j < \ell$) and especially $\mathrm{ann}(\mathrm{Ext}^\ell((0 : P^\infty), S)) = \mathrm{ann}((0 : P^\infty))$. Obviously $P^m \subset \mathrm{ann}(0 : P^\infty) = \mathrm{ann}(\mathrm{Ext}^\ell_S(S/I, S))$.

On the other hand, $\mathrm{ann}(0 : P^\infty) \subset P$ if and only if $P \in \mathrm{Ass}(I)$.

This proves the proposition. $\square$

We obtain the following algorithm:

Algorithm 2.5.
EQUIDIMENSIONAL (I)

Input: an ideal I
Output: the equidimensional part of I

- compute a Gröbner basis of I and the codimension $d = \mathrm{codim}(I)$;
- choose the first d elements in a set of minimal generators of I and set $I_0 = \langle f_1, \ldots, f_d\rangle$;
- If I_0 is a complete intersection
  return $I_0 : (I_0 : I)$;
- return $\mathrm{ann}\mathrm{Ext}^d_R(R/I, R)$;

2.2.3 Zerodimensional primary decomposition

We shall first give the theoretical background, which is used for the algorithm of Gianni, Trager, Zaharias ([GTZ]). Notice that in [GMT], Gianni, Miller and Trager generalize the Berlecamp algorithm to obtain a zero–dimensional decomposition. We do not treat this approach here.

Let K be a field of characteristic zero, or sufficiently large.

Definition 2.7. Let P be a maximal ideal in $K[x_1, \dots, x_n]$. P is called **in general position** with respect to the lexicographical ordering $x_1 > \cdots > x_n$, if the reduced Gröbner basis of P is $\{x_1 - f_1(x_n), \dots, x_{n-1} - f_{n-1}(x_n),\ f_n(x_n)\}$ with $f_i \in K[x_n]$.

Remark 2.3. Notice that automatically f_n is irreducible and $\deg f_i < \deg f_n$.

Proposition 2.3. *For every maximal ideal $P \subset K[x_1, \dots, x_n]$ there exists a dense open subset $U \subset K^{n-1}$ such that for every $\underline{a} = (a_1, \dots, a_{n-1})$, the associated map $\varphi_{\underline{a}}$ defined by $\varphi_{\underline{a}}(x_i) = x_i$ if $i < n$ and $\varphi_{\underline{a}}(x_n) = x_n + \sum\limits_{i=1}^{n-1} a_i x_i$ maps P to $\varphi(P)$, an ideal in general position with respect to the lexicographical ordering $x_1 > \cdots > x_n$.*

Proof. The field $K[x_1, \dots, x_n]/P$ is a finite extension of K and there exists a dense open subset $U \subset K^{n-1}$ such that for $\underline{a} = (a_1, \dots, a_{n-1}) \in U$ the element $z = x_n + \sum\limits_{i=1}^{n-1} a_i x_i$ is a primitive element for the field extension (theorem of the primitive element).

Using the corresponding map $\varphi_{\underline{a}}$ we may assume that x_n is a primitive element, that is,

$$K[x_1, \dots, x_n]/P = K[x_n]/f_n(x_n)$$

for an irreducible polynomial $f_n(x)$.

Now define $f_i(x_n)$ by $x_i \mod P = f_i(x_n) \mod f_n(x_n)$ and we obtain

$$\langle x_1 - f_1(x_n), \dots, x_{n-1} - f_{n-1}(x_n),\ f_n(x_n)\rangle = P.$$

The set of these generators is obviously a Gröbner basis with the required properties. $\square$

Definition 2.8. Let $I \subset K[x_1, \dots, x_n]$ be zero–dimensional. I is called **in general position** with respect to the lexicographical ordering $x_1 > \cdots > x_n$ if the following holds: let $I = Q_1 \cap \cdots \cap Q_s$ be the minimal primary decomposition with associated primes $P_1, \dots, P_s$, then

1) $P_1, \dots, P_s$ are in general position with respect to the lexicographical ordering $x_1 > \cdots > x_n$.

2) $P_1 \cap K[x_n], \dots, P_s \cap K[x_n]$ are coprime.

Proposition 2.4. *Let $I \subset K[x_1, \dots, x_n]$ be a zero–dimensional ideal. There is a dense open subset $U \subset K^{n-1}$ such that for $\underline{a} \in U$, $\varphi_{\underline{a}}(I)$ is in general position with respect to the lexicographical ordering $x_1 > \dots > x_n$.*

Proof. Let $I = Q_1 \cap \dots \cap Q_s$ be the primary decomposition with associated primes $P_1, \dots, P_s$, then $\varphi_{\underline{a}}(P_j)$ are in general position with respect to the lexicographical ordering $x_1 > \dots > x_n$ for almost all $\underline{a} \in K^{n-1}$. On the other hand, the zero set of I is just a set of s different points which project to different points for almost all $\underline{a}$. $\square$

Theorem 2.3. *Let $I \subset K[x_1, \dots, x_n]$ be in general position with respect to the lexicographical ordering $x_1 > \dots > x_n$ and G a minimal Gröbner basis, $\{g\} = G \cap K[x_n]$.*

Let $g = g_1^{\rho_1} \cdot \ldots \cdot g_s^{\rho_s}$ be the decomposition of g into a power product of irreducible factors g_i, then

(1) $I = \bigcap\limits_{k=1}^{s} (I, g_k^{\rho_k})$;

(2) the ideals $(I, g_k^{\rho_k})$ are primary ideals.

Proof. (2) let $I = Q_1 \cap \dots \cap Q_\ell$ with associated primes $P_1, \dots, P_\ell$ and let $P_i \cap K[x_n] = \langle p_i \rangle$. Then by assumption $p_1, \dots, p_\ell$ are coprime and, therefore, $\cap P_i \cap K[x_n] = \cap \langle p_i \rangle = \langle \prod\limits_{i=1}^{\ell} p_i \rangle$. On the other hand, $I \cap K[x_n] = \langle g \rangle$ implies that g divides a power of $\prod\limits_{i=1}^{\ell} p_i$. This implies $\ell = s$ and that we may assume $g_i = p_i$ for $i = 1, \dots, s$. This implies $P_i \supset (I, g_i^{\rho_i})$ and $P_j \not\supset (I, g_i^{\rho_i})$ for $i \neq j$. Because of $I \subset (I, g_k^{\rho_k})$ we know that $\mathrm{Ass}(I, g_k^{\rho_k}) \subset \mathrm{Ass}(I)$ and, therefore, (2) is proved.

To prove (1) note that

$$I \cap K[x_n] = \bigcap_{k=1}^{s} (I, g_k^{\rho_k}) \cap K[x_n].$$

Let $f \in \cap (I, g_k^{\rho_k})$, $f = f_v + \xi_v g_v^{\rho_v}$ with $f_v \in I$, then $g^{(v)} f = g^{(v)} f^{(v)} + g^{(v)} \xi_v \cdot g$ for $g^{(v)} = g / g_v^{\rho_v}$. Let $\sum\limits_{v=1}^{s} \eta_v g^{(v)} = 1$, then

$$f = \sum_{v=1}^{s} \eta_v g^{(v)} f^{(v)} + \sum_{v=1}^{s} \eta_v g^{(v)} \xi_v g \in I,$$

which proves (1). $\square$

Using Theorem 2.3 we obtain the following algorithm

Algorithm 2.6.
ZEROPRIMDEC(I)

Input: $I \subset K[x_1, \ldots, x_n]$ zero–dimensional
Output: $\{Q_1, P_1, \ldots, Q_s, P_s\}$, Q_i primary, $\sqrt{Q_i} = P_i$ and $I = Q_1 \cap \cdots \cap Q_s$

- Result $= \emptyset$, Rest $= \emptyset$;
- perform a random coordinate change $J = \varphi_a(I)$, $\varphi_{\underline{a}}$ defined by $\varphi_{\underline{a}}(x_i) = x_i$ if $i < n$ and $\varphi_{\underline{a}}(x_n) = x_n + \sum\limits_{i=1}^{n-1} a_i x_i$;
- compute a Gröbner basis G of J with respect to the lexicographical ordering $x_1 > \cdots > x_n$;
- let $\{f\} = G \cap K[x_n]$, factorize f:
  $f = f_1^{\rho_1} \cdot \ldots \cdot f_s^{\rho_s}$;
- For $k = 1$ to s do

  test whether $(I, f_k^{\rho_k})$ is primary:

  This is the case if and only if a Gröbner basis with respect to the lexicographical ordering $x_1 > \cdots > x_n$ contains $h_1^{(k)}, \ldots, h_n^{(k)}$ such that

  - $h_n^{(k)} = f_k^{\rho_k}$
  - $h_i^{(k)} = \big(x_i - g_i^{(k)}(x_n)\big)^{n_i^{(k)}} \mod (h_{i+1}^{(k)}, \ldots, h_n^{(k)})$.

  If $(J, f_k^{\rho_k})$ is prime, then $P_k := (x_1 - g_1^{(k)}, \ldots, x_{n-1} - g_{n-1}^{(k)}, f_k)$ is the associated prime to $Q_k := (J, f_k^{\rho_k})$;
  Result $=$ Result $\cup\{\varphi_a^{-1}(Q_k),\ \varphi_a^{-1}(P_k)\}$
  else
  Rest $=$ Rest $\cup \big\{\big(I, \varphi_a^{-1}(f_k^{\rho_k})\big)\big\}$;
- If Rest $= \emptyset$, then return Result
  else
      let Rest $= \{I_1, \ldots, I_r\}$
      for $i = 1$ to r
          Result $=$ Result $\cup$ ZEROPRIMDEC(I_i)

  return Result.

Remark 2.4. To make this algorithm really efficient, it is necessary to do some preprocessing to avoid a random coordinate change whenever possible. Random coordinate change destroys sparseness and usually makes the Gröbner basis computation very difficult. Therefore, we use the properties (cf. Lemma 2.4).

- $I = (I : b) \cap (I, b)$ if $I : b = I : b^2$,
- $(I, f \cdot g) = (I, f) \cap (I, g)$ if $\langle f, g\rangle = \langle 1\rangle$,

to split the ideal as often as possible before starting the algorithm. To do this, we produce as many reducible elements as possible. This leads to the following preprocessing algorithm:

Algorithm 2.7.
SPLIT(I)

Input: an ideal I
Output: two sets of ideals: Primary $= \{Q_1, P_1, \ldots, Q_s, P_s\}$ and Rest $= \{I_1, \ldots, I_k\}$ such that $I = (\cap Q_i) \cap (\cap I_i)$, Q_i primary and $\sqrt{Q_i} = P_i$

- Primary $= \emptyset$, Rest $= \emptyset$;
- compute $\langle P_i\rangle = I \cap K[x_i]$ and add them to the generators of I;
- factorize all the generators of I and split the ideal as often as possible;
- compute for all splitting ideals a Gröbner basis with respect to the lexicographical ordering $x_1 > \cdots > x_n$;
  if possible split the generators again;
- test whether the splitting ideals are primary and in general position with respect to the lexicographical ordering $x_1 > \cdots > x_n$. Put the detected primary ideals and their associated primes to Primary and the other ideals to Rest;
- return Primary, Rest.

Remark 2.5. The ideals of Rest have the following property:

They have a set of generators (which is a Gröbner basis with respect to the lexicographical ordering $x_1 > \cdots > x_n$) and every generator is a power of an irreducible element.

Remark 2.6. The decomposition of a zero–dimensional radical ideal is, with respect to the preprocessing, simpler. We can use the fact that

$$\sqrt{I, f \cdot g} = \sqrt{I, f} \cap \sqrt{I, g}.$$

This simplifies the splitting. In particular, we can use the factorizing Gröbner basis algorithm to split the ideal. Also the prime test for a zero–dimensional ideal is simpler than a primary test:

I is prime if there is an irreducible $g \in I \cap K[x_i]$ for some i and $\dim_K K[x_1, \ldots, x_n]/I = \deg(g)$. Especially, we obtain:

I is prime and in general position with respect to the lexicographical ordering $x_1 > \cdots > x_n$ if and only if for a minimal Gröbner basis G and $G \cap K[x_n] = \{g\}$ we have $\dim_K K[x_1, \ldots, x_n]/I = \deg(g)$ and g is irreducible.

Remark 2.7. An equivalent approach, also going to general position, is the following algorithm proposed by Eisenbud, Huneke, Vasconcelos ([EHV]):

Algorithm 2.8.
DECOMP EHV(I)

Input: a zero–dimensional radical ideal I
Output: the associated prime ideals

- Choose a generic $f \in K[x_1, \ldots, x_n]$ and test whether f is a zero–divisor $\mod I$ (this is the case if $I : f \supsetneqq I$). If f is a zero–divisor $\mod I$ (which implies $I = \big(I : f\big) \cap (I, f)\big)$, then
  return DECOMP EHV($I : f$)$\cup$ DECOMP EHV(I, f);
- Choose m minimal such that $1, f, \ldots, f^m$ is linearly dependent $\mod I$. If $m < \dim_K K[x_1, \ldots, x_n]/I$ start the algorithm again;
  let $P \in K[T]$ be the minimal polynomial of f; if P is irreducible, then
  return $\{I\}$;
  If $P = Q_1 \cdot Q_2$, then
  return DECOMP EHV$\big(I, Q_1(f)\big)\cup$ DECOMP EHV$\big(I, Q_2(f)\big)$

2.2.4 Higher dimensional primary decomposition

Prime decomposition of a radical ideal

Algorithm 2.9.
MINASSPRIMES(I)

Input: an ideal I
Output: the minimal associated prime ideals of I

- Result $= \emptyset$
- use the factorizing Gröbner basis algorithm to split I;
  the result $\mathfrak{m}$ is a set of ideals such that
  - all elements of their Gröbner bases are irreducible
  - the radical of the intersection of the elements of $\mathfrak{m}$ is the radical of I.
- For $J \in \mathfrak{m}$ do

– compute $\mathcal{X}$ the set of maximal independent sets of variables of the leading ideal $L(J)$;

– for $u \in \mathcal{X}$ do

  - compute
    $\mathrm{Ass}(JK(u)[x \smallsetminus u])$ using zero–dimensional prime decomposition.
    For $P \in \mathrm{Ass}(JK(u)[x \smallsetminus u])$ do
      Result = Result $\cup \{P \cap K[x]\}$
    compute h such that
    $JK(u)[x \smallsetminus u] \cap K[x] = J : h$
    $J = (J, h)$

  - Result = Result $\cup$ minAssPrimes(J)

- return Result

A second possibility is based on the computation of the irreducible characteristic sets associated to I (cf. [W], [Mi]). We do not treat this approach here.

The computation of the primary ideals

The first approach, proposed by Eisenbud, Huneke, Vasconelos, is based on the following lemma:

Lemma 2.6. *Let I be an ideal and $P \in \min Ass(I)$, let m satisfy $I : P^m \not\subseteq P$, then the equidimensional part of $I + P^m$ is a primary ideal of I with associated prime P.*

Proof. Let Q be the primary ideal in the primary decomposition of I which has P as associated prime. By assumption there exist ξ, $\xi \notin P$ and $\xi P^m \subseteq I \subseteq Q$. This implies $P^m \subseteq Q$ and, therefore, $I + P^m \subseteq Q$. Localizing by P, we obtain $(I+P^m)_P \subseteq Q_P = I_P$ which implies $(I + P^m)_P = Q_P$ and, therefore, Q = equidimensional part of $I + P^m$. This proves the lemma. □

Remark 2.8. If $P \in \mathrm{Ass}(I)$ is an embedded prime, then one can also obtain a primary ideal Q of the decomposition of I as

$$Q = \text{EQUIDIMENSIONAL}(I + P^m).$$

In this case, it is more difficult to estimate m (cf. [EHV]):

Let $I_{[P]} = \{b \in R | I : b \not\subseteq P\}$ and consider the map $(I_{[P]} : P^\infty)/I_{[P]}) \longrightarrow R/Q$. Then Q is a primary ideal of a decomposition of I if and only if the above map is injective.

The second approach, proposed by Shimoyama and Yokoyama ([SY]), is based on the following two lemmata:

Lemma 2.7. *Let I be an ideal and $minAss(I) = \{P_1, \ldots, P_r\}$. Assume there are $f_1, \ldots, f_r$ such that*

- $f_i \in \bigcap\limits_{j \neq i} P_j$;

- $f_i \notin P_i$.

Let k_i be defined by $I : f_i^\infty = I : f_i^{k_i}$, $Q_i := I : f_i^\infty$ and $J = I + \langle f_1^{k_1}, \ldots, f_r^{k_r} \rangle$, then

1) $\sqrt{Q_i} = P_i$, *that is, Q_i is pseudo primary;*

2) $I = \bigcap\limits_{i=1}^{r} Q_i \cap J$;

3) $\mathrm{codim}(J) > \mathrm{codim}(I)$.

4) *Let $Q_i = \bigcap\limits_j Q_j^{(i)}$ be a minimal primary decomposition of Q_i, $i = 1, \ldots, r$, then $\bigcap\limits_{i,j} Q_j^{(i)}$ is a minimal primary decomposition of $\bigcap\limits_{i=1}^{r} Q_i$ (no redundant components!) and $\bigcup\limits_i \mathrm{Ass}(Q_i) \cap \mathrm{Ass}(J) = \emptyset$.*

Remark 2.9. Let I be an ideal and $\mathrm{minAss}(I) = \{P_1, \ldots, P_r\}$. Assume that $G_1, \ldots, G_r$ are Gröbner bases of $P_1, \ldots, P_r$. Since P_i is minimal in $\mathrm{Ass}(I)$, there are always elements t_j in G_j not being in P_i for $i \neq j$. Now define $f_i := \prod\limits_{j \neq i} t_j$, then $f_1, \ldots, f_r$ satisfy the assumptions of Lemma 2.7.

Lemma 2.8. *Let Q be pseudo primary with $\sqrt{Q} = P$ prime and $u \subseteq x$ a maximal independent set for Q. Then $QK(u)[x \smallsetminus u] \cap K[x] =: Q'$ is primary. Let $g \in K[u]$ be chosen such that $QK(u)[x \smallsetminus u] \cap K[x] = Q : g = Q : g^2$, then $Q = Q' \cap (Q, g)$ and* $\mathrm{codim}(Q) < \mathrm{codim}(Q, g)$.

Proof. $QK(u)[x \smallsetminus u]$ is zero–dimensional and $\sqrt{Q}$ is prime, this implies $QK(u)[x \smallsetminus u]$ is primary and, therefore, $QK(u)[x \smallsetminus u] \cap K[x] = Q'$ is primary. Using Lemma 2.3 we obtain $Q = Q' \cap (Q, g)$. Since $g \in K[u]$ we have $g \notin P$ and, therefore, $(P, g) \subseteq \sqrt{Q, g}$, which implies $\mathrm{codim}(Q) < \mathrm{codim}(Q, g)$. □

The algorithm of Eisenbud, Huneke, Vasconcelos

Algorithm 2.10.
PRIMARYDECEHV(I)

Input: an ideal $I \subseteq K[x_1, \ldots, x_n] = R$,
Output: a set Result $= \{Q_1, P_1, \ldots, Q_s, P_s\}$ such that $I = \cap Q_v$ is a minimal primary decomposition and $\sqrt{Q_v} = P_v$.)

- compute $E = \{\mathrm{ann}\big(\mathrm{Ext}_R^j(R/I, R)\big),\ j \geq \mathrm{codim}(I)\}$;

- compute $\mathfrak{m} = \{\mathrm{Equiradical}(J) \mid J \in E,\ J \neq R\}$;

- compute $\mathrm{Ass}(I) = \bigcup\limits_{L \in \mathfrak{m}} \mathrm{Ass}(L)$;

- Let $\mathrm{Ass}(I) = \{P_1, \ldots, P_s\}$.
  For $i = 1$ to s do

  compute $Q_i =$ Equidimensional $(I + P_i^m)$;
  (m as in Lemma 2.6)

- Return $\{Q_1, P_1, \ldots, Q_s, P_s\}$

The algorithm of Gianni/Trager/Zacharias

Algorithm 2.11.
PRIMARYDECGTZ(I)

Input and *Output* as in the previous algorithm)

- Result $= \emptyset$;

- compute $\mathcal{X}$ the set of maximal independent sets of variables of the leading ideal $L(I)$;

- For $u \in \mathcal{X}$ do

  – compute $\mathfrak{m} =$ ZEROPRIMDEC$(IK(u)[x \setminus u])$;

  – Result $=$ Result $\cup\{J \cap K[x] | J \in \mathfrak{m}\}$;

  – compute h such that
  $IK(u)[x \setminus u] \cap K[x] = I : h = I : h^2$;
  $I = (I, h)$

- Result $=$ Result $\cup$ PRIMARYDECGTZ(I);

- return Result

Remark 2.10. During the previous algorithm one should always try to avoid the computation of redundant components, respectively remove them as soon as possible. This can be arranged as in the next algorithm.

The algorithm of Shimoyama and Yokoyama

Algorithm 2.12.
PRIMARYDECSY$(I,$ check$)$

Input and *Output* as in the previous algorithm, additionally we have, for recursive use of the procedure, a test ideal check to avoid redundant components, which is $\langle 1 \rangle$ at the beginning

- Result $= \emptyset$;
- if check $\subseteq I$ return Result;
- compute $\text{minAss}(I) = \{P_1, \ldots, P_r\}$;
  let $G_1, \ldots, G_r$ be Gröbner bases of $P_1, \ldots, P_r$
- choose $t_j \in G_j$ not being in P_i for $i \neq j$ and define $f_i := \prod\limits_{j \neq i} t_j$;
- For $i = 1$ to r do
  - compute k_i such that $I : f_i^\infty = I : f_i^{k_i} =: Q_i$;
  - if check $\subseteq Q_i$ then $Q_i = \langle 1 \rangle$;
- $J := I + \langle f_1^{k_1}, \ldots, f_r^{k_r} \rangle$;
- For $i = 1$ to r do
  - for $Q_i \neq \langle 1 \rangle$ compute maximal independent sets u_i of the leading ideal $L(Q_i)$ and g_i such that $Q_i K(u_i)[x \smallsetminus u_i] \cap K[x] = Q_i : g_i = Q_i : g_i^2 =: Q_i'$ and let $J_i := (Q_i, g_i)$;
    If check $\subseteq Q_i'$ then
        $Q_i' = \langle 1 \rangle$
    else
        Result = Result $\cup \{Q_i', P_i\}$
    If check $\subseteq J_i$ then
        $J_i = \langle 1 \rangle$
    else
        Result = Result $\cup$ PRIMARYDECSY$(J_i,$ check$)$;
- check = check $\cap(\cap Q_i)$;
- Result = Result $\cup$ primarydecSY$(J,$ check$)$;
- return Result

2.2.5 The normalization

Here we describe an algorithm which goes back to Grauert and Remmert [GR] and was proposed by T. de Jong ([J]). Other algorithms were given, for example, by Seidenberg [Se], Stolzenberg [St], Gianni, Trager [GT] and Vasconcelos [V1].

The algorithm is based on the following criterion for normality due to Grauert and Remmert [GR]:

Proposition 2.5. *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 Spec(R). Then R is normal if and only if $R = \mathrm{Hom}_R(J, J)$.*

Remark 2.11. Let J, R be as in the proposition and x a non–zero divisor of J. It is not difficult to see

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

and, consequently,

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

3) Let $u_0 = x, u_1, \ldots, u_s$ be generators of $xJ : J$ as R–module. Because $\mathrm{Hom}_R(J, J)$ is a ring we have $\frac{s(s+1)}{2}$ relations $\frac{u_i}{x} \cdot \frac{u_j}{x} = \sum\limits_{k=0}^{s} \xi_k^{ij} \frac{u_k}{x}$, $s \geq i \geq j \geq 1$, $\xi_k^{ij} \in R$ in $\frac{1}{x}(xJ : J)$. Together with the linear relations, the syzygies between $u_0, \ldots, u_s$, they define the ring structure of $\mathrm{Hom}_R(J, J)$:
$$\begin{array}{ccc} R[T_1, \ldots, T_s] & \twoheadrightarrow & \mathrm{Hom}_R(J, J) \\ T_i & \rightsquigarrow & \dfrac{u_i}{x}. \end{array}$$
The kernel of this map is the ideal generated by $T_i T_j - \sum\limits_{k=0}^{s} \xi_k^{ij} T_k \quad (T_0 = 1)$ and $\sum\limits_{k=0}^{s} \eta_k T_k$ such that $\sum\limits_{k=0}^{s} \eta_k u_k = 0$.

Now we are prepared to give the normalization algorithm:

Algorithm 2.13.
NORMAL(I[, INFORM])

Input: a radical ideal $I \subseteq K[x_1, \ldots, x_n]$.
Output: s polynomial rings $R_1, \ldots, R_s$ and s ideals $I_1 \subset R_1, \ldots, I_s \subset R_s$ and s maps $\pi_i : R \to R_i$, such that the induced map $\pi : K[x_1, \ldots, x_n]/I \to R_1/I_1 \times \cdots \times R_s/I_s$ is the normalization of $K[x_1, \ldots, x_n]/I$

Additional information by the user (respectively by the algorithm) can be given in the optional list inform, as for instance,

– I defines an an isolated singularity
– some elements of the radical of the non–normal locus, which are already known

- Result $= \emptyset$

- For $i = 1$ to s do
  - compute $J =$ singular locus of I
  - choose $f \in J \setminus I$ and compute $I : f$ to check whether f is a zero divisor
  - if $I : f \supsetneq I$

    Result = Result $\cup$ normal$(I : (I : f))\cup$ normal$(I : f)$

    (Notice that $\sqrt{I, f} = I : (I : f)$ in this situation.)

    else

    If we have an isolated singularity at $0 \in K^n$ then $J = (x_1, \ldots, x_n)$.

    In general, if J_0 is the radical of the singular locus of a normalization loop before, given by the list inform, then $J = \sqrt{I, f + J_0}$

    else

    $J = \sqrt{I, f}$

    $H = fJ : J$

    if $H = \langle f \rangle$

    Result = Result $\cup\{K[x_1, \ldots, x_n], I, \mathrm{id}\}$

    else

    assume $H = fJ : J = \langle f, u_1, \ldots, u_s \rangle$

    then compute an ideal L,

    $L \subseteq K[x_1, \ldots, x_n, T_1, \ldots, T_s]$

    (as described in the remark above) such that

    $$K[x_1, \ldots, x_n, T_1, \ldots, T_s]/L \xrightarrow{\sim} \mathrm{Hom}(J, J)$$
    $$T_i \rightsquigarrow \tfrac{u_i}{f},$$

    let $\varphi : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n, T_1, \ldots, T_s]$ be the inclusion.

    $S =$ normal(L),

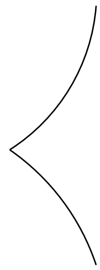
    compose the maps of S with φ.

    Result = Result $\cup S$
- return Result

The above algorithm has been implemented by the authors. The implementation in SINGULAR is available as SINGULAR library normal.lib.

To have an efficient version of the normalization algorithm, we had to take care of several special cases and tricks for the implementation.

We illustrate the algorithm by computing the normalization of the cuspidal plane cubic:



$$R = K[x,y]/y^2 - x^3$$

- Radical of the singular locus : $J = (x, y)$
- $R \subsetneqq \mathrm{Hom}_R(J, J) = (1, \frac{y}{x})$
- the linear relations are $x^2 - yT_1, y - xT_1$
  the quadratic relation is $T_1^2 - x$
  and, therefore

$$\mathrm{Hom}_R(J,J) = R[T_1]/(x^2 - yT_1, y - xT_1, T_1^2 - x)$$

- reducing the number of variables by $y = xT_1,\ x = T_1^2$ we obtain $\bar{R} = K[T_1]$ and as map

$$\begin{array}{ccc} R & \to & K[t_1], \\ x & \rightsquigarrow & T_1^2, \\ y & \rightsquigarrow & T_1^3. \end{array}$$

3 Applications to Singularity Theory

3.1 Basic concepts and invariants

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 $f_1, \ldots, f_k$ holomorphic (complex analytic) functions on U, then we may consider

$$V = V(f_1, \ldots, f_k) = \{x \in U | f_1(k) = \cdots = f_k(x) = 0\},$$

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

In practice, $f_1, \ldots, f_k$ will be polynomials, but singularity theory is interested only in the behaviour of $V(f_1, \ldots, f_k)$ 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 $f_1, \ldots, f_k$ in the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ but in the ideal I generated by $f_1, \ldots, f_k$ in the convergent power series ring $\mathbb{C}\{x_1 - p_1, \ldots, x_n - p_n\} = \mathbb{C}\{x - p\}$.

For arbitrary fields K, where the notion of convergence does not make sense, we consider instead the formal power series ring $K[[x]] = K[[x_1, \ldots, x_n]]$ and ideals I generated by formal power series (in practice polynomials) $f_1, \ldots, f_k \in K[[x]]$. In order to have a uniform notation, we write

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

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

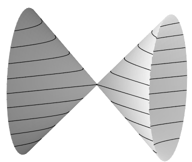
As in the affine case, we have the Hilbert Nullstellensatz (also called the Hilbert–Rückert Nullstellensatz), stating that

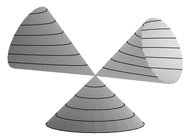
$$\sqrt{I} = I(V, p) := \{f \in \mathbb{C}\{x - p\} \mid f|_{(V,p)} = 0\}$$

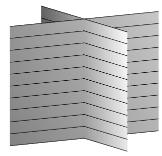
for $I \subset \mathbb{C}\{x - p\}$ and (V, p) the complex analytic germ defined by I.

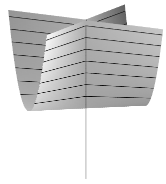
A **(complex) singularity** is, by definition, nothing but a complex analytic germ (V,p) (together with its analytic local ring $\mathbb{C}\{x-p\}/I$). (V,p) is called **non–singular** or **regular** or **smooth** if $\mathbb{C}\{x_1-p_1,\ldots,x_n=p_n\}/I$ is isomorphic (as local ring) to a power series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









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

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 is generated by polynomials, which follows easily from the theory of dimensions by Hilbert–Samuel series (cf. [AM]). Using this fact, we can compute $\dim(V,p)$ by using standard bases.

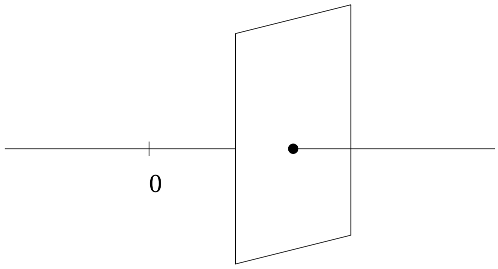
Algorithm 3.1.
DIM(I)

Input: $f_1,\ldots,f_k\in K[x_1,\ldots,x_n]$ such that $I=\langle f_1,\ldots,f_k\rangle$
Output: $\dim K\langle x\rangle/I$

- compute a standard basis $\{g_1,\ldots,g_s\}$ of the ideal $\langle f_1,\ldots,f_k\rangle_{\mathrm{Loc}\,K[x]}$ with respect to any *local* monomial ordering on $K[x]$;
- compute the dimension of the monomial ideal $\langle \mathrm{lm}(g_1),\ldots,\mathrm{lm}(g_s)\rangle_{K[x]}$.

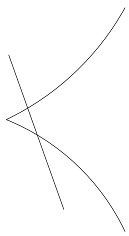
Correctness was proved in [GP, 3.6]. The second step is combinatorial and the same as for global orderings.

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** $\mathrm{mt}(V,p)$ of the singularity (V,p). If (V,p) is reduced, that is, $I = \sqrt{I}$, then $\mathrm{mt}(V,p)$ 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 $\mathrm{mt}(V,p)$ is the smallest degree in the Taylor expansion of f in p.



$$V : y^2 - x^3 = 0, \quad \mathrm{mt}(V,0) = 2$$

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

Algorithm 3.2.
MULT(I)

Input: $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$ such that $I = \langle f_1, \ldots, f_k \rangle$.
Output: multiplicity of $\langle x_1, \ldots, x_n \rangle$ in $K\langle x \rangle / \langle f_1, \ldots, f_k \rangle$, respectively in $K[x]_{(x)} / \langle f_1, \ldots, f_k \rangle$

- compute a standard basis $\{g_1, \ldots, g_s\}$ of the ideal $\langle f_1, \ldots, f_k \rangle_{\mathrm{Loc}\, K[x]}$ with respect to a *local degree ordering* on $K[x]$;
- compute the (usual) degree of the monomial ideal $\langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s) \rangle$.

Correctness was proved in [GP, 3.7]; indeed, the Hilbert function of $\langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s) \rangle$ coincides with the Hilbert–Samuel function of $\langle f_1, \ldots, f_k \rangle$ with respect to $\langle x_1, \ldots, x_n \rangle$.

The answer to Zariski's multiplicity question, whether the multiplicity of a hypersurface singularity is a topological invariant (for $K = \mathbb{C}$), is still open. We shall report on this in the last section.

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**

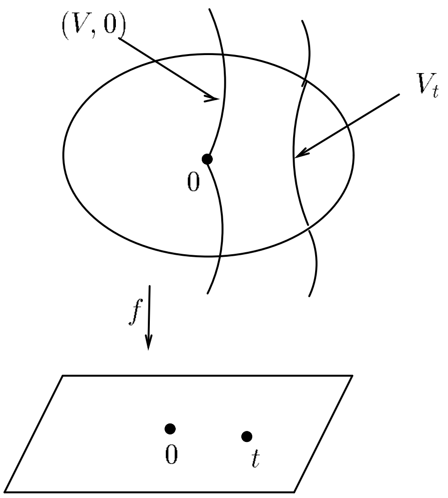
$$\mu(f) := \dim_K K\langle x \rangle / \langle f_{x_1}, \ldots, f_{x_n} \rangle$$

(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 $f \in \mathbb{C}\{x_1, \ldots, x_n\}$ defining an isolated singularity at 0, let

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

$0 < |t| << 1$ 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 char $K = 0$).
MILNOR(f)

Input: $f \in K[x_1, \ldots, x_n]$
Output: $\mu(f)$

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

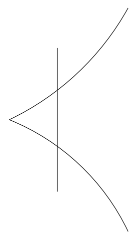
The correctness of this algorithm follows from [GP, 3.7].

Similarly, we can compute the **Tjurina number**

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

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

To see the difference between local and global orderings, consider the affine plane curve



$$f(x,y) = (y^2 - x^3)(x-1) = 0$$

The affine variety $V(f_x, f_y) = V\big(y^2 - 4x^3 + 3x^2, y(2x-2)\big) \subset \mathbb{C}^2$ describes the four critical points of the function f, $(0,0)$, $(1,\pm 1)$ and $(\frac{3}{4}, 0)$, $V(f, f_x, f_y)$ consists of the three points $(0,0)$, $(1,\pm 1)$, while $\tau(f) = \mu(f) = 2$ is the multiplicity of the point $(0,0)$. Hence, $\dim_K K[x,y]/\langle f_x, f_y\rangle = 5$, $\dim_K K[x,y]/\langle f, f_x, f_y\rangle = 4$.

A standard basis of $\langle f_x, f_y\rangle_{\mathrm{Loc}\,K[x,y]} = \langle f; f_x, f_y\rangle_{\mathrm{Loc}\,K[x,y]}$, with respect to ds, is $\{y, x^2\}$ a standard basis of $\langle f_x, f_y\rangle_{K[x,y]}$, with regard to dp, is $\{xy - y, y^3 - y, 4x^3 - 3x^2 - y^2\}$ and a standard basis of $\langle f, f_x, f_y\rangle_{K[x,y]}$, with regard to dp, is $\{xy - y, x^2 - y^2, y^3 - y\}$.

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].

3.2 Deformations

Let $(V,0) \subset (\mathbb{C}^n, 0)$ be a singularity given by convergent power series $f_1(x), \ldots, f_k(x)$, 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 $F_1(t,x), \ldots, F_k(t,x)$ 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

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

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

$$\begin{array}{ccll} (V,0) & \stackrel{i}{\hookrightarrow} & (\mathcal{U},0) & = \{(t,x) \in S \times U \mid F_1(t,x) = \cdots = F_k(t,x) = 0\} \\ \downarrow & & \downarrow \ \phi & \\ \{0\} & \in & (S,0) & \end{array}$$

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 $\sum r_i(x) f_i(x) = 0$ between the f_i lifts to a relation $\sum R_i(t,x) F_i(t,x)$, $R_i(x,0) = r_i(x)$, between the F_i. Equivalently, for any generator $(r_1, \ldots, r_k)$ of $\mathrm{syz}(\langle f_1, \ldots, f_k \rangle)$ there exists an element $(R_1, \ldots, R_k) \in \mathrm{syz}(\langle F_1, \ldots, F_k \rangle)$ satisfying $R_i(0,x) = r_i(x)$.

The notion of flatness is not easy to explain geometrically. Mumford [Mu] states: "The concept of flatness is a riddle that comes out of algebra, but which is technically the answer to many prayers." 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 [Schl1] for the formal case), every isolated singularity admits a semi-universal or mini-versal deformation $\phi : (\mathcal{U}, 0) \longrightarrow (S, 0)$ of $(V, 0)$, which, in some sense, contains the information upon all possible deformations.

Definition 3.1. A deformation $\phi : (\mathcal{U}, 0) \longrightarrow (S, 0)$ of $(V, 0)$ is **semi-universal**, if the following holds:

1) Any deformation $(\mathcal{U}', 0) \xrightarrow{\phi'} (S', 0)$ is isomorphic to the pull–back $\varphi^*)(\phi)$ by some map $\varphi : (S', 0) \longrightarrow (S, 0)$, φ is not unique but may be prescribed on a subspace of $(S', 0)$.

2) The (Zariski) tangent map of φ is unique.

Property 1) is called the "versality" property, 2) the "semi-universality". Once the semi-universal deformation (which is unique up to isomorphism) of $(V, 0)$ is known, "all" deformations of $(V, 0)$ are known (in the sense of 1)).

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]; for an elaboration of this, see the recent article of Martin [Ma]. (This algorithm has been implemented in SINGULAR.)

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

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

where $1 = g_1, g_2, \ldots, g_\tau$ represent a basis of the Tjurina algebra $K\langle x\rangle /\langle f, f_{x_1}, \ldots, f_{x_n}\rangle$, τ being the Tjurina number.

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

Algebraically, deformations can be described on the algebra level. Let $R = K[x_1, \ldots, x_n]/I$ be an affine algebra or $R = K\langle x_1, \ldots, x_n\rangle/I$ an analytic algebra. A **deformation** of R over a local ring (A, m) with $K = A/m$ is a cartesian diagram,

$$\begin{array}{ccl} R & \twoheadleftarrow & R_A \\ \uparrow & & \uparrow \text{flat} \\ K & \twoheadleftarrow & A. \end{array}$$

As in the geometric situation, we have the notion of a **formal (semi–uni)versal deformation**, where, in part 1) of the definition, we consider only deformations over Artinian algebras A.

If R has only isolated singularities, a formal semi-universal deformation of R exists by the theorem of Schlessinger [Schl1], which even has algebraic representation by Elkik [El] (cf. also [Ar], [KPR].

Consider now "the thick point"

$$T_\varepsilon = \operatorname{Spec} K[\varepsilon], \varepsilon^2 = 0,$$

which is a point, together with a tangent direction.

Definition 3.2.

1) A **first–order infinitesimal deformation** of $(V, 0)$ is, by definition, a deformation of $(V, 0)$ over T_ε. The $\mathcal{O}_{V,0}$–module of isomorphism classes of first–order infinitesimal deformations of $(V, 0)$ is denoted by

$$T^1_{V,0}.$$

2) $\tau(V,0) := \dim_K T^1_{V,0}$ is called the **Tjurina number** of $(V,0)$.

If $(V,0)$ has an isolated singularity, then $\tau(V,0)$ is finite, the converse is, in general, not true, but holds for hypersurface singularities or, more generally, for complete intersections.

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 $K\langle x_1,\ldots,x_n\rangle$ for the polynomial ring over the field K as well as for power series ring over K.

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

An **embedded deformation of R** over an analytic algebra $A = K\langle t_1,\ldots,t_m\rangle/J = K\langle t\rangle/J$ 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,

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

lifts to a relation between the F_i,

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

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

By definition, $F_1,\ldots,F_k$ and $F_1',\ldots,F_k'$ define the same embedded deformation, if they generate the same ideal.

Setting

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

we obtain a commutative cartesian diagram

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

with φ flat, which is called a **deformation of R over A** (and which is just the algebraic translation of the geometric definition). Two deformations $A \longrightarrow R_A$ and $A \longrightarrow R'_A$ 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 $\mathrm{Spec}(K[\varepsilon])$ 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 3.1.

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

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

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

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

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

Proof. [Schl2]

1) Given an infinitesimal deformation

$$F_i(\varepsilon, x) = f_i(x) + \varepsilon g_i(x),$$

then $(g_1,\dots,f_k)$ determines an element of

$$N_R = \mathrm{Hom}_R(I/I^2, R) \cong \mathrm{Hom}_{K\langle x\rangle}(I, R)$$

by $\sum a_i f_i \mapsto \sum a_i g_i$. This map from I to R is well–defined by the flatness assumption: a relation $\sum r_i f_i = 0$ lifts to a relation $\sum (r_i + \varepsilon s_i)(f_i + \varepsilon g_i) = 0$, whence $\varepsilon \sum (s_i f_i + r_i g_i) = 0$, which implies $\sum r_i g_i \in I$.

Conversely, given $\varphi : I \longrightarrow R$, choose a representative

$$(g_1, \ldots, g_k) \in K[\langle x \rangle^k$$

of $\big(\varphi(f_1), \ldots, \varphi(f_k)\big) \in R^k$, defining a deformation $f_i + \varepsilon g_i$ of R.

To verify the flatness condition, let $\sum r_i f_i = 0$. Then $\sum r_i \varphi(f_i) = 0$, hence, $\sum r_i g_i = -\sum s_i f_i \in I$, which defines a lifting of the relations. Moreover, if g_i' are different liftings of $\varphi(f_i)$ we have $g_i' - g_i = \sum\limits_j c_{ji} f_j \in I$. Therefore,

$$\begin{aligned}(f_1 + \varepsilon g_1', \ldots, f_k + \varepsilon g_k') &= (f_1 + \varepsilon g_1, \ldots, f_k + \varepsilon g_k) + \varepsilon (f_1, \ldots, f_k) \cdot C \\ &= (f_1 + \varepsilon g_1, \ldots, f_k + \varepsilon g_k)(\mathbb{1} + \varepsilon C),\end{aligned}$$

with $C = (c_{ji})$ showing that the two liftings define the same embedded deformation.

2) An infinitesimal deformation $F_i = f_i + \varepsilon g_i$ is trivial, if and only if

$$K\langle \varepsilon, x \rangle / \langle F_1, \ldots, F_k \rangle \cong K\langle \varepsilon, x \rangle / \langle f_1, \ldots, f_k \rangle,$$

that is, if there is an auto-morphism φ of $K\langle \varepsilon, x \rangle$ over $K\langle \varepsilon \rangle$, $x_j \mapsto x_j + \varepsilon \delta_j(x)$, $\delta_j \in K\langle x \rangle$, such that

$$\big\langle f_i\big(x + \varepsilon \delta(x)\big)\big\rangle = \langle f_i + \varepsilon g_i \rangle.$$

Taylor's formula gives $f_i\big(x + \varepsilon \delta(x)\big) = f_i(x) + \varepsilon \sum\limits_j \frac{\partial f_i}{\partial x_j}(x) \delta_j(x)$, which shows that for a trivial deformation,

$$g_i(x) = \partial(f_i) \in I$$

with $\partial = \sum\limits_j \delta_j(x) \frac{\partial}{\partial x_i} \in \operatorname{Der}_K K\langle x \rangle$, that is, $(g_1, \ldots, f_k)$ is in the image of α. Conversely, any element from the image of α defines a trivial deformation.

Let $\operatorname{Def}_R(A)$ denote the set of isomorphism classes of deformations of R over the analytic K–algebra A. Part 2) of the proposition states

$$\operatorname{Def}_R(K[\varepsilon] =\cong T_R^1.$$

□

Remarks:

1) Schlessinger's theorem [Schl1] states that R admits a formal semi-universal deformation $B \longrightarrow R_B = B\langle x \rangle / \langle F_1, \ldots, F_k \rangle$ 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 $R = K[x_1, \ldots, x_n]/I$ if the affine variety $V(I)$ has only isolated singularities (necessarily finitely many) or in the analytic case $R = K\langle x_1, \ldots, x_n \rangle / I$ if the singularity $\big(V(I), 0\big)$ has an isolated singularity.

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

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 $\operatorname{Spec} B$ at the maximal ideal of B. This shows, with $t_1, \ldots, t_m$ a K–basis of T_R^{1*}, that $B \cong K\langle T_R^1\rangle/J \cong K\langle t_1, \ldots, t_m\rangle/J$ 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 $t_1, \ldots, t_m$ of a K–basis of the dual of T_R^1 and these relations generate J.

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

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

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

Now choose a resolution of N_R

$$\begin{tikzcd}
R^k & R^s \arrow[l, "s_1"'] \arrow[dl] & R^t \arrow[l, "s_2"'] \\
N_R \arrow[u, phantom, sloped, "\subseteq"] & &
\end{tikzcd}$$

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 $\left(\frac{\partial f_i}{\partial x_j}\right)_{\substack{i \le k \\ j \le n}}$. 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.

$$
\begin{tikzcd}
R^l & R^k \arrow[l, "r^t"'] & & R^s \arrow[ll, "s_1"'] \arrow[dl] & R^t \arrow[l, "s_2"'] \\
& & N_R \arrow[ul] & & \\
& & R^n \arrow[u, "\pi"] \arrow[uul, "j"] \arrow[uur, dashed, "lj"'] & &
\end{tikzcd}
$$

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

$$0 \longleftarrow T^1_R \longleftarrow R^s \xleftarrow{s_2 \oplus lj} R^t \oplus R^n.$$

Algorithm 3.4.
T1(I)

Input: an ideal $I = \langle f_1, \ldots, f_k \rangle \subseteq K\langle x \rangle$,
Output: a matrix $M \in M_{a,b}(K\langle x \rangle)$ which defines a representation

$$T^1_{K\langle x \rangle/I} \twoheadleftarrow K\langle x \rangle^a \xleftarrow{M} K\langle x \rangle^b$$

- compute $r = \operatorname{syz}(I)$ the matrix of the syzygies of $f_1, \ldots, f_k$;
- 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 $M_0 \mod I = t1$;
- choose a matrix $L \in M_{s,k \cdot s}$ (corresponding to $IK\langle x \rangle^s$), such that

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

  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 $K[[t_1,\ldots,f_n]]$, $t_1,\ldots,t_n$ a K–basis of T_R^{1*}, and if J denotes the ideal generated by them, $B = K[[t_1,\ldots,t_m]]/J$ 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 $A = K\langle t_1,\ldots,t_n\rangle/\langle t_1,\ldots,t_n\rangle^2$.

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

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

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

$$\mathrm{Kos} = \langle f_i e_j - f_j e_i | 1 \le i < j \le j\rangle.$$

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

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

Proposition 3.2.

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*

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

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

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

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

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

Proof. 2) follows from 1) and Grothendieck's criterion for formal smoothness.

1) for simplicity we give the proof only for $A = K\langle t\rangle/\langle t^p\rangle$, $A' = K\langle t\rangle/\langle t^{p+1}\rangle$ with $J = \langle t^p\rangle/\langle t^{p+1}\rangle$.

So, we are given a deformation over A,

$$F_i(x,t) = f_i(x) + \sum_{j=1}^{p-.1} t^j g^i_j(x)$$

with relations (using the dot product for the corresponding vectors),

$$F(x,t)\cdot r(x;t) := \sum_{i=1}^{k} F_i(x,t) r_i(x,t) = 0 \in A\langle x\rangle.$$

We want to lift the deformation and the relations to A'. That is, we are looking for $g' \in K\langle x\rangle^k$ such that, setting

$$F'(x,t) = F(x,t) + t^{\wp} g'(x),$$

there exist

$$r'(x,t) = r(x,t) + t^{\wp} h'(x)$$

satisfying $F'(x,t)\cdot r'(x,t) = 0$ in $A'\langle x\rangle$.

A deformation over A is given by $F = (F_1, \ldots, F_k)$,

$$F_i(t,x) = f_i(x) + \sum_{\nu=1}^{p-1} t^\nu g^i_\nu(x) \in K\langle t,x\rangle$$

and a relation by $R = (R_1, \ldots, R_k)$

$$R_j(t,x) = r_j(x) + \sum^{p-1} \nu = 1 t^\nu h^j_\nu(x) \in K\langle t,x\rangle$$

satisfying

$$R(t,x)\cdot F(t,x) = \sum_1^k R_i(x,t)F_i(x,t) = 0$$

in $A\langle x\rangle = K\langle t,x\rangle/\langle t^p\rangle$.

We want to lift this deformation to A'. That is, we are looking for $g' \in K\langle x\rangle^k$ such that, setting

$$F'(t,x) = F(t,x) + t^p g'(x),$$

there exists for any relation $R(t,x)$ a lifting

$$R'(t,x) = R(t,x) + t^p h'(x)$$

satisfying $R'(t,x)\cdot F'(t,x) = 0$ in $A'\langle x\rangle = K\langle t,x\rangle/\langle t^{p+1}\rangle$. Computing the dot product $R'\cdot F'$, we obtain modulo $\langle t^{p+1}\rangle$, since $F\cdot R \in \langle t^p\rangle$,

$$\begin{aligned} R'\cdot F' &= T^p\left(\sum_{\nu=1}^{p-1} h_{p-\nu}g_\nu + h'\cdot f + r\cdot g'\right) \text{ in } J\otimes_K K\langle x\rangle \\ &= t^p(t^{-p}R\cdot F + r\cdot g') \text{ in } J\otimes_K R. \end{aligned}$$

It follows that the deformation given by F admits a lifting f' over A' if and only if $R'\cdot F' = 0$, which is equivalent to $t^{-p}RF$ being of the form $r\cdot g'$ for some $g'\in K\langle x\rangle^k$ (in $J\otimes_K R$). $\square$

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

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

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

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

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

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

$$\begin{tikzcd} K\langle x\rangle^k & & K\langle x\rangle^\ell \arrow[ll, "r"'] \arrow[dl] & K\langle x\rangle^t \arrow[l, "s"'] \\ & \mathrm{Rel} \arrow[ul] & & \\ & \mathrm{Rel}_0 \arrow[u] & & \\ K\langle x\rangle^{\binom{k}{2}} \arrow[uuu, "\mathrm{Kos}"] \arrow[ur] \arrow[uuurr, dashed, "l\,\mathrm{Kos}"'] & & & \end{tikzcd}$$

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

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

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

Now we are interested in a representation of $T^2_R = \operatorname{coker}\bigl(\operatorname{Hom}_R(R^k,R) \longrightarrow \operatorname{Hom}_R(\operatorname{Rel}/\operatorname{Rel}_0,R)\bigr)$.

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

$$\begin{array}{ccccccc}
0 & \to & \operatorname{Hom}_{K\langle x\rangle}(\operatorname{Rel}/\operatorname{Rel}_0,R) & \to & \operatorname{Hom}_{K\langle x\rangle}(K\langle x\rangle^\ell,R) & \xrightarrow{s\ell^t} & \operatorname{Hom}_{K\langle x\rangle}(K\langle x\rangle^{t_1},R) \\
 & & \| & & \| & & \| \\
 & & \operatorname{Hom}_R(\operatorname{Rel}/\operatorname{Rel}_0,R) & & \operatorname{Hom}_R(R^\ell,R) & & \operatorname{Hom}_R(R^{t_1},R),
\end{array}$$

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

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

$$\begin{tikzcd}
R^{t_1} & R^\ell \arrow[l, "s\ell^t"'] \arrow[dr, phantom, "\supseteq"] & & R^{\ell_1} \arrow[ll, "r_1"'] \arrow[dl] & R^{\ell_2} \arrow[l, "r_2"'] \\
 & & \operatorname{Hom}_R(\operatorname{Rel}/\operatorname{Rel}_0,R) & &
\end{tikzcd}$$

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

$$\begin{tikzcd}
R^\ell & & R^{\ell_1} \arrow[ll, "r_1"'] \arrow[dl] & R^{\ell_2} \arrow[l, "r_2"'] \\
 & \operatorname{Hom}(\operatorname{Rel}/\operatorname{Rel}_0,R) \arrow[ul] & & \\
 & R^k \arrow[u] \arrow[uul, "r^t"] \arrow[uur, dotted, "\ell rt"'] & &
\end{tikzcd}$$

Then $T^2_R = \operatorname{coker}\bigl(R^k \longrightarrow \operatorname{Hom}(\operatorname{Rel}/\operatorname{Rel}_0,R)\bigr) \simeq R^{\ell_1}/\operatorname{Im}(r_2)+\operatorname{Im}(\ell rt)$ gives the required representation

$$0 \longleftarrow T^2_R \longleftarrow R^{\ell_1} \xleftarrow{r_2\oplus\ell rt} R^{\ell_2}\oplus R^k.$$

We obtain the following algorithm:

Algorithm 3.5.
T2(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

$$T^2_{K\langle x\rangle/I} \twoheadleftarrow K\langle x\rangle^a \xrightarrow{M} K\langle x\rangle^b$$

- compute $r = \mathrm{syz}(I) \in M_{k,\ell}(K\langle x\rangle)$, the matrix of the syzygies of $f_1, \dots, f_k$ and $s = \mathrm{syz}(\mathrm{syz}(I)) \in M_{\ell,t}(K\langle x\rangle)$ to obtain a representation of $K\langle x\rangle/I$;
- compute the matrix Kos $\in M_{k,(k/2)}$, the Koszul matrix of the relations of $f_1, \dots, f_k$;
- lift Kos to a matrix $\ell\,\mathrm{Kos} \in M_{\ell,(k/2)}$ such that $r \cdot \ell\,\mathrm{Kos} = \mathrm{Kos}$;
- concatenate $\ell\,\mathrm{Kos}$ and s to obtain the matrix $s\ell = \ell\,\mathrm{Kos}, s \in M_{\ell,(k/2)+t}$;
- compute in $K\langle x\rangle/I$ a representation of the kernel $\ker(s\ell^t)$ given by matrices r_1 and r_2 $\big(r_1 = \mathrm{syz}(s\ell^t) \in M_{\ell,\ell_1}(K\langle x\rangle/I)$, $r_2 = \mathrm{syz}(r_1) \in M_{\ell_1,\ell_2}(K\langle x\rangle/I)\big)$;
- lift the matrix r^t to a matrix $\ell rt \in M_{\ell_1,k}(K\langle x\rangle/I)$ such that $r_1 \cdot \ell rt = r^t$;
- concatenate ℓrt and r_2 to obtain the matrix $t2 = \ell rt, r_2 \in M_{\ell_1,k+\ell_2}(K\langle x\rangle/I)$;
- choose a matrix $M_0 \in M_{\ell_1,k+\ell_2}(K\langle x\rangle)$ such that $M_0 \mod I = t2$;
- choose a matrix $L \in M_{\ell_1,k\cdot\ell_1}$ (corresponding to $IK\langle x\rangle^{\ell_1}$) such that

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

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

References

[ADHP] Aure, A.; Decker, W.; Hulek, K.; Popescu,S.; Ranestad, K: Syzygies of abelian and bielliptic surfaces in $\P_4$. (to appear in International J. Math.)

[ADS] Abo, H.; Decker, W.; Sasakura, N.: An elliptic conic bundle in $\P_4$ arising from a stable rank-3 vector bundle. (submitted to Math. Z.)

[AM] Atiyah, M.F.; Macdonald, I.G.: Introduction to commutative algebra. Addison–Wesley, London (1969).

[Ar] Artin, M.: Lectures on deformations of singularities. Tata Institute, Bombay (1976).

[BE] Bayer, D.; Eisenbud, D.: Graph curves. Advances in Math. **86**, 1–40 (1991).

[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.: Gröbner bases: an algorithmic method in polynomial ideal theory. In: Recent trends in multidimensional system theory, N.B. Bose, ed., Reidel (1985).

[Bu3] Buchberger, B.: Introduction to Gröbner bases. This volume.

[BW] Becker, E.; Wörmann, T.: Radical computations of zero–dimensional ideals and real root counting. Mathematics and Computers in Simulation 42, 561–569 (1996).

[BWe] Becker, T.; Weispfennig, V.: Gröbner Bases, A Computational Approach to commutative Algebra. Graduate Texts in Mathematics 141, Springer 1993.

[CCT] Caboara, M.; Conti, P.; Traverso, C.: Yet another ideal decomposition algorithm. To appear in AAECC Proceedings.

[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.

[DES] Decker, W.; Ein, L.; Schreyer, F.-O.: Construction of Surfaces in $\P_4$. J. Algebraic Geometry **2**, 185–237 (1993).

[DMS] Decker, W.; Manolache, N.; Schreyer, F.-O.: Geometry of the Horrocks-bundle on ¶$_5$. In: Complex Projective Geometry. London Math. Soc. Lecture Notes Series 179, 128–148 (1992).

[DNS] Decker, W.; Narasimhan, M.S.; Schreyer, F.-O.: Rank 2 vector bundles on ¶$_4$ with c_1 odd and contact curves. Math. Z. **205**, 123–136 (1990).

[DP] Decker, W.; Popescu, S.: On surfaces in ¶$_4$ and 3-folds in ¶$_5$. In: Vector Bundles in Algebraic Geometry, Cambridge Univ. Press (1995).

[EDS] Eisenbud, D., Diaconis, P.; Sturmfels, B.: Lattice walks and primary decomposition. To appear in the Rotafest Proceedings 1996.

[Ei] Eisenbud, D: Commutative Algebra with a view toward Algebraic Geometry. Springer 1995.

[Ei2] Eisenbud, D.: Introduction to algebras with straightening laws. In Ring Theory and algebra III, Norman Oklahoma (1979), Lect. Notes in pure and appl. Math., Marcel Dekker, New York 243–268 (1980).

[EHV] Eisenbud, D.; Huneke, C.; Vasconcelos, W.: Direct methods for primary decomposition. Invent. math. 110, 207–235 (1992).

[EK] Eisenbud, D.; Koh, J.: Nets of skew forms and the linear syzygy conjecture, Adv. in Math. **106** 1–35, (1994).

[El] Elkrik ??????????????????????????????????????

[EPS] Eisenbud, D.; Peeva, I.; Sturmfels, B.: Noncommutative Gröbner bases for commutative ideals. To appear in Proc. Am. Math. Soc.

[ER] Eisenbud, D.; Robbiano, L.: Open Problems in Computational Algebraic Geometry and commutative Algebra. In Computational Algebraic Geometry and Commutative Algebra, Cortona 1991, Cambridge University Press, Cambridge, England, 49–71 (1993).

[ERS] Eisenbud, D.; Riemenschneider, O.; Schreyer, F.-O.: Resolutions of Cohen-Macaulay Algebras. Math Ann.**257** (1981).

[ERT] Eisenbud, D.; Reeves, A.; Totaro, B.: Initial ideals of Veronese subrings. Advances in Math. **109** 168–187 (1994).

[ES1] Eisenbud, D.; Sturmfels, B.: Finding sparse systems of parameters. J. of Pure and Appl. Alg. **94** 143–157 (1994).

[ES2] Eisenbud, D.; Sturmfels, B.: Binomial ideals. Duke Math. J. 84 1–45 (1996).

[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).

[GP3] Greuel, G.-M.; G.Pfister: Geometric quotients of unipotent group actions II. Accepted for the Brieskorn–Festschrift, Birkhaeuser.

[GP2] Greuel, G.-M.; G.Pfister: On moduli spaces of semiquasihomogeneous singularities. In Progress in Mathematics, Vol. 134, Birkhäuser 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.

[GMT] Gianni, P.; Miller, V.; Trager, B.: Decomposition of algebras. ISSAC 88, Springer LNC 358, 300–308.

[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.

[GTZ] Gianni, P.; Trager, B.; Zacharias, G.: Gröbner Bases and Primary Decomposition of Polynomial Ideals. J. Symbolic Computation 6, 149–167 (1988).

[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.

[Ka] Kalkbrenner, M.: Prime decomposition of radicals in polynomial rings. J. Symbolic Computation 18, 365–372 (1994).

[KL] Krick, T.; Logar, A.: An algorithm for the computation of the radical of an ideal in the ring of polynomials. AAECC9, Springer LNCS 539, 195–205.

[KPR] (1975) ???????????????????????????????????????

[Ku] Kunz, E.: Einführung in die kommutative Algebra und algebraische Geometrie. Vieweg (1980).

[KS] Kollár, J.; Schreyer, F.-O.: The Moduli of Curves is Stably Rational for $g \geq q6$. Duke Math. J. **51** (1984).

[La] Laudal, O.A.: Formal Moduli of Algebraic Structures. LNM **754**, Springer (1979).

[M] Matsumura, H.: Commutative ring theory, Cambridge studies in advanced math. 8.

[Ma] Martin, B.: Computing Massey products using SINGULAR. Preprint M-02, Cottbus (1996).

[Mat] ?????????????????????????????

[Mi] Mishra, B: Algorithmic Algebra, Texts and Monographs in Computer Science, Springer, 1993.

[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. AAECC 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).

[Mu] Mumford, D.: The Red Book of Varieties and Schemes, LNM **1358**, Springer (1989).

[MS] Martens, G.; Schreyer, F.-O.: Syzygies and line bundles of trigonal curves. Abh. Math. Sem. Hamburg **56** (1986).

[PS] Peeva, I.; Sturmfels, B.: Generic lattice ideals. To appear in Journal of the American Mathematical Society.

[Ro] ???????????????

[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).

[Se] Seidenberg, A.: Construction of the integral closure of a finite integral domain II. Proc. Amer. Math. Soc. 52, 368–372 (1975).

[SS] Scheja, G.; Storch, U.: Über Spurfunktionen bei vollständigen Durchschnitten. J. reine angew. Math. 278, 174–190 (1975).

[St] Sturmfels, B.: Algorithms in Invariant Theory. Springer Verlag (1993).

[SY] Shimoyama, T.; Yokoyama, K.: Localization and Primary Decomposition of Polynomial ideals. J. Symbolic Computation 22, 247–277 (1996).

[St] Stolzenberg, G.: Constructive normalization of an algebraic variety. Bull. Amer. Math. Soc. 74, 595-599 (1968).

[V1] Vasconcelos, W.: Computing the integral closure of an affine domain. Proc. AMS 113 (3), 633–638 (1991).

[V2] Vasconcelos, W.: Arithmetic of Blowup Algebras. Lecture notes of the London Math. Soc. 195 (1994).

[V3] Vasconcelos, W. ????????????????

[W] Wang, D.: Irreducible Decomposition of Algebraic Varieties via Characteristic Sets and Gröbner Bases. Computer Aided Geometric Design 9, 471–484 (1992).