Primary Decomposition: Algorithms and Comparisons

Wolfram Decker[1] Gert-Martin Greuel[2] and Gerhard Pfister[2]

[1] Universität des Saarlandes, Fachbereich 9 Mathematik, Postfach 151 150, D-66041 Saarbrücken
[2] Universität Kaiserslautern, Fachbereich Mathematik, Erwin-Schrödinger-Strasse, D-67663 Kaiserslautern

1 Introduction

Primary decomposition of an ideal in a polynomial ring over a field belongs to the indispensable theoretical tools in commutative algebra and algebraic geometry. Geometrically it corresponds to the decomposition of an affine variety into irreducible components and is, therefore, also an important geometric concept.

The decomposition of a variety into irreducible components is, however, slightly weaker than the full primary decomposition, since the irreducible components correspond only to the minimal primes of the ideal of the variety, which is a radical ideal. The embedded components, although invisible in the decomposition of the variety itself, are, however, responsible for many geometric properties, in particular, if we deform the variety slightly. Therefore, they cannot be neglected and the knowledge of the full primary decomposition is important also in a geometric context.

In contrast to the theoretical importance, one can find in mathematical papers only very few concrete examples of non–trivial primary decompositions because carrying out such a decomposition by hand is almost impossible. This experience corresponds to the fact that providing efficient algorithms for primary decomposition of an ideal $I \subset K[x_1, \ldots, x_n]$, K a field, is also a difficult task and still one of the big challenges for computational algebra and computational algebraic geometry.

All known algorithms require Gröbner bases respectively characteristic sets and multivariate polynomial factorization over some (algebraic or transcendental) extension of the given field K. The first practical algorithm for computing the minimal associated primes is based on characteristic sets and the Ritt–Wu process ([R1], [R2], [Wu], [W]), the first practical and general primary decomposition algorithm was given by Gianni, Trager and Zacharias [GTZ]. New ideas from homological algebra were introduced by Eisenbud, Huneke and Vasconcelos in [EHV]. Recently, Shimoyama and Yokoyama [SY] provided a new algorithm, using Gröbner bases, to obtain the primary decompositon from the given minimal associated primes.

In the present paper we present all four approaches together with some improvements and with detailed comparisons, based upon an analysis of 34 examples using the computer algebra system SINGULAR [GPS]. Since primary decomposition is a fairly complicated task, it is, therefore, best explained by dividing it into several subtasks, in particular, while sometimes only one of these subtasks is needed in practice. The paper is organized in such a way that we consider the subtasks separately and present the different approaches of the above–mentioned authors, with several tricks and improvements incorporated. Some of these improvements and the combination of certain steps from the different algorithms are essential for improving the practical performance.

Section 2 contains the algorithms. After explaining some important splitting tools, we explain two different approaches for computing the radical of I respectively the radical of the equidimensional hull. In Subsection 2.2 we present two algorithms for computing the equidimensional hull itself and a weak, that is, up to radical, decomposition of the equidimensional hull.

The algorithms of [GTZ] and [EHV] both reduce the general problem to primary decomposition of zero–dimensional ideals. We, therefore, consider the 0–dimensional case, together with some theoretical background, in Subsection 2.3.

In Subsection 2.4 we describe the three algorithms of [GTZ], [EHV] and [SY] for the general case, together with an algorithm to compute the minimal associated primes of I. The algorithm of [EHV] uses the normalization of $K[x_1, \ldots, x_n]/I$ and we present a new algorithm ([J]), based on a criterion of Grauert and Remmert, in Subsection 2.5. Another algorithm for computing the minimal associated primes is based on characteristic sets and this is presented, together with some basic facts about characteristic sets, in Subsection 2.6.

Section 3 is devoted to the examples and comparisons of the different approaches. The examples were taken from a still larger list and they demonstrate our present knowledge about the relative performance. Our table on the last page shows that a general best strategy does not exist. Generally speaking, the characteristic set method has problems if the examples require too many factorizations over extension fields, while [GTZ] has problems if the examples require going to general position by a random coordinate change. So far, we can only recommend a combination of the different subalgorithms, depending on the example. In contrast to the opinion of some authors, our experience is that one should use factorization as often as possible, since usually the Gröbner bases computations are the hardest part. This is, in particular, true for the algorithm computing the minimal primes, where we use the factorizing Gröbner, but also there are exceptions. We are aware of the fact that comparison of algorithms by examples is certainly affected by the choice of the examples and by tricky implementation features. On the other hand, the present paper appears to be the first systematic comparison of the four, so far, most important algorithms under equal conditions.

All algorithms presented in this paper are, or are about to be, implemented in SINGULAR with options for the user to combine his own favourite subalgorithms and are available in the library primdec.lib and distributed with the programme (cf. [GPS]).

Throughout this paper, we assume that Gröbner bases computations and multivariate polynomial factorization are possible over all fields considered. All Gröbner bases are minimal, if not mentioned otherwise. For some assertions and algorithms, if $\mathrm{char}(K) = p$, we need to assume $p = 0$ or $p >> 0$.

Acknowledgement: the authors were supported by the Deutsche Forschungsgemeinschaft through projects within the Schwerpunktprogramm.

2 The Algorithms

In this section, K is a field, $R = K[x_1, \dots, x_n]$, and $I \subseteq R$ is an ideal.

Our aim is to explain how to compute several decompositions of I, its radical $\sqrt{I}$, and the normalization of the factor ring R/I. Our main tools are Gröbner bases, but, for a complete primary decomposition, we also need multivariate polynomial factorization. All algorithms presented in this note are, or are about to be, implemented in SINGULAR.

If $I = \bigcap\limits_{i=1}^{r} Q_i$ is a minimal primary decomposition (that is, r is minimal) with associated primes $P_i = \sqrt{Q_i}$, then we write $E_v(I) := \bigcap\limits_{\mathrm{codim}(Q_i)=v} Q_i$ for the equidimensional part of I of codimension v (if $\mathrm{codim}(Q_i) \neq v$ for all i let $E_v(I) = R$).

We are interested in solving the following problems:

1. Compute the equidimensional hull $E_c(I)$, $c = \mathrm{codim}(I)$.
2. More generally, compute the equidimensional decomposition of I, that is, for $v \geq c$ compute $E_v(I)$.

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

3. Compute $\mathrm{Ass}(I) = \{P_1, \dots, P_r\}$ and $\mathrm{minAss}(I) = \{P_i \in \mathrm{Ass}(I) \mid P_i \subsetneqq Pj$ for $i \neq j\}$.
4. Compute the radical $\sqrt{I} = \bigcap\limits_{i=1}^{r} P_i = \bigcap\limits_{P \in \min \mathrm{Ass}(I)} P$ and the equidimensional radical $\sqrt[\mathrm{equi}]{I} = \sqrt{E_c(I)}$, $c = \mathrm{codim}(I)$.
5. Compute, for I radical, the normalization of R/I, that is the integral closure of R/I in its quotient ring $Q(R/I)$.
6. Compute a minimal primary decomposition of I.

Splitting tools may allow the reduction of a given problem to a problem involving ideals which are easier to handle.

Lemma 1 (splitting tools). *Let $I \subseteq R$ be an ideal.*

1. *If $I : f = I : f^2$ for some $f \in R$, then $I = (I : f) \cap \langle I, f \rangle$.*
2. *If $f \cdot g \in I$, and $\langle f, g \rangle = R$, then $I = \langle I, f \rangle \cap \langle I, g \rangle$.*
3. *If $f \cdot g \in I$, then $\sqrt{I} = \sqrt{\langle I, f \rangle} \cap \sqrt{\langle I, g \rangle}$.*
4. *If $f^n \in I$, then $\sqrt{I} = \sqrt{\langle I, f \rangle}$.*
5. *If $J \subseteq R$ is an ideal, then $\sqrt{I} = \sqrt{I : J} \cap \sqrt{I + J} = \sqrt{I : J} \cap \sqrt{I : (I : J)}$.*

Remark 2. Our experience shows that in all algorithms one should use Lemma 1 to split the ideal as often as possible.

Remark 3. Polynomials f as in Lemma 1, 1. can be found via saturation: if $I : h^\infty = I : h^N$, then $I = (I : h^N) \cap \langle I, h^N \rangle$. If $h_1 \cdot \ldots \cdot h_s$ is the square–free part of h, then we may replace h^N by $h_1^{k_1} \cdot \ldots \cdot h_s^{k_s}$, where $I : h^\infty = I : h_1^{k_1} \cdot \ldots \cdot h_s^{k_s}$. In fact, we may compute $I : h^\infty$ via ideal quotients by successively increasing the powers of the h_i.

This idea applies, in particular, in the following case.

Lemma 4. *Let $I \subseteq K[x]$, $x = \{x_1, \ldots, x_n\}$, be an ideal, and let $u \subseteq x$ be a subset of variables. Fix a block–ordering $<$ on $K[x]$ with $u << x \smallsetminus u$, that is, with $x_a < x_b$ whenever $x_a \in u$ and $x_b \in x \smallsetminus u$. Let S be a Gröbner basis of I with respect to $<$. Then S is a (not necessarily minimal) Gröbner basis of $IK(u)[x \smallsetminus u]$ with respect to the order $<$ restricted to $x \smallsetminus u$. Set $h = \mathrm{lcm}\{\mathrm{lc}(g) \mid g \in S\}$, where $\mathrm{lc}(g) \in K[u]$ is taken of g as a polynomial in $K(u)[x \smallsetminus u]$. Then*

1. *$IK(u)[x \smallsetminus u] \cap K[x] = (I : h^\infty)$.*
2. *Assume that $IK(u)[x \smallsetminus u] = \sqrt{IK(u)[x \smallsetminus u]}$. Then $\sqrt{I} = (I : h^\infty) \cap \sqrt{\langle I, h \rangle}$.*

An important application of extension and contraction as in Lemma 4 reflects the dimension of I. In fact, the following may be taken as a definition of $\dim(I)$:

$$\dim(I) = \max\{\#u \mid u \subseteq x, u \text{ is independent mod } I\}.$$

Recall that u is independent mod I if $I \cap k[u] = \{0\}$. In particular, I is zero–dimensional if and only if I contains for each i a non–constant polynomial in the variable x_i. Let

$$\mathcal{X}_I := \{u \subseteq x \mid u \text{ is a maximal independent set mod } I \text{ with } \#u = \dim(I)\}.$$

Then for $u \in \mathcal{X}_I$ the extension $IK(u)[x \smallsetminus u]$ is zero–dimensional, and the contraction $IK(u)[x \smallsetminus u] \cap K[x]$ is equidimensional of dimension $\dim(I)$.

Instead of computing $\mathcal{X}_I$ it is much easier to compute the (possibly proper) subset $\mathcal{X}_I^< := \mathcal{X}_{L(I)}$, where $<$ is a given admissible term–ordering on $K[x]$, and $L(I)$ is the corresponding leading or initial ideal of I.

2.1 Radicals

We shall describe two different approaches to the computation of radicals. Another approach, which will not be treated here, is due to Becker and Wörmann ([BW]).

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

Proposition 5. *Let $I \subseteq K[x_1, \ldots, x_n]$ be a zero–dimensional ideal. For $i = 1, \ldots, n$ let $F_i(x_i) \in K[x_i] \cap I$ be a polynomial of minimal degree, and let $L_i(x_i)$ be the square free part of F_i. Then $\sqrt{I} = I + \langle L_1, \ldots, L_n \rangle$.*

The general case can be reduced to the zero–dimensional case via Lemma 4.

Algorithm 1.

RADICAL(I)
Input: an ideal I in $K[x_1, \ldots, x_n]$
Output: $\sqrt{I}$

- choose any admissible term–ordering $<$ on $K[x_1, \ldots, x_n]$;
- use the factorizing Gröbner basis algorithm to split I;
  the result $\mathfrak{m}$ is a set of ideals given by Gröbner bases such that
  - all elements of the 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 $\mathcal{X}_J^<$;
  - Result := $\langle 1 \rangle$, $W := J$;
  - for $u \in \mathcal{X}_J^<$ do
    - $*$ compute a Gröbner basis S of W with respect to a block–ordering $<$ with $u << x \smallsetminus u$;
    - $*$ using linear algebra and the Gröbner basis S, compute for all $x_i \in x \smallsetminus u$ a polynomial $F_i(x_i)$ such that $\langle F_i(x_i) \rangle = WK(u)[x \smallsetminus u] \cap K(u)[x_i]$;
    - $*$ compute the square free part L_i of F_i;
    - $*$ compute a Gröbner basis T of $WK(u)[x \smallsetminus u] + \langle \{L_i | x_i \in x \smallsetminus u\} \rangle$ such that the elements of T are polynomials in $K[x]$;
    - $*$ compute the least common multiple $h \in K[u]$ of the leading coefficients of the elements in T as in Lemma 4;
    - $*$ compute Result := Result $\cap (\langle T \rangle : h^\infty)$ in $K[x]$;
    - $*$ $W := \langle W, h \rangle$;
  - (at this point Result equals the equidimensional radical of J if $\dim W < \dim J$; this condition is not necessarily fulfilled since $\mathcal{X}_J^<$ might be a proper subset of $\mathcal{X}_J$);
  - Result := Result $\cap$ RADICAL(W);
- return Result

A quite different approach is due to Eisenbud, Huneke, and Vasconcelos ([EHV]). We suppose that K is a field of characteristic 0, or of characteristic $p > 0$, p sufficiently large.

Let $A = K[x_1, \ldots, x_n]/I$ be a K–algebra of finite type. We denote by $J_a(A)$ the a–th fitting ideal of the module of Kähler differentials $\Omega_{A|K}$, and by $J_a(I)$ the pull–back of $J_a(A)$ in $K[x_1, \ldots, x_n]$. Recall that if $I = \langle f_1, \ldots, f_m \rangle$, then $J_a(I) = I +$ the ideal generated by the $(n-a)$–minors of the Jacobian matrix $\left(\frac{\partial f_i}{\partial x_j}\right)$. Note, that the formation of $J_a(A)$ commutes with localization and base change.

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

Theorem 6. *Let A be a local Artinian K–algebra with maximal ideal $\mathcal{M}_A$. Then A is a complete intersection if and only if $(0) : J_0(A) = \mathcal{M}_A$.*

In our case $A = K[x_1, \ldots, x_n]/I$; this result can be formulated as follows. Let $I \subseteq K[x_1, \ldots, x_n]$ be an $\langle x_1, \ldots, x_n\rangle$–primary ideal. Then I is a complete intersection if and only if $I : J_0(I) = \langle x_1, \ldots, x_n\rangle$.

Corollary 7. *Let $I \subseteq K[x_1, \ldots, x_n]$ be a complete intersection of dimension d. Then $\sqrt{I} = I : J_d(I)$.*

Corollary 8. *Let $I \subseteq K[x_1, \ldots, x_n]$ be an equidimensional ideal of codimension c and $f_1, \ldots, f_c \in I$ a regular sequence. If $I_0 = \langle f_1, \ldots, f_c\rangle$, then*

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

Remark 9. Write $I = I_1 \cap I_2$, where I_1 is the equidimensional part of I intersected with the embedded components corresponding to the equidimensional part, and where I_2 is the remaining 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.

EQUIRADICAL(I)
Input: an ideal I in $K[x_1, \ldots, x_n]$
Output: the radical of the equidimensional hull of I

- choose any admissible term–ordering $<$ on $K[x_1, \ldots, x_n]$;
- compute a Gröbner basis of I and $c := \text{codim}(I)$;
- choose a regular sequence $f_1, \ldots, f_c$ in I (try the first c elements of a minimal set of generators of I; if this does not work, choose c elements as generic linear combinations of the generators of I with coefficients in K);
- compute the Jacobian ideal $J_0 := J_{n-c}(I_0)$ of $I_0 := \langle f_1, \ldots, f_c\rangle$;
- compute $\sqrt{I_0} = I_0 : J_0$;
- return $\sqrt{I_0} : (\sqrt{I_0} : I)$

Algorithm 3.

RADICAL(I)
Input: an ideal I in $K[x_1, \ldots, x_n]$
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($I : I_1^N$)

The main drawback of Algorithms 2 and 3 is the computation of regular sequences via random linear combinations. A second approach of Eisenbud, Huneke, and Vasconcelos ([EHV]) avoids the computation of regular sequences. This is based on

Proposition 10. *Let K be a perfect field, and let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal of dimension d. If K has characteristic $p > 0$, suppose that the nil–radical of $K[x_1, \ldots, x_n]/I$ is generated by elements whose index of nil–potency is smaller than p. If for some $a \geq d$*

$$\dim J_{a+1}(I) < d \ ,$$

then $I_1 := I : J_a(I)$ has the same equidimensional radical as I. If $a = d$ then I_1 is radical in dimension d, that is, the primary components of I_1 having dimension d are prime.

The proof of Proposition 10 relies on the following

Theorem 11. *Let K be a perfect field, $A = K[x_1, \ldots, x_n]/I$ and $P \supset I$ a prime ideal. Then the following conditions are equivalent:*

1. $(\Omega_{A|K})_P$ *is free of rank d;*
2. $I : J_{d-1}(I) \not\subset P$ *and* $J_d(I) \not\subset P$;
3. A_P *is regular of dimension d.*

Algorithm 4.

EquiRadical(I)
Input: an ideal I in $K[x_1, \ldots, x_n]$
Output: the radical of the equidimensional hull of I

- choose any admissible term–ordering $<$ on $K[x_1, \ldots, x_n]$;
- compute a Gröbner basis of I and $d := \dim(I)$;
- $a := n - 1$;
- while $a > d$ do
  - while $\dim J_a(I) = d$ do
    $I := I : J_a(I)$;
  - $a := a - 1$;
- return $I : J_d(I)$

2.2 Equidimensional Hulls and Equidimensional Decompositions

Again we present two different approaches. The first approach, which is used in several papers ([GTZ], [KL], ...), is based on Lemma 4.

Algorithm 5.

Equidimensional(I)
Input: an ideal I in $K[x_1, \ldots, x_n]$
Output: two ideals, the equidimensional hull $E_c(I)$ of I ($c = \operatorname{codim} I$), and an ideal W of codimension $> c$ such that $I = E_c(I) \cap W$

- choose any admissible term–ordering $<$ on $K[x_1, \ldots, x_n]$;
- compute $c := \operatorname{codim}(I)$;

- compute $\mathcal{X}_I^<$;
- Result := $\langle 1\rangle$, $W := I$;
- for $u \in \mathcal{X}_I^<$ do
  - compute a Gröbner basis S of W with respect to a block–ordering $<$ with $u << x \smallsetminus u$;
  - choose T, a subset of S, which is a minimal Gröbner basis of $WK(u)[x \smallsetminus u]$ and compute the least common multiple $h \in K[u]$ of the leading coefficients of the elements in T as in Lemma 4;
  - Result := Result $\cap(\langle T\rangle : h^\infty)$ in $K[x]$;
  - $W := \langle W, h\rangle$;
  - if $\dim(W) < \dim(I)$, then
    return {Result, W};
- Result = Result $\cap$ EQUIDIMENSIONAL(W)[1];
- return {Result, EQUIDIMENSIONAL(W)[2]}.

Caboara, Conti and Traverso ([CCT]) propose a modification of this approach as follows: choose a set $u \subseteq x$ such that $I \cap K[u]$ is one–codimensional. If $I \cap K[u]$ is not principal, then its generators need to have a non–trivial common divisor and we can split $I \cap K[u]$ by applying Lemma 1, 1. to a suitable power of this divisor. If $I \cap K[u] = \langle g\rangle$ and g factorizes into different factors, we can again split the ideal. If g is the power of an irreducible polynomial, and if G is a Gröbner basis of I, with respect to a block–ordering on $K[x]$ with $u << x \smallsetminus u$, such that $G \cap K[u] = \{g\}$, then we may consider the ideal $\langle G \smallsetminus \{g\}\rangle K(u)[x \smallsetminus u]$ and choose a subset T of G, which is a minimal Gröbner basis of this ideal. Let $h \in K[u]$ be the least common multiple of the leading coefficients of the elements in T as in Lemma 4. If $I : h^\infty \underset{\neq}{\supseteq} I$, then we can split again. If $I = I : h^\infty$, and if g and h have no common divisor, then I is already equidimensional because $\operatorname{Spec} K[x]_h/I \longrightarrow \operatorname{Spec} K[u]_h/\langle g\rangle$ is flat. If g and h have a common divisor, then we have to apply Algorithm 5.

Remark 12. The approach above has the advantage that it also yields the equidimensional decomposition of I (use recursion). With the next approach this will be much more difficult.

The second approach goes back to Eisenbud, Huneke, and Vasconcelos ([EHV]). It is based on the following proposition:

Proposition 13. *Let $I \subseteq R = K[x_1, \ldots, x_n]$ be an ideal of codimension c. For $v \geq c$ let $E_v(I)$ be the equidimensional part of I of codimension v. Then*

1. $E_c(I) = \operatorname{ann} \operatorname{Ext}_R^c(R/I, R)$.
2. *If $I_0 \subseteq I$ is a complete intersection of codimension c, then*
$$E_c(I) = I_0 : (I_0 : I) \ .$$
3. *For $v \geq c$*
$$\sqrt{E_v(I)} = \sqrt{E_v\big(\operatorname{ann}(\operatorname{Ext}_R^v(R/I, R))\big)} \ .$$

We obtain the following algorithm:

Algorithm 6.

EQUIDIMENSIONAL(I)
Input: an ideal I in $K[x_1, \ldots, x_n]$
Output: the equidimensional hull of I

- choose any admissible term-ordering $<$ on $K[x_1, \ldots, x_n]$;
- compute a Gröbner basis of I and $c := \mathrm{codim}(I)$;
- choose the first c elements $f_1, \ldots, f_c$ in a set of minimal generators of I and set $I_0 := \langle f_1, \ldots, f_c \rangle$;
- if I_0 is a complete intersection, then
  return $I_0 : (I_0 : I)$;
- return $\mathrm{annExt}_R^c(R/I, R)$

If we compare Algorithms 5 and 6, the second algorithm looks more elegant, but our experience shows that it is very efficient only for small codimensions, or for a small number of variables. Furthermore, with Algorithm 6, it is difficult to obtain the other equidimensional parts of I, because, in general, $\bigcap\limits_v \mathrm{ann}\big(\mathrm{Ext}_R^v(R/I, R)\big)$ is strictly bigger than I, as one can see in the example $R = K[x, y]$ and $I = \langle x^2, xy \rangle$.

In [V2] the following approach to this problem is proposed: let $J_v = \mathrm{ann}\big(\mathrm{Ext}_R^v(\mathrm{Ext}_R^v(R/I, R), R)\big)$. Then J_v is equidimensional of codimension v or $J_v = R$. Assume that the equidimensional parts $I_c, \ldots, I_s$ are already computed and let $L_s = I_c \cap \cdots \cap I_s$. Then the equidimensional hull I_{s+1} of $(I + J_{s+1}^N) : L_s$ is the $(s+1)$–st equidimensional part of I. Here N is a number satisfying $(I + J_{s+1}^N) : L_s = (I + J_{s+1}^{N+1}) : L_s$ and $J_{s+1}^N \cap L_s \subset J_{s+1} L_s$.

In any case, Proposition 13 yields an algorithm to compute a set of equidimensional ideals I_v of codimension v with $\sqrt{E_v(I)} = \sqrt{I_v}$.

Algorithm 7.

WEAKEQUIDIMENSIONAL(I)
Input: an ideal I in $K[x_1, \ldots, x_n]$
Output: equidimensional ideals I_v, such that $\sqrt{E_v(I)} = \sqrt{I_v}$

- choose any admissible term–ordering $<$ on $K[x_1, \ldots, x_n]$;
- compute a Gröbner basis of I and $c := \mathrm{codim}(I)$;
- Result := {EQUIDIMENSIONAL(I)};
- for $v := c + 1$ to n do
  - $J := \mathrm{ann}\big(\mathrm{Ext}_R^v(R/I, R)\big)$;
  - if $\mathrm{codim}(J) = v$, then
    Result := Result $\cup${EQUIDIMENSIONAL(J)};
- return Result

Remark 14. If we need the output ideals to be radical, we just have to replace EQUIDIMENSIONAL( ) by EQUIRADICAL( ).

2.3 Zero–dimensional Primary Decomposition

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

Let K be a field of characteristic zero, or of characteristic $p > 0$, p sufficiently large.

Definition 15. Let P be a maximal ideal in $K[x_1, \ldots, x_n]$. P is called *in general position* with respect to the lexicographical ordering induced from $x_1 > \cdots > x_n$, if the reduced Gröbner basis of P is of type

$$\{x_1 - f_1(x_n), \ldots, x_{n-1} - f_{n-1}(x_n),\ f_n(x_n)\}$$

with $f_i \in K[x_n]$.

Remark 16. Notice that automatically f_n is irreducible and $\deg f_i < \deg f_n$, $i < n$.

Every $\underline{a} = (a_1, \ldots, a_{n-1}) \in K^{n-1}$ defines an automorphism $\varphi_{\underline{a}}$ of $K[x_1, \ldots, x_n]$ by $\varphi_{\underline{a}}(x_i) = x_i$ if $i < n$, and $\varphi_{\underline{a}}(x_n) = x_n + \sum\limits_{i=1}^{n-1} a_i x_i$.

Proposition 17. *Let $P \subset K[x_1, \ldots, x_n]$ be a maximal ideal. Then there exists a dense open subset $U \subset K^{n-1}$ such that every $\varphi_{\underline{a}}(P)$, $\underline{a} \in U$, is in general position with respect to the lexicographical ordering induced from $x_1 > \cdots > x_n$.*

Definition 18. Let $I \subset K[x_1, \ldots, x_n]$ be a zero–dimensional ideal. I is called *in general position* with respect to the lexicographical ordering induced from $x_1 > \cdots > x_n$, if the following holds for the minimal primary decomposition $I = Q_1 \cap \cdots \cap Q_s$ with associated primes $P_1, \ldots, P_s$:

1. $P_1, \ldots, P_s$ are in general position with respect to the lexicographical ordering induced from $x_1 > \cdots > x_n$.
2. $P_1 \cap K[x_n], \ldots, P_s \cap K[x_n]$ are coprime.

Proposition 19. *Let $I \subset K[x_1, \ldots, x_n]$ be a zero–dimensional ideal. Then there is a dense open subset $U \subset K^{n-1}$ such that every $\varphi_{\underline{a}}(I)$, $\underline{a} \in U$, is in general position with respect to the lexicographical ordering induced from $x_1 > \cdots > x_n$.*

Theorem 20. *Let $I \subset K[x_1, \ldots, x_n]$ be a zero–dimensional ideal in general position with respect to the lexicographical ordering induced from $x_1 > \cdots > x_n$, G a corresponding minimal Gröbner basis of I, and $\{f\} = G \cap K[x_n]$. Let $f = f_1^{\rho_1} \cdot \ldots \cdot f_s^{\rho_s}$ be the decomposition of f into a power product of pairwise non–associated irreducible factors f_k. Then the minimal primary decomposition of I is given by*

$$I = \bigcap_{k=1}^{s} (I, f_k^{\rho_k}) \ .$$

Theorem 20 yields the following algorithm.

Algorithm 8.

ZEROPRIMDEC(I [, CHECK])
Input: a zero-dimensional ideal in $K[x_1, \dots, x_n]$
Output: $\{Q_1, P_1, \dots, Q_s, P_s\}$, Q_i primary, $\sqrt{Q_i} = P_i$, $P_i \neq P_j$ for $i \neq j$ and $I = Q_1 \cap \dots \cap Q_s$

The ideal CHECK and all commands involving CHECK are optional;
CHECK is needed later on for the higher dimensional decomposition
in order to avoid redundant components.

- Result := $\emptyset$;
- [if CHECK $\subseteq I$, then
  return Result;]
- compute a Gröbner basis G of I with respect to the lexicographical ordering induced from $x_1 > \dots > x_n$;
- let $G \cap K[x_n] = \{f\}$;
- factorize $f = f_1^{\rho_1} \cdot \ldots \cdot f_s^{\rho_s}$;
- for $k := 1$ to s do
  - [if CHECK $\not\subseteq \langle I, f_k^{\rho_k} \rangle$, then]
    test whether $\langle I, f_k^{\rho_k} \rangle$ is primary and in general position, that is, compute a Gröbner basis S of $\langle I, f_k^{\rho_k} \rangle$ with respect to the lexicographical ordering induced from $x_1 > \dots > x_n$, and check whether S contains $h_1^{(k)}, \dots, h_n^{(k)}$ such that
    1. $h_n^{(k)} = f_k^{\rho_k}$
    2. $h_i^{(k)} = \left(x_i - g_i^{(k)}(x_n)\right)^{n_i^{(k)}} \mod \langle h_{i+1}^{(k)}, \dots, h_n^{(k)} \rangle$, $i < n$;

    if $\langle I, f_k^{\rho_k} \rangle$ is primary and in general position, then
    * $P_k := \langle x_1 - g_1^{(k)}, \dots, x_{n-1} - g_{n-1}^{(k)}, f_k \rangle$ is the associated prime to $Q_k := \langle I, f_k^{\rho_k} \rangle$;
    * Result := Result $\cup \{Q_k,\ P_k\}$;

    else
    * choose $\underline{a} \in K^{n-1}$ by random;
    * Result:=Result$\cup \varphi_{\underline{a}}^{-1}\big($ZEROPRIMDEC$(\varphi_a(\langle I, f_k^{\rho_k} \rangle)[,\varphi_a($CHECK$)])\big)$
- return Result.

Remark 21. To make this algorithm really efficient, it is necessary to do some preprocessing in order to avoid as many random coordinate changes as possible. A random coordinate change destroys sparseness, and usually makes the subsequent Gröbner basis computations very difficult. Therefore, we use the splitting tools

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

to split the ideal as often as possible before starting Algorithm 8 (if in 2. the condition $\langle f, g\rangle = \langle 1\rangle$ is not fulfilled, we still can apply 1. to a suitable power of f). In order to use 1. and 2., we produce as many reducible elements as possible. This leads to the following preprocessing algorithm.

Algorithm 9.

$\textsc{Split}(I)$
Input: a zero–dimensional ideal I in $K[x_1, \dots, x_n]$
Output: two sets of ideals, Primary $= \{Q_1, P_1, \dots, Q_s, P_s\}$, and Rest $= \{I_1, \dots, I_k\}$, such that $I = (\cap Q_i) \cap (\cap I_i)$, Q_i primary, and $\sqrt{Q_i} = P_i$

- Primary := $\emptyset$, Rest := $\emptyset$;
- for $i := 1$ to n do
  - compute $\langle F_i\rangle := I \cap K[x_i]$;
  - enlarge the system of generators of I by F_i;
- factorize all the generators of I and split the ideal and the resulting ideals as often as possible;
- compute for all ideals obtained in this way a Gröbner basis with respect to the lexicographical ordering induced from $x_1 > \dots > x_n$;
- test whether the ideals are primary and in general position with respect to the lexicographical ordering induced from $x_1 > \dots > x_n$; put the detected primary ideals and their associated primes to Primary and the other ideals to Rest;
- return Primary, Rest

Remark 22. Each ideal in Rest comes with a set of generators (which in fact is a Gröbner basis with respect to the lexicographical ordering induced from $x_1 > \dots > x_n$) such that every generator is a power of an irreducible element.

Remark 23. The preprocessing for a zero–dimensional ideal, which we know to be radical, is simpler than in the general case: we can use the fact that

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

which holds without the assumption $\langle f, g\rangle = \langle 1\rangle$. 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 the primary test:
I is prime if there is an irreducible $g \in I \cap K[x_i]$ for some i such that $\deg(g) = \dim_K K[x_1, \dots, x_n]/I$.
Especially, we obtain:
I is prime and in general position with respect to the lexicographical ordering induced from $x_1 > \dots > x_n$ if and only if for a corresponding minimal Gröbner basis G, and $\{g\} = G \cap K[x_n]$, we have $\deg(g) = \dim_K K[x_1, \dots, x_n]/I$, and g is irreducible.

The following probabilistic algorithm, proposed by Eisenbud, Huneke, and Vasconcelos ([EHV]), also goes to general position.

Algorithm 10.

DecompEHV(I)
Input: a zero–dimensional radical ideal I in $K[x_1, \dots, x_n]$
Output: the associated prime ideals

- choose a generic $f \in K[x_1, \dots, x_n]$, and test whether f is a zero–divisor $\bmod I$ (that is, check whether $I : f \supsetneqq I$);
- if f is a zero–divisor $\bmod I$ (which implies $I = \big(I : f\big) \cap \langle I, f\rangle$), then
  return DecompEHV($I : f$)$\cup$ DecompEHV$\big(\langle I, f\rangle\big)$;
- choose m minimal such that $1, f, \dots, f^m$ are linearly dependent mod I, and denote by $F \in K[T]$ the corresponding dependence relation;
- if $m < \dim_K K[x_1, \dots, x_n]/I$ restart the algorithm with another f;
- if F is irreducible, then
  return $\{I\}$;
- if F factors as $F = G_1 \cdot G_2$, then
  return DecompEHV$\big(\langle I, Q_1(f)\rangle\big)\cup$ DecompEHV$\big(\langle I, Q_2(f)\rangle\big)$

2.4 Higher Dimensional Primary Decomposition

The minimal associated primes

One approach, proposed by Eisenbud, Huneke, and Vasconcelos ([EHV]), starts with a radical ideal, computes *all* associated primes, and uses normalization.

The normalization algorithm presented later on in 2.5 has, as input, a radical ideal $I \subset R = K[x_1, \dots, x_n]$ and, as output, r polynomial rings $R_1, \dots, R_r$, r prime ideals $I_1 \subset R_1, \dots, I_r \subset R_r$, and r maps $\pi_i : R \longrightarrow R_i$ such that the induced map

$$\pi : R/I \longrightarrow R_1/I_1 \times \cdots \times R_r/I_r,\ \pi(\bar{f}) = \big(\pi_1(\bar{f}), \dots, \pi_r(\bar{f})\big)$$

is the normalization of R/I. In fact, if we plug in the computation of idempotents as explained in 2.5, then the result of the normalization algorithm is the minimal prime decomposition $I = \pi_1^{-1}(I_1) \cap \cdots \cap \pi_r^{-1}(I_r)$ of I (recall that normalization commutes with localization). Notice, however, that the computation of the idempotents still needs zero–dimensional prime decomposition.

Another possibility, also reducing the problem to the zero–dimensional case, does not necessarily need a radical ideal to start with. This approach, relying on Lemma 4, goes back to Gianni, Trager, and Zacharias ([GTZ]).

Algorithm 11.

MinAssPrimes(I)
Input: an ideal I in $K[x_1, \dots, x_n]$
Output: the minimal associated prime ideals of I

- Result := $\emptyset$;
- choose any admissible term order $<$ on $K[x_1, \dots, x_n]$;

– use the factorizing Gröbner basis algorithm to split I;
  the result $\mathfrak{m}$ is a set of ideals given by Gröbner bases such that
  1. all elements of the Gröbner bases are irreducible;
  2. the radical of the intersection of the elements of $\mathfrak{m}$ is the radical of I;
– for $J \in \mathfrak{m}$ do
  - compute $\mathcal{X}_J^<$;
  - for $u \in \mathcal{X}_J^<$ do
    * compute $\mathrm{Ass}(JK(u)[x \smallsetminus u])$ by 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 $JK(u)[x \smallsetminus u] \cap K[x] = J : h$;
    * $J := \langle J, h\rangle$;
  - Result := Result $\cup$ MinAssPrimes(J);
– return Result

A third possibility, also starting not necessarily with a radical ideal, is based on characteristic sets. We will treat this approach later.

Associated Primary Ideals

The first approach, proposed by Eisenbud, Huneke, and Vasconcelos ([EHV]), is based on the following lemma:

Lemma 24. *Let I be an ideal, $P \in \mathrm{minAss}(I)$, and m an integer satisfying $I : P^m \not\subset P$. Then the equidimensional hull of $I + P^m$ is a P–primary ideal of a decomposition of I.*

Remark 25. If $P \in \mathrm{Ass}(I)$ is an embedded prime, then one can obtain a P–primary ideal Q of a decomposition of I as

$$Q = \textsc{Equidimensional}(I + P^m)$$

for some m. In this case, it is more difficult to estimate m (cf. [EHV]): let $I_{[P]} = \{b \in R \mid I : b \not\subset P\}$. Then Q is a P–primary ideal of a decomposition of I if and only if the map $(I_{[P]} : P^\infty)/I_{[P]}) \longrightarrow R/Q$ is injective.

The Algorithm of Eisenbud, Huneke, and Vasconcelos

Algorithm 12.

PrimarydecEHV(I)
Input: an ideal I in $R = K[x_1, \ldots, x_n]$
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 $\sqrt{Q_v} = P_v$, $v = 1 \ldots s$.

– $E := \{\mathrm{ann}\big(\mathrm{Ext}_R^v(R/I, R)\big),\ v \geq \mathrm{codim}(I)\}$;
– $\mathfrak{m} := \{\textsc{Equiradical}(J) \mid J \in E,\ J \neq R\}$;

- compute $\mathrm{Ass}(I) = \{P_1, \ldots, P_s\} := \bigcup\limits_{L \in \mathfrak{m}} \mathrm{Ass}(L)$ (by using the normalization algorithm; notice that here *all* associated primes of I are computed);
- for $i := 1$ to s do

  compute $Q_i :=$ EQUIDIMENSIONAL$(I + P_i^m)$ with m as in Lemma 24 or Remark 25;
- Return $\{Q_1, P_1, \ldots, Q_s, P_s\}$

A second approach, based on Lemma 4, is due to Gianni, Trager, and Zacharias ([GTZ]).

The Algorithm of Gianni, Trager, and Zacharias

Algorithm 13.

PRIMARYDECGTZ(I [, CHECK])

- Result $:= \emptyset$;
- if CHECK is not defined, then

  CHECK:=$\langle 1 \rangle$;
- choose any admissible term–ordering $<$ on $K[x_1, \ldots, x_n]$;
- if CHECK $\subseteq I$, then

  return Result;
- compute $\mathcal{X}_I^<$;
- for $u \in \mathcal{X}_I^<$ do
  - $\mathfrak{m} :=$ ZEROPRIMDEC$(IK(u)[x \smallsetminus u]$, CHECK$)$;
  - Result := Result $\cup \{Q \cap K[x], P \cap K[x] \mid (Q, P) \in \mathfrak{m}\}$;
  - compute h such that $IK(u)[x \smallsetminus u] \cap K[x] = I : h = I : h^2$;
  - $I := \langle I, h \rangle$;
  - for $(Q, P) \in \mathfrak{m}$ do

    CHECK = CHECK $\cap\, Q$;
- Result = Result $\cup$ PRIMARYDECGTZ(I, CHECK);
- return Result

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

Lemma 26. *Let I be an ideal and* $\mathrm{minAss}(I) = \{P_1, \ldots, P_r\}$*. 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 $I : f_i^\infty = I : f_i^{k_i}$, $\bar{Q}_i := I : f_i^\infty$ and $J := I + \langle f_1^{k_1}, \ldots, f_r^{k_r} \rangle$. Then

1. *$\sqrt{\bar{Q}_i} = P_i$, that is, $\bar{Q}_i$ is pseudo–primary with associated prime P_i;*

2. $I = \bigcap_{i=1}^{r} \bar{Q}_i \cap J$;
3. $\operatorname{codim}(J) > \operatorname{codim}(I)$;
4. *let* $\bar{Q}_i = \bigcap_j Q_j^{(i)}$ *be a minimal primary decomposition of* $\bar{Q}_i$, $i = 1, \dots, r$. *Then* $\bigcap_{i,j} Q_j^{(i)}$ *is a minimal primary decomposition of* $\bigcap_{i=1}^{r} \bar{Q}_i$ *(no redundant components!) and* $\bigcup_i \operatorname{Ass}(\bar{Q}_i) \cap \operatorname{Ass}(J) = \emptyset$.

Remark 27. Let I be an ideal and $\operatorname{minAss}(I) = \{P_1, \dots, P_r\}$. Assume that $G_1, \dots, G_r$ are Gröbner bases of $P_1, \dots, P_r$. Since P_i is minimal in $\operatorname{Ass}(I)$, there are always elements t_j in G_j not being in P_i for $i \neq j$. Now define $f_i := \prod_{j \neq i} t_j$. Then $f_1, \dots, f_r$ satisfy the assumptions of Lemma 26.

Lemma 28. *Let* $\bar{Q}$ *be pseudo–primary with* $\sqrt{\bar{Q}} = P$ *prime and* $u \subseteq x$ *a maximal independent set* $\bmod \bar{Q}$. *Then* $\bar{Q}K(u)[x \smallsetminus u] \cap K[x] =: Q$ *is* P*–primary. Let* $h \in K[u]$ *be chosen such that* $\bar{Q}K(u)[x \smallsetminus u] \cap K[x] = \bar{Q} : h = \bar{Q} : h^2$, *and set* $J := \langle \bar{Q}, h \rangle$. *Then*

1. $\bar{Q} = Q \cap J$;
2. $\operatorname{codim} J > \operatorname{codim}(\bar{Q})$.

Definition 29. 1. Polynomials f_i as in Lemma 26 are called *separators*.
2. A decomposition as in Lemma 26, 2. is called a *pseudo–primary decomposition*, with *remaining component J* and *pseudo–primary components $\bar{Q}_i$*.
3. A decomposition as in Lemma 28, 1. is called *extraction* of Q from $\bar{Q}$, with *remaining component J*.

We obtain the following two procedures:

Algorithm 14.

PSEUDOPRIMARYDECOMP(I)
Input: an ideal I in $K[x_1, \dots, x_n]$
Output: a set Result $= \{(\bar{Q}_1, P_1, f_1), \dots, (\bar{Q}_r, P_r, f_r), J\}$ with $\bar{Q}_i$, P_i, f_i, and J as in Lemma 26

- compute $\operatorname{minAss}(I) := \{P_1, \dots, P_r\}$ (use your favourite algorithm);
- if $r = 1$, then
  return $\{(I, P_1, 1), \langle 1 \rangle\}$;
- Result $:= \emptyset$;
- $J := I$;
- compute separators $f_1, \dots, f_r$;
- for $i = 1$ to r do
  - compute k_i such that $I : f_i^\infty = I : f_i^{k_i} =: \bar{Q}_i$;
  - Result := Result $\cup (\bar{Q}_i, P_i, f_i)$;
  - $J := \langle J, f_i^{k_i} \rangle$;

– return Result $\cup$ J

Algorithm 15.

EXTRACTION($\bar{Q}$)
Input: a pseudo–primary ideal $\bar{Q}$ in $K[x_1, \ldots, x_n]$, and $P = \sqrt{\bar{Q}}$
Output: (Q, J) as in Lemma 28

– choose any admissible term–ordering $<$ on $K[x_1, \ldots, x_n]$;
– compute $\mathcal{X}_I^<$;
– for $u \in \mathcal{X}_I^<$ do
  compute h_u such that $\bar{Q}K(u)[x \smallsetminus u] \cap K[x] = \bar{Q} : h_u^\infty$;
– choose $h = h_u$ of minimal degree among all h_u;
– compute N with $Q := \bar{Q} : h^N = \bar{Q} : h^{N+1}$;
– return $(Q, \langle \bar{Q}, h^N \rangle)$

By combining pseudo–primary decompositions and extractions, we obtain an algorithm for the computation of a not necessarily minimal primary decomposition. Criteria such as Lemma 26, 4. simplify the search for redundant components. In fact, we can do better. We may eliminate ideals, which only lead to redundant components, much earlier in the process. This idea of Shimoyama and Yokoyama ([SY]) is based on the next lemma. Let us first introduce some notations.

Definition 30. 1. Pseudo–primary decomposition and extraction are also called *elementary operations*. Any ideal arising from a given ideal V by one elementary operation is called a *son* of V.

2. When computing a primary decomposition of a given ideal I as indicated above, the ideals arising from I via elementary operations fit as vertices into a tree $\mathcal{T}$. The edges of $\mathcal{T}$ are ordered pairs (W, V) such that V is a son of W. $\mathcal{T}$ is called a *decomposition tree* of I. Vertices which are a primary component of the resulting decomposition of I (possibly redundant), are called *component vertices*.
3. Let V be a vertex in a decomposition tree of I. The *weighted tree depth* of V is the number of edges in the path from I to V, where any edge (W, V), V a remaining component arising from W by a pseudo–primary decomposition, is counted twice.
4. Let V be a vertex in a decomposition tree of I. Let (V_i, V_{i+1}), $i = 1, \ldots, r$, be all edges in the path from I to V such that V_{i+1} is a pseudo–primary component of V_i arising by a pseudo–primary decomposition. The tester of V is the product $f = \prod_{i=1}^r f_i$, where f_i is the separator corresponding to (V_i, V_{i+1}). V satisfies the *separating condition* if $\sqrt{V}$ does not contain f.
5. Let $\mathcal{T}$ be a decomposition tree of I. The associated *reduced decomposition tree* $\mathcal{T}_{\text{red}}$ is obtained from $\mathcal{T}$ by eliminating all subtrees whose roots do not satisfy the separating condition.

Lemma 31. *Let I be an ideal in $K[x_1, \ldots, x_n]$, and let $\mathcal{T}$ be a decomposition tree of I. Then:*

1. *In $\mathcal{T}_{\mathrm{red}}$ all component vertices have distinct associated primes.*
2. *For each prime $P \in \mathrm{Ass}(I)$ there exists a unique component vertex Q_P in $\mathcal{T}_{\mathrm{red}}$ associated to P.*
3. *$I = \cap\{Q_P \mid P \in \mathrm{Ass}(I)\}$ is a minimal primary decomposition.*

Altogether, we obtain the following algorithm:

The Algorithm of Shimoyama and Yokoyama

Algorithm 16.

PRIMARYDECSY(I)

Input: an ideal I in $K[x_1, \dots, x_n]$
Output: a set Result $= \{Q_1, P_1, \dots, Q_s, P_s\}$ such that $I = \cap Q_v$ is a minimal primary decomposition, and $\sqrt{Q_v} = P_v$, $v = 1 \dots s$.

- Result $:= \emptyset$, $\mathcal{V} := \{I\}$;
- $L := \{1\}$;
- $w := 0$;
- while $I \subsetneqq L$ do
  - if $\{V \in \mathcal{V} \mid$ weighted tree depth of $V = w\}$ is empty, then
    $w := w + 1$;
  - choose a vertex $V \in \mathcal{V}$ of weighted tree depth w;
  - $\mathcal{V} := \mathcal{V} \setminus \{V\}$;
  - $\mathcal{W} := \{$sons of $V\}$ (apply either PSEUDOPRIMARYDECOMP(V), or EXTRACTION(V));
  - if there is a component vertex $Q \in \mathcal{W}$, then
    - * if $L \not\subset Q$, then
      - · Result:=Result $\cup \{(Q, P)\}$, where P is the radical of Q, which is known from a pseudo–primary decomposition before;
      - · $L := L \cap Q$;
    - * $\mathcal{W} := \mathcal{W} \setminus \{\mathcal{Q}\}$;
  - $\mathcal{V} := \mathcal{V} \cup \{V \in \mathcal{W} \mid V$ satifies the seperating condition$\}$;
- return Result

2.5 The Normalization

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

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

Proposition 32. *Let R be a Noetherian, reduced ring. Let 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* $\mathrm{Spec}(R)$. *Then R is normal if and only if $R = \mathrm{Hom}_R(J, J)$.*

Remark 33. Let R and J be as in the proposition, and let f be a non–zero divisor of J. Then

1. $fJ : J = f \cdot \mathrm{Hom}_R(J, J)$,

and, consequently,

2. $R = \mathrm{Hom}_R(J, J)$ if and only if $fJ : J \subseteq \langle f \rangle$.
3. Let $f_0 = f, f_1, \ldots, f_s$ be generators of $fJ : J$ as an R–module. Because $\mathrm{Hom}_R(J, J)$ is a ring, we have $\frac{s(s+1)}{2}$ quadratic relations of type

$$\tfrac{f_i}{f} \cdot \tfrac{f_j}{f} = \sum_{k=0}^{s} \xi_k^{ij} \tfrac{f_k}{f}, \quad s \geq i \geq j \geq 1, \quad \xi_k^{ij} \in R \ ,$$

in $\frac{1}{f}(fJ : J)$. Together with the linear relations, that is, the R–module syzygies between $f_0, \ldots, f_s$, the quadratic relations define the ring structure of $\mathrm{Hom}_R(J, J)$: the map

$$R[T_1, \ldots, T_s] \twoheadrightarrow \mathrm{Hom}_R(J, J), \quad T_i \rightsquigarrow \frac{f_i}{f}$$

is surjective, and its kernel is the ideal generated by the elements of type $T_i T_j - \sum_{k=0}^{s} \xi_k^{ij} T_k$ (with $T_0 = 1$), and $\sum_{k=0}^{s} \eta_k T_k$, where $\sum_{k=0}^{s} \eta_k f_k = 0$.

Now we are prepared to give the normalization algorithm:

Algorithm 17.

NORMAL(I [, INFORM])
Input: a radical ideal I in $K[x_1, \ldots, x_n]$
Output: r polynomial rings $R_1, \ldots, R_r$, r prime ideals $I_1 \subset R_1, \ldots, I_r \subset R_r$, and r maps $\pi_i : R \to R_i$, such that the induced map $\pi : K[x_1, \ldots, x_n]/I \to R_1/I_1 \times \cdots \times R_r/I_r$ is the normalization of $K[x_1, \ldots, x_n]/I$

Additional information provided by the user (respectively by the algorithm)
can be given in the optional list INFORM. For example, INFORM may contain
– the information that I defines an isolated singularity at $0 \in K^n$
– some elements of the radical of the non–normal locus,
which are already known.

- Result := $\emptyset$;
- compute the idempotents of $K[x_1, \ldots, x_n]/I$;
  this is optional; the splitting

  $$K[x_1, \ldots, x_n]/I = K[x_1, \ldots, x_n]/I_1 \times \cdots \times K[x_1, \ldots, x_n]/I_t$$

  defined by the idempotents is needed for the computation of the associated primes of I as explained at the beginning of 2.4;

– for $i := 1$ to t do

- compute the singular locus J of I_i;
- choose $f \in J \setminus I_i$ and compute $I_i : f$ to check whether f is a zero divisor mod I_i;
- if $I_i : f \supsetneqq I_i$, then
  Result := Result $\cup$ NORMAL$(I_i : (I_i : f))\cup$ NORMAL$(I_i : f)$;
  (notice that $\sqrt{\langle I_i, f\rangle} = I_i : (I_i : f)$ in this situation;)

  else

  if I_i has an isolated singularity at $0 \in K^n$, then
  $J := \langle x_1, \ldots, x_n\rangle$;

  else

  if J_0 is the radical of the singular locus of a normalization loop before, given by the list INFORM, then
  $J := \sqrt{\langle I_i, f + J_0\rangle}$;

  else

  $J := \sqrt{\langle I_i, f\rangle}$;
- compute $H := fJ : J =: \langle f, f_1, \ldots, f_s\rangle$;
- if $H = \langle f\rangle$, then
  Result := Result $\cup\{K[x_1, \ldots, x_n], I_i, \mathrm{id}_{K[x_1,\ldots,x_n]}\}$

  else

  ∗ compute, as described in Remark 33, an ideal L such that
  $K[x_1, \ldots, x_n, T_1, \ldots, T_s]/L \xrightarrow{\sim} \mathrm{Hom}(J, J), \quad T_i \rightsquigarrow \frac{f_i}{f}$;
  ∗ $S :=$NORMAL(L);
  ∗ let $\iota : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n, T_1, \ldots, T_s]$ be the inclusion;
  ∗ replace S by S with all ring maps composed with ι;
  ∗ Result := Result $\cup S$;

– return Result

It remains to give an algorithm to compute the idempotents.

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

An idempotent e, that is, $e^2 - e \in I$, has to be homogeneous of degree 0. Therefore, no idempotent will occur in the first loop.

Idempotents may occur after one normalization loop in $\mathrm{Hom}(J, J) \simeq K[x_1, \ldots, x_n, T_1, \ldots, T_s]/L$ because some of the generators may have the same degree.

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

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

For this situation there is an easy algorithm:

Algorithm 18.

IDEMPOTENTS(I)
Input: $I \subseteq K[x_1, \ldots, x_n]$ a (weighted) homogeneous radical ideal, $\deg(x_1) = \cdots = \deg(x_k) = 0, \deg(x_i) > 0$ for $i > k$, $I \cap K[x_1, \ldots, x_k]$ zero–dimensional.

Output: ideals $I_1, \dots, I_t$ such that $K[x_1, \dots, x_n]/I = K[x_1, \dots, x_n]/I_1 \times \cdots \times K[x_1, \dots, x_n]/I_t$, and such that $I \cap K[x_1, \dots, x_k] = \cap(I_v \cap K[x_1, \dots, x_k])$ is the prime decomposition

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

2.6 Minimal Associated Primes via Characteristic Sets

The concept of characteristic sets goes back to Ritt ([R1], [R2]) and Wu [Wu]. In our context, when applying this concept, the basic strategy is the following.

Let X be a finite set of generators for the given ideal $I \subset K[x_1, \dots, x_n]$. Compute a characteristic set of X. Successively extend this characteristic set via pseudo–division. Split the radical of I with the help of the extended characteristic set $\mathcal{F}$. Distinguish two different types of splitting, depending on whether $\mathcal{F}$ is irreducible (then $\mathcal{F}$ corresponds to a prime ideal) or not. When applying the above idea recursively, the prime ideals corresponding to irreducible extended characteristic sets provide a not necessarily minimal prime decomposition of $\sqrt{I}$.

Let us be more precise and recall the basic definitions and facts. We refer to [Ch], [Mi], and [W] for details and proofs.

Definition 34. Let f be a polynomial in $K[x_1, \dots, x_n]$.

1. We define the *class* of f, class(f), and the *class–degree* of f, cdeg(f), as follows. If f is constant, let class$(f) := 0$ and cdeg$(f) := 0$. Otherwise, let class(f) be the maximal k such that $\deg_{x_k}(f)$ is non–zero, and let cdeg$(f) := \deg_{x_{\mathrm{class}(f)}}(f)$.
2. Let class$(f) > 0$. Then the *initial* of f, In(f), is the leading coefficient of f considered as a polynomial in $x_{\mathrm{class}(f)}$.
3. A polynomial $g \in K[x_1, \dots, x_n]$ is *Ritt–Wu reduced with respect to* $f \neq 0$ if $\deg_{x_{\mathrm{class}(f)}}(g) < \deg_{x_{\mathrm{class}(f)}}(f)$.

Remark 35. The lexicographical ordering on $\mathbb{N} \times \mathbb{N}$ induces an ordering $\prec$ on $K[x_1, \dots, x_n]$ via the map

$$K[x_1, \dots, x_n] \to \mathbb{N} \times \mathbb{N}, \quad f \mapsto (\mathrm{class}(f), \mathrm{cdeg}(f)) .$$

$\prec$ is well–founded, that is, every non–empty subset of $K[x_1, \dots, x_n]$ has a minimal element. $\prec$ is, however, not a total ordering.

Definition 36. Let $f, g \in K[x_1, \ldots, x_n]$. f is said to be of *lower rank* than g if $f \prec g$. f and g are said to be of the *same rank*, $f \sim g$, if neither $f \prec g$ nor $g \prec f$, that is, $\mathrm{class}(f) = \mathrm{class}(g)$ and $\mathrm{cdeg}(f) = \mathrm{cdeg}(g)$.

Definition 37. A finite sequence of polynomials $\mathcal{F} = \{f_1, \ldots, f_r\} \subset K[x_1, \ldots, x_n]$ is called an *ascending set*, if either

1. $r = 1$ and $f_1 \neq 0$, or
2. $r > 1$, $0 < \mathrm{class}(f_1) < \cdots < \mathrm{class}(f_r)$, and each f_i, $i = 2, \ldots, n$, is *Ritt–Wu reduced* with respect to $\{f_1, \ldots, f_{i-1}\}$, that is, f_i is Ritt–Wu reduced with respect to f_j, $j < i$.

The basic computational tool in the context of ascending sets is *pseudo–division* (or *Ritt–Wu reduction*).

Remark 38.

1. If $f \neq 0$, g are polynomials in $K[x_1, \ldots, x_n]$, with $\mathrm{class}(f) = k$, then *pseudo–division* yields an expression
$$\mathrm{In}(f)^\alpha g = qf + r, \text{ with } \deg_{x_k}(r) < \deg_{x_k}(f) \ ,$$
and with $\alpha := \max\{0, \deg_{x_k}(g) - \deg_{x_k}(f) + 1\}$. The *pseudo–quotient* $\mathrm{pquot}(g|f) = q$ and the *pseudo–remainder* $\mathrm{prem}(g|f) = r$ are uniquely determined. Clearly, g is Ritt–Wu reduced with respect to f if and only if $\mathrm{prem}(g|f) = g$.
2. Let $\mathcal{F} = \{f_1, \ldots, f_r\} \subset K[x_1, \ldots, x_n]$ be an ascending set with $\mathrm{class}(f_1) > 0$, and $g \in K[x_1, \ldots, x_n]$. The *pseudo–remainder* $\mathrm{prem}(g|\mathcal{F}) = \mathrm{prem}(g|f_1, \ldots, f_r)$ is inductively defined by $\mathrm{prem}(g|f_1, \ldots, f_r) = \mathrm{prem}(\mathrm{prem}(g|f_2, \ldots, f_r)|f_1)$. Note that there is an expression of type
$$\mathrm{In}(f_1)^{s_1} \cdot \ldots \cdot \mathrm{In}(f_r)^{s_r} g = q_1 f_1 + \cdots + q_r f_r + \mathrm{prem}(g|\mathcal{F}) \ .$$
Clearly, g is Ritt–Wu reduced with respect to $\mathcal{F}$ if and only if $\mathrm{prem}(g|\mathcal{F}) = g$.

Remark 39. A well–founded ordering $\prec$ on the set of ascending sets is defined as follows. If two such sets $\mathcal{F} = \{f_1, \ldots, f_r\}$ and $\mathcal{G} = \{g_1, \ldots, g_s\}$ are given, then $\mathcal{F} \prec \mathcal{G}$, if either

1. $f_i \prec g_i$ for the first i with $f_i \not\sim g_i$, or
2. $r > s$ and $f_i \sim g_i$, $i = 1, \ldots, s$.

Definition 40. Let X be any non–empty subset of $K[x_1, \ldots, x_n] \setminus \{0\}$. A minimal element of the set of ascending sets contained in X is called a *characteristic set* of X.

Since $\prec$ is a well–founded ordering, minimal elements do exist. If X is finite, then there is an obvious algorithm for the computation of a characteristic set:

Algorithm 19.

CharSet(I)
Input: a finite subset X of $K[x_1, \ldots, x_n] \setminus \{0\}$
Output: a characteristic set of X

- Result := $\emptyset$, Rest := X;
- while Rest $\neq \emptyset$ do
  - choose f of lowest rank in Rest;
  - Result := Result $\cup \{f\}$;
  - if class$(f) = 0$, then
    Rest := $\emptyset$;
    else
    Rest:= $\{g \in$ Rest $\setminus \{f\} \mid g$ is Ritt-Wu reduced with respect to $f\}$;
- return Result

Definition 41. Let X be any finite subset of $K[x_1, \ldots, x_n] \setminus \{0\}$, and $I = \langle X \rangle$ the ideal generated by X. An ascending set $\mathcal{F} = \{f_1, \ldots, f_r\} \subset I$ is called an *extended characteristic set* of X, if either

1. $r = 1$ and f_1 is constant, or
2. class$(f_1) > 0$ and prem$(g|\mathcal{F}) = 0$ for all $g \in X$.

The existence of extended characteristic sets is clear from the following algorithm (*Ritt-Wu process*) for the computation of an extended characteristic set. Since $\prec$ is a well–founded ordering, the termination of this and the subsequent algorithms is guaranteed by

Remark 42. Let X be any non–empty subset of $K[x_1, \ldots, x_n] \setminus \{0\}$, $\mathcal{F}$ a characteristic set of X, and $g \in K[x_1, \ldots, x_n] \setminus \{0\}$ Ritt-Wu reduced with respect to $\mathcal{F}$. Then $\mathcal{G} \prec \mathcal{F}$ for every characteristic set $\mathcal{G}$ of $X \cup \{g\}$.

Algorithm 20.

ExtCharSet(I)
Input: a finite subset X of $K[x_1, \ldots, x_n] \setminus \{0\}$
Output: an extended characteristic set of X

- Int := Rest := X;
- while Rest $\neq \emptyset$ do
  - Result := CharSet(Int);
  - if Result = $\{f\}$ with $f \in K$, then
    Rest := $\emptyset$;
    else
    Rest := $\{$prem$(g|$ Result$) \neq 0 \mid g \in$ Int $\setminus$ Result $\}$;
  - Int := Int $\cup$ Rest;
- return Result

We next explain how characteristic sets are related to primary decomposition.

Definition 43. Let $\mathcal{F} = \{f_1, \ldots, f_r\} \subset K[x_1, \ldots, x_n]$ be an ascending set, and let $m = n-r$. After renaming the variables we may assume that $\mathrm{class}(f_i) = x_{m+i}$, $i = 1, \ldots, r$. With this assumption $\mathcal{F}$ is called *irreducible*, if each f_i is irreducible in $K_i[x_{m+i}]$, where K_i is inductively defined by $K_1 := K(x_1, \ldots, x_m)$, and $K_i := K_{i-1}[x_{m+i-1}]/\langle f_{i-1}\rangle$.

Proposition 44. *Let $\mathcal{F} = \{f_1, \ldots, f_r\} \subset K[x_1, \ldots, x_n]$ be an irreducible ascending set. Then*

$$P := \{g \in K[x_1, \ldots, x_n] \mid \mathrm{prem}(g|f_1, \ldots, f_r) = 0\}$$

is a prime ideal with $\mathcal{F}$ as a characteristic set.

It follows from the pseudo–remainder formula in Remark 38, 2. that P can be computed via Gröbner bases:

Lemma 45. *Let $\mathcal{F} = \{f_1, \ldots, f_r\} \subset K[x_1, \ldots, x_n]$ be an irreducible ascending set, $J = \langle \mathcal{F}\rangle$ the ideal generated by $\mathcal{F}$, and P the prime ideal with characteristic set $\mathcal{F}$ as in Proposition 44. Then*

$$P = (\ldots((J : \mathrm{In}(f_1)^\infty) : \mathrm{In}(f_2)^\infty) : \ldots) : \mathrm{In}(f_r)^\infty \quad .$$

Now we come to the two different types of splitting.

Lemma 46. *Let X be any finite subset of $K[x_1, \ldots, x_n] \setminus \{0\}$, $I = \langle X\rangle$ the ideal generated by X and $\mathcal{F} = \{f_1, \ldots, f_r\}$ an extended characteristic set of X. Suppose that $\mathcal{F}$ is irreducible, and let P be the prime ideal with characteristic set $\mathcal{F}$ as in Proposition 44. Then*

$$\sqrt{I} = P \cap \sqrt{\langle X \cup \{\mathrm{In}(f_1)\}\rangle} \cap \cdots \cap \sqrt{\langle X \cup \{\mathrm{In}(f_r)\}\rangle}$$

The following remark allows the application of Lemma 1.

Remark 47. Let $\mathcal{F} = \{f_1, \ldots, f_r\} \subset K[x_1, \ldots, x_n]$ be a reducible ascending set. Assume that the variables are ordered as in Definition 43 with $m = n - r$.Choose i minimal with $\{f_1, \ldots, f_i\}$ reducible. Let $f_i = \tilde{h}_1^{\rho_1} \cdot \ldots \cdot \tilde{h}_s^{\rho_s}$ be the factorization of f_i into irreducible factors over K_i. Then there is a relation of type $g = Gf_i - h_1^{\rho_1} \cdot \ldots \cdot h_s^{\rho_s}$ in $K[x_1, \ldots, x_n]$, where h_j is obtained from $\tilde{h}_j$ by clearing denominators, and where $G \in K[x_1, \ldots, x_m]$. Then g, considered as a polynomial in $K_{i-1}[x_{m+i}]$, is zero. The irreducibility of $\{f_1, \ldots, f_{i-1}\}$ implies that $\mathrm{prem}(g|f_1, \ldots, f_{i-1}) = 0$. Hence there exist $s_1, \ldots, s_{i-1}$ such that $\mathrm{In}(f_1)^{s_1} \cdot \ldots \cdot \mathrm{In}(f_{i-1})^{s_{i-1}} h_1^{\rho_1} \cdot \ldots \cdot h_s^{\rho_s} \in \langle f_1, \ldots, f_i\rangle$. Define $g_j := \mathrm{prem}(h_j|f_1, \ldots, f_{i-1})$, $j = 1, \ldots, s$. Then all g_j are Ritt-Wu reduced with respect to $\mathcal{F}$, $\mathrm{class}(g_j) = \mathrm{class}(f_i)$, and $\mathrm{In}(f_1)^{s_1} \cdot \ldots \cdot \mathrm{In}(f_{i-1})^{s_{i-1}} g_1^{p_1} \cdot \ldots \cdot g_s^{p_s} \in \langle f_1, \ldots, f_i\rangle$.

Altogether we obtain the

Algorithm 21.

MINASSPRIMESCHARSETS(I)
Input: an ideal I in $K[x_1, \ldots, x_n]$
Output: the minimal associated primes of I

- let $Y \subset K[x_1, \ldots, x_n] \setminus \{0\}$ be a finite set of generators of I;
- Result := $\emptyset$, Rest := $\{Y\}$;
- while Rest $\neq \emptyset$ do
  - choose $X \in$ Rest;
  - Rest:= Rest $\setminus\{X\}$;
  - $\mathcal{F}$:= EXTCHARSET(X);
  - if $\mathcal{F} = \{f\}$ with $f \in K$, then
    return $\langle 1 \rangle$;
    else
    if $\mathcal{F}$ is irreducible, then
      * Result := Result $\cup$ $\{\mathcal{F}\}$;
      * Rest := Rest $\cup$ $\{X \cup \mathcal{F} \cup \{\mathrm{In}(f)\} \mid f \in \mathcal{F}, \mathrm{class}(\mathrm{In}(f)) > 0\}$;

    else
      * find $f_1, \ldots, f_{i-1} \in \mathcal{F}$ and $g_1, \ldots, g_s$ as in Remark 47;
      * Rest := Rest $\cup\{X \cup \mathcal{F} \cup \mathrm{In}(f_j) | j = 1, \ldots, i-1\}$
        $\cup\{X \cup \mathcal{F} \cup \{g_j\} | j = 1, \ldots, s, \mathrm{class}(\mathrm{In}(f_j)) > 0\}$;
- let Result = $\{\mathcal{F}_1, \ldots, \mathcal{F}_k\}$;
- for $i = 1$ to k do
  - $J := \langle \mathcal{F}_i \rangle$;
  - for $f \in \mathcal{F}_i$ do
    $J := J : \mathrm{In}(f)^\infty$;
  - Result := $\big($Result $\setminus\{\mathcal{F}_i\}\big) \cup \{J\}$;
- omit redundant prime ideals in Result;
- return Result

3 Examples

All algorithms described in Section 2 are, or are about to be, implemented in SINGULAR.

In this Section we compare the implementations. In the table below we give the timings (in seconds) for 34 examples computed on a HP 720. "$*$" means that the computation was stopped after three hours. All computations are done over the prime field $K = \mathbb{F}_{32003}$. The ordering of the monomials is always the degree reverse lexicographical ordering with the underlying ordering of the alphabet.

In the `first` column we give the timings for the computation of the minimal associated primes via characteristic sets (Algorithm 22). In the `second` column, we list the timings for the computation of the associated primes by first using Algorithm 7 (WEAKEQUIDIMENSIONAL), followed by a prime decomposition of the equidimensional parts via Algorithm 11. The `third` column gives the timings for the minimal associated primes by using Algorithm 11. The `fourth` column contains the timings for a complete primary decomposition following Gianni, Trager, and Zacharias (Algorithm 13). The `fifth` column gives the timings for the primary decomposition by using the Algorithm 16 of Shimoyama and Yokoyama and computing the minimal associated primes via characteristic sets. In this column "$*$, 46" means that the characteristic sets algorithm could not compute the minimal associated primes, and that we need 46 seconds with Algorithm 16, if we first compute the minimal associated primes via Algorithm 11. In all other cases, the timings for Algorithm 16, based on Algorithm 11, can be obtained by subtracting the first column from the fifth column and adding the third column. The next two columns give the timings of the computation of the equidimensional radical and the radical by using a combination of the Algorithms 1, 2, and 3 (we use 2 and 3, if the first c generators of a c–codimensional ideal already form a regular sequence, and if the number of variables is less or equal to 5). Column 8 contains the information on the number and the dimension of the components. $\underbrace{3,\ldots,3}_{15},0$, for instance, means 15 components of dimension 3 and one component of dimension 0. Column 9 indicates, whether the given ideal is already radical or not. Finally, column 10 contains the number of embedded components.

The examples show that there is no unique strategy for the computation of primary decompositions. Sometimes much more time is used for computing the radical or the minimal associated primes than for the complete primary decomposition à la Gianni, Trager, and Zacharias. The reason for this is the use of the factorizing Buchberger algorithm, which is usually very efficient (in a few cases, however, it can be quite time–consuming).

1. Chemistry (describes a chemical processes in glass melting)

$$\begin{aligned}
&a+2b+c-d+g,\\
&f^2gh-a,\\
&efg-c,\\
&fg^2j-b,\\
&a+b+c+f+g-1,\\
&3ad+3bd+2cd+df+dg-a-2b-c-g.
\end{aligned}$$

2. Sturmfels and Eisenbud (the 2×2– permanents of a generic 3×3–matrix, cf. [ES, Example 3.5])

$$\begin{aligned}
&su+bv,\\
&tu+bw,\\
&tv+sw,\\
&sx+by,\\
&tx+bz,\\
&ty+sz,\\
&vx+uy,\\
&wx+uz,
\end{aligned}$$

$wy + vz.$

3. Schimoyama/Yokoyama (cf. [SY, Example J])

$xy^2z^2 - xy^2z + xyz^2 - xyz,$
$xy^3z + xy^2z,$
$xy^4 - xy^2,$
$x^2yz^2 - x^2yz,$
$x^2y^3 - x^2y^2,$
$x^4z^3 - x^4z^2 + 2x^3z^3 - 2x^3z^2 + x^2z^3 - x^2z^2,$
$x^2y^2z,$
$x^4yz + x^3yz,$
$2x^4y^2 + 6x^3y^2 + 6x^2y^2 + xy^3 + xy^2,$
$x^5z + x^4z^2 + x^4z + 2x^3z^2 - x^3z + x^2z^2 - x^2z,$
$x^6y + 3x^5y + 3x^4y + x^3y.$

4. Schimoyama/Yokoyama (cf. [SY, Example St])

$su - bv,$
$tv - sw,$
$vx - uy,$
$wy - vz.$

5. Butcher(cf. [W, Example 12], [BGK], POSSO test suite)

$a + c + d - e - h,$
$2df + 2cg + 2eh - 2h^2 - h - 1,$
$3df^2 + 3cg^2 - 3eh^2 + 3h^3 + 3h^2 - e + 4h,$
$6bdg - 6eh^2 + 6h^3 - 3eh + 6h^2 - e + 4h,$
$4df^3 + 4cg^3 + 4eh^3 - 4h^4 - 6h^3 + 4eh - 10h^2 - h - 1,$
$8bdfg + 8eh^3 - 8h^4 + 4eh^2 - 12h^3 + 4eh - 14h^2 - 3h - 1,$
$12bdg^2 + 12eh^3 - 12h^4 + 12eh^2 - 18h^3 + 8eh - 14h^2 - h - 1,$
$-24eh^3 + 24h^4 - 24eh^2 + 36h^3 - 8eh + 26h^2 + 7h + 1.$

6. Gonnet (cf. [BGK], POSSO test suite)

$ag,$
$gj + am + np + q,$
$bl,$
$nq,$
$bg + bk + al + lo + lp + b + c,$
$ag + ak + jl + bm + bn + go + ko + gp + kp + lq + a + d + f + h + o + p,$
$gj + jk + am + an + mo + no + mp + np + gq + kq + e + j + q + s - 1,$
$jm + jn + mq + nq,$
$jn + mq + 2nq,$
$gj + am + 2an + no + np + 2gq + kq + q + s,$

$2ag + ak + bn + go + gp + lq + a + d,$
$bg + al,$
$an + gq,$
$2jm + jn + mq,$
$gj + jk + am + mo + 2mp + np + e + 2j + q,$
$jl + bm + gp + kp + a + f + o + 2p,$
$lp + b,$
$jn + mq,$
$gp + a.$

7. Horrocks (related to the Horrock bundle on $\mathbb{P}^5$, cf. [DMS])

$2adef + 3be^2f - cef^2,$
$4ad^2f + 5bdef + cdf^2,$
$2abdf + 3b^2ef - bcf^2,$
$4a^2df + 5abef + acf^2,$
$4ad^2e + 3bde^2 + 7cdef,$
$2acde + 3bce^2 - c^2ef,$
$4abde + 3b^2e^2 - 4acdf + 2bcef - c^2f^2,$
$4a^2de + 3abe^2 + 7acef,$
$4acd^2 + 5bcde + c^2df,$
$4abd^2 + 3b^2de + 7bcdf,$
$16a^2d^2 - 9b^2e^2 + 32acdf - 18bcef + 7c^2f^2,$
$2abcd + 3b^2ce - bc^2f,$
$4a^2cd + 5abce + ac^2f,$
$4a^2bd + 3ab^2e + 7abcf,$
$abc^2f - cdef^2,$
$ab^2cf - bdef^2,$
$2a^2bcf + 3be^2f^2 - cef^3,$
$ab^3f - 3bdf^3,$
$2a^2b^2f - 4adf^3 + 3bef^3 - cf^4,$
$a^3bf + 4aef^3,$
$3ac^3e - cde^3,$
$3b^2c^2e - bc^3f + 2cd^2ef,$
$abc^2e - cde^2f,$
$6a^2c^2e - 4ade^3 - 3be^4 + ce^3f,$
$3b^3ce - b^2c^2f + 2bd^2ef,$
$2a^2bce + 3be^3f - ce^2f^2,$
$3a^3ce + 4ae^3f,$
$4bc^3d + cd^3e,$
$4ac^3d - 3bc^3e - 2cd^2e^2 + c^4f,$
$8b^2c^2d - 4ad^4 - 3bd^3e - cd^3f,$
$4b^3cd + 3bd^3f,$
$4ab^3d + 3b^4e - b^3cf - 6bd^2f^2,$
$4a^4d + 3a^3be + a^3cf - 8ae^2f^2$

8. Arnborg-Lazard (POSSO test suite)

$$x^2yz + xy^2z + xyz^2 + xyz + xy + xz + yz,$$
$$x^2y^2z + xy^2z^2 + x^2yz + xyz + yz + x + z,$$
$$x^2y^2z^2 + x^2y^2z + xy^2z + xyz + xz + z + 1.$$

9. Schwarz (constructing idempotents in group theory)

$$-ab - b^2 - 2de - 2ch,$$
$$-ac - 2bc - e^2 - 2dh,$$
$$-c^2 - ad - 2bd - 2eh,$$
$$-2cd - ae - 2be - h^2,$$
$$-d^2 - 2ce - ah - 2bh.$$

10. Katsura4 (POSSO test suite)

$$2t^2 + u^2 + 2x^2 + 2y^2 + 2z^2 - u,$$
$$2tu + xy + 2tz + 2yz - t,$$
$$t^2 + 2ty + 2uz + 2xz - z,$$
$$2tx + 2uy + 2tz - y,$$
$$2t + u + 2x + 2y + 2z - 1.$$

11. Katsura5 (POSSO test suite)

$$2x^2 + 2y^2 + 2z^2 + 2t^2 + 2u^2 + v^2 - v,$$
$$xy + yz + 2zt + 2tu + 2uv - u,$$
$$2xz + 2yt + 2zu + u^2 + 2tv - t,$$
$$2xt + 2yu + 2tu + 2zv - z,$$
$$t^2 + 2xv + 2yv + 2zv - y,$$
$$2x + 2y + 2z + 2t + 2u + v - 1.$$

12. Cyclic roots 5 homog (cf. [BF])

$$a + b + c + d + e,$$
$$ab + bc + cd + ae + de,$$
$$abc + bcd + abe + ade + cde,$$
$$abcd + abce + abde + acde + bcde,$$
$$abcde - h^5.$$

13. Cyclic roots 5 (cf. [BF], POSSO test suite)

$$a + b + c + d + e,$$
$$ab + bc + cd + ae + de,$$
$$abc + bcd + abe + ade + cde,$$
$$abcd + abce + abde + acde + bcde,$$

$abcde - 1$

14. Cyclic roots 4 (cf. [BF], POSSO test suite)

$$
\begin{aligned}
&a + b + c + d,\\
&ab + bc + ad + cd,\\
&abc + abd + acd + bcd,\\
&abcd - 1.
\end{aligned}
$$

15. Roczen (related to the classification of singularities in positive characteristic)

$$
\begin{aligned}
&o + 1,\\
&k^4 + k,\\
&hk,\\
&h^4 + h,\\
&gk,\\
&gh,\\
&g^3 + h^3 + k^3 + 1,\\
&fk,\\
&f^4 + f,\\
&eh,\\
&ef,\\
&f^3h^3 + e^3k^3 + e^3 + f^3 + h^3 + k^3 + 1,\\
&e^3g + f^3g + g,\\
&e^4 + e,\\
&dh^3 + dk^3 + d,\\
&dg,\\
&df,\\
&de,\\
&d^3 + e^3 + f^3 + 1,\\
&e^2g^2 + d^2h^2 + c,\\
&f^2g^2 + d^2k^2 + b,\\
&f^2h^2 + e^2k^2 + a.
\end{aligned}
$$

16. De Jong (related to the base space of a semi–universal deformation of a rational quadruple point)

$$
\begin{aligned}
&-2hjk + 4ef + bj + ak,\\
&-2hjl + 4eg + cj + al,\\
&-4fhj - 4ehk - djk + 2be + 2af,\\
&-4ghj - 4ehl - djl + 2ce + 2ag,\\
&-2dfj - 2dek + ab,\\
&-2dgj - 2del + ac.
\end{aligned}
$$

17. Becker-Niermann (example for testing FGLM)

$$y^4 + xy^2z + x^2 - 2xy + y^2 + z^2,$$
$$-x^3y^2 + xyz^3 + y^4 + xy^2z - 2xy,$$
$$xy^4 + yz^4 - 2x^2y - 3.$$

18. Caprasse4 (POSSO test suite)

$$y^2z + 2xyt - 2x - z,$$
$$-x^3z + 4xy^2z + 4x^2yt + 2y^3t + 4x^2 - 10y^2 + 4xz - 10yt + 2,$$
$$2yzt + xt^2 - x - 2z,$$
$$-xz^3 + 4yz^2t + 4xzt^2 + 2yt^3 + 4xz + 4z^2 - 10yt - 10t^2 + 2.$$

19. Cassou (POSSO test suite)

$$6b^4c^3 + 21b^4c^2d + 15b^4cd^2 + 9b^4d^3 - 8b^2c^2e - 28b^2cde + 36b^2d^2e - 144b^2c$$
$$-648b^2d - 120, 9b^4c^4 + 30b^4c^3d + 39b^4c^2d^2 + 18b^4cd^3 - 24b^2c^3e - 16b^2c^2de$$
$$+16b^2cd^2e + 24b^2d^3e$$
$$-432b^2c^2 - 720b^2cd - 432b^2d^2 + 16c^2e^2 - 32cde^2 + 16d^2e^2 + 576ce - 576de$$
$$-240c + 5184,$$
$$-15b^2c^3e + 15b^2c^2de - 81b^2c^2 + 216b^2cd - 162b^2d^2 + 40c^2e^2 - 80cde^2$$
$$+40d^2e^2 + 1008ce - 1008de + 5184,$$
$$-4b^2c^2 + 4b^2cd - 3b^2d^2 + 22ce - 22de + 261.$$

20. mat3^2 (the square of a generic 3×3–matrix, POSSO test suite)

$$a^2 + bd + cg,$$
$$ab + be + ch,$$
$$ac + bf + ci,$$
$$ad + de + fg,$$
$$bd + e^2 + fh,$$
$$cd + ef + fi,$$
$$ag + dh + gi,$$
$$bg + eh + hi,$$
$$cg + fh + i^2.$$

21. Shimoyama/Yokoyama (cf. [SY, Example I_8]

$$-k^9 + 9k^8l - 36k^7l^2 + 84k^6l^3 - 126k^5l^4 + 126k^4l^5 - 84k^3l^6 + 36k^2l^7 - 9kl^8 + l^9,$$
$$-bk^8 + 8bk^7l + k^8l - 28bk^6l^2 - 8k^7l^2 + 56bk^5l^3 + 28k^6l^3 - 70bk^4l^4 - 56k^5l^4 +$$
$$56bk^3l^5 + 70k^4l^5 - 28bk^2l^6 - 56k^3l^6 + 8bkl^7 + 28k^2l^7 - bl^8 - 8kl^8 + l^9,$$
$$ck^7 - 7ck^6l - k^7l + 21ck^5l^2 + 7k^6l^2 - 35ck^4l^3 - 21k^5l^3 + 35ck^3l^4 + 35k^4l^4 -$$
$$21ck^2l^5 - 35k^3l^5 + 7ckl^6 + 21k^2l^6 - cl^7 - 7kl^7 + l^8,$$
$$-dk^6 + 6dk^5l + k^6l - 15dk^4l^2 - 6k^5l^2 + 20dk^3l^3 + 15k^4l^3 - 15dk^2l^4 - 20k^3l^4 +$$
$$6dkl^5 + 15k^2l^5 - dl^6 - 6kl^6 + l^7,$$
$$ek^5 - 5ek^4l - k^5l + 10ek^3l^2 + 5k^4l^2 - 10ek^2l^3 - 10k^3l^3 + 5ekl^4 + 10k^2l^4 -$$

$el^5 - 5kl^5 + l^6,$
$- fk^4 + 4fk^3l + k^4l - 6fk^2l^2 - 4k^3l^2 + 4fkl^3 + 6k^2l^3 - fl^4 - 4kl^4 + l^5,$
$gk^3 - 3gk^2l - k^3l + 3gkl^2 + 3k^2l^2 - gl^3 - 3kl^3 + l^4,$
$- hk^2 + 2hkl + k^2l - hl^2 - 2kl^2 + l^3,$
$jk - jl - kl + l^2.$

22. Gerdt (cf. [BGK], POSSO test suite)

$2tw + 2wy - wz,$
$2uw^2 - 10vw^2 + 20w^3 - 7tu + 35tv - 70tw,$
$6tw^2 + 2w^2y - 2w^2z - 21t^2 - 7ty + 7tz,$
$2v^3 - 4uvw - 5v^2w + 6uw^2 + 7vw^2 - 15w^3 - 42vy,$
$6tw + 9wy + 2vz - 3wz - 21x,$
$9uw^3 - 45vw^3 + 135w^4 + 14tv^2 - 70tuw + 196tvw - 602tw^2 - 14v^2z + 28uwz +$
$14vwz - 28w^2z + 147ux - 735vx + 2205wx - 294ty + 98tz + 294yz - 98z^2,$
$36tw^3 + 6w^3y - 9w^3z - 168t^2w - 14v^2x + 28uwx + 14vwx - 28w^2x - 28twy +$
$42twz + 588tx + 392xy - 245xz,$
$2uvw - 6v^2w - uw^2 + 13vw^2 - 5w^3 - 28tw + 14wy,$
$u^2w - 3uvw + 5uw^2 - 28tw + 14wy,$
$tuw + tvw - 11tw^2 - 2vwy + 8w^2y + uwz - 3vwz + 5w^2z - 21wx,$
$5tuw - 17tvw + 33tw^2 - 7uwy + 22vwy - 39w^2y - 2uwz + 6vwz - 10w^2z + 63wx,$
$20t^2w - 12uwx + 30vwx - 15w^2x - 10twy - 8twz + 4wyz,$
$4t^2w - 6uwx + 12vwx - 6w^2x + 2twy - 2wy^2 - 2twz + wyz,$
$8twx + 8wxy - 4wxz$

23. Möller (cf. [Moe])

$a + b + c + d,$
$u + v + w + x,$
$3ab + 3ac + 3bc + 3ad + 3bd + 3cd + 2,$
$bu + cu + du + av + cv + dv + aw + bw + dw + ax + bx + cx,$
$bcu + bdu + cdu + acv + adv + cdv + abw + adw + bdw + abx + acx + bcx,$
$abc + abd + acd + bcd,$
$bcdu + acdv + abdw + abcx.$

24. Riemenschneider (related to deformations of quotient singularities)

$su,$
$vx,$
$qu,$
$xz,$
$stx + ux,$
$uv^3 - uvw + ux,$
$- pu^2v^2 + pu^2w + qtx,$
$tx^2y - uv^2z + uwz.$

25. Mikro (coming from analyzing analog circuits)

$59ad + 59ah + 59dh - 705d - 1199h,$
$330acde + 330aceh + 330cdeh - 407acd - 1642ade - 1410cde - 407ach - 407cdh - 1642aeh - 2398ceh - 1642deh,$
$-483acd - 483ach - 483cdh + 821ad + 705cd + 821ah + 1199ch + 821dh,$
$13926abcde + 13926abceh + 13926bcdeh - 9404abcd - 9239abde - 4968acde - 13157bcde - 9404abch - 9404bcdh - 9239abeh - 4968aceh - 13025bceh - 9239bdeh - 4968cdeh,$
$-cde - 377cdh - ceh - deh,$
$-54acf - 54adf + a + d,$
$adfg + a + d.$

26. Amrhein (cf. [AGK, Example S6])

$a^2 + d^2 + 2ce + 2bf + a,$
$2ab + 2de + 2cf + b,$
$b^2 + 2ac + e^2 + 2df + c,$
$2bc + 2ad + 2ef + d,$
$c^2 + 2bd + 2ae + f^2 + e,$
$2cd + 2be + 2af + f.$

27. Buchberger (POSSO test suite)

$t - b - d,$
$x + y + z + t - a - c - d,$
$xz + yz + xt + zt - ac - ad - cd,$
$xzt - acd.$

28. Lanconelli (POSSO test suite)

$a + c + d + e + f + g + h + j - 1,$
$-c^2k - 2cdk - d^2k - cek - dek - cfk - dfk - cgk - dgk - egk - fgk - chk - dhk - ehk - fhk + c + d,$
$-c^2l - cdl - cel - cfl - cgl - dgl - egl - fgl + c^2 + 2cd + d^2 + cg + dg + ch + dh,$
$-b + c + e + g + j.$

29. Huneke

$s^{15},$
$t^{15},$
$u^{15},$
$u^5 - s^3tx + s^2t^2x + s^2t^2y - st^3y.$

30. Wang1 (cf. [W, Example 13])
$f^2h - 1,$

$ek^2 - 1,$
$g^2 l - 1,$
$2ef^2g^2hk^2 + f^2g^2h^2k^2 + 2ef^2g^2k^2l + 2f^2g^2hk^2l + f^2g^2k^2l^2 + ck^2,$
$2e^2fg^2hk^2 + 2efg^2h^2k^2 + 2e^2fg^2k^2l + 4efg^2hk^2l + 2fg^2h^2k^2l + 2efg^2k^2l^2 +$
$2fg^2hk^2l^2 + 2bfh,$
$2e^2f^2ghk^2 + 2ef^2gh^2k^2 + 2e^2f^2gk^2l + 4ef^2ghk^2l + 2f^2gh^2k^2l + 2ef^2gk^2l^2 +$
$2f^2ghk^2l^2 + 2dgl,$
$e^2f^2g^2k^2 + 2ef^2g^2hk^2 + 2ef^2g^2k^2l + 2f^2g^2hk^2l + f^2g^2k^2l^2 + bf^2,$
$2e^2f^2g^2hk + 2ef^2g^2h^2k + 2e^2f^2g^2kl + 4ef^2g^2hkl + 2f^2g^2h^2kl + 2ef^2g^2kl^2 +$
$2f^2g^2hkl^2 + 2cek,$
$e^2f^2g^2k^2 + 2ef^2g^2hk^2 + f^2g^2h^2k^2 + 2ef^2g^2k^2l + 2f^2g^2hk^2l + dg^2,$
$-e^2f^2g^2hk^2 - ef^2g^2h^2k^2 - e^2f^2g^2k^2l - 2ef^2g^2hk^2l - f^2g^2h^2k^2l - ef^2g^2k^2l^2 -$
$f^2g^2hk^2l^2 + a^2.$

31. Wang2(cf. [W, Example 7])

    $x^2 + y^2 + z^2 - t^2,$
    $xy + z^2 - 1,$
    $xyz - x^2 - y^2 - z + 1.$

32. Siebert
    $w^2xy + w^2xz + w^2z^2,$
    $tx^2y + x^2yz + x^2z^2,$
    $twy^2 + ty^2z + y^2z^2,$
    $t^2wx + t^2wz + t^2z^2.$

33. Macaulay (Macaulay2 tutorial)

    $b^4 - a^3d,$
    $ab^3 - a^3c,$
    $bc^4 - ac^3d - bcd^3 + ad^4,$
    $c^6 - bc^3d^2 - c^3d^3 + bd^5,$
    $ac^5 - b^2c^3d - ac^2d^3 + b^2d^4,$
    $a^2c^4 - a^3d^3 + b^3d^3 - a^2cd^3,$
    $b^3c^3 - a^3d^3,$
    $ab^2c^3 - a^3cd^2 + b^3cd^2 - ab^2d^3,$
    $a^2bc^3 - a^3c^2d + b^3c^2d - a^2bd^3,$
    $a^3c^3 - a^3bd^2,$
    $a^4c^2 - a^3b^2d.$

34. Amrhein2 (cf. [AGK])

    $a^2 + 2de + 2cf + 2bg + a,$
    $2ab + e^2 + 2df + 2cg + b,$
    $b^2 + 2ac + 2ef + 2dg + c,$
    $2bc + 2ad + f^2 + 2eg + d,$

$$
\begin{aligned}
&c^2 + 2bd + 2ae + 2fg + e, \\
&2cd + 2be + 2af + g^2 + f, \\
&d^2 + 2ce + 2bf + 2ag + g.
\end{aligned}
$$

	Ass			primary dec.		radical		dim	is	embed.
	char Set	EHV	GTZ	GTZ	SY	equiR	rad		reduced	comps.
1	2	9	3	1	35	6	11	3,3,3,3	no	no
2	6	32	5	31	35	2	2	$\underbrace{3,\dots,3}_{15},0$	no	1
3	1	0	0	4	3	0	0	$2,1,1,1,1,\underbrace{0,\dots,0}_{6}$	no	7
4	1	1	3	11	13	0	1	6,6,5,4	no	1
5	3	$*$	12	1210	20	9	9	3,3,3,2,2,2,2,0,0,0	no	2
6	9	$*$	2	1	20	9	9	3,3,3	no	no
7	15	25	2	5	16	1	1	3,3,3,3,3,3	yes	no
8	5	2	4	1	22	4	5	$\underbrace{0,\dots,0}_{14}$	yes	no
9	$*$	3	10	4	$*$,46	2	2	$\underbrace{1,\dots,1}_{12}$	yes	no
10	6	5	2	2	12	1	2	$\underbrace{1,\dots,1}_{9}$	yes	no
11	$*$	83	7	5	$*$,41	9	9	$\underbrace{1,\dots,1}_{6}$	yes	no
12	44	89	70	111	452	35	35	$\underbrace{1,\dots,1}_{25}$	no	no
13	$*$	52	402	35	$*$,548	396	396	$\underbrace{0,\dots,0}_{20}$	no	no
14	2	0	1	3	3	0	1	$1,1,\underbrace{0,\dots,0}_{6}$	no	6
15	103	$*$	14	12	123	2	2	$\underbrace{0,\dots,0}_{30}$	no	no
16	21	98	354	6	31	9	270	8,7,6,5	yes	no
17	123	14	26	18	125	14	14	0,0	yes	no
18	18	52	93	7	64	19	19	$\underbrace{0,\dots,0}_{19}$	no	no
19	$*$	2	71	1	$*$,42	44	88	1,1	yes	no
20	114	360	2	5	122	3	27	4,0	no	1
21	1	167	1	6	12	1	2	9,8,7,6,5,4,3,2,1	no	8
22	5	$*$	3	10	13	2	2	2,2,2,1,1,1,1,1,0	no	2
23	17	$*$	10	16	68	6	6	$\underbrace{2,\dots,2}_{10},\underbrace{1,\dots,1}_{17}$	no	12
24	3	21	1	11	11	0	1	8,6,6,4,4,4	no	1
25	35	$*$	2	325	43	5	342	5,4,3,3,1,1	no	2
26	$*$	101	14	13	$*$,224	12	13	$\underbrace{0,\dots,0}_{40}$	no	no
27	7	2	1	1	9	1	1	4,4,4	yes	no
28	25	4	1	2	91	4	4	7,7	yes	no
29	1	$*$	1	1734	4266	11	$*$	$2,\underbrace{1,\dots,1}_{10},0$	no	11
30	26	$*$	51	58	115	7	7	$\underbrace{1,\dots,1}_{18}$	no	no
31	6	0	2	2	6	0	0	1	yes	no
32	2	$*$	1	50	21	1	1	$2,2,2,2,2,2,2,\underbrace{1,\dots,1}_{10},0$	no	9
33	1	0	1	2	2	0	0	2,1,1	no	no
34	$*$	$*$	7132	110	$*$,$*$	7190	7190	$\underbrace{1,\dots,1}_{128}$	yes	no

References

[AGK] Amrhein, B.; Gloor, O.; Küchlin, W.: Walking faster. DISCO 1996, LNCS 1996.

[BF] Backelin, J.; Fröhberg, R.: How we prove that there are exactly 924 cyclic 7–roots. Proc. ISSAC 91, 103-111.

[BGK] Boege, R.; Gebauer, R.; Kredel, H.: Some examples for solving systems of algebraic equations by calculating Gröbner bases. J. Symb. Comp. 2, 83-89 (1987).

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

[Ch] Chou, S.-C.: Mechanical geometry theorem proving. Mathematics and Its Applications, D. Reidel, 1988.

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

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

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

[ES] Eisenbud, D.; Sturmfels, B.: Binomial Ideals. Duke Mathematical Journal 84, 1–45 (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.

[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).

[J] de Jong, T.: An algorithm for computing the integral closure. J. Symbolic Computation (to appear).

[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.

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

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

[Moe] Möller, H.M.: Solving of algebraic equations — an interplay of symbolical and numerical methods. Multivariate Approximation, Recent Trends and Results, Akademie Verlag, 161-176, 1997.

[R1] Ritt, J.F.: Differential equations from the algebraic standpoint. Colloquium Publications XIV, AMS, 1932.

[R2] Ritt, J.F.: Differential algebra. Colloquium Publications XXXIII, AMS, 1950.

[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).

[W] Wang, D.: Characteristic sets and zero structures of polynomial sets. Preprint, RISC-LINZ, 1989.

[Wu] Wu, W.T.: Basic principles of mechanical theorem proving in elementary geometries. J. of System Science and Mathematical Science, 4(3), 1984, 207-235.