J. Symbolic Computation (1998) **26**, 525–581
Article No. sy980227

Algorithmic Properties of Polynomial Rings

MICHAEL KALKBRENER

Department of Mathematics, Swiss Federal Institute of Technology, Zurich, Switzerland

In this paper we investigate how algorithms for computing heights, radicals, unmixed and primary decompositions of ideals can be lifted from a Noetherian commutative ring R to polynomial rings over R.

1. Introduction

It is a standard problem in mathematics to study which properties of a mathematical structure are preserved in derived structures. A typical result of this kind is the Hilbert Basis Theorem which says that polynomial rings over Noetherian commutative rings are Noetherian. In this paper we prove that certain algorithmic properties of coefficient rings are preserved in polynomial rings. The proofs are based on lifting techniques.

Studying algorithmic properties of polynomial rings by means of lifting techniques has a long history (see, for instance, Richman (1974) Seidenberg (1974, 1984), Shtokhamer (1988)) and different lifting algorithms have been proposed. In our approach two fundamental and, compared with classical methods, efficient algorithmic tools are used in this lifting process: Gröbner bases (Buchberger, 1965, 1970) and an algorithm which can be considered as a generalization of Ritt's prime decomposition algorithm for radicals (Ritt, 1950; Wu, 1984). In order to ensure the existence of these algorithms (see Trinks (1978), Zacharias (1978), Schaller (1978)) we assume that linear equations are solvable in the coefficient ring R, i.e. ideal membership is decidable and bases of syzygy modules are computable in R. Note that solvability of linear equations itself is an algorithmic property which is preserved in polynomial rings.

In this paper we study whether this is also true for the algorithmic properties

(1) heights of ideals are computable,
(2) radicals of ideals are computable,
(3) unmixed decompositions of ideals are computable,
(4) primary decompositions of ideals are computable.

More precisely, let R be a Noetherian commutative ring with identity and assume that linear equations are solvable in R. We want to know for each of these four algorithmic properties whether it holds in $R[x_1, \ldots, x_n]$ if it holds in R.

0747–7171/98/110525 + 57 $30.00/0

We give complete solutions for the four lifting problems by proving the following results:

(1) If heights of ideals are computable in R then heights of ideals are computable in $R[x_1, \ldots, x_n]$. We show that only one Gröbner basis in $R[x_1, \ldots, x_n]$ with respect to an arbitrary order and the heights of some ideals in R have to be computed in order to determine the height of an ideal in $R[x_1, \ldots, x_n]$.
(2) We give necessary and sufficient conditions for the computability of radicals in $R[x_1, \ldots, x_n]$ and construct a structurally simple and efficient algorithm using a combination of Ritt–Wu and Gröbner bases techniques.
(3) Unmixed decompositions of ideals are computable in $R[x_1, \ldots, x_n]$ if unmixed decompositions of ideals are computable in R. This central result is proved by Ritt–Wu and Gröbner bases techniques as well.
(4) We give necessary and sufficient conditions for the computability of isolated primes in $R[x_1, \ldots, x_n]$. Note that a primary decomposition algorithm can be easily constructed by combining an unmixed decomposition algorithm with an algorithm for computing isolated primes. Therefore it follows from the above result on the computability of unmixed decompositions that primary decompositions and associated primes of ideals are computable in $R[x_1, \ldots, x_n]$ if primary decompositions are computable in R and isolated primes of ideals are computable in $R[x_1, \ldots, x_n]$.

The construction of primary decomposition algorithms in polynomial rings is a classical problem in commutative algebra (Hermann, 1926). In recent years the increasing availability of computer algebra systems has led to a renewed interest in algorithmic problems and several methods for computing heights, radicals, unmixed and primary decompositions have been developed. Apart from Seidenberg's primary decomposition algorithm (Seidenberg, 1984) based on the Cohen structure theorem for complete local rings (Cohen, 1946) these methods work in polynomial rings over fields or PIDs only. The algorithms developed in the present paper do not have this restriction.

The paper has the following structure.

Section 2: Basic definitions.
Section 3: Gröbner bases.
Section 4: The Ritt–Wu approach.
Section 5: Computing heights.
Section 6: Computing radicals.
Section 7: Computing unmixed decompositions.
Section 8: Computing primary decompositions.

After giving some definitions and known results in Section 2 we turn to Gröbner bases. We will use Gröbner bases mainly for computing intersections of ideals, ideal quotients and localizations at single elements in $R[x_1, \ldots, x_n]$. In Section 3 we generalize some results in Gianni *et al.* (1988) and show that these operations can be performed with Gröbner bases even if some of the polynomials involved are zero-divisors. For an extensive introduction to Gröbner bases over rings we refer to Adams and Loustaunau (1994).

Not only the solvability of linear equations is preserved in polynomial rings. In Section 4 we prove that another basic algorithm can be lifted from a Noetherian commutative ring R with identity to polynomial rings over R. This algorithm solves the following

"splitting problem" for radicals: given a radical J in R and $f \in R$, compute radicals J' and J'' defined by

$J' :=$ intersection of those associated primes of J which contain f,

$J'' :=$ intersection of those associated primes of J which do not contain f.

If we want to lift this algorithm from R to $R[x_1, \ldots, x_n]$ we first have to decide how to represent radicals. Of course we could represent each radical by a finite basis. For polynomial rings over fields an alternative concept based on irreducible ascending sets has been developed by J.F. Ritt. We will not restrict ourselves to either one of these two possible ways of representing radicals but will use the following more general concept: let S be a set of finite subsets of R and *Rep* a function which maps every element of S to a radical different from R. This function need not be onto but we assume that for every radical J there exist $C_1, \ldots, C_r$ in S with $J = Rep(C_1) \cap \cdots \cap Rep(C_r)$ and that we have an algorithm $\mathbf{decompose}_R$ which actually computes these C_is from any basis of an ideal whose radical is J. Furthermore, we assume that there exists an algorithm $\mathbf{split}_R$ which solves the above splitting problem for any radical J which is given by finitely many elements $C_1, \ldots, C_r$ of S, i.e. $J = Rep(C_1) \cap \cdots \cap Rep(C_r)$. We call the set S together with the function *Rep* and the algorithms $\mathbf{decompose}_R$ and $\mathbf{split}_R$ a system of representations in R. Furthermore, $(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$ is a system of unmixed resp. prime representations if $Rep(A)$ is unmixed resp. prime for every $A \in S$.

In a polynomial ring $K[x_1, \ldots, x_n]$ over a field K a system of representations can be constructed in the following way (see Example 4.1): let S be the set of all those finite subsets of R which do not generate R and define the function *Rep* by $Rep(C) := \sqrt{C}$ for every $C \in S$, where $\sqrt{C}$ denotes the radical of the ideal generated by C. In this case $\mathbf{decompose}_R(F)$ is $\{F\}$ if F does not generate R and $\emptyset$ otherwise. The algorithm $\mathbf{split}_R$ is based on localization by means of Gröbner bases.

If K has characteristic 0 we can construct another system of representations using irreducible ascending sets: let S' be the set of irreducible ascending sets in $K[x_1, \ldots, x_n]$ and $S := S' \cup \{\{0\}\}$. We define the function *Rep* by mapping $\{0\}$ to the prime ideal $\{0\}$ and every irreducible ascending set C to the prime ideal whose generic point is given by C. The algorithm $\mathbf{decompose}_R$ is now the prime decomposition algorithm of Ritt. We can decide for every $f \in K[x_1, \ldots, x_n]$ and every prime ideal $P \subseteq K[x_1, \ldots, x_n]$ given by an irreducible ascending set whether $f \in P$ using pseudodivision (Wu, 1984). As $Rep(A)$ is prime for every $A \in S$ we obtain an algorithm $\mathbf{split}_R$. Therefore, the set S together with the function *Rep* and these two algorithms is a system of prime representations.

The usefulness of systems of representations is based on the following lifting theorem which is the main result in Section 4:

(a) If there exists a system of (unmixed) representations in R, a Noetherian commutative ring with identity, then there exists a system of (unmixed) representations in $R[x]$.

(b) Let $(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$ be a system of prime representations in R. Assume that for every $C \in S$ there exists an algorithm for expressing every non-constant element of $K(P)[x]$ as a product of irreducible polynomials, where $P := Rep(C)$ and $K(P)$ is the quotient field of the residue class ring R/P. Then there exists a system of prime representations in $R[x]$.

For proving this result we explicitly construct systems of representations $(\bar{S}, \overline{Rep}, \mathbf{decompose}_{R[x]}, \mathbf{split}_{R[x]})$ in $R[x]$. In the proof of **(b)** the elements of $\bar{S}$ are general-

izations of Ritt's irreducible ascending sets: each element of $\bar{S}$ is either in S or it has the form $C \cup \{f\}$, where $C \in S$, $P := Rep(C)$ and f is a non-constant polynomial in $R[x]$ which is irreducible in $K(P)[x]$. The algorithm $\mathbf{decompose}_{R[x]}$ is a generalization of the prime decomposition algorithm of Ritt. In the proof of **(a)** the elements of $\bar{S}$ are again elements of S or of the form $C \cup \{f\}$, where $C \in S$ and f is a non-constant polynomial in $R[x]$. In contrast to **(b)** no irreducibility condition is imposed on f but it is only assumed that its leading coefficient is not an element of an associated prime of $Rep(C)$. The algorithm $\mathbf{decompose}_{R[x]}$ constructed in the proof of **(a)** does not use factorization but the lazy decomposition strategy implemented in Axiom under the name **D5** (Della Dora *et al.*, 1985; Dicrescenzo and Duval, 1988; Lazard, 1992). It can be considered as a generalization of the unmixed decomposition algorithm for radicals in polynomial rings over fields presented in Kalkbrener (1993). Similar techniques are used in Wu (1987), Lazard (1991), Wang (1993) and Möller (1993). Implementations and comparisons of these algorithms can be found in Aubry *et al.* (1998) and Aubry and Moreno Maza (1998).

We have written an implementation of the algorithms in the proof of the above theorem which works for multivariate polynomial rings over the rationals. Experiments show that the practical performance of this implementation is rather good. At the end of Section 4 a short description of the implementation and timings on well known examples from computer algebra literature are given.

We will now describe how Gröbner bases and systems of representations can be used for computing heights, radicals and unmixed resp. primary decompositions in $R[x_1, \ldots, x_n]$. We first recall how heights of ideals in multivariate polynomial rings over fields can be computed by means of Gröbner bases. Let J be an ideal in $K[x_1, \ldots, x_n]$, where K is a field, and $\Delta(J)$ its independence complex, i.e.

$$\Delta(J) := \{\{x_{i_1}, \ldots, x_{i_m}\} \subseteq \{x_1, \ldots, x_n\} \mid J \cap K[x_{i_1}, \ldots, x_{i_m}] = \{0\}\}.$$

It is well known (see Gröbner (1970)) that the dimension resp. the height of J can be easily obtained from $\Delta(J)$:

$$height(J) = n - dim(J) = n - \max(\{|X| \mid X \in \Delta(J)\}). \tag{1.1}$$

Furthermore, for an arbitrary admissible order

$$height(J) = height(lm(J)), \tag{1.2}$$

where $lm(J)$ denotes the ideal generated by the leading monomials of the polynomials in J (see, for instance, Kalkbrener and Sturmfels (1995)). For total degree orders the ideals J and $lm(J)$ even have the same Hilbert function. Several papers for computing Hilbert functions (Buchberger, 1965; Möller and Mora, 1983, 1987; Kondrat'eva and Pankrat'ev, 1987; Bayer and Stillman, 1992; Bigatti *et al.*, 1991, 1993) and dimensions (Kandri-Rody, 1985; Kredel and Weispfenning, 1988; Giusti, 1988; Galligo and Traverso, 1989) of ideals in multivariate polynomial rings over fields are based on these results. It immediately follows from the equalities (1.1) and (1.2) that for computing the dimension resp. the height of an ideal J in $K[x_1, \ldots, x_n]$ it suffices to compute a single Gröbner basis with respect to an arbitrary order and the maximal cardinality c of the elements in $\Delta(lm(J))$. As $lm(J)$ is a monomial ideal c can be easily determined. Our main objective in Section 5 is the generalization of this algorithm to multivariate polynomial rings over R. We show that (1.2) holds for ideals in $R[x_1, \ldots, x_n]$ as well and we replace independence complexes by a more general concept with similar properties. It follows that even for

the computation of the height of an ideal in $R[x_1, \ldots, x_n]$ only one Gröbner basis with respect to an arbitrary order and the heights of some ideals in R have to be computed. In particular, if heights of ideals are computable in R and Gröbner bases are computable in $R[x_1, \ldots, x_n]$ then heights of ideals are computable in $R[x_1, \ldots, x_n]$. Furthermore we present a second algorithm for computing heights of ideals in $R[x_1, \ldots, x_n]$ which does not use Gröbner bases but the algorithm **decompose**.

In Section 6 we investigate the computability of radicals in $R[x_1, \ldots, x_n]$, i.e. whether there exists an algorithm which computes for every finite subset F of $R[x_1, \ldots, x_n]$ a finite basis of $\sqrt{F}$. It is well known that an ideal generated by a single polynomial f in a polynomial ring over a field K is a radical if and only if f is squarefree. In Lemma 92 in Seidenberg (1974) it is shown that if $I \subseteq K[x_1, \ldots, x_n]$ is a zero-dimensional ideal which contains a polynomial $f_i \in K[x_i]$ with $gcd(f_i, f_i') = 1$ for every $i \in \{1, \ldots, n\}$, where f' denotes the derivative of f, then I is an intersection of finitely many maximal ideals and therefore a radical. Based on these results algorithms for computing radicals are given in Gianni *et al.* (1988), Giusti and Heintz (1990), Alonso *et al.* (1990), Krick and Logar (1991) and Becker and Weispfenning (1993). In Eisenbud *et al.* (1992) methods are introduced which involve the use of the Jacobian matrix and homological techniques. In Armendáriz and Solerno (1995) it is shown that under certain assumptions radicals can be computed in single exponential time. Most of these algorithms not only compute the radical but an unmixed decomposition of the radical.

If K is a perfect field then a non-constant polynomial f in $K[x]$ is squarefree iff $gcd(f, f') = 1$. Hence, the above results give a relation between the computability of radicals and the squarefree parts of polynomials. The main objective of Section 6 is a formalization of this relation in the general setting of multivariate polynomial rings over R. More precisely, assume that radicals are computable and linear equations are solvable in R. Then the following two conditions are equivalent:

(a) For any natural number n radicals are computable in $R[x_1, \ldots, x_n]$.

(b) For any natural number n there exists an algorithm **squarefree** which computes for a given finite basis F of a radical in $R[x_1, \ldots, x_{n-1}]$ and a polynomial f in $R[x_1, \ldots, x_n]$ finite bases $F_1, \ldots, F_r$ of radicals in $R[x_1, \ldots, x_{n-1}]$ and $g_1, \ldots, g_r$ in $R[x_1, \ldots, x_n]$ with the following two properties:

- **(1)** The set of associated primes of $\sqrt{F}$ is the union of the sets of associated primes of the $\sqrt{F_i}$s.
- **(2)** Let $i \in \{1, \ldots, r\}$, P an associated prime of $\sqrt{F_i}$ and consider g_i and f as polynomials in $K(P)[x_n]$. Then g_i is a squarefree part of f.

For proving the implication (**b**) $\Rightarrow$ (**a**) it suffices to show that radicals are computable in the univariate polynomial ring $R[x]$. This is done in the following way. As radicals are computable and linear equations are solvable in R there exists a system of representations $(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$ in R such that S is the set of the finite bases of radicals different from R. By the lifting theorem we obtain a system of representations $(\bar{S}, \overline{Rep}, \mathbf{decompose}_{R[x]}, \mathbf{split}_{R[x]})$ in $R[x]$. Let F be a finite subset of $R[x]$ and assume that we want to compute a basis of $\sqrt{F}$. Using $\mathbf{decompose}_{R[x]}$ we first compute $C_1, \ldots, C_r \in \bar{S}$ with

$$\sqrt{F} = \bigcap_{i=1}^{r} \overline{Rep}(C_i).$$

In the next step, bases of the radicals $\overline{Rep}(C_1), \ldots, \overline{Rep}(C_r)$ are constructed. This is done by making the non-constant polynomials in the C_is squarefree and by localizing at the leading coefficients of these squarefree polynomials by means of Gröbner bases. As we can compute intersections in $R[x]$ we finally obtain a basis of $\sqrt{F}$ from the bases of the $\overline{Rep}(C_i)$.

The structure of the above algorithms for computing heights and radicals in polynomial rings over R is almost as simple as the structure of their counterparts in polynomial rings over fields. In contrast, the problem of computing unmixed (resp. primary) decompositions over R seems to be much more difficult than over K. Efficient algorithms for computing unmixed decomposition of ideals over fields resp. PIDs can be obtained by modifying the primary decomposition algorithms in Gianni *et al.* (1988) and Becker and Weispfenning (1993) (see Alonso *et al.* (1990)). In Eisenbud *et al.* (1992) an interesting homological approach to the computation of the equidimensional hull (= intersection of the primary components of maximal dimension) of an ideal in $K[x_1, \ldots, x_n]$ is given.

In Section 7 we show that if linear equations are solvable and unmixed decompositions of ideals are computable in R then unmixed decompositions of ideals are computable in $R[x_1, \ldots, x_n]$ for any number of variables. Again it suffices to prove this result for the univariate polynomial ring $R[x]$. We construct an algorithm based on the following strategy. As unmixed decompositions of ideals are computable and linear equations are solvable in R there exists a system of unmixed representations $(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$ in R. By the lifting theorem we obtain a system of unmixed representations

$$(\bar{S}, \overline{Rep}, \mathbf{decompose}_{R[x]}, \mathbf{split}_{R[x]})$$

in $R[x]$. Let F be a finite subset of $R[x]$, I the ideal generated by F and assume that we want to compute an unmixed decomposition of I. Using $\mathbf{decompose}_{R[x]}$ we first compute $C_1, \ldots, C_r \in \bar{S}$ with

$$\sqrt{F} = \bigcap_{i=1}^{r} \overline{Rep}(C_i).$$

It is now easy to construct finite bases of ideals $I_1, \ldots, I_r$ such that $I = I_1 \cap \cdots \cap I_r$ and $\sqrt{I_j}$ is unmixed. It remains to decompose those I_js which are not unmixed. We distinguish two cases:

(a) I_j has an embedded prime P with $height(P \cap R) > height(I_j \cap R)$. In this case a decomposition is obtained by a localization technique which can be considered as a generalization of the decomposition strategy in Gianni *et al.* (1988).
(b) $height(P \cap R) = height(I_j \cap R)$ for every embedded prime P. If x is an element of some associated prime of I_j we decompose I_j by localization at x. Otherwise, we choose a sufficiently large natural number m and decompose $I_j + \langle x^m \rangle$ by the same technique as in (a). From the decomposition of $I_j + \langle x^m \rangle$ we compute a decomposition of I_j.

In the last section we deal with the computation of primary decompositions of ideals. This classical problem was first solved for ideals in multivariate polynomial rings over fields in Hermann (1926) (see also Seidenberg (1974)). In the last 20 years several new methods for computing primary decompositions of ideals in multivariate polynomial rings over fields (Lazard, 1985; Kredel, 1987; Eisenbud *et al.*, 1992; Shimoyama and Yokoyama, 1994; Gräbe, 1995), the integers (Seidenberg, 1978), factorially closed principal ideal

domains (Ayoub, 1982; Gianni *et al.*, 1988) and commutative Noetherian rings with identity (Seidenberg, 1984) have been proposed. A related problem is the computation of the isolated primes of an ideal I or, equivalently, the associated primes of $\sqrt{I}$ (Ritt, 1950; Chistov and Grigoryev, 1983; Wu, 1984; Giusti and Heintz, 1990; Wang, 1993). Just as the computation of radicals is closely connected with the computation of squarefree parts of polynomials, the computation of isolated primes is closely connected with the factorization of polynomials. More precisely, assume that linear equations are solvable and isolated primes of ideals are computable in R. Using similar techniques as in the proof of the theorem about the computability of radicals we show that the following two conditions are equivalent:

(a) For every number of variables n isolated primes of ideals are computable in the polynomial ring $R[x_1, \ldots, x_n]$.

(b) For every number of variables n and every finite basis of a prime ideal P in the polynomial ring $R[x_1, \ldots, x_n]$ there exists an algorithm for expressing every non-constant element of the univariate polynomial ring $K(P)[x]$ as a product of irreducible polynomials.

Assume that linear equations are solvable and primary decompositions are computable in R and isolated primes of ideals are computable in $R[x_1, \ldots, x_n]$. Then it is easy to compute for an arbitrary ideal I in $R[x_1, \ldots, x_n]$ a decomposition $I = I_1 \cap \cdots \cap I_r$ such that the radicals of the ideals $I_1, \ldots, I_r$ are prime. We now apply the strategy developed for the computation of unmixed decompositions to the I_js. It is easy to see that in this way we obtain primary decompositions of the I_js and therefore a primary decomposition of I. Hence we have proved that primary decompositions and associated primes of ideals are computable in $R[x_1, \ldots, x_n]$ if linear equations are solvable and primary decompositions are computable in R and isolated primes of ideals are computable in $R[x_1, \ldots, x_n]$.

2. Basic Definitions

Throughout this paper let K be a field and R a Noetherian commutative ring with identity. We assume that R is effectively given, i.e. we can carry out the ring operations in R. Let F be a subset of R. The ideal generated by F is denoted by $\langle F \rangle$ and the radical of $\langle F \rangle$ by $\sqrt{F}$. If $F = \{f_1, \ldots, f_r\}$ we write $\langle f_1, \ldots, f_r \rangle$ instead of $\langle \{f_1, \ldots, f_r\} \rangle$. Let $h : R \to R'$ be a ring homomorphism and J an ideal in R. The ideal generated by the image of J in R' is denoted by $J\,R'$. For $c \in R$ we define

$$J : c^\infty \;:=\; \{a \in R \mid c^m \cdot a \in J \text{ for some natural number } m\}.$$

Let f be a polynomial in $R[x_1, \ldots, x_n]$. The image of f in $(R/J)[x_1, \ldots, x_n]$ is denoted by f^J. If J is prime then the quotient field of the residue class ring R/J is denoted by $K(J)$.

We recall the definition of the height of an ideal (see Zariski and Samuel (1975a, p.240), Zariski and Samuel (1975b, p. 90) or Matsumura (1970, p.71)). A prime ideal $P \neq R$ is said to have height h if there exists at least one chain $P_0 \subset P_1 \subset \ldots \subset P_h = P$, where the P_i are prime ideals, and there exists no such chain with more than $h+1$ ideals. The height of an arbitrary ideal $J \neq R$ is the minimum of the heights of the prime ideals containing J. We denote the height of J by $height(J)$ and define $height(R) := \infty$. As R

is Noetherian every ideal $\neq R$ has finite height (Zariski and Samuel, 1975a, p.241). The following result (Kaplansky, 1970, Theorem 149) will be frequently used.

THEOREM 2.1. *Let P be a prime ideal in R with $height(P) = m$ and Q a prime ideal in the univariate polynomial ring $R[x]$ with $Q \neq P\,R[x]$ and $Q \cap R = P$. Then*

$$height(P\,R[x]) = m \text{ and } height(Q) = m + 1.$$

Let I be an ideal in $R[x_1, \ldots, x_n]$ and $I = Q_1 \cap \cdots \cap Q_r$ an irredundant primary decomposition. The equidimensional hull of I, denoted by $hull(I)$, is the intersection of the primary components of minimal height. The ideal I is unmixed if

$$height(Q_i) = height(Q_j)$$

for $i, j \in \{1, \ldots, r\}$. It is strongly unmixed if

$$height(Q_i \cap R[x_1, \ldots, x_k]) = height(Q_j \cap R[x_1, \ldots, x_k])$$

for $i, j \in \{1, \ldots, r\}$ and $k \in \{0, \ldots, n\}$. We denote the set $\{\sqrt{Q_1}, \ldots, \sqrt{Q_r}\}$ of associated primes of I by $ap(I)$.

Let $PP(x_1, \ldots, x_n)$ denote the set of power products in the variables $x_1, \ldots, x_n$ and $\prec$ an arbitrary admissible order on $PP(x_1, \ldots, x_n)$. For any non-zero polynomial $f \in R[x_1, \ldots, x_n]$ write $f = cX + f'$, where $c \in R \setminus \{0\}$ and $X \in PP(x_1, \ldots, x_n)$ with $X \succ X'$ for every power product X' in f'. With this notation we set

$$\begin{array}{ll} lc(f) := c, & \text{the leading coefficient of } f, \\ lpp(f) := X, & \text{the leading power product of } f, \\ lm(f) := cX, & \text{the leading monomial of } f. \end{array}$$

The total degree of f in $x_1, \ldots, x_n$ is denoted by $deg(f)$ and the degree of f in the variable x_i by $deg_{x_i}(f)$. Furthermore, we define $lc(0) := lpp(0) := lm(0) := 0$ and $deg(0) := deg_{x_i}(0) := -1$. For an ideal I in $R[x_1, \ldots, x_n]$ we denote the ideal $\langle \{lm(f) \mid f \in I\} \rangle$ by $lm(I)$.

Let $f, g \in R[x]$ with $g \neq 0$. There exist polynomials $pquo(f, g)$ and $prem(f, g)$, called the pseudoquotient and pseudoremainder of f and g, such that

$$(lc(g))^d \cdot f = pquo(f, g) \cdot g + prem(f, g),$$

$$deg(pquo(f, g)) < d \text{ and } deg(prem(f, g)) < deg(g),$$

where $d := max(\{deg(f) - deg(g) + 1, 0\})$. Note that the pseudoquotient and pseudoremainder of f and g are usually not uniquely determined if R is not an integral domain. Let g be a non-constant polynomial in a polynomial ring $K[x_1, \ldots, x_n]$ and write g in the form $g = a \cdot \prod_{m=1}^{r} p_m^{i_m}$, where a is a constant and $p_1, \ldots, p_r \in K[x_1, \ldots, x_n]$ are irreducible and pairwise relatively prime. If $i_1 = \ldots = i_r = 1$ then g is called squarefree. The polynomial $\prod_{m=1}^{r} p_m$ is called a squarefree part of g. Obviously, two squarefree parts of g differ by a multiplicative constant only. We denote a fixed squarefree part of g by $squarefree(g)$ and define $squarefree(g) := g$ for every $g \in K$.

The natural numbers are denoted by $\mathbf{N}$, the rationals by $\mathbf{Q}$ and the complex numbers by $\mathbf{C}$.

3. Gröbner Bases

The Gröbner basis algorithm (Buchberger, 1965, 1970) is undoubtedly the most important algorithmic tool in commutative algebra. In this section we discuss the use of Gröbner bases to perform some basic ideal operations in polynomial rings over R. For an extensive introduction to Gröbner bases over rings we refer to Adams and Loustaunau (1994).

Let $\prec$ be an arbitrary admissible order on $PP(x_1, \ldots, x_n)$. A finite subset G of an ideal $I \subseteq R[x_1, \ldots, x_n]$ is a Gröbner basis of I w.r.t. $\prec$ if

$$\langle \{lm(g) \mid g \in G\} \rangle = lm(I).$$

For actually computing Gröbner bases in $R[x_1, \ldots, x_n]$ we have to assume certain computability conditions on R. We say that linear equations are solvable in R if

(1) for given $a, a_1, \ldots, a_m \in R$ it is possible to decide whether a is in the ideal generated by $a_1, \ldots, a_m$ in R and if so, find $b_1, \ldots, b_m \in R$ such that $a = \sum b_i a_i$,
(2) for given $a_1, \ldots, a_m \in R$ one can find a finite set of generators for the R-module $\{(b_1, \ldots, b_m) \in R^m \mid \sum b_i a_i = 0\}$.

Example 3.1. (a)Linear equations are solvable in R if R is a Euclidean domain or a finite ring.

(b) Assume that linear equations are solvable in R and let I be an ideal in R and f an element of R. Then linear equations are solvable in $R[x_1, \ldots, x_n]$, R/I and R_f, where R_f denotes the localization of R at f.

It has been shown in Trinks (1978), Zacharias (1978) and Schaller (1978) that there exists an algorithm which computes for any finite subset F of $R[x_1, \ldots, x_n]$ a Gröbner basis of $\langle F \rangle$ if linear equations are solvable in R. An improved version of this algorithm based on results in Möller (1988) can be found in Adams and Loustaunau (1994).

We will use Gröbner bases mainly for computing intersections of ideals, ideal quotients and localizations at elements of $R[x_1, \ldots, x_n]$. All these operations are based on the following properties of Gröbner bases with respect to elimination orders (Spear, 1977; Trinks, 1978).

Lemma 3.1. *Let I be an ideal in $R[y_1, \ldots, y_m, x_1, \ldots, x_n]$. Given any two orders $\prec_1$ and $\prec_2$ on $PP(y_1, \ldots, y_m)$ and $PP(x_1, \ldots, x_n)$ respectively, define an order $\prec$ by $Y_1 X_1 \prec Y_2 X_2$ if $X_1 \prec_2 X_2$, or $X_1 = X_2$ and $Y_1 \prec_1 Y_2$ for $Y_1, Y_2 \in PP(y_1, \ldots, y_m)$ and $X_1, X_2 \in PP(x_1, \ldots, x_n)$. Let $G \subseteq R[y_1, \ldots, y_m, x_1, \ldots, x_n]$ be a Gröbner basis of I with respect to $\prec$. Then*

(a) *G is a Gröbner basis of I with respect to $\prec_2$ on $R[y_1, \ldots, y_m][x_1, \ldots, x_n]$, the polynomial ring in $x_1, \ldots, x_n$ with coefficients in $R[y_1, \ldots, y_m]$,*
(b) *$G \cap R[y_1, \ldots, y_m]$ is a Gröbner basis of $I \cap R[y_1, \ldots, y_m]$ with respect to $\prec_1$.*

Proof. See Proposition 3.1 in Gianni *et al.* (1988). □

Theorem 3.1. *Assume that linear equations are solvable in R.*

Let I and J be ideals in $R[x_1, \ldots, x_n]$ and f an element of $R[x_1, \ldots, x_n]$. Then the following can be computed:

(a) $I \cap J$, **(b)** $I : J$, **(c)** $I : f^\infty$.

If the generators of J and f are not zero divisors then simpler proofs of **(b)** and **(c)** are given in Gianni *et al.* (1988, Corollary 3.2).

PROOF. Let y be a new indeterminate.

(a) Observe that

$$I \cap J = (yI + (y-1)J) \cap R[x_1, \ldots, x_n].$$

Hence, $I \cap J$ can be computed because of the above elimination property of Gröbner bases.

(b) Let $\{f_1, \ldots, f_r\}$ be a basis of J. Then $I : J = \bigcap I : \langle f_i \rangle$, so $I : J$ can be constructed provided each $I : \langle f_i \rangle$ can. Let $i \in \{1, \ldots, r\}$. We can compute a basis $\{q_1, \ldots, q_t\}$ of $\{0\} : \langle f_i \rangle$, a basis $\{p_1, \ldots, p_s\}$ of $I \cap \langle f_i \rangle$ and polynomials $g_1, \ldots, g_s$ with $g_j f_i = p_j$. Obviously,

$$\langle g_1, \ldots, g_s, q_1, \ldots, q_t \rangle \subseteq I : \langle f_i \rangle.$$

Conversely, let $g \in I : \langle f_i \rangle$. Then $gf_i \in I \cap \langle f_i \rangle$ and therefore $gf_i = h_1 p_1 + \cdots + h_s p_s$ for some $h_1, \ldots, h_s \in R[x_1, \ldots, x_n]$. Hence, $h_1 g_1 + \cdots + h_s g_s - g \in \{0\} : \langle f_i \rangle$ and therefore $g \in \langle g_1, \ldots, g_s, q_1, \ldots, q_t \rangle$ and $\langle g_1, \ldots, g_s, q_1, \ldots, q_t \rangle = I : \langle f_i \rangle$.

(c) Let I' be the ideal $\langle I \cup \{1 - yf\} \rangle$ in $R[x_1, \ldots, x_n, y]$ and $I'' := I' \cap R[x_1, \ldots, x_n]$. We will show that $I : f^\infty$ equals I''.

If $g \in I''$ then $g = h_1 p_1 + \cdots + h_s p_s + h(1 - yf)$ for $h_1, \ldots, h_s, h \in R[x_1, \ldots, x_n, y]$ and $p_1, \ldots, p_s \in I$. Writing $h_1, \ldots, h_s, h$ in the form

$$h_j = a_{jr} y^r + \cdots + a_{j0}, \quad h = b_r y^r + \cdots + b_0,$$

where $j \in \{1, \ldots, s\}$, $r := \max(deg_y(h_1), \ldots, deg_y(h_s), deg_y(h))$ and the as and bs are in $R[x_1, \ldots, x_n]$, we obtain

$$g = a_{10} p_1 + \cdots + a_{s0} p_s + b_0, \quad 0 = a_{1i} p_1 + \cdots + a_{si} p_s + b_i - b_{i-1} f \text{ for } i \in \{1, \ldots, r+1\}.$$

Hence, for

$$h'_j := a_{jr} f + a_{jr-1} f^2 + \cdots + a_{j0} f^{r+1}, \qquad h' := b_r + b_{r-1} f + \cdots + b_0 f^r$$

we obtain

$$\begin{aligned} gf^{r+1} &= \sum_{i=0}^{r+1} f^{r+1-i}(a_{1i} p_1 + \cdots + a_{si} p_s + b_i - b_{i-1} f) \\ &= h'_1 p_1 + \cdots + h'_s p_s + h'(f - f) \\ &= h'_1 p_1 + \cdots + h'_s p_s \in I. \end{aligned}$$

Thus, $I'' \subseteq I : f^\infty$.

Conversely, if $g \in I : f^\infty$ then $f^k g \in I$ and therefore $(yf)^k g \in I'$ for some natural number k. Hence,

$$g = (yf)^k g - ((yf)^k - 1)g = (yf)^k g - (yf - 1)((yf)^{k-1} + \cdots + 1)g \in I'$$

and therefore $I : f^\infty \subseteq I''$. □

Note that in proving **(a)** and **(c)** we did not use that linear equations are solvable in R but only that Gröbner bases are computable in $R[x_1, \ldots, x_n]$.

4. The Ritt–Wu Approach

In this section we formally define systems of representations and prove a lifting theorem for these systems. Furthermore, we present an application to geometry theorem-proving, and we discuss implementation issues.

4.1. DEFINITIONS

A system of representations $(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$ in R consists of

(1) a set S of finite subsets of R,
(2) a function Rep from S to the set of radicals in R which are unequal to R,
(3) an algorithm $\mathbf{decompose}_R$ that computes for a finite subset F of R a subset $\{C_1, \ldots, C_r\}$ of S such that

$$\sqrt{F} = \bigcap_{i=1}^{r} Rep(C_i),$$

(4) an algorithm $\mathbf{split}_R$ that computes for a given $A \in S$ and $f \in R$ a pair $(\{B_1, \ldots, B_r\}, \{C_1, \ldots, C_s\})$ of subsets of S such that

$$\bigcup_{i=1}^{r} ap(Rep(B_i)) = \{P \in ap(Rep(A)) \mid f \in P\},$$
$$\bigcup_{i=1}^{s} ap(Rep(C_i)) = \{P \in ap(Rep(A)) \mid f \notin P\}.$$

We call $(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$ a system of unmixed (resp. prime) representations if $Rep(A)$ is unmixed (resp. prime) for every $A \in S$.

EXAMPLE 4.1. Let R be the multivariate polynomial ring $K[x_1, \ldots, x_n]$.

(a) One possibility of representing radicals is the following: let S be the set of all those finite subsets of R which do not generate R and define the function Rep by $Rep(C) := \sqrt{C}$ for every $C \in S$. In this case $\mathbf{decompose}_R(F)$ is $\{F\}$ if $\langle F\rangle \neq R$ and $\emptyset$ otherwise. It remains to construct $\mathbf{split}_R$. Let $F \in S$, $f \in R$ and $G = \{g_1, \ldots, g_k\}$ a finite basis of $\langle F\rangle : f^\infty$. As $\sqrt{F} = \sqrt{F \cup \{f\}} \cap \sqrt{G}$ it is tempting to define $\mathbf{split}_R$ as the algorithm which returns $(\{F \cup \{f\}\}, \{G\})$ for given F, f. Note, however, that $\sqrt{F \cup \{f\}}$ may have associated primes which are not associated primes of $\sqrt{F}$. Therefore, let B_i be a finite basis of $\langle F\rangle : g_i^\infty$ for $i \in \{1, \ldots, k\}$ and consider the algorithm which computes $(\bar{B}, \bar{G})$ for given F, f, where

$$\bar{B} := \{B_i \mid i \in \{1, \ldots, k\},\ \langle B_i\rangle \neq R\}, \qquad \bar{G} := \emptyset \text{ otherwise.}$$
$$\bar{G} := \{G\} \text{ if } \langle G\rangle \neq R,$$

We will show that this algorithm satisfies the specification of $\mathbf{split}_R$.

Denote $\langle F\rangle$ by I and let

$$I = Q_1 \cap \cdots \cap Q_r \cap Q_{r+1} \cap \cdots \cap Q_s$$

be an irredundant primary decomposition of I and assume that f is in each of the

$\sqrt{Q_1}, \ldots, \sqrt{Q_r}$ but in none of the $\sqrt{Q_{r+1}}, \ldots, \sqrt{Q_s}$. Then $\langle G \rangle = Q_{r+1} \cap \cdots \cap Q_s$. Hence, for every $i \in \{1, \ldots, k\}$

$$\langle B_i \rangle = I : g_i^\infty = \bigcap_{j \in J_i} Q_j \text{ for some } J_i \subseteq \{1, \ldots, r\}.$$

If $B_i \in \bar{B}$ and $P \in ap(Rep(B_i))$ then P is an isolated prime ideal of $\bigcap_{j \in J_i} Q_j$. Thus P is also an isolated prime ideal of I and $f \in P$. Therefore,

$$\bigcup_{i=1}^{k} ap(Rep(B_i)) \subseteq \{P \in ap(Rep(F)) \mid f \in P\}.$$

On the other hand, if $P \in ap(Rep(F))$ and $f \in P$ then P is an isolated prime ideal of I and therefore $Q_{r+1} \cap \cdots \cap Q_s \not\subseteq P$. Let $i \in \{1, \ldots, k\}$ with $g_i \notin P$. Obviously, $P \in ap(Rep(B_i))$ and the first equality in the specification of $\mathbf{split}_R$ is proved.

The correctness of the algorithm now follows from

$$\begin{aligned} ap(Rep(G)) &= \{P \mid P \text{ isolated prime of } Q_{r+1} \cap \cdots \cap Q_s\} \\ &= \{\sqrt{Q_i} \mid i \in \{r+1, \ldots, s\}, \sqrt{Q_i} \text{ isolated prime of } I\} \\ &= \{P \in ap(Rep(F)) \mid f \notin P\}. \end{aligned}$$

If radicals are computable in $K[x_1, \ldots, x_n]$ we could also define S as the set of finite bases of radicals unequal to $K[x_1, \ldots, x_n]$. In this case the function *Rep* and the algorithm $\mathbf{split}_R$ are defined as above but $\mathbf{decompose}_R$ is now an algorithm which computes for an arbitrary finite subset F of $K[x_1, \ldots, x_n]$ a finite basis of $\sqrt{F}$.

(b) If K has characteristic 0 we can represent radicals by means of irreducible ascending sets: let S' be the set of irreducible ascending sets in $K[x_1, \ldots, x_n]$ and $S := S' \cup \{\{0\}\}$. We define the function *Rep* by mapping $\{0\}$ to the prime ideal $\{0\}$ and every irreducible ascending set C to the prime ideal whose generic point is given by C. The algorithm $\mathbf{decompose}_R$ is now the prime decomposition algorithm of Ritt. We can decide for every $f \in K[x_1, \ldots, x_n]$ and every prime ideal $P \subseteq K[x_1, \ldots, x_n]$ given by an irreducible ascending set whether $f \in P$ using pseudodivision (Wu, 1984). As $Rep(A)$ is prime for every $A \in S$ we obtain an algorithm $\mathbf{split}_R$. Therefore, the set S together with the function *Rep* and these two algorithms is a system of prime representations.

4.2. LIFTING THEOREM

If linear equations are solvable in R then linear equations are solvable in polynomial rings over R. We will now prove a similar lifting theorem for systems of representations.

THEOREM 4.1. **(a)** *If there exists a system of (unmixed) representations in R then there exists a system of (unmixed) representations in $R[x]$.*

(b) *Let $(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$ be a system of prime representations in R. Assume that for every $C \in S$ there exists an algorithm for expressing every non-constant element of $K(P)[x]$ as a product of irreducible polynomials, where $P := Rep(C)$. Then there exists a system of prime representations in $R[x]$.*

Throughout this section let $(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$ be a system of representations in R.

For proving part **(a)** of Theorem 4.1 we first construct a set $\bar{S}$ of finite subsets of $R[x]$ and a function $\overline{Rep}$ from $\bar{S}$ to the set of radicals in $R[x]$: we define $\bar{S}$ as the union

$$S \ \cup \ \bigcup_{C \in S} \{C \cup \{g\} \mid g \in R[x] \setminus R \text{ with } lc(g) \notin P \text{ for every } P \in ap(Rep(C))\}$$

and

$$\begin{array}{lll} \text{for } B \in S: & \overline{Rep}(B) & := \{f \in R[x] \mid f^P = 0 \text{ for every } P \in ap(Rep(B))\}, \\ \text{for } B \in \bar{S} \setminus S: & \overline{Rep}(B) & := \{f \in R[x] \mid squarefree(g^P) \text{ divides } f^P \text{ in } K(P)[x] \\ & & \quad \text{for every } P \in ap(Rep(B \cap R))\}, \\ & & \quad \text{where } \{g\} = B \setminus R. \end{array}$$

For showing that $\overline{Rep}(B)$ is a radical for every $B \in \bar{S}$ we need the following lemma which is proved in Kalkbrener (1994).

LEMMA 4.1. *Let I be an ideal in $R[x]$. Then the following three conditions are equivalent.*

(a) *I is a prime ideal in $R[x]$.*
(b) *$I \cap R$ is prime in R, J is prime in $K(I \cap R)[x]$ and $I\,(R/I \cap R)[x] = J \cap (R/I \cap R)[x]$, where J is the ideal $I\,K(I \cap R)[x]$.*
(c) *$I \cap R$ is prime in R and there exists a polynomial $q \in K(I \cap R)[x]$ which is either irreducible over $K(I \cap R)$ or zero and*

$$\text{for every } f \in R[x]: \quad f \in I \text{ iff } f^{I \cap R} \in \langle q \rangle.$$

LEMMA 4.2. *Let $B \in \bar{S}$. Then $\overline{Rep}(B)$ is a radical different from $R[x]$ and*

$$\begin{array}{lll} height(\overline{Rep}(B)) & = & height(Rep(B)) \qquad \text{if } B \in S, \\ height(\overline{Rep}(B)) & = & height(Rep(B \cap R)) + 1 \qquad \text{if } B \notin S. \end{array}$$

If $Rep(B \cap R)$ is unmixed then $\overline{Rep}(B)$ is unmixed.

PROOF. Let $P_1, \ldots, P_r$ be the associated prime ideals of $Rep(B \cap R)$. If $B \in S$ then $\overline{Rep}(B) = Rep(B)\,R[x]$ and therefore $\overline{Rep}(B)$ is a radical. The ideals $P_1\,R[x], \ldots, P_r\,R[x]$ are the associated prime ideals of $\overline{Rep}(B)$. By Theorem 2.1,

$$height(\overline{Rep}(B)) = height(Rep(B)).$$

Therefore, if $Rep(B \cap R)$ is unmixed then $\overline{Rep}(B)$ is unmixed.

Now assume that $B = C \cup \{g\}$ for some $C \in S$ and $g \in R[x] \setminus R$ with $lc(g) \notin P_i$ for every $i \in \{1, \ldots, r\}$. For $i \in \{1, \ldots, r\}$ let

$$g^{P_i} = lc(g^{P_i}) \cdot \prod_{j=1}^{l_i} q_{ij}^{k_{ij}}$$

be a factorization of g^{P_i} in $K(P_i)[x]$. By the previous lemma, the set

$$P_{ij} := \{f \in R[x] \mid q_{ij} \text{ divides } f^{P_i} \text{ in } K(P_i)[x]\}$$

is a prime ideal for every $j \in \{1, \ldots, l_i\}$. Obviously, $\overline{Rep}(B) = \bigcap P_{ij}$ and therefore $\overline{Rep}(B)$ is a radical. As $P_{ij} \cap R = P_i$ and $P_i\,R[x] \neq P_{ij}$ for every $i \in \{1, \ldots, r\}$, $j \in \{1, \ldots, l_i\}$ it follows from Theorem 2.1 that

$$height(\overline{Rep}(B)) = height(Rep(B \cap R)) + 1$$

and $\overline{Rep}(B)$ is unmixed if $Rep(B \cap R)$ is unmixed. □

We now come to the construction of an important algorithmic tool: an algorithm for computing gcd's modulo radicals.

$\mathbf{ggcd}_{R[x]}(C, F)$

Input: C, an element of S,
$F = \{f_1, \ldots, f_k\}$, a finite subset of $R[x]$.
Output: $\{(C_1, g_1), \ldots, (C_l, g_l)\}$, where $C_1, \ldots, C_l \in S$ and $g_1, \ldots, g_l \in R[x]$ such that $ap(Rep(C)) = \bigcup_{i=1}^{l} ap(Rep(C_i))$ and for every $i \in \{1, \ldots, l\}$ and $P \in ap(Rep(C_i))$:

(1) g_i^P is the gcd of $f_1^P, \ldots, f_k^P$ in $K(P)[x]$ (up to a multiplicative constant) if $F \neq \emptyset$ and $g_i = 0$ otherwise,
(2) if $g_i \neq 0$ then $lc(g_i) \notin P$,
(3) $g_i \in \langle Rep(C_i) \cup F \rangle$.

if $F \subseteq \{0\}$ **then**
  $O := \{(C, 0)\}$
else
  $f :=$ a non-zero element in F with minimal degree in x
  $F' := F \setminus \{f\}$
  $(M', M'') := \mathbf{split}_R(C, lc(f))$
  $h := f - lm(f)$
  $F'' := \{prem(g, f) \mid g \in F'\}$
  if $F'' \subseteq \{0\}$ **then**
    $O := \bigcup_{B' \in M'} \mathbf{ggcd}_{R[x]}(B', F' \cup \{h\}) \cup \bigcup_{B'' \in M''} \{(B'', f)\}$
  else
    $O := \bigcup_{B' \in M'} \mathbf{ggcd}_{R[x]}(B', F' \cup \{h\}) \cup \bigcup_{B'' \in M''} \mathbf{ggcd}_{R[x]}(B'', F'' \cup \{f\})$
  end
end
return(O)

Proof of termination and correctness of $\mathbf{ggcd}_{R[x]}$. Let G be a finite non-empty subset of $R[x]$. Define

$$sumdeg(\emptyset) := 0 \text{ and } sumdeg(G) := \sum_{g \in G} (deg(g) + 1).$$

Let C and F be sets which satisfy the input specification. We will prove termination and correctness by induction on $sumdeg(F)$.

It follows from $sumdeg(F) = 0$ that $F \subseteq \{0\}$ and therefore termination and correctness are obvious.

Let $sumdeg(F) > 0$. Obviously, $sumdeg(F' \cup \{h\}) < sumdeg(F)$. Furthermore, if $F'' \not\subseteq \{0\}$ then $sumdeg(F'' \cup \{f\}) < sumdeg(F)$. Hence, the termination of $\mathbf{ggcd}_{R[x]}$ follows from the induction hypothesis.

The equality $ap(Rep(C)) = \bigcup_{i=1}^{l} ap(Rep(C_i))$ and condition (2) in the specification of $\mathbf{ggcd}_{R[x]}$ immediately follow from the specification of $\mathbf{split}_R$ and the induction hypothesis.

Let (C_i, g_i) be an element of the output set and $P \in ap(Rep(C_i))$.

Assume that there exists a $B' \in M'$ with $(C_i, g_i) \in \mathbf{ggcd}_{R[x]}(B', F' \cup \{h\})$. By the induction hypothesis, $P \in ap(Rep(B'))$ and therefore $lc(f) \in P$ by the specification of $\mathbf{split}_R$. Hence, $h^P = f^P$ and condition (1) follows from the induction hypothesis. As $lc(f) \in Rep(C_i)$, the polynomial h is in the ideal generated by $Rep(C_i) \cup F$. Thus, condition (3) follows from the induction hypothesis.

If there exists a $B'' \in M''$ with $(B'', f) = (C_i, g_i)$ then conditions (1) and (3) are obviously satisfied. Otherwise, there exists a $B'' \in M''$ with $(C_i, g_i) \in \mathbf{ggcd}_{R[x]}(B'', F'' \cup \{f\})$. By the induction hypothesis, $P \in ap(Rep(B''))$ and therefore $lc(f) \notin P$ by the specification of $\mathbf{split}_R$. Therefore, the polynomials in the set $\{g^P \mid g \in F\}$ and the polynomials in the set $\{g^P \mid g \in F'' \cup \{f\}\}$ have the same gcd and condition (1) follows from the induction hypothesis. Condition (3) follows from the fact that $F'' \cup \{f\}$ is a subset of $\langle F \rangle$ and the induction hypothesis. □

Using this algorithm we construct $\mathbf{decompose}_{R[x]}$.

$\mathbf{decompose}_{R[x]}(F)$

Input: F, a finite subset of $R[x]$.
Output: $\{C_1, \ldots, C_r\}$, a subset of $\bar{S}$ with $\sqrt{F} = \bigcap_{i=1}^{r} \overline{Rep}(C_i)$.

$M := \mathbf{decompose}_R(F \cap R)$
forall $C \in M$ **do**
  $\{(C_1, g_1), \ldots, (C_k, g_k)\} := \mathbf{ggcd}_{R[x]}(C, F)$
  $J_C := \{i \in \{1, \ldots, k\} \mid g_i \neq 0\}$
  $O_C := \{C_i \mid i \in \{1, \ldots, k\} \setminus J_C\} \cup$
    $\{C_i \cup \{g_i\} \mid i \in \{1, \ldots, k\},\ g_i \notin R\} \cup$
    $\bigcup_{i \in J_C} \mathbf{decompose}_{R[x]}(F \cup \{lc(g_i)\})$
end
return$(\bigcup_{C \in M} O_C)$

Proof of termination of $\mathbf{decompose}_{R[x]}$. Let F be a finite subset of $R[x]$ and $C \in M$. It follows from the specification of $\mathbf{ggcd}_{R[x]}$ that for every $i \in J_C$ the leading coefficient of g_i is not in $Rep(C_i)$ and therefore not in $\langle F \cap R \rangle$. As R is Noetherian $\mathbf{decompose}_{R[x]}$ terminates. □

It is well known (see, for instance, Becker and Weispfenning (1993, Lemma 8.95)) that for an ideal $I \subseteq R[x]$ and $f \in R[x]$

$$\sqrt{I} = \sqrt{I : f^\infty} \cap \sqrt{I \cup \{f\}}. \tag{4.1}$$

We will now show that the correctness of $\mathbf{decompose}_{R[x]}$ is based on this fundamental decomposition formula.

Lemma 4.3. *Let $C \in S$ and $g \in R[x]$ such that $C \cup \{g\} \in \bar{S}$. Then*

$$\sqrt{\langle Rep(C) \cup \{g\} \rangle : lc(g)^\infty} = \overline{Rep}(C \cup \{g\}).$$

If $g^P \in K(P)[x]$ is squarefree for every $P \in ap(Rep(C))$ then

$$\langle Rep(C) \cup \{g\} \rangle : lc(g)^\infty = \overline{Rep}(C \cup \{g\}).$$

Proof. Let $f \in R[x]$. If $f \in \langle Rep(C) \cup \{g\} \rangle : lc(g)^\infty$ then g^P divides f^P in $K(P)[x]$ for

every $P \in ap(Rep(C))$ and therefore $f \in \overline{Rep}(C \cup \{g\})$. As $\overline{Rep}(C \cup \{g\})$ is a radical,

$$\sqrt{\langle Rep(C) \cup \{g\}\rangle : lc(g)^\infty} \subseteq \overline{Rep}(C \cup \{g\}). \tag{4.2}$$

On the other hand, if $f \in \overline{Rep}(C \cup \{g\})$ then there exists a natural number m such that g^P divides $(f^m)^P$ for every $P \in ap(Rep(C))$. Thus, $prem(f^m, g)^P = 0$ for every $P \in ap(Rep(C))$ and therefore $prem(f^m, g) \in \overline{Rep}(C)$ and $f^m \in \langle Rep(C) \cup \{g\}\rangle : lc(g)^\infty$. Together with (4.2) this completes the proof of the first equality.

If g^P is squarefree for every $P \in ap(Rep(C))$ we can choose m as 1 and the second equality immediately follows. □

Proof of correctness of $\mathbf{decompose}_{R[x]}$. Let O be the output set with input F. We will show correctness by induction.

Induction basis: $\langle F \cap R\rangle = R$. Then the output set O is empty and correctness is obvious.

Induction step: $\langle F \cap R\rangle \neq R$. It follows from the specification of $\mathbf{ggcd}_{R[x]}$, the definition of $\overline{Rep}$ and the induction hypothesis that $\sqrt{F} \subseteq \bigcap_{A \in O} \overline{Rep}(A)$. It remains to show that for every prime ideal P with $\sqrt{F} \subseteq P$

$$\text{there exists an } A \in O \text{ with } \overline{Rep}(A) \subseteq P. \tag{4.3}$$

Obviously, there exists a $C \in M$ and an $i \in \{1, \ldots, k\}$ with $Rep(C_i) \cup \{g_i\} \subseteq P$, where $\{(C_1, g_1), \ldots, (C_k, g_k)\} := \mathbf{ggcd}_{R[x]}(C, F)$. If $g_i = 0$ then (4.3) is obviously satisfied. Otherwise, by (4.1),

$$\sqrt{I} = \sqrt{I : lc(g_i)^\infty} \cap \sqrt{I \cup \{lc(g_i)\}},$$

where $I := \langle Rep(C_i) \cup \{g_i\}\rangle$. Therefore, by Lemma 4.3,

$$\overline{Rep}(C \cup \{g_i\}) \subseteq P \text{ or } lc(g_i) \in P.$$

In the second case (4.3) follows from the induction hypothesis. □

It remains to construct the algorithm $\mathbf{split}_{R[x]}$. First we need a subalgorithm which computes for given polynomials f, g the biggest factor h of f such that h and g are relatively prime.

Let $f, g \in K[x]$ with $f \neq 0$ and $f = lc(f) \cdot \prod_{m=1}^{r} p_m^{i_m}$ a factorization into irreducible monic factors. Define $M := \{m \in \{1, \ldots, r\} \mid p_m \text{ does not divide } g\}$ and

$$h := \prod_{m \in M} p_m^{i_m} \text{ if } M \neq \emptyset \text{ and } h := 1 \text{ if } M = \emptyset.$$

Note that h and g are relatively prime and that h is the biggest factor of f with this property. We denote h by $rpf(f, g)$.

$\mathbf{relatively\_prime}_{R[x]}(C, f, g)$

Input: C, an element of S,
f, g, polynomials in $R[x]$ such that $lc(f) \notin P$ for every $P \in ap(Rep(C))$.

Output: $\{(C_1, f_1), \ldots, (C_s, f_s)\}$, where $C_1, \ldots, C_s \in S$ and $f_1, \ldots, f_s \in R[x]$ such that $ap(Rep(C)) = \bigcup_{i=1}^{s} ap(Rep(C_i))$ and for every $i \in \{1, \ldots, s\}$ and $P \in ap(Rep(C_i))$ and some non-zero constant $c \in K(P)$

$$f_i^P = c \cdot rpf(f^P, g^P) \text{ and } lc(f_i) \notin P.$$

$\{(D_1, g_1), \ldots, (D_r, g_r)\} := \mathbf{ggcd}_{R[x]}(C, \{f, g\})$
$J := \{j \in \{1, \ldots, r\} \mid g_j \notin R\}$
$O := \{(D_j, f) \mid j \in \{1, \ldots, r\} \setminus J\} \cup \bigcup_{j \in J} \mathbf{relatively\_prime}_{R[x]}(D_j, pquo(f, g_j), g)$
return(O)

Proof of termination and correctness of $\mathbf{relatively\_prime}_{R[x]}$. Let C, f, g satisfy the input specification and let (C_i, f_i) be an element of the output $\{(C_1, f_1), \ldots, (C_s, f_s)\}$ of $\mathbf{relatively\_prime}_{R[x]}$. We do the proof by induction on $deg(f)$.

If $deg(f) = 0$ termination and correctness follow from the specification of **ggcd**.

Let $deg(f) > 0$. Obviously, $lc(pquo(f, g_j)) \notin P$ and $deg(f) > deg(pquo(f, g_j))$ for every $j \in J$ and $P \in ap(Rep(D_j))$. Therefore, $D_j, pquo(f, g_j), g$ satisfy the input specification of $\mathbf{relatively\_prime}_{R[x]}$ and the algorithm terminates.

It follows from the specification of $\mathbf{ggcd}_{R[x]}$ that $ap(Rep(C)) = \bigcup_{j=1}^{s} ap(Rep(C_j))$ and $lc(f_i) \notin P$ for every $P \in ap(Rep(C_i))$. If $(C_i, f_i) = (D_j, f)$ for some $j \in \{1, \ldots, r\} \setminus J$ then $g_j \in R$. Therefore, f^P and g^P are relatively prime for every $P \in ap(Rep(C_i))$ and correctness is obvious. Otherwise, there exists a $j \in J$ such that (C_i, f_i) is an element of the output of $\mathbf{relatively\_prime}_{R[x]}$ with input $D_j, pquo(f, g_j), g$. By definition of g_j,

$$rpf(f^P, g^P) = rpf(pquo(f, g_j)^P, g^P) \text{ for every } P \in ap(Rep(D_j)).$$

Therefore correctness follows from the induction hypothesis. □

$\mathbf{split}_{R[x]}(C, f)$

Input: C, an element of $\bar{S}$,
f, a polynomial in $R[x]$.
Output: $(\{B_1, \ldots, B_r\}, \{C_1, \ldots, C_s\})$, a pair of subsets of $\bar{S}$ such that

$$\bigcup_{i=1}^{r} ap(\overline{Rep}(B_i)) = \{P \in ap(\overline{Rep}(C)) \mid f \in P\}, \tag{4.4}$$

$$\bigcup_{i=1}^{s} ap(\overline{Rep}(C_i)) = \{P \in ap(\overline{Rep}(C)) \mid f \notin P\}. \tag{4.5}$$

$\{(D_1, g_1), \ldots, (D_m, g_m)\} := \mathbf{ggcd}_{R[x]}(C \cap R, (C \setminus R) \cup \{f\})$
if $C \subseteq R$ **then**
$O_1 := \{D_j \mid j \in \{1, \ldots, m\}$ and $g_j = 0\}$
$O_2 := \{D_j \mid j \in \{1, \ldots, m\}$ and $g_j \neq 0\}$
else
$O_1 := \{D_j \cup \{g_j\} \mid j \in \{1, \ldots, m\}$ and $g_j \notin R\}$
$g :=$ the only element in $C \setminus R$
$\{(E_1, h_1), \ldots, (E_k, h_k)\} := \mathbf{relatively\_prime}_{R[x]}(C \cap R, g, f)$
$O_2 := \{E_j \cup \{h_j\} \mid j \in \{1, \ldots, k\}$ and $h_j \notin R\}$
end
return$((O_1, O_2))$

Proof of termination and correctness of $\mathbf{split}_{R[x]}$. As $\mathbf{split}_{R[x]}$ obviously terminates it remains to show its correctness. Let C and f satisfy the input specification and let $(\{B_1, \ldots, B_r\}, \{C_1, \ldots, C_s\})$ be the output of $\mathbf{split}_{R[x]}$ with input C and f. It immediately follows from the specifications of $\mathbf{ggcd}_{R[x]}$ and $\mathbf{relatively\_prime}_{R[x]}$ that $\{B_1, \ldots, B_r\}$ and $\{C_1, \ldots, C_s\}$ are subsets of $\bar{S}$. Let P be a prime ideal in $R[x]$.

Case: $C \subseteq R$. $P \in ap(\overline{Rep}(B_i))$ for some $i \in \{1,\ldots,r\}$ iff $P = (P \cap R)\,R[x]$ and $P \cap R \in ap(Rep(C))$ and ${f^{P\cap R}} = 0$ iff $P \in ap(\overline{Rep}(C))$ and $f \in P$. Equality (4.5) can be shown in the same way.

Case: $C \not\subseteq R$. Denote the element of $C \setminus R$ by g and the set $\{j \in \{1,\ldots,m\} \mid g_j \notin R\}$ by J. $P \in ap(\overline{Rep}(B_i))$ for some $i \in \{1,\ldots,r\}$ iff $P \in ap(\overline{Rep}(D_j \cup \{g_j\}))$ for some $j \in J$ iff there exists a $j \in J$ and an irreducible factor $q \in K(P \cap R)[x]$ of ${g_j}^{P\cap R}$ with $P = \{h \in R[x] \mid q \text{ divides } h^{P\cap R}\}$ and $P \cap R \in ap(Rep(D_j))$ iff there exists an irreducible $q \in K(P\cap R)[x]$ which divides $g^{P\cap R}$ and $f^{P\cap R}$, $P = \{h \in R[x] \mid q \text{ divides } h^{P\cap R}\}$ and $P \cap R \in ap(Rep(C \cap R))$ iff $P \in ap(\overline{Rep}(C))$ and $f \in P$. Equality (4.5) can be shown in the same way. □

Therefore part **(a)** in Theorem 4.1 is proved. Before we give the proof of part **(b)** we compute a simple example and show how **decompose** can be applied to geometry theorem proving.

Example 4.2. First of all, we construct a system of unmixed representations $(S, Rep, \mathbf{decompose_Q}, \mathbf{split_Q})$ in $\mathbf{Q}$:

$$S := \{\emptyset\}, \quad Rep(\emptyset) := \{0\},$$

for input $\emptyset$ or $\{0\}$ $\mathbf{decompose_Q}$ returns $\{\emptyset\}$ and $\emptyset$ otherwise and $\mathbf{split_Q}(\emptyset, a)$ is $(\{\emptyset\}, \emptyset)$ if $a = 0$ and $(\emptyset, \{\emptyset\})$ otherwise. Using the constructions in the proof of Theorem 4.1(a) we obtain a system of unmixed representations in every multivariate polynomial ring over $\mathbf{Q}$. In particular, let $(\bar{S}, \overline{Rep}, \mathbf{decompose_{Q[x,y]}}, \mathbf{split_{Q[x,y]}})$ be a system of unmixed representations in $\mathbf{Q}[x, y]$.

We will now compute for $F := \{y^2 + x, xy + x^2\}$ elements $A_1, \ldots, A_r$ of $\bar{S}$ with

$$\sqrt{F} = \bigcap_{i=1}^{r} \overline{Rep}(A_i).$$

Computation of $\mathbf{decompose_{Q[x,y]}}(\{y^2 + x, xy + x^2\})$:

$\{\emptyset\} = \mathbf{decompose_{Q[x]}}(\emptyset)$,

$\{(\emptyset, x^4 + x^3)\} = \mathbf{ggcd_{Q[x,y]}}(\emptyset, \{y^2 + x, xy + x^2\})$.

Therefore,

$$\mathbf{decompose_{Q[x,y]}}(\{y^2 + x, xy + x^2\}) = \mathbf{decompose_{Q[x,y]}}(\{x^4 + x^3, y^2 + x, xy + x^2\}).$$

Computation of $\mathbf{decompose_{Q[x,y]}}(\{x^4 + x^3, y^2 + x, xy + x^2\})$:

$\{\{x^4 + x^3\}\} = \mathbf{decompose_{Q[x]}}(\{x^4 + x^3\})$.

This time the gcd of $y^2 + x$ and $xy + x^2$ has to be computed modulo the radical $\langle x^2 + x\rangle$, i.e. we have to compute

$$\mathbf{ggcd_{Q[x,y]}}(\{x^4 + x^3\}, \{x^4 + x^3, y^2 + x, xy + x^2\}).$$

In the course of the computation we divide $y^2 + x$ by $xy + x^2$. As the associated primes of $\langle x^2 + x\rangle$ are $\langle x\rangle$ and $\langle x + 1\rangle$ and the leading coefficient of $xy + x^2 \in \mathbf{Q}[x][y]$ is in $\langle x\rangle$ but not in $\langle x + 1\rangle$ the computation splits:

$\mathbf{ggcd_{Q[x,y]}}(\{x^4 + x^3\}, \{x^4 + x^3, y^2 + x, xy + x^2\}) =$

$\mathbf{ggcd}_{\mathbf{Q}[x,y]}(\{x\}, \{0, y^2 + x, x^2\}) \cup \mathbf{ggcd}_{\mathbf{Q}[x,y]}(\{x+1\}, \{0, xy + x^2, x^4 + x^3) =$
$\{(\{x\}, y^2 + x), (\{x+1\}, xy + x^2)\}$.

Therefore, we obtain

$$\mathbf{decompose}_{\mathbf{Q}[x,y]}(\{y^2 + x, xy + x^2\}) = \{\{x, y^2 + x\}, \{x + 1, xy + x^2\}\}.$$

The structure of $\mathbf{decompose}_{R[x]}$ is simple. Elimination is done by the subalgorithm **ggcd** and not by characteristic set computations as in Ritt's prime decomposition algorithm. Each time **ggcd** is called it computes new information about the elimination ideal of the input ideal. This information is used in the next approximation step.

Example 4.3. In the late 1970s and early 1980s the work of Wu Wen-tsun (Wu, 1978, 1984) renewed the interest in algebraic approaches to automated geometry theorem proving. In the following years it was demonstrated in a number of papers (see, for instance, Chou (1988), Chou and Gao (1990), Ko and Hussain (1985), Kapur and Wan (1990), Wang (1995), Chou and Schelter (1986), Kapur (1986), Kutzler and Stifter (1986)) that the characteristic set method of Ritt and Wu as well as the Gröbner basis algorithm are useful tools for proving theorems in Euclidean geometry although the applicability of the algebraic approach based on these methods is limited by the following two restrictions:

(a) Geometrical statements cannot be decided in real space but only in complex space. Therefore theorems in real geometry can only be confirmed by proving them in complex space but they cannot be disproved.
(b) This approach only works for those geometrical statements whose hypotheses and conclusions can be translated into algebraic equations.

The reason for the first restriction is that methods like Gröbner bases or characteristic sets can decide the solvability of a system of algebraic equations over algebraically closed fields only. Fortunately, it has turned out that only very few geometrical statements hold over the reals but not over the complex. See MacLane 8_3 in Kutzler (1988) for an example. Because of the second restriction we can use this algebraic approach to prove theorems about incidence, parallelism, perpendicularity, cocircularity, congruence, etc., but not about "betweenness", because no order predicate is available.

Often a geometrical statement is true only in a "generic" sense, i.e. after certain degenerate situations have been ruled out. Such degenerate situations typically occur when triangles collapse to a line segment, circles to a point, etc., and they are usually not explicitly mentioned. An automatic procedure for proving geometrical statements has to be able to deal with this problem, that means it has to be able to automatically find suitable nondegeneracy conditions which make the statement a theorem, if such conditions exist at all.

Hence this algebraic approach to automated geometry theorem proving leads to the following algebraic problem. Let $h_1, \ldots, h_m$ and c be polynomials in $\mathbf{Q}[x_1, \ldots, x_n]$ obtained by translating the hypotheses and conclusion of a geometrical statement into algebraic equations. During this translation process a set $X \subset \{x_1, \ldots, x_n\}$ of independent variables w.r.t. $\langle h_1, \ldots, h_m \rangle$ can be identified. We assume without loss of generality that $X = \{x_1, \ldots, x_t\}$. Now the problem is to decide whether there exists a d in $\mathbf{Q}[x_1, \ldots, x_t] \setminus \{0\}$ such that for all a in $\mathbf{C}^n$

$$(h_1(a) = \cdots = h_m(a) = 0 \wedge d(a) \neq 0) \Rightarrow c(a) = 0, \tag{4.6}$$

and, if so, to find such a nondegeneracy condition d.

For a subset F of $\mathbf{Q}[x_1, \ldots, x_n]$ let $V(F)$ denote the variety of F in $\mathbf{C}^n$, i.e.

$$V(F) = \{a \in \mathbf{C}^n \mid f(a) = 0 \text{ for every } f \in F\}.$$

Let $V(\{h_1, \ldots, h_r\}) = V_1 \cup \ldots \cup V_k$ be a decomposition into irreducible varieties. We may assume that for some $l \in \{0, \ldots, k\}$ no non-zero element of $\mathbf{Q}[x_1, \ldots, x_t]$ vanishes on V_i for $i \in \{1, \ldots, l\}$ but there exists a non-zero $d_j \in \mathbf{Q}[x_1, \ldots, x_t]$ which vanishes on V_j for $j \in \{l+1, \ldots, k\}$. Define $V' := \bigcup_{i=1}^{l} V_i$ and $V'' := \bigcup_{j=l+1}^{k} V_j$. Obviously, (4.6) is true if and only if

$$c \text{ vanishes on } V'. \tag{4.7}$$

In this case $\prod_{j=l+1}^{k} d_j$ is a nondegeneracy condition. Hence the correctness of (4.6) can be decided by decomposing V into $V' \cup V''$ and by deciding (4.7).

We will now apply systems of representations to this problem. We construct a system of unmixed representations $(\bar{S}, \overline{Rep}, \mathbf{decompose}_R, \mathbf{split}_R)$ in $R := \mathbf{Q}[x_1, \ldots, x_n]$ as in the previous example. For the hypotheses polynomials $h_1, \ldots, h_m$ we compute $C_1, \ldots, C_r \in \bar{S}$ with

$$\sqrt{\{h_1, \ldots, h_m\}} = \bigcap_{i=1}^{r} \overline{Rep}(C_i)$$

using $\mathbf{decompose}_R$. W.l.o.g. we assume that there exists an $s \in \{0, \ldots, r\}$ such that $C_i \cap \mathbf{Q}[x_1, \ldots, x_t] = \emptyset$ for $i \in \{1, \ldots, s\}$ and $C_j \cap \mathbf{Q}[x_1, \ldots, x_t] \neq \emptyset$ for $j \in \{s+1, \ldots, r\}$. Obviously,

$$V' = \bigcup_{i=1}^{s} V(\overline{Rep}(C_i)) \text{ and } V'' = \bigcup_{j=s+1}^{r} V(\overline{Rep}(C_j))$$

and therefore (4.6) holds if and only if the conclusion polynomial c vanishes on the variety of $Rep(C_i)$ for every $i \in \{1, \ldots, s\}$. This can be easily checked using $\mathbf{split}_R$.

We illustrate this procedure by means of the

Apollonios' Circle Theorem. *The altitude pedal of the hypotenuse of a right-angled triangle and the midpoints of the three sides of the triangle lie on a circle.*

We use the algebraic formulation given in Buchberger (1987). We have eight hypotheses polynomials $h_1, \ldots, h_8$ in $R := \mathbf{Q}[x_1, x_2, \ldots, x_{10}]$:

$$\begin{aligned}
h_1 &:= 2x_3 - x_1, & h_5 &:= (x_7 - x_3)^2 + x_8^2 - (x_7 - x_4)^2 - (x_8 - x_5)^2,\\
h_2 &:= 2x_4 - x_1, & h_6 &:= (x_7 - x_3)^2 + x_8^2 - (x_8 - x_6)^2 - x_7^2,\\
h_3 &:= 2x_5 - x_2, & h_7 &:= (x_9 - x_1)x_2 + x_1x_{10},\\
h_4 &:= 2x_6 - x_2, & h_8 &:= -x_1x_9 + x_2x_{10}.
\end{aligned}$$

The conclusion is

$$c := (x_7 - x_3)^2 + x_8^2 - (x_7 - x_9)^2 - (x_8 - x_{10})^2.$$

The set of independent variables is $\{x_1, x_2\}$.

We compute $\mathbf{decompose}_R(\{h_1, \ldots, h_8\})$ using our test implementation in Maple (see Subsection 4.3). The output set consists of 4 subsets of $\mathbf{Q}[x_1, \ldots, x_{10}]$:

$$\begin{aligned}
C_1 := \{\, & x_1x_{10} + x_2x_9 - x_2x_1, -x_1^2x_9 - x_2^2x_9 + x_2^2x_1, 4x_8 - x_2, -4x_7 + x_1, 2x_6 - x_2,\\
& 2x_5 - x_2, 2x_4 - x_1, 2x_3 - x_1 \,\},
\end{aligned}$$

$C_2 := \{ x_{10}, x_9, 4x_8 - x_2, 2x_6 - x_2, 2x_5 - x_2, x_4, x_3, x_1 \}$,
$C_3 := \{ x_{10}, x_9, -4x_7 + x_1, x_6, x_5, 2x_4 - x_1, 2x_3 - x_1, x_2 \}$,
$C_4 := \{ x_6, x_5, x_4, x_3, x_2, x_1 \}$.

Only C_1 does not contain an element of $\mathbf{Q}[x_1, x_2]$. Thus we can check whether the Apollonios' Circle Theorem is true by computing $\mathbf{split}_R(C_1, c)$. It turns out that c vanishes on the variety of $\overline{Rep}(C_1)$. Hence Apollonios' Circle Theorem is true and the polynomial $x_1 x_2$ is a nondegeneracy condition, because x_1 is in C_2 and C_4 and x_2 is in C_3.

An alternative strategy for deciding the correctness of a geometrical statement is based on localization: we add the negated conclusion to the hypotheses polynomials and use this enlarged set as input for **decompose**. It can be easily shown (Kalkbrener, 1995) that the geometrical statement is true if and only if every element B_i of the output set $\{B_1, \ldots, B_r\}$ contains a polynomial $g_i \in \mathbf{Q}[x_1, \ldots, x_t]$. In this case the product $\prod_{i=1}^{r} g_i$ is a nondegeneracy condition. Therefore, for proving Apollonios' Circle Theorem we have to compute $\mathbf{decompose}_{R[x_{11}]}(\{h_1, \ldots, h_8, cx_{11} - 1\})$, where x_{11} is a new variable. The output set only contains $C := C_4 \cup \{cx_{11} - 1\}$. As $C \cap \mathbf{Q}[x_1, x_2] = \{x_1, x_2\}$, Apollonios' Circle Theorem is true and x_1 and x_2 are both nondegeneracy conditions.

Sometimes it is important to find the simplest nondegeneracy condition with respect to some criterion. Our approach can be used for constructing the simplest nondegeneracy condition with respect to a lexicographical degree ordering (see Kalkbrener (1995)). A different approach to the computation of simplest nondegeneracy conditions can be found in Winkler (1990).

Part **(b)** of Theorem 4.1 has already been proved in Kalkbrener (1994). We review the constructions in this paper.

Even if $(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$ is a system of prime representations the system of representations in $R[x]$ constructed in part **(a)** is not. We therefore have to modify our constructions. We assume that $(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$ is a system of prime representations and define a new set $\bar{S}$ and a new function $\overline{Rep}$:

$$\bar{S} := S \cup \bigcup_{C \in S} \{C \cup \{f\} \mid f \in R[x] \text{ such that } f^{P_C} \text{ is irreducible over } K(P_C)\},$$

where $P_C := Rep(C)$, and

$$\begin{aligned} &\text{for } B \in S: && \overline{Rep}(B) := \{f \in R[x] \mid f^P = 0\}, \text{ where } P := Rep(B), \\ &\text{for } B \in \bar{S} \setminus S: && \overline{Rep}(B) := \{f \in R[x] \mid g^P \text{ divides } f^P \text{ in } K(P)[x]\}, \\ & && \qquad \text{where } \{g\} = B \setminus R \text{ and } P := Rep(B \cap R). \end{aligned}$$

It follows from Lemma 4.1 that $\overline{Rep}(B)$ is a prime ideal for every $B \in \bar{S}$. If $B \in \bar{S}$ is given membership for $\overline{Rep}(B)$ can be algorithmically decided using pseudodivision. As $\overline{Rep}(B)$ is a prime ideal for every $B \in \bar{S}$ the construction of $\mathbf{split}_{R[x]}$ is trivial.

It remains to construct the algorithm $\mathbf{decompose}_{R[x]}$. As we are working with prime ideals instead of radicals we can replace $\mathbf{ggcd}_{R[x]}$ by the following simpler algorithm: using $\mathbf{split}_R$ we can algorithmically decide for every $C \in S$ and $f \in R$ whether $f \in Rep(C)$. Hence, using pseudodivision we can easily construct an algorithm that satisfies the following specification.

$\mathbf{gcd}_{R[x]}(C, F)$

Input: C, an element of S,
$F = \{f_1, \ldots, f_r\}$, a non-empty finite subset of $R[x]$.
Output: g, a polynomial in $\langle P \cup F\rangle$ such that g^P is the greatest common divisor of ${f_1}^P, \ldots, {f_r}^P$ in $K(P)[x]$ (up to a multiplicative constant), where $P := Rep(C)$.

By assumption, there exists the following factorization algorithm.

$\mathbf{factor}_{R[x]}(C, f)$

Input: C, an element of S,
f, a polynomial in $R[x]$ with $f^P \neq 0$, where $P := Rep(C)$.
Output: $\{g_1, \ldots, g_k\}$, a set of polynomials in $R[x]$ such that $lc(g_i) \notin P$ and ${g_i}^P$ is either constant or irreducible over $K(P)$ for every $i \in \{1, \ldots, k\}$ and there exists a q in R with $q^P \cdot f^P = \prod_{i=1}^k {g_i}^P$.

Using these algorithms we construct $\mathbf{decompose}_{R[x]}$:

$M := \mathbf{decompose}_R(F \cap R)$
forall $C \in M$ **do**
  if $f^{Rep(C)} = 0$ for every $f \in F$ **then**
    $O_C := \{C\}$
  else
    $g := \mathbf{gcd}_{R[x]}(C, F)$
    $\{g_1, \ldots, g_k\} := \mathbf{factor}_{R[x]}(C, g)$
    $O_C := \{C \cup \{g_i\} \mid i \in \{1, \ldots, k\},\ g_i \notin R\} \cup$
      $\bigcup_{i=1}^k \mathbf{decompose}_{R[x]}(F \cup \{lc(g_i)\})$
  end
end
return$(\bigcup_{C \in M} O_C)$

Note that in general $\mathbf{decompose}_{R[x]}$ does not compute an irreducible prime decomposition of a given radical.

The proof of termination and correctness of $\mathbf{decompose}_{R[x]}$ can be found in Kalkbrener (1994). It is based on the following modification of Lemma 4.3.

LEMMA 4.4. *Let $C \in S$ and $f \in R[x]$ such that $lc(f) \notin P$ and f^P is irreducible over $K(P)$, where $P := Rep(C)$. Then*

$$\langle P \cup \{f\}\rangle : lc(f)^\infty = \overline{Rep}(C \cup \{f\}).$$

4.3. IMPLEMENTATION AND COMPLEXITY ISSUES

We are currently experimenting with an implementation of the algorithm **decompose** developed in the proof of Theorem 4.1**(a)**. This implementation is written in Maple and works for multivariate polynomial rings over the rationals only.

For implementing **decompose** efficiently it is necessary to modify the subalgorithm

ggcd. Otherwise, the enormous coefficient growth caused by the pseudodivisions in **ggcd** will lead to an unacceptable performance of the whole algorithm. For controlling the coefficient growth subresultant techniques (Collins, 1967; Brown and Traub, 1971) or trial division can be used (Hearn, 1979; Stoutemyer, 1985). Furthermore, in the current implementation the polynomials computed by **ggcd** are factored in order to keep the intermediate polynomials as small as possible.

The computation usually splits into lots of different branches. Many of these branches lead to the computation of superfluous components. In order to avoid some of these unnecessary computations Krull's Primidealkettensatz (see, for instance, Zariski and Samuel (1975a, p.240)) is used: the components with height greater than the cardinality of the input set are removed. Because of the recursive structure of **decompose** this criterion is useful even if the input ideal is 0-dimensional.

Despite these improvements large intermediate polynomials have been computed in some of the examples. This phenomenon is easy to understand. During the computation of **decompose**(F), where $F \subseteq \mathbf{Q}[x_1, \ldots, x_n]$, approximations of the elimination ideals of $\sqrt{F}$ are computed. These approximations are improved step by step till the elimination ideals are finally obtained. Sometimes the first approximations are much smaller than the elimination ideals and generated by rather large polynomials. Some of these large polynomials are constructed during the computation. For instance, the computation of Fee's system (see Czapor (1989, Problem 4) or Czapor and Geddes (1986, Problem 5)) with order $c > d > q > b > p$ could not be completed because of too large intermediate polynomials. However, the current implementation of **decompose** performed rather well in most of the examples we computed.

Example 4.4. The following class of examples is rather popular in the computer algebra literature. For any natural number n define

$$\begin{aligned} f_1 &:= x_1 + x_2 + \cdots + x_{n-1} + x_n, \\ f_2 &:= x_1x_2 + x_2x_3 + \cdots + x_{n-1}x_n + x_nx_1, \\ &\cdots \\ f_{n-1} &:= x_1x_2\cdots x_{n-1} + x_2x_3\cdots x_n + \cdots + x_{n-1}x_n\cdots x_{n-3} + x_nx_1\cdots x_{n-2}, \\ f_n &:= x_1x_2\cdots x_n - 1. \end{aligned}$$

We choose $n = 5$. The computation of a Gröbner basis is already rather time-consuming if a purely lexicographic order is used. The polynomials $f_1, \ldots, f_5$ have 70 common solutions (Lazard, 1992). The algorithm **decompose** computes a decomposition

$$\sqrt{\{f_1, \ldots, f_5\}} = I_1 \cap \cdots \cap I_{15},$$

where each I_j is a radical with at most 12 zeros. The computing time on a Sparc 4 is 659 s.

The following examples are taken from Böge *et al.* (1986). The computing times are given in seconds (s). The computations have been done on a Sparc 4.

Trinks 1	*Katsura 4*	*Rose*	*Hairer 2*	*Butcher*
8	113	2084	164	162

The variables have been ordered as in Böge *et al.* (1986). If in *Katsura 4* the order $U4 > U2 > U0 > U3 > U1$ is chosen (Czapor, 1989, Problem 2(a)) the computing time

is 26 s and if in *Rose* the order $U4 > U3 > A46$ is chosen (Czapor, 1989, Problem 3) the computing time is 181 s.

Because of the structure of **decompose** we expect that the performance of this algorithm can be significantly improved by parallelization.

Assume that R is a polynomial ring over a field. We do not know the complexity of $\mathbf{decompose}_{R[x]}$. However, in Szanto (1997) the complexity of a modified version has been analysed and bounds similar to those in Chistov and Grigoryev (1983) and Giusti and Heintz (1990) have been proved. In Gallo and Mishra (1990) bounds for computing characteristic sets are given.

5. Computing Heights

Let J be an ideal in $K[x_1, \ldots, x_n]$ and $\Delta(J)$ its independence complex, i.e.

$$\Delta(J) := \{\{x_{i_1}, \ldots, x_{i_m}\} \subseteq \{x_1, \ldots, x_n\} \mid J \cap K[x_{i_1}, \ldots, x_{i_m}] = \{0\}\}.$$

It immediately follows from the equalities (5.1) and (5.2) that for computing the dimension (resp. the height) of J it suffices to compute a single Gröbner basis with respect to an arbitrary order and the maximal cardinality c of the elements in $\Delta(lm(J))$:

$$height(J) = n - dim(J) = n - \max(\{|X| \mid X \in \Delta(J)\}) \tag{5.1}$$

and for an arbitrary admissible order

$$height(J) = height(lm(J)). \tag{5.2}$$

Our main objective in this section is the generalization of this algorithm to multivariate polynomial rings over R. We show that even for the computation of the height of an ideal in $R[x_1, \ldots, x_n]$ only one Gröbner basis with respect to an arbitrary order and the heights of some ideals in R have to be computed. Furthermore, we present a second algorithm for computing heights of ideals in $R[x_1, \ldots, x_n]$ which does not use Gröbner bases but the algorithm **decompose**. We finish this section by generalizing a result about the connectedness of independence complexes of prime ideals proved in Kalkbrener and Sturmfels (1995).

Obviously, we could define independence complexes for ideals in $R[x_1, \ldots, x_n]$ as well. Unfortunately, not enough information is contained in the independence complex of an ideal in $R[x_1, \ldots, x_n]$ and therefore (5.1) does not hold in general. Instead of independence complexes we will use independence functions. Their definition is motivated by the following observation. For the ideal $J \subseteq K[x_1, \ldots, x_n]$ consider the function δ_J from the power set of $\{x_1, \ldots, x_n\}$ to $\{0, \infty\}$:

$$\delta_J(X) = 0 \text{ if } J_X = \{0\} \text{ and } \delta_J(X) = \infty \text{ if } J_X = K,$$

where $X \subseteq \{x_1, \ldots, x_n\}$ and J_X is the smallest ideal in K with $J \cap K[X] \subseteq J_X\, K[X]$. Obviously, $\delta_J(X) = 0$ if and only if $X \in \Delta(J)$. Hence, (5.1) becomes

$$height(J) = n - dim(J) = \min_{X \subseteq \{x_1, \ldots, x_n\}} (\delta_J(X) + n - |X|). \tag{5.3}$$

We now generalize the independence function δ to ideals in $R[x_1, \ldots, x_n]$. For an ideal I in $R[x_1, \ldots, x_n]$ let δ_I be the function from the power set of $\{x_1, \ldots, x_n\}$ to $\mathbf{N}_0 \cup \{\infty\}$ defined by

$$\delta_I(X) = height(I_X) \text{ if } I_X \neq R \text{ and } \delta_I(X) = \infty \text{ if } I_X = R,$$

where $X \subseteq \{x_1, \ldots, x_n\}$ and I_X is the smallest ideal in R with $I \cap R[X] \subseteq I_X\, R[X]$.

If $\{f_1, \ldots, f_r\}$ is a basis of $I \cap R[X]$ then I_X is the ideal generated by all the coefficients of the polynomials $f_1, \ldots, f_r$. Hence, we can obtain $\delta_I(X)$ by computing a Gröbner basis of I with respect to an appropriate elimination order and the height of an ideal in R.

EXAMPLE 5.1. Let $R := \mathbf{Q}[a, b]_P$ be the bivariate polynomial ring over the rationals localized at the prime $P := \langle b \rangle$ and $I \subseteq R[x, y]$ the ideal generated by

$$F := \{b^3 + b^2 + ab,\ b^2x + bx + ax,\ y^2 - b^2 - b\}.$$

F is a Gröbner basis w.r.t. the purely lexicographic order $\prec$ with $x \prec y$ (see Proposition 3.4 in Gianni *et al.* (1988)). Hence, $\delta_I(\emptyset) = 1$ because the height of $I_\emptyset = \langle b^3 + b^2 + ab \rangle$ in R is 1 and $\delta_I(\{x\}) = \infty$ because

$$I_{\{x\}} = \langle b^3 + b^2 + ab,\ b^2 + b + a \rangle = \langle b^2 + b + a \rangle = R.$$

The function δ and the complex Δ have similar properties. We summarize some basic facts about the function δ in the following lemma whose proof is immediate from the definitions.

LEMMA 5.1. *Let I and J be ideals in $R[x_1, \ldots, x_n]$ and X a subset of $\{x_1, \ldots, x_n\}$.*

(a) *If $I \subseteq J$ then $\delta_I(X) \leq \delta_J(X)$.*
(b) $\delta_{\sqrt{I}}(X) = \delta_I(X)$.
(c) $\delta_{I \cap J}(X) = \delta_{I \cdot J}(X) = \min(\delta_I(X), \delta_J(X))$.
(d) *Let $P_1, \ldots, P_r$ be the associated prime ideals of I. Then*

$$\delta_I(X) = \min(\delta_{P_1}(X), \ldots, \delta_{P_r}(X)).$$

By applying the previous lemma to monomial ideals we obtain the following result.

LEMMA 5.2. *Let I and J be ideals in $R[x_1, \ldots, x_n]$, X a subset of $\{x_1, \ldots, x_n\}$ and $\prec$ an arbitrary admissible order.*

(a) *If $I \subseteq J$ then $\delta_{lm(I)}(X) \leq \delta_{lm(J)}(X)$.*
(b) $\delta_{lm(\sqrt{I})}(X) = \delta_{lm(I)}(X)$.
(c) $\delta_{lm(I \cap J)}(X) = \delta_{lm(I \cdot J)}(X) = \min(\delta_{lm(I)}(X), \delta_{lm(J)}(X))$.
(d) *Let $P_1, \ldots, P_r$ be the associated prime ideals of I. Then*

$$\delta_{lm(I)}(X) = \min(\delta_{lm(P_1)}(X), \ldots, \delta_{lm(P_r)}(X)).$$

PROOF. Statement **(a)** follows from $lm(I) \subseteq lm(J)$.

Let $f \in \sqrt{I}$. Then there exists a natural number m with $f^m \in I$. If $lm(f)^m \neq 0$ then $lm(f)^m = lm(f^m)$ and therefore $lm(f) \in \sqrt{lm(I)}$. Otherwise, $lm(f)^m = 0$ implies $lm(f) \in \sqrt{lm(I)}$. Therefore,

$$\sqrt{lm(I)} = \sqrt{lm(\sqrt{I})}$$

and **(b)** holds.

The left equality in **(c)** follows from part **(b)** and $\sqrt{I \cdot J} = \sqrt{I \cap J}$. The inequality

$$\delta_{lm(I \cdot J)}(X) \geq \min(\delta_{lm(I)}(X), \delta_{lm(J)}(X))$$

follows from

$$lm(I) \cdot lm(J) \subseteq lm(I \cdot J),$$

while the reverse inclusion follows from **(a)**.

Part **(d)** is a direct consequence of **(b)** and **(c)**. □

For every ideal I in $K[x_1, \ldots, x_n]$ we have $\Delta(lm(I)) \subseteq \Delta(I)$. However, there is nothing similar for the function δ.

EXAMPLE 5.2. Let R be the bivariate polynomial ring $\mathbf{Q}[a, b]$, I the ideal generated by $\{ax + by\}$ in $R[x, y]$ and $\prec$ an admissible order with $x \succ y$. Then

$$\delta_I(\emptyset) = \delta_I(\{x\}) = \delta_I(\{y\}) = 0, \quad \delta_I(\{x, y\}) = 2$$

and

$$\delta_{lm(I)}(\emptyset) = \delta_{lm(I)}(\{y\}) = 0, \quad \delta_{lm(I)}(\{x\}) = \delta_{lm(I)}(\{x, y\}) = 1.$$

Before generalizing (5.3) we note two easy consequences of Theorem 2.1. Let $I \subseteq R[x_1, \ldots, x_n]$ be an ideal, $X \subseteq \{x_1, \ldots, x_n\}$ and $P \subseteq R$ a prime ideal with $I \cap R[X] \subseteq P\,R[X]$. Then

$$\begin{aligned} height(P) &= height(P\,R[X]) \\ &\geq height(I \cap R[X]) \\ &\geq height(I) + |X| - n. \end{aligned} \tag{5.4}$$

Furthermore, if I is prime there exists a $Y \subseteq \{x_1, \ldots, x_n\}$ such that

$$(I \cap R)\,R[Y] = I \cap R[Y] \text{ and } height(I) = height(I \cap R[Y]) + n - |Y|. \tag{5.5}$$

THEOREM 5.1. *Let I be an ideal in $R[x_1, \ldots, x_n]$. Then*

$$height(I) = \min_{X \subseteq \{x_1, \ldots, x_n\}} (\delta_I(X) + n - |X|).$$

PROOF. Assume that I is prime. By (5.4) and (5.5),

$$height(I) \leq \min_X(\delta_I(X) + n - |X|)$$

and for some $Y \subseteq \{x_1, \ldots, x_n\}$

$$\delta_I(Y) = height(I \cap R[Y]) = height(I) + |Y| - n.$$

Hence, the theorem is proved for prime ideals.

For an arbitrary ideal I in $R[x_1, \ldots, x_n]$ with associated primes $P_1, \ldots, P_r$ it follows from Lemma 5.1 that

$$\begin{aligned} height(I) &= \min(height(P_1), \ldots, height(P_r)) \\ &= \min_i(\min_X(\delta_{P_i}(X) + n - |X|)) \\ &= \min_X(\min_i(\delta_{P_i}(X) + n - |X|)) \\ &= \min_X(\delta_I(X) + n - |X|). \end{aligned}$$

□

This theorem leads to a first algorithm for computing the height of an ideal in the polynomial ring $R[x_1, \ldots, x_n]$. But this approach suffers from the fact that several Gröbner bases with respect to elimination orders have to be computed. In order to construct a more efficient algorithm we prove that $height(I) = height(lm(I))$ for every ideal I in $R[x_1, \ldots, x_n]$ and every admissible order on $PP(x_1, \ldots, x_n)$. If R is a field this can be done by showing that $R[x_1, \ldots, x_n]/lm(I)$ and $R[x_1, \ldots, x_n]/I$ are fibres of the same flat family (Theorem 15.17 in Eisenbud (1995) or Bayer and Mumford (1991)) and using Corollary 9.6 in Hartshorne (1977). Another proof can be found in Kalkbrener and Sturmfels (1995). We will now generalize this proof. First we need a couple of lemmata.

LEMMA 5.3. *Let I be an ideal in $R[x_1, \ldots, x_n]$ and P a prime ideals in R with $I \cap R \subseteq P$. Then*

(a) $height(I) \leq height(P) + height(I\,K(P)[x_1, \ldots, x_n])$.
(b) *If I is prime and $I \cap R = P$ then*

$$height(I) = height(P) + height(I\,K(P)[x_1, \ldots, x_n]).$$

PROOF. Let $X \in \Delta(I\,K(P)[x_1, \ldots, x_n])$. Then $I \cap R[X] \subseteq P\,R[X]$. Hence, **(a)** follows from (5.4) and

$$height(I\,K(P)[x_1, \ldots, x_n]) = n - \max(\{|X| \mid X \in \Delta(I\,K(P)[x_1, \ldots, x_n])\}). \tag{5.6}$$

By (5.5), there exists a $Y \subseteq \{x_1, \ldots, x_n\}$ with

$$P\,R[Y] = I \cap R[Y] \text{ and } height(I) = height(P) + n - |Y|.$$

As $Y \in \Delta(I\,K(P)[x_1, \ldots, x_n])$ we obtain **(b)** from (5.6) and **(a)**. □

We recall the representation of an order $\prec$ by a non-negative weight vector $\omega = (\omega_1, \ldots, \omega_n) \in \mathbf{N}_0^n$. Let $f(x_1, \ldots, x_n)$ be any polynomial in $R[x_1, \ldots, x_n]$. We consider $f(t^{\omega_1}x_1, \ldots, t^{\omega_n}x_n)$ as a univariate polynomial in t. Its leading coefficient $init(f)$ is a polynomial in $R[x_1, \ldots, x_n]$. We call it the initial form of f (with respect to ω).

For an ideal $I \subseteq R[x_1, \ldots, x_n]$ and $\omega \in \mathbf{N}_0^n$ we define the initial ideal $init(I)$ to be the ideal generated by $\{init(f) \mid f \in I\}$. We say that the vector ω represents the order $\prec$ for I if

$$lm(I) = init(I).$$

It is well known that for a fixed ideal J in $K[x_1, \ldots, x_n]$ every order $\prec$ can be represented by some $\omega \in \mathbf{N}_0^n$ (see, for instance, Mora and Robbiano (1988)). This result can be easily generalized to ideals in $R[x_1, \ldots, x_n]$.

LEMMA 5.4. *Let $\omega \in \mathbf{N}_0^n$ and G a Gröbner basis of the ideal $I \subseteq R[x_1, \ldots, x_n]$ with respect to $\prec$. If $init(g) = lm(g)$ for all $g \in G$ then ω represents $\prec$ for I.*

PROOF. As $\{lm(g) \mid g \in G\}$ generates $lm(I)$ we have $lm(I) \subseteq init(I)$. Let $f \in I$ and u a monomial in $init(f)$. It remains to show that $u \in lm(I)$. We do the proof by induction on $\prec$.

Induction basis: $1 = lpp(f)$. Obviously, $u \in lm(I)$.

Induction step: $1 \prec lpp(f)$. If $u = lm(f)$ then $u \in lm(I)$. If $u \neq lm(f)$ we can choose polynomials $g_1, \ldots, g_r \in G$ and monomials $v_1, \ldots, v_r$ such that $v_i \cdot lm(g_i) \neq 0$ and $lpp(v_i) \cdot lpp(g_i) = lpp(f)$ for every $i \in \{1, \ldots, r\}$ and

$$lm(f) = \sum_{i=1}^{r} v_i \cdot lm(g_i).$$

Hence, for $h := f - \sum_{i=1}^{r} v_i \cdot g_i$ we have $lpp(h) \prec lpp(f)$. From $init(v_i \cdot g_i) = v_i \cdot lm(g_i)$ we obtain that u occurs in $init(h)$. Hence, $u \in lm(I)$ follows from the induction hypothesis. □

Every admissible order on $PP(x_1, \ldots, x_n)$ is the lexicographical product of n weight orders (see Eisenbud (1995), Robbiano (1986)). Hence, Lemma 5.4 implies that for a fixed ideal I every order $\prec$ can be represented by some $\omega \in \mathbf{N}_0^n$. Using this result and Theorem 2.1 we now generalize Lemma 3 in Kalkbrener and Sturmfels (1995).

LEMMA 5.5. *Let $I \subseteq R[x_1, \ldots, x_n]$ be a prime ideal and $\prec$ any admissible order. Then there exists a prime ideal I' in $R[x_1, \ldots, x_n, x_{n+1}]$ such that $height(I') = height(I)$ and*

$$\langle lm(I) \cup \{x_{n+1}\}\rangle = \langle I' \cup \{x_{n+1}\}\rangle.$$

PROOF. Denote $K(I \cap R)$ by $\bar{K}$ and let π be the natural homomorphism from R to $\bar{K}$. Note that π induces a one-to-one correspondence between the set

$$\{P \mid P \text{ is a prime ideal in } R[x_1, \ldots, x_n] \text{ with } P \cap R = I \cap R\}$$

and the set of prime ideals in $\bar{K}[x_1, \ldots, x_n]$. Let $(s_1, \ldots, s_n)$ denote the generic point of $I\,\bar{K}[x_1, \ldots, x_n]$ and let t be a new variable which is algebraically independent of $\{s_1, \ldots, s_n\}$. Suppose that $\omega = (\omega_1, \ldots, \omega_n) \in \mathbf{N}_0^n$ represents $\prec$ for I. Let I' be the prime ideal in $R[x_1, \ldots, x_n, x_{n+1}]$ such that $I' \cap R = I \cap R$ and $I'\,\bar{K}[x_1, \ldots, x_{n+1}]$ has the generic point $(s_1 t^{\omega_1}, \ldots, s_n t^{\omega_n}, t)$. As ω represents $\prec$ for I, it suffices to prove that

$$\langle init(I) \cup \{x_{n+1}\}\rangle = \langle I' \cup \{x_{n+1}\}\rangle. \tag{5.7}$$

To prove the inclusion "$\subseteq$" in (5.7), we consider any $g \in I$ and we define

$$g' := g\left(\frac{x_1}{x_{n+1}^{\omega_1}}, \ldots, \frac{x_n}{x_{n+1}^{\omega_n}}\right) \cdot x_{n+1}^m,$$

where m is the smallest non-negative integer such that $g' \in R[x_1, \ldots, x_n, x_{n+1}]$. It follows from the definition of $init(g)$ that g' can be written in the form $g' = init(g) + h$, where $h \in R[x_1, \ldots, x_{n+1}]$ is divisible by x_{n+1}. From

$$\pi(g')(s_1 t^{\omega_1}, \ldots, s_n t^{\omega_n}, t) = \pi(g)(s_1, \ldots, s_n) \cdot t^m = 0$$

we conclude that $g' = init(g) + h$ is in I'. Therefore $init(g) \in \langle I' \cup \{x_{n+1}\}\rangle$.

To prove the reverse inclusion in (5.7), we consider any $f \in I'$. Writing $f = f_m x_{n+1}^m + \cdots + f_1 x_{n+1} + f_0$ as a polynomial in x_{n+1} with coefficients f_i in $R[x_1, \ldots, x_n]$, we need to show that f_0 lies in the initial ideal $init(I)$. We can assume that f_0 is unequal to 0.

We define $f' := f(x_1 x_{n+1}^{\omega_1}, \ldots, x_n x_{n+1}^{\omega_n}, x_{n+1})$, and we note that

$$\pi(f')(s_1, \ldots, s_n, t) = \pi(f)(s_1 t^{\omega_1}, \ldots, s_n t^{\omega_n}, t) = 0.$$

Write $f' = p_r x_{n+1}^r + \cdots + p_1 x_{n+1} + p_0$ as a polynomial in x_{n+1} with coefficients p_i in

$R[x_1, \ldots, x_n]$. As t is algebraically independent of $\{s_1, \ldots, s_n\}$, the polynomials $\pi(p_0), \ldots, \pi(p_r)$ are elements of $I\,\bar{K}[x_1, \ldots, x_n]$ and therefore $p_0, \ldots, p_r$ are elements of I. We have

$$\begin{aligned} f &= f'\left(\frac{x_1}{x_{n+1}^{\omega_1}}, \ldots, \frac{x_n}{x_{n+1}^{\omega_n}}, x_{n+1}\right) \\ &= p_r\left(\frac{x_1}{x_{n+1}^{\omega_1}}, \ldots, \frac{x_n}{x_{n+1}^{\omega_n}}\right) \cdot x_{n+1}^r + \cdots + p_0\left(\frac{x_1}{x_{n+1}^{\omega_1}}, \ldots, \frac{x_n}{x_{n+1}^{\omega_n}}\right). \end{aligned}$$

This identity implies that there exist $i_1, \ldots, i_k \in \{0, \ldots, r\}$ such that $f_0 = init(p_{i_1}) + \cdots + init(p_{i_k}) \in init(I)$. Thus, (5.7) is proved.

As

$$\begin{aligned} height(I' \cap R) &= height(I \cap R) \text{ and} \\ height(I'\,\bar{K}[x_1, \ldots, x_{n+1}]) &= height(I\,\bar{K}[x_1, \ldots, x_n]) \end{aligned}$$

we obtain from Lemma 5.3

$$\begin{aligned} height(I) &= height(I \cap R) + height(I\,\bar{K}[x_1, \ldots, x_n]) \\ &= height(I' \cap R) + height(I'\,\bar{K}[x_1, \ldots, x_{n+1}]) \\ &= height(I'). \end{aligned}$$

□

Now we are able to generalize (5.2) to polynomial rings over Noetherian commutative rings with identity.

THEOREM 5.2. *Let I be an ideal in $R[x_1, \ldots, x_n]$ and $\prec$ any admissible order. Then $height(I) = height(lm(I))$.*

PROOF. We first prove this theorem under the additional assumption that I is prime.

By Lemma 5.5 there exists a prime ideal I' in $R[x_1, \ldots, x_{n+1}]$ with

$$\langle lm(I) \cup \{x_{n+1}\}\rangle = \langle I' \cup \{x_{n+1}\}\rangle \text{ and } height(I) = height(I').$$

It follows from the definition of I' that $x_{n+1} \notin I'$ and therefore

$$height(\langle lm(I) \cup \{x_{n+1}\}\rangle) = height(\langle I' \cup \{x_{n+1}\}\rangle) > height(I).$$

By Theorem 2.1,

$$height(lm(I)) = height(\langle lm(I) \cup \{x_{n+1}\}\rangle) - 1 \geq height(I). \tag{5.8}$$

Define $P := I \cap R$. From Corollary 3.7 and Lemma 3.9 in Bayer *et al.* (1991), Lemma 5.3 and (5.2) we obtain

$$\begin{aligned} height(I) &= height(P) + height(I\,K(P)[x_1, \ldots, x_n]) \\ &= height(P) + height(lm(I\,K(P)[x_1, \ldots, x_n])) \\ &= height(P) + height(lm(I)\,K(P)[x_1, \ldots, x_n]) \\ &\geq height(lm(I)). \end{aligned}$$

Hence, the theorem is proved for prime ideals.

Let I be an arbitrary ideal in $R[x_1, \ldots, x_n]$ with associated primes $P_1, \ldots, P_r$. By Lemma 5.2 and Theorem 5.1,

$$height(I) = \min(height(P_1), \ldots, height(P_r))$$

$$
\begin{aligned}
&= \min(height(lm(P_1)), \ldots, height(lm(P_r))) \\
&= \min_i(\min_X(\delta_{lm(P_i)}(X) + n - |X|)) \\
&= \min_X(\min_i(\delta_{lm(P_i)}(X)) + n - |X|) \\
&= \min_X(\delta_{lm(I)}(X) + n - |X|) \\
&= height(lm(I)).
\end{aligned}
$$

□

We assume that we have given an algorithm $\mathbf{height}_R$ which computes for every finite subset F of R the height of $\langle F\rangle$. From Theorem 5.1 and Theorem 5.2 we obtain the following algorithm for computing heights of ideal in $R[x_1, \ldots, x_n]$.

$\mathbf{height}_{R[x_1,\ldots,x_n]}(F)$

Input: F, a finite subset of $R[x_1, \ldots, x_n]$.
Output: h, the height of $\langle F\rangle$.

$G :=$ Gröbner basis of $\langle F\rangle$ w.r.t. an arbitrary order
forall $X \subseteq \{x_1, \ldots, x_n\}$ **do**
    $C_X := \{lc(g) \in R \mid g \in G, lpp(g) \in PP(X)\}$
    $h_X := \mathbf{height}_R(C_X)$
end
return$(\min_{X\subseteq\{x_1,\ldots,x_n\}}(h_X + n - |X|))$

In general, it is not necessary to compute the height of $\langle C_X\rangle$ for each $X \subseteq \{x_1, \ldots, x_n\}$. For instance, if we know that $a := height(\langle C_X\rangle) - |X|$ is negative for some $X \subseteq \{x_1, \ldots, x_n\}$ we only have to compute the heights of $\langle C_{X'}\rangle$ with $|X'| > -a$.

By constructing $\mathbf{height}_{R[x_1,\ldots,x_n]}$ we have proved the following theorem.

THEOREM 5.3. *If heights of ideals are computable in R and Gröbner bases are computable in $R[x_1, \ldots, x_n]$ then heights of ideals are computable in $R[x_1, \ldots, x_n]$.*

EXAMPLE 5.3. Let $R := \mathbf{Q}[a, b]_P$ be the bivariate polynomial ring over the rationals localized at the prime $P := \langle b\rangle$. As in Example 5.1 we consider the ideal $I \subseteq R[x, y]$ generated by

$$F := \{b^3 + b^2 + ab,\ b^2x + bx + ax,\ y^2 - b^2 - b\}.$$

As F is a Gröbner basis w.r.t. the purely lexicographic order $\prec$ with $x \prec y$ we have

$$lm(I) \ = \ \langle b^3 + b^2 + ab,\ b^2x + bx + ax,\ y^2\rangle.$$

Hence,

$$
\begin{array}{lcll}
\delta_{lm(I)}(\emptyset) & = & height(\langle b^3 + b^2 + ab\rangle) & = \ 1, \\
\delta_{lm(I)}(\{x\}) & = & height(\langle b^3 + b^2 + ab,\ b^2 + b + a\rangle) & = \ \infty, \\
\delta_{lm(I)}(\{y\}) & = & height(\langle b^3 + b^2 + ab,\ 1\rangle) & = \ \infty, \\
\delta_{lm(I)}(\{x, y\}) & = & height(\langle b^3 + b^2 + ab,\ b^2 + b + a,\ 1\rangle) & = \ \infty
\end{array}
$$

and

$$height(I) = height(lm(I)) = \min_{X\subseteq\{x_1,\ldots,x_n\}}(\delta_{lm(I)}(X) + n - |X|) = 3.$$

We will now present a second algorithm for computing the height of an ideal in $R[x_1, \ldots, x_n]$. Assume that there exists a system of representations

$$(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$$

in R. It can be shown as in Example 4.1 that such a system exists if linear equations are solvable in R. Furthermore, we assume that there exists an algorithm which computes for every $A \in S$ the height of $Rep(A)$. By Theorem 4.1, we can construct a system of representations

$$(\bar{S}, \overline{Rep}, \mathbf{decompose}_{R[x_1,\ldots,x_n]}, \mathbf{split}_{R[x_1,\ldots,x_n]})$$

in $R[x_1, \ldots, x_n]$. Let I be an ideal in $R[x_1, \ldots, x_n]$ given by a finite basis F. We compute the height of I in the following way: by applying $\mathbf{decompose}_{R[x_1,\ldots,x_n]}$ to F we obtain $A_1, \ldots, A_r \in \bar{S}$ with

$$\sqrt{I} = \bigcap_{i=1}^{r} \overline{Rep}(A_i).$$

Hence, by Lemma 4.2,

$$\begin{aligned} height(I) &= \min_i(height(\overline{Rep}(A_i))) \\ &= \min_i(height(Rep(A_i \cap R)) + |A_i \setminus R|). \end{aligned}$$

We finish this section by generalizing the notion of an independence complex. For a proper ideal $I \subset R[x_1, \ldots, x_n]$ the set

$$\Delta(I) := \{X \subseteq \{x_1, \ldots, x_n\} \mid \delta_I(X) = height(I \cap R)\}$$

is called the independence complex of I. Note that if R is a field then this definition coincides with the usual definition. By Theorem 5.1, we have for an ideal $I \subset R[x_1, \ldots, x_n]$

$$height(I) \leq \min_{X \in \Delta(I)} (\delta_I(X) + n - |X|) = height(I \cap R) + n - \max(\{|X| \mid X \in \Delta(I)\}).$$

If I is prime equality follows from (5.5).

COROLLARY 5.1. *Let I be a prime ideal in $R[x_1, \ldots, x_n]$. Then*

$$height(I) = height(I \cap R) + n - \max(\{|X| \mid X \in \Delta(I)\}).$$

Note that Corollary 1 does not hold for arbitrary ideals.

EXAMPLE 5.4. Let R be the bivariate polynomial ring $Q[a, b]$ and I the ideal generated by $\{a, bx_1, bx_2\}$ in $R[x_1, x_2]$. Then $\Delta(I) = \{\emptyset\}$ and

$$height(I) = 2 \neq 1 + 2 - 0 = height(I \cap R) + n - \max(\{|X| \mid X \in \Delta(I)\}).$$

The independence complex $\Delta(I)$ is called pure if all its maximal elements have the same cardinality and it is called strongly connected if for any two maximal elements X, X' there exists a sequence of maximal elements $X = X_0, X_1, X_2, \ldots, X_k = X'$ such that $|X_i \setminus X_{i-1}| = |X_{i-1} \setminus X_i| = 1$ for $i = 1, \ldots, k$. It has been shown in Kalkbrener and Sturmfels (1995) (see also Gräbe (1993)) that if R is a field and I is prime

$$\Delta(lm(I)) \text{ is pure and strongly connected for any admissible order.} \tag{5.9}$$

This result can be easily generalized.

COROLLARY 5.2. *Let I be a prime ideal in $R[x_1, \ldots, x_n]$ and $\prec$ any admissible order. Then $\Delta(lm(I))$ is pure and strongly connected.*

PROOF. Obviously, $I\,K(I \cap R)[x_1, \ldots, x_n]$ is a prime ideal and

$$\Delta(lm(I)) = \Delta(lm(I\,K(I \cap R)[x_1, \ldots, x_n])).$$

Thus, Corollary 5.2 follows from (5.9). □

6. Computing Radicals

The main objective of this section is a formalization of the relation between the computability of squarefree parts of polynomials and radicals in the general setting of multivariate polynomial rings over R.

We say that radicals are computable in R if there exists an algorithm $\mathbf{radical}_R$ which computes for every finite subset F of R a basis of the radical of $\langle F \rangle$.

THEOREM 6.1. *The following two conditions are equivalent if radicals are computable and linear equations are solvable in R.*

- **(a)** *For any natural number n radicals are computable in $R[x_1, \ldots, x_n]$.*
- **(b)** *For any natural number n there exists an algorithm $\mathbf{squarefree}_{R[x_1,\ldots,x_n]}$ which computes for a finite basis $F \subseteq R[x_1, \ldots, x_{n-1}]$ of a radical different from $R[x_1, \ldots, x_{n-1}]$ and a polynomial f in $R[x_1, \ldots, x_n]$ finite bases $F_1, \ldots, F_r$ of radicals in $R[x_1, \ldots, x_{n-1}]$ and polynomials $g_1, \ldots, g_r$ in $R[x_1, \ldots, x_n]$ such that*

$$ap(\langle F \rangle) = \bigcup_{i=1}^{r} ap(\langle F_i \rangle)$$

and g_i^P is a squarefree part of f^P in $K(P)[x_n]$ for every $i \in \{1, \ldots, r\}$ and $P \in ap(\langle F_i \rangle)$.

PROOF. Obviously it suffices to prove that the following two conditions are equivalent.

- **(1)** Radicals are computable in the univariate polynomial ring $R[x]$.
- **(2)** There exists an algorithm $\mathbf{squarefree}_{R[x]}$ which computes for a given finite basis $F \subseteq R$ of a radical different from R and a polynomial f in $R[x]$ finite bases $F_1, \ldots, F_r$ of radicals in R and polynomials $g_1, \ldots, g_r$ in $R[x]$ such that

$$ap(\langle F \rangle) = \bigcup_{i=1}^{r} ap(\langle F_i \rangle)$$

and g_i^P is a squarefree part of f^P in $K(P)[x]$ for every $i \in \{1, \ldots, r\}$ and $P \in ap(\langle F_i \rangle)$.

We first construct a system of representations

$$(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$$

in R. Let S be the set of those finite subsets of R which generate radicals different from R and define Rep by $Rep(F) := \langle F\rangle$. By assumption, we can compute for a finite subset $F \subseteq R$ a finite basis G of its radical. Let $\mathbf{decompose}_R$ be the algorithm which returns for given F the empty set if $\langle F\rangle = R$ and $\{G\}$ otherwise. It remains to show that there exists an algorithm $\mathbf{split}_R$. Let $F \in S$, $f \in R$, $G = \{g_1, \ldots, g_k\}$ a finite basis of $\langle F\rangle : f^\infty$ and B_i a finite basis of $\langle F\rangle : g_i^\infty$ for every $i \in \{1, \ldots, k\}$. As linear equations are solvable in R it follows from Theorem 3.1 that we can compute G and $B_1, \ldots, B_k$ using Gröbner bases. Consider now the algorithm which computes $(\bar{B}, \bar{G})$ for given F, f, where

$$\begin{array}{lcll} \bar{B} & := & \{B_i \mid i \in \{1,\ldots,k\},\ \langle B_i\rangle \neq R\}, & \\ \bar{G} & := & \{G\} \text{ if } \langle G\rangle \neq R, & \bar{G} := \emptyset \text{ otherwise.} \end{array}$$

As in Example 4.1 we can show that this algorithm satisfies the specification of $\mathbf{split}_R$.

We apply Theorem 4.1 and obtain a system of representations

$$(\bar{S}, \overline{Rep}, \mathbf{decompose}_{R[x]}, \mathbf{split}_{R[x]})$$

in $R[x]$.

(**1**) $\Leftarrow$ (**2**) It is now easy to construct an algorithm $\mathbf{radical}_{R[x]}$ for computing radicals in $R[x]$: let F be a finite subset of $R[x]$. If $\emptyset = \mathbf{decompose}_{R[x]}(F)$ then F generates $R[x]$ and $\mathbf{radical}_{R[x]}$ returns $\{1\}$ for given F. Otherwise, $\mathbf{decompose}_{R[x]}$ computes $C_1, \ldots, C_r \in \bar{S}$ with

$$\sqrt{F} = \bigcap_{i=1}^{r} \overline{Rep}(C_i).$$

Assume that the C_i are ordered in such a way that there exists an $s \in \{0, \ldots, r\}$ with $C_i \subseteq R$ for $i \in \{1, \ldots, s\}$ and $C_i \not\subseteq R$ for $i \in \{s+1, \ldots, r\}$. Define $F_{i1} := C_i$ and $k_i := 1$ for $i \in \{1, \ldots, s\}$. Let f_i be the uniquely determined element of $C_i \setminus R$ for $i \in \{s+1, \ldots, r\}$. Using $\mathbf{squarefree}_{R[x]}$ we can compute finite basis $G_{i1}, \ldots, G_{ik_i}$ of radicals in R and polynomials $g_{i1}, \ldots, g_{ik_i}$ in $R[x]$ such that

$$ap(\langle C_i \cap R\rangle) = \bigcup_{j=1}^{k_i} ap(\langle G_{ij}\rangle)$$

and g_{ij}^P is a squarefree part of f_i^P in $K(P)[x]$ for every $j \in \{1, \ldots, k_i\}$ and $P \in ap(\langle G_{ij}\rangle)$. W.l.o.g. assume that $lc(g_{ij}) \notin P$ for every $P \in ap(\langle G_{ij}\rangle)$. Hence,

$$\overline{Rep}(C_i) = \bigcap_{j=1}^{k_i} \overline{Rep}(G_{ij} \cup \{g_{ij}\}).$$

For $i \in \{s+1, \ldots, r\}$ and $j \in \{1, \ldots, k_i\}$ let F_{ij} be a basis of $\langle G_{ij} \cup \{g_{ij}\}\rangle : lc(g_{ij})^\infty$. Then, by Lemma 4.3, for every $i \in \{s+1, \ldots, r\}$ and $j \in \{1, \ldots, k_i\}$

$$\overline{Rep}(G_{ij} \cup \{g_{ij}\}) = \langle F_{ij}\rangle$$

and therefore

$$\sqrt{F} = \bigcap_{i=1}^{r} \bigcap_{j=1}^{k_i} \langle F_{ij}\rangle$$

is a decomposition into radicals. Since we can compute intersections of ideals in $R[x]$ we can compute a basis of $\sqrt{F}$.

(**1**) ⇒ (**2**) We will now use $\mathbf{ggcd}_{R[x]}$ and $\mathbf{radical}_{R[x]}$ for constructing algorithm $\mathbf{squarefree}_{R[x]}$. Let f be an element of $R[x]$ and F a finite basis of a radical $\neq R$. Then $F \in S$ and we can compute
$G := \mathbf{radical}_{R[x]}(F \cup \{f\})$
$\{(F_1, g_1), \ldots, (F_r, g_r)\} := \mathbf{ggcd}_{R[x]}(F, G)$
It follows from the specification of $\mathbf{ggcd}_{R[x]}$ that $F_1, \ldots, F_r$ are bases of radicals in R and

$$ap(\langle F\rangle) = \bigcup_{i=1}^{r} ap(\langle F_i\rangle).$$

Let $i \in \{1, \ldots, r\}$ and $P \in ap(\langle F_i\rangle)$. If $f^P \in K(P)$ then g_i^P is obviously a squarefree part of f^P. Assume that $f^P \notin K(P)$. Let $q_1, \ldots, q_s \in K(P)[x]$ be the irreducible factors of f^P and define $P_i := \{h \in R[x] \mid q_i \text{ divides } h^P\}$ for $i \in \{1, \ldots, s\}$. Obviously, $P_i \cap R = P$ and therefore, by Lemma 4.1, $P_1, \ldots, P_s$ are isolated prime ideals of $\langle G\rangle$. Hence,

$$\langle G\rangle = P_1 \cap \cdots \cap P_s \cap P_{s+1} \cap \cdots \cap P_r,$$

where $P_{s+1}, \ldots, P_r$ are prime ideals with $P_j \cap R \not\subseteq P$. It follows that there exists an $h \in \langle G\rangle$ such that h^P equals $\prod_{j=1}^{s} q_j$ up to a multiplicative constant. Hence, g_i^P equals $\prod_{j=1}^{s} q_j$ up to a multiplicative constant. Therefore, g_i^P is squarefree and divides f^P. As a power of h is in $\langle F \cup \{f\}\rangle$, f^P divides a power of g_i^P. Hence, g_i^P is a squarefree part of f^P. □

We will now write down the algorithm $\mathbf{radical}_{R[x]}$ in pseudocode.

If radicals are computable and linear equations are solvable in R then there exists a system of representations

$$(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$$

in R such that S is the set of those finite subsets of R which generate radicals different from R and $Rep(F) := \langle F\rangle$. Using the constructions in the proof of Theorem 4.1 we obtain a system of representations

$$(\bar{S}, \overline{Rep}, \mathbf{decompose}_{R[x]}, \mathbf{split}_{R[x]})$$

in $R[x]$. Furthermore, we assume that there exists an algorithm $\mathbf{squarefree}_{R[x]}$ with the following specification.

$\mathbf{squarefree}_{R[x]}(F, f)$

Input: $F \subseteq R$, a finite basis of a radical different from R,
f, a polynomial in $R[x]$.
Output: $\{(G_1, g_1), \ldots, (G_r, g_r)\}$, where $g_1, \ldots, g_r \in R[x]$ and $G_1, \ldots, G_r$ are finite bases of radicals in R with $ap(\langle F\rangle) = \bigcup_{i=1}^{r} ap(\langle G_i\rangle)$ and for every $i \in \{1, \ldots, r\}$ and $P \in ap(\langle G_i\rangle)$

(1) the polynomial g_i^P is a squarefree part of f^P in $K(P)[x]$ and
(2) $g_i = 0$ or $lc(g_i) \notin P$.

Based on $\mathbf{decompose}_{R[x]}$ and $\mathbf{squarefree}_{R[x]}$ we can now construct the algorithm $\mathbf{radical}_{R[x]}$:

radical$_{R[x]}(F)$

Input: F, a finite subset of $R[x]$.
Output: G, a basis of $\sqrt{F}$.

$M :=$ **decompose**$_{R[x]}(F)$
if $M = \emptyset$ **then**
  return$(\{1\})$
else
  forall $C \in M$ **do**
    if $C \subseteq R$ **then**
      $O_C := \{C\}$
    else
      $f :=$ the only element in $C \setminus R$
      $\{(G_1, g_1), \ldots, (G_r, g_r)\} :=$ **squarefree**$_{R[x]}(C \cap R, f)$
      forall $i \in \{1, \ldots, r\}$ **do**
        $F_i :=$ basis of $\langle G_i \cup \{g_i\}\rangle : lc(g_i)^\infty$
      end
      $O_C := \{F_1, \ldots, F_r\}$
    end
  end
  $G :=$ basis of $\bigcap_{C \in M} \bigcap_{H \in O_C} \langle H\rangle$
  return(G)
end

Assume that the set S consists of bases of unmixed radicals and that **radical**$_{R[x]}$ returns the set $\bigcup_{C \in M} O_C$ instead of a basis of $\bigcap_{C \in M} \bigcap_{H \in O_C} \langle H\rangle$. Then **radical**$_{R[x]}$ does not compute a basis of $\sqrt{F}$ but an unmixed decomposition of $\sqrt{F}$.

Example 6.1. We will now compute a simple example with **radical**$_{R[x]}$.

Let $\mathbf{Z}_4 = \{0, 1, 2, 3\}$ be the residue class ring of the integers modulo the ideal $\langle 4\rangle$ and define $R := \mathbf{Z}_4 \times \mathbf{Z}_4$. We are interested in the radical of the ideal generated by the polynomial $(1, 2) \cdot x^2 + (1, 1)$ in the univariate polynomial ring $R[x]$. First we need some information on the ideal structure of R. It is easy to see that R is a principal ideal ring with 8 ideals unequal to R. The two prime ideals are generated by $(1, 2)$ resp. $(2, 1)$ and their intersection is generated by $(2, 2)$. It is the radical of $\langle(0, 0)\rangle$. For constructing a suitable system of representations $(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$ in R we choose S as $\{\{(2, 2)\}, \{(1, 2)\}, \{(2, 1)\}\}$ and define Rep, **decompose**$_R$ and **split**$_R$ in the obvious way.

When we apply the algorithm **radical**$_{R[x]}$ to $\{(1, 2) \cdot x^2 + (1, 1)\}$ we first have to compute **decompose**$_{R[x]}(\{(1, 2) \cdot x^2 + (1, 1)\})$:

$\{\{(2, 2)\}\} =$ **decompose**$_R(\emptyset)$,
$\{(\{(2, 1)\}, (1, 2) \cdot x^2 + (1, 1)), (\{(1, 2)\}, (1, 1))\} =$ **ggcd**$(\{(2, 2)\}, \{(1, 2) \cdot x^2 + (1, 1)\})$

and therefore

$$\{\{(2, 1), (1, 2) \cdot x^2 + (1, 1)\}\} = \mathbf{decompose}_{R[x]}(\{(1, 2) \cdot x^2 + (1, 1)\}).$$

Now we compute a squarefree part of $(1, 2) \cdot x^2 + (1, 1)$ in $(R/I)[x]$, where $I := \langle(2, 1)\rangle$.

As R/I is isomorphic to $\mathbf{Z}_2$ we easily see that in $(R/I)[x]$

$$(1,1)\cdot x+(1,1) \text{ is a squarefree part of } (1,2)\cdot x^2+(1,1).$$

Finally, we localize $\langle (2,1),(1,1)\cdot x+(1,1)\rangle$ at $(1,1)$ by computing a basis of

$$\langle (2,1),(1,1)\cdot x+(1,1),(1,1)\cdot y-(1,1)\rangle \cap R[x].$$

We obtain $\{(2,1),(1,1)\cdot x+(1,1)\}$ and therefore this set is a basis of the radical of $\langle (1,2)\cdot x^2+(1,1)\rangle$.

We have seen that in order to compute radicals in $R[x]$ we must be able to compute for every prime ideal $P \subseteq R$ and $f \in R[x]$ a squarefree part of f in $K(P)[x]$. If the characteristic of $K(P)$ is 0 then $\mathit{squarefree}(f) = f/\mathit{gcd}(f,f')$ in $K(P)[x]$, where f' denotes the derivative of f. Furthermore, $\mathit{squarefree}(f)$ can be computed if $K(P)$ is a perfect field of characteristic $p>0$ and p-th roots can be computed in $K(P)$. The computability of p-th roots is closely connected to Seidenberg's condition **(P)** (see, for instance, Mines *et al.* (1988, p.186)):

(P) If the characteristic p of $K(P)$ is not 0 then there exists an algorithm which decides whether a finite system of linear homogeneous equations with coefficients in $K(P)$ has a non-trivial solution in the subfield $K(P)^p$ of p-th powers of elements of $K(P)$, and if so finds one.

In Seidenberg (1974, p.295) a field of characteristic $p>0$ is given which does not satisfy **(P)**. Furthermore, it is shown that radicals of primary ideals are computable in a multivariate polynomial ring over a field if and only if the field satisfies **(P)** (Seidenberg, 1974, p.293).

7. Computing Unmixed Decompositions

We say that unmixed decompositions of ideals are computable in R if there exists an algorithm which computes for an arbitrary finite subset F of R finite bases $F_1,\ldots,F_r$ of unmixed ideals in R with

$$\langle F\rangle = \langle F_1\rangle \cap \cdots \cap \langle F_r\rangle.$$

In this section we construct an unmixed decomposition algorithm for ideals in $R[x]$ based on the following strategy. By applying the techniques in Section 4 a decomposition $I = I_1 \cap \cdots \cap I_l$ of the ideal I is constructed such that each $\sqrt{I_j}$ is strongly unmixed. In a second step each of the I_js which is not unmixed is decomposed. We distinguish two cases:

(a) I_j has an embedded prime P with $\mathit{height}(P\cap R) > \mathit{height}(I_j \cap R)$. Then a decomposition is obtained by localization using Theorem 7.5.
(b) $\mathit{height}(P\cap R) = \mathit{height}(I_j\cap R)$ for every embedded prime P. If x is an element of some associated prime of I_j then we decompose I_j by localizing at x. Otherwise, we choose a sufficiently large natural number m and decompose $I_j + \langle x^m\rangle$ by the same technique as in (a). From the decomposition of $I_j + \langle x^m\rangle$ we compute a decomposition of I_j.

By lifting this algorithm to $R[x_1,\ldots,x_n]$ we obtain a proof of the following theorem.

THEOREM 7.1. *If linear equations are solvable and unmixed decompositions of ideals are computable in R then for any number of variables n unmixed decompositions of ideals are computable in $R[x_1, \ldots, x_n]$.*

Before we present the algorithm we prove some results on localization.

7.1. LOCALIZATION

A fundamental technique for decomposing ideals is localization at a polynomial.

THEOREM 7.2. *Let I be an ideal in $R[x_1, \ldots, x_n]$, $f \in R[x_1, \ldots, x_n]$, J the ideal $\langle I \cup \{1-yf\}\rangle$ in $R[x_1, \ldots, x_n, y]$, where y is a new indeterminate, and $J' := J \cap R[x_1, \ldots, x_n]$.*

(a) *If d is a natural number with $I : f^d = I : f^\infty$ then $I = (I : f^\infty) \cap (I + \langle f^d \rangle)$.*
(b) *If $\{f_1, \ldots, f_k\}$ is a basis of I and $\{g_1, \ldots, g_m\}$ a basis of J' with*

$$g_i = h_i(1 - yf) + \sum_{j=1}^{k} h_{ij} f_j \quad (1 \le i \le m, h_i, h_{ij} \in R[x_1, \ldots, x_n, y])$$

then

$$d := \max(\{deg_y(h_{ij}) \mid 1 \le i \le m, 1 \le j \le k\})$$

satisfies $I : f^d = I : f^\infty$.

In Becker and Weispfenning (1993, Proposition 6.37) a proof of **(b)** is given if R is a field. In this case one can pass to the quotient field of $R[x_1, \ldots, x_n]$ and use the existence of $1/f$. As this is not possible in the general setting of Theorem 7.2 we have to modify the proof of Proposition 6.37 in Becker and Weispfenning (1993).

PROOF OF THEOREM 7.2. For the proof of **(a)** see Lemma 8.95 in Becker and Weispfenning (1993).
(b) Define

$$t := \max(\{deg_y(h_{ij}) \mid 1 \le i \le m, 1 \le j \le k\} \cup \{deg_y(h_i) \mid 1 \le i \le m\}) + 1$$

and let $g \in I : f^\infty$. By Theorem 3.1, $I : f^\infty = J'$. Hence, there exist $q_1, \ldots, q_m \in R[x_1, \ldots, x_n]$ with

$$\begin{aligned} g &= \sum_{i=1}^{m} q_i g_i \\ &= \sum_{i=1}^{m} q_i \Big(h_i(1 - yf) + \sum_{j=1}^{k} h_{ij} f_j \Big) \\ &= \sum_{l=0}^{t} y^l \Big(\sum_{i=1}^{m} q_i \Big(a_{i,l} - a_{i,l-1} f + \sum_{j=1}^{k} b_{i,j,l} f_j \Big) \Big), \end{aligned}$$

where for $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, k\}$

$$h_i = a_{i,t-1} y^{t-1} + \cdots + a_{i,0}, \qquad h_{ij} = b_{i,j,t-1} y^{t-1} + \cdots + b_{i,j,0}.$$

Therefore,

$$g = \sum_{i=1}^{m} q_i \Big(a_{i,0} + \sum_{j=1}^{k} b_{i,j,0} f_j \Big), \qquad 0 = \sum_{i=1}^{m} q_i \Big(a_{i,l} - a_{i,l-1} f + \sum_{j=1}^{k} b_{i,j,l} f_j \Big)$$

for $l \in \{1, \ldots, t\}$. Define

$$h'_i := a_{i,t-1} + a_{i,t-2} f + \cdots + a_{i,0} f^{t-1}, \qquad h'_{ij} := b_{i,j,t-1} f + b_{i,j,t-2} f^2 + \cdots + b_{i,j,0} f^t.$$

Hence,

$$\begin{aligned} g f^t &= \sum_{l=0}^{t} f^{t-l} \Big(\sum_{i=1}^{m} q_i \Big(a_{i,l} - a_{i,l-1} f + \sum_{j=1}^{k} b_{i,j,l} f_j \Big) \Big) \\ &= \sum_{i=1}^{m} q_i \Big(h'_i (f - f) + \sum_{j=1}^{k} h'_{ij} f_j \Big) \\ &= \sum_{i=1}^{m} q_i \Big(\sum_{j=1}^{k} h'_{ij} f_j \Big). \end{aligned}$$

Note that each h'_{ij} is divisible by f^{t-d}. Hence

$$g f^d = \sum_{i=1}^{m} q_i \Big(\sum_{j=1}^{k} (h'_{ij} / f^{t-d}) f_j \Big)$$

and therefore $I : f^\infty \subseteq I : f^d$. □

Let I be an ideal in $R[x_1, \ldots, x_n]$ and $I = Q_1 \cap \cdots \cap Q_r$ an irredundant primary decomposition of I. If $r > 1$ we can compute a non-trivial decomposition

$$I = (I : f^\infty) \cap (I + \langle f^d \rangle)$$

if we are able to find an $f \in R[x_1, \ldots, x_n]$ which is an element of some but not of all the $\sqrt{Q_i}$, i.e. $I \subset I : f^\infty \subset R[x_1, \ldots, x_n]$. We will develop a technique for computing such an f (see Theorem 7.5) whenever $\sqrt{Q_i \cap R} \neq \sqrt{Q_j \cap R}$ for some $i, j \in \{1, \ldots, r\}$ which is based on the following result.

Let $\prec$ be an arbitrary admissible order on $PP(x_1, \ldots, x_n)$ and define for an element X of $PP(x_1, \ldots, x_n)$

$$lc_X(I) := \{ lc(f) \mid f \in I \text{ and } lpp(f) = X \} \cup \{0\}.$$

THEOREM 7.3. *Let $I \subseteq R[x_1, \ldots, x_n]$ be an ideal, $I = Q_1 \cap \cdots \cap Q_r$ an irredundant primary decomposition of I and $i \in \{1, \ldots, r\}$. Then there exists an $X \in PP(x_1, \ldots, x_n)$ such that $\sqrt{Q_i \cap R}$ is an associated prime ideal of $lc_X(I)$.*

PROOF. Denote the ideal $Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_r$ by I' and the prime ideal $\sqrt{Q_i \cap R}$ by P. As $Q_1 \cap \cdots \cap Q_r$ is an irredundant decomposition we can choose an element $f \in I' \setminus Q_i$ with $lpp(f) \preceq lpp(g)$ for every $g \in I' \setminus Q_i$. Denote $lpp(f)$ by X. Obviously,

$$Q_i \cap R \subseteq lc_X(I) : lc(f). \tag{7.1}$$

On the other hand, let a be an element of $lc_X(I) : lc(f)$. If $a \cdot lc(f) = 0$ denote $a \cdot f$ by h.

Otherwise, there exists a $g \in I$ with $lpp(g) = X$ and $lc(g) = lc(f) \cdot a$. Define $h := g - a \cdot f$. If $a \notin P$ then in both cases the polynomial h is in I' but not in Q_i and $lpp(h) \prec X$. This is a contradiction to the definition of f. Hence, $a \in P$. Together with (7.1) we obtain that P is the radical of $lc_X(I) : lc(f)$. Thus, by Theorem 4.5 in Atiyah and Macdonald (1969), P is an associated prime ideal of $lc_X(I)$. □

We will now show that the correctness of the decomposition techniques used in Gianni *et al.* (1988) and Becker and Weispfenning (1993) easily follows from the above theorem.

Assume that R is an integral domain, $\langle p \rangle$ a principal prime ideal in R, $I = Q_1 \cap \cdots \cap Q_r$ an irredundant primary decomposition of the ideal $I \subseteq R[x_1, \ldots, x_n]$, J the set $\{j \in \{1, \ldots, r\} \mid Q_j \cap R \subseteq \langle p \rangle\}$ and $G = \{g_1, \ldots, g_k\}$ a Gröbner basis of I. As R is an integral domain, $\bigcap_{i=1}^{\infty} \langle p^i \rangle = \{0\}$ (Krull (1928), see also van der Waerden (1967, p.150)). Hence, we can write every $lc(g_i)$ in the form $lc(g_i) = a_i p^{t_i}$, where a_i is not divisible by p. We define $f := \prod_{i=1}^{k} a_i$ and let $j \in \{1, \ldots, r\} \setminus J$. It follows from the above theorem that there exists an $X \in PP(x_1, \ldots, x_n)$ such that $\sqrt{Q_j \cap R}$ is an associated prime ideal of $lc_X(I)$. As $lc_X(I)$ is generated by a subset of $\{lc(g_1), \ldots, lc(g_k)\}$ and $\sqrt{Q_j \cap R} \not\subseteq \langle p \rangle$ it follows that $f \in \sqrt{Q_j \cap R}$. Hence, we obtain Proposition 3.7 in Gianni *et al.* (1988):

$$I : f^{\infty} = \bigcap_{j \in J} Q_j = I\, R_{\langle p \rangle}[x_1, \ldots, x_n] \cap R[x_1, \ldots, x_n], \tag{7.2}$$

where $R_{\langle p \rangle}$ is the localization of R at $\langle p \rangle$. Based on this result an algorithm for computing primary decompositions of ideals in multivariate polynomial rings over principal ideal domains has been developed in Gianni *et al.* (1988). Localization is used to reduce the primary decomposition computation to its zero-dimensional counterpart.

In Becker and Weispfenning (1993) a particular instance of (7.2) is used for computing primary decompositions of ideals in multivariate polynomial rings over fields. Let R be the polynomial ring $K[y_1, \ldots, y_m]$ and take p as 0. Then (7.2) becomes

$$I : f^{\infty} = I\, K(y_1, \ldots, y_m)[x_1, \ldots, x_n] \cap K[y_1, \ldots, y_m, x_1, \ldots, x_n].$$

(see Proposition 8.94 in Becker and Weispfenning (1993)). Assume now that $\{y_1, \ldots, y_m\}$ is an element of maximal cardinality in the independence complex $\Delta(I)$ of $I \subseteq K[y_1, \ldots, y_m, x_1, \ldots, x_n]$. Then $I : f^{\infty}$ can be considered as a zero-dimensional ideal in the polynomial ring $K(y_1, \ldots, y_m)[x_1, \ldots, x_n]$ over the field $K(y_1, \ldots, y_m)$ and primary decomposition techniques for the zero-dimensional case can be applied. According to Theorem 7.2 we have $I = (I : f^{\infty}) \cap (I + \langle f^d \rangle)$ for sufficiently large d. As I is a proper subideal of $I + \langle f^d \rangle$ the computation of a primary decomposition of I can be completed by repeating the same procedure with $I + \langle f^d \rangle$.

We finish this subsection by proving an easy lemma which will also be useful for computing fs with $I \subset I : f^{\infty} \subset R[x_1, \ldots, x_n]$.

Lemma 7.1. *Let $I \subset R[x_1, \ldots, x_n]$ be an ideal which is not primary, Q an isolated primary component of I, $h \in Q \setminus I$ and G a Gröbner basis of the ideal quotient $I : h$. Then there exists an $f \in G$ with $I \subset I : f^{\infty} \subset R[x_1, \ldots, x_n]$.*

Proof. Let $I = Q_1 \cap \cdots \cap Q_k$ be an irredundant primary decomposition of I. W.l.o.g. we assume that $h \notin Q_k$. Then

$$I : h \subseteq \sqrt{Q_k}. \tag{7.3}$$

As $\sqrt{Q}$ is an isolated prime ideal of I the ideal quotient $I : h$ is not contained in $\sqrt{Q}$. Hence, there exists an $f \in G$ with $f \notin \sqrt{Q}$. Together with (7.3) we obtain

$$I \subset \bigcap_{j=1}^{k-1} Q_j \subseteq I : f^\infty \subseteq Q \subset R[x_1, \ldots, x_n].$$

□

7.2. CONSTRUCTION OF AN UNMIXED DECOMPOSITION ALGORITHM

We will now prove Theorem 7.1. Obviously it suffices to construct an unmixed decomposition algorithm in the univariate polynomial ring $R[x]$.

Before we apply the localization technique from the previous subsection we will first compute a decomposition

$$I = I_1 \cap \cdots \cap I_l \tag{7.4}$$

of the ideal $I \subseteq R[x]$ such that each $\sqrt{I_i}$ is strongly unmixed.

We construct a system of unmixed representations

$$(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$$

in R: let S be the set of finite subsets of R which generate unmixed ideals different from R and define $Rep(A) := \sqrt{A}$. By assumption, we can compute for a finite subset F of R finite bases $G_1, \ldots, G_r$ of unmixed ideals with

$$\langle F \rangle = \langle G_1 \rangle \cap \cdots \cap \langle G_r \rangle.$$

Let $\mathbf{decompose}_R$ be the algorithm which returns the set consisting of those G_i which do not generate R. It remains to construct $\mathbf{split}_R$. Let $F \in S$, $f \in R$, $G = \{g_1, \ldots, g_k\}$ a finite basis of $\langle F \rangle : f^\infty$ and B_i a finite basis of $\langle F \rangle : g_i^\infty$ for every $i \in \{1, \ldots, k\}$. As linear equations are solvable in R it follows from Theorem 3.1 that we can compute G and $B_1, \ldots, B_k$ using Gröbner bases. Consider now the algorithm which computes $(\bar{B}, \bar{G})$ for given F, f, where

$\bar{B}$:=$\{B_i \mid i \in \{1, \ldots, k\},\ \langle B_i \rangle \neq R\}$,
$\bar{G}$:=$\{G\}$ if $\langle G \rangle \neq R$,
$\bar{G}$:=$\emptyset$ otherwise.

As in Example 4.1 we can show that this algorithm satisfies the specification of $\mathbf{split}_R$.

We apply Theorem 4.1 and obtain a system of unmixed representations

$$(\bar{S}, \overline{Rep}, \mathbf{decompose}_{R[x]}, \mathbf{split}_{R[x]})$$

in $R[x]$.

Let F be a finite basis of I, $\{C_1, \ldots, C_l\} := \mathbf{decompose}_{R[x]}(F)$ and $i \in \{1, \ldots, l\}$. It follows from the construction of $\bar{S}$ that each $\overline{Rep}(C_i)$ is a strongly unmixed radical in $R[x]$. If $C_i \subseteq R$ we define $G_i := C_i$. Otherwise, there exists exactly one non-constant polynomial g_i in C_i. Let G_i be a Gröbner basis of $\langle C_i \rangle : lc(g_i)^\infty$. By Lemma 4.3, $\overline{Rep}(C_i) = \sqrt{G_i}$ and therefore, by specification of $\mathbf{decompose}_{R[x]}$,

$$\sqrt{F} = \bigcap_{i=1}^{l} \sqrt{G_i}. \tag{7.5}$$

It is now easy to construct the decomposition (7.4): we compute for every $i \in \{1, \ldots, l\}$

a natural number m_i such that $I + \langle G_i\rangle^{m_i} = I + \langle G_i\rangle^{m_i+1}$. Then

$$I = (I + \langle G_1\rangle^{m_1}) \cap \cdots \cap (I + \langle G_l\rangle^{m_l}).$$

For every $i \in \{1, \ldots, l\}$ the radical of $I + \langle G_i\rangle^{m_i}$ is $\sqrt{G_i}$ and therefore strongly unmixed.

A more sophisticated strategy for computing decomposition (7.4) from decomposition (7.5) is based on Theorem 7.4 which is a generalization of Theorem 3.7 in Shimoyama and Yokoyama (1994). Using $\mathbf{split}_{R[x]}$ and Gröbner bases computations we can compute for the given basis F of I finite subsets $F_1, \ldots, F_r$ of $R[x]$ and polynomials $f_1, \ldots, f_r$ in $R[x]$ such that for $i, j \in \{1, \ldots, r\}$ with $i \neq j$ the polynomial f_i is in $\sqrt{F_j}$ but not in $\sqrt{F_i}$, the radical $\sqrt{F_i}$ is strongly unmixed and $\sqrt{F} = \bigcap_{k=1}^{r} \sqrt{F_k}$. Hence we can use the following theorem in order to obtain the decomposition (7.4).

THEOREM 7.4. *Let I be an ideal in $R[x]$ and $P_1, \ldots, P_l$ strongly unmixed radicals with $\sqrt{I} = P_1 \cap \cdots \cap P_l$. Assume that for every $i \in \{1, \ldots, l\}$ there exists an $f_i \in P_j$ for $j \neq i$ and $f_i \notin P_i$ and let d_i be a natural number with $I : f_i^{d_i} = I : f_i^{\infty}$. Then*

$$I = I : f_1^{\infty} \cap \cdots \cap I : f_l^{\infty} \cap I', \tag{7.6}$$

where $I' := I + \langle f_1^{d_1}, \ldots, f_l^{d_l}\rangle$. Furthermore, $I \subset I'$ and the radical of $I : f_i^{\infty}$ is strongly unmixed for every $i \in \{1, \ldots, l\}$.

PROOF. Let i be an element of $\{1, \ldots, l\}$. From

$$\sqrt{I : f_i^{\infty}} = \sqrt{I} : f_i^{\infty} = (P_1 \cap \cdots \cap P_l) : f_i^{\infty} = P_i : f_i^{\infty}$$

we obtain that $\sqrt{I : f_i^{\infty}}$ is strongly unmixed. Obviously, $f_i^{d_i} \notin I$ and therefore $I \subset I'$.

Let $j \in \{1, \ldots, l\}$ with $i \neq j$. As $f_j \in P_i$ there exists a natural number k with $f_j^k \in I : f_i^{\infty}$. As $f_j^{d_j} \notin I : f_i^{\infty}$ then there exists a natural number m with $f_i^m \in (I : f_j^k)$ but $f_i^m \notin (I : f_j^{d_j})$. This is a contradiction to $(I : f_j^{d_j}) = I : f_j^{\infty}$. Hence,

$$f_j^{d_j} \in I : f_i^{\infty} \text{ for } i \neq j. \tag{7.7}$$

Note that for ideals J_1, J_2 in $R[x]$ and $f \in J_1$ we have

$$(J_1 \cap J_2) + \langle f\rangle = J_1 \cap (J_2 + \langle f\rangle). \tag{7.8}$$

It follows from Theorem 7.2 that $I = (I : f_i^{d_i}) \cap (I + \langle f_i^{d_i}\rangle)$. Hence, by (7.7) and (7.8),

$$\begin{aligned} I &= (I : f_1^{d_1}) \cap (I + \langle f_1^{d_1}\rangle) \\ &= (I : f_1^{d_1}) \cap (((I : f_2^{d_2}) \cap (I + \langle f_2^{d_2}\rangle)) + \langle f_1^{d_1}\rangle) \\ &= (I : f_1^{d_1}) \cap (I : f_2^{d_2}) \cap (I + \langle f_1^{d_1}, f_2^{d_2}\rangle). \end{aligned}$$

Continuing in this way we obtain (7.6). □

It remains to solve the problem of computing an unmixed decomposition of an ideal $I \subset R[x]$ whose radical is strongly unmixed. We will use the following strategy: we construct a finite subset U of $R[x]$ with the property that if I is not strongly unmixed then $I \subset I : f^{\infty} \subset R[x]$ for some $f \in U$. In this case we compute a non-trivial decomposition

$$I = (I : f^{\infty}) \cap (I + \langle f^d\rangle)$$

using Theorem 7.2 and continue by decomposing the ideals $I : f^{\infty}$ and $I + \langle f^d\rangle$.

The difficult part in this decomposition strategy is the computation of U. If I has an embedded prime P with $height(P \cap R) > height(I \cap R)$ we can use a technique based on Theorem 7.3 for decomposing I. Let G be a Gröbner basis of I and $m := \max(\{deg(g) \mid g \in G\})$. For every $j \in \{0, \ldots, m\}$ let

$$lc_{x^j}(I) = I_{j1} \cap \cdots \cap I_{jr_j}$$

be an unmixed decomposition of $lc_{x^j}(I)$ and F_{ji} a finite basis of I_{ji} for $i \in \{1, \ldots, r_j\}$.

THEOREM 7.5. *Let $I \subset R[x]$ be an ideal whose radical is strongly unmixed.*

(a) *If I has an embedded prime P with $height(P \cap R) > height(I \cap R)$ then*

$$\text{there exist } j \in \{0, \ldots, m\},\ i \in \{1, \ldots, r_j\},\ f \in F_{ji} \text{ with } I \subset I : f^\infty \subset R[x]. \quad (7.9)$$

(b) *If $(\sqrt{I} \cap R)\, R[x] \neq \sqrt{I}$ and (7.9) does not hold then I is strongly unmixed.*

PROOF. (**a**) Note that for $k > m$

$$lc_{x^m}(I) = lc_{x^k}(I).$$

Hence, by Theorem 7.3, there exists a $j \in \{0, \ldots, m\}$ such that $P \cap R$ is an associated prime of $lc_{x^j}(I)$. Thus, $P \cap R$ is an isolated prime of I_{ji} for some $i \in \{1, \ldots, r_j\}$. Because of $height(I_{ji}) = height(P \cap R) > height(I \cap R)$ there exists an element f in F_{ji} which is in P but not in $\sqrt{I}$. Hence, $I : f^\infty$ is neither I nor $R[x]$.

(b) Assume that I is not strongly unmixed. As $\sqrt{I}$ is strongly unmixed I has an embedded prime P. Let $\bar{P}$ be an isolated prime with $\bar{P} \subset P$. Since $\sqrt{I}$ is strongly unmixed and $(\sqrt{I} \cap R)\, R[x] \neq \sqrt{I}$ we obtain from Theorem 2.1 that

$$height(\bar{P} \cap R) = height(\bar{P}) - 1 < height(P) - 1 \leq height(P \cap R).$$

It follows from **(a)** that (7.9) holds. □

Assume that $\sqrt{I}$ is strongly unmixed and $(\sqrt{I} \cap R)\, R[x] \neq \sqrt{I}$. Either I is strongly unmixed or, by the Theorems 7.2 and 7.5, we can find an $f \in R$ and a natural number d such that

$$I = (I : f^\infty) \cap (I + \langle f^d \rangle)$$

is a non-trivial decomposition of I. Note that $\sqrt{I : f^\infty}$ is strongly unmixed and

$$(\sqrt{I : f^\infty} \cap R)\, R[x] \neq \sqrt{I : f^\infty}.$$

Hence, we can apply the same decomposition strategy to $I : f^\infty$. After finitely many steps we obtain a decomposition

$$I = I' \cap I_1 \cap \cdots \cap I_i, \quad (7.10)$$

such that $I \subset I_j$ for every $j \in \{1, \ldots, i\}$ and I' is the intersection of some of the primary components of I with minimal height.

If the ideal I has an embedded prime P with $height(P \cap R) > height(I \cap R)$ then we can use Theorem 7.5 for decomposing I. If $(\sqrt{I} \cap R)\, R[x] \neq \sqrt{I}$ the same theorem can be used for deciding whether I is unmixed and for computing a decomposition of I if I is not unmixed. Therefore, we assume for the rest of this subsection that $I \subset R[x]$ is an ideal with the following properties:

(1) $\sqrt{I}$ is strongly unmixed,
(2) $(\sqrt{I} \cap R)\, R[x] = \sqrt{I}$,
(3) $height(P \cap R) = height(I \cap R)$ for each associated prime P of I.

For deciding whether I is unmixed we will analyse ideals of the form $I + \langle x^n \rangle$, where n is an arbitrary natural number. This strategy only works if $I : x^\infty = I$. This does not cause any problems because if $I : x^\infty \neq I$ we compute a non-trivial decomposition

$$I = (I : x^\infty) \cap (I + \langle x^d \rangle)$$

and continue with $I : x^\infty$ and $I + \langle x^d \rangle$. Hence, we can assume that I has the additional property

(4) $I : x^\infty = I$.

Let

$$I = Q_1 \cap \cdots \cap Q_s \cap Q_{s+1} \cap \cdots \cap Q_r$$

be an irredundant primary decomposition of I such that $\sqrt{Q_1}, \ldots, \sqrt{Q_s}$ are the isolated prime ideals of I. Denote $\sqrt{Q_i}$ by P_i for $i \in \{1, \ldots, r\}$. Let A be a non-empty subset of $\{1, \ldots, s\}$ and define

$$hull_A(I) := \{f \in R[x] \mid g \cdot f \in I \text{ for some } g \in S\}, \text{ where } S := R[x] \setminus \bigcup_{j \in A} P_j.$$

Because of van der Waerden (1967, p.139), Matsumura (1970, p.2) and the fact that $\sqrt{I}$ is strongly unmixed,

$$hull_A(I) = \bigcap_{j \in A} Q_j, \quad hull_{\{1,\ldots,s\}}(I) = hull(I).$$

Obviously, $P_1 \cap R, \ldots, P_s \cap R$ are the isolated prime ideals of $I \cap R$ and $P_1 + \langle x \rangle, \ldots, P_s + \langle x \rangle$ are the isolated primes of $I + \langle x^n \rangle$ for every natural number n. We define

$$\begin{aligned} hull_A(I \cap R) &:= \{f \in R \mid g \cdot f \in I \cap R \text{ for some } g \in S\}, \\ &\quad \text{where } S := R \setminus \bigcup_{j \in A} (P_j \cap R), \\ hull_A(I + \langle x^n \rangle) &:= \{f \in R[x] \mid g \cdot f \in I + \langle x^n \rangle \text{ for some } g \in S\}, \\ &\quad \text{where } S := R[x] \setminus \bigcup_{j \in A} (P_j + \langle x \rangle). \end{aligned}$$

We will study the relation between $hull_A(I)$ and $hull_A(I + \langle x^n \rangle)$. This will lead to the following strategy for decomposing I in case I is not unmixed: we consider the ideal $I + \langle x^n \rangle$ for a natural number n. The radical $\sqrt{I + \langle x^n \rangle}$ is strongly unmixed and $(\sqrt{I + \langle x^n \rangle} \cap R)\, R[x] \neq \sqrt{I + \langle x^n \rangle}$. Therefore we can compute a Gröbner basis H of $hull_A(I + \langle x^n \rangle)$ for some $A \subseteq \{1, \ldots, s\}$ (see (7.10)). We will show that for "sufficiently large" n the Gröbner basis H contains a polynomial in $hull_A(I) \setminus I$. Together with Lemma 7.1 we obtain a decomposition of I.

For defining "sufficiently large" we need the concept of the length of an ideal. Let Q be a primary ideal in R with prime ideal P. It is well known (see, for instance, van der Waerden (1967, p.152)) that there exists a natural number $\lambda(Q)$, called the length of Q, with the following property: every strictly ascending chain of primary ideals

$$Q = Q'_1 \subset Q'_2 \subset \ldots \subset Q'_i = P$$

belonging to P has at most $\lambda(Q)$ terms and there exists such a chain with exactly $\lambda(Q)$ terms. For an ideal J having an irredundant primary decomposition $J = \bigcap_{j=1}^{k} Q'_j$ without embedded components we define $\lambda(J) := \sum_{j=1}^{k} \lambda(Q'_j)$.

THEOREM 7.6. *Let A be a non-empty subset of $\{1, \ldots, s\}$, G a Gröbner basis of I, F a finite basis of $hull_A(I)$, $\beta := \max(\{deg(h) \mid h \in G \cup F\})$ and α a natural number greater than $\beta \cdot (\lambda(hull_A(I \cap R)) + 1)$. Then*

(a) *$hull_A(I) \subseteq hull_A(I + \langle x^n \rangle)$ for every natural number n;*
(b) *the set $\{f \in hull_A(I + \langle x^\alpha \rangle) \mid deg(f) \leq \beta\}$ generates $hull_A(I)$.*

The proof of this theorem is based on the following rather technical lemma.

LEMMA 7.2. *Let A be a non-empty subset of $\{1, \ldots, s\}$, m a non-negative integer, f a polynomial in $R[x]$, d a non-negative integer $\geq deg(f)$ and $M = \{n_1, \ldots, n_t\}$ a set of natural numbers whose cardinality t is greater than $m \cdot \lambda(hull_A(I \cap R))$. Assume that for every $i \in \{1, \ldots, t\}$ there exists a polynomial $g_i \in R[x]$ with $deg(g_i) < n_i$ and $g_i(0) \notin \bigcup_{j \in A} P_j$ and a polynomial h_i in $R[x]$ with $deg(h_i) < m$ and*

$$h_i \cdot x^{d+n_i} + g_i \cdot f \in I.$$

Then there exists a polynomial $p \in R[x]$ with $p(0) \notin \bigcup_{j \in A} P_j$ and $p \cdot f \in I$.

PROOF. We do the proof by induction on m.

If $m = 0$ then $h_i = 0$ for every $i \in \{1, \ldots, t\}$ and the claim is obvious.

Assume that $m > 0$ and let $n_1 < \ldots < n_t$. For every $i \in \{1, \ldots, t\}$ write h_i in the form $h_i = a_{m-1,i} \cdot x^{m-1} + \cdots + a_{0,i}$ and denote $h_i \cdot x^{d+n_i} + g_i \cdot f$ by q_i. Furthermore, for every $i \in \{0, \ldots, t\}$ let I_i be the ideal $(I \cap R) + \langle a_{m-1,1}, a_{m-1,2}, \ldots, a_{m-1,i} \rangle$ in R. As $\sqrt{I}$ is strongly unmixed and $(\sqrt{I} \cap R)\, R[x] = \sqrt{I}$ we know that $P_j \cap R$ is an isolated prime of I_i for $i \in \{0, \ldots, t\}$ and $j \in A$. Denote the uniquely determined isolated primary component of I_i with radical $P_j \cap R$ by Q_{ij} and define $E_i := \bigcap_{j \in A} Q_{ij}$. Obviously, $E_0 = hull_A(I \cap R)$. Furthermore,

$$Q_{0j} \subseteq Q_{1j} \subseteq \cdots \subseteq Q_{tj}$$

and therefore

$$|M'| > (m-1) \cdot \sum_{j \in A} \lambda(Q_{0j}) = (m-1) \cdot \lambda(hull_A(I \cap R)), \tag{7.11}$$

where $M' := \{i \in \{1, \ldots, t\} \mid E_{i-1} = E_i\}$. For every $i \in M'$ there exists an ideal J_{i-1} in R with $I_{i-1} = E_{i-1} \cap J_{i-1}$ and J_{i-1} is not contained in any of the $P_j \cap R$ for $j \in A$. By Matsumura (1970, p.2), we can choose a $c_i \in J_{i-1}$ which is not in $\bigcup_{j \in A} P_j$. By definition of M', $c_i \cdot a_{m-1,i} \in I_{i-1}$. We write $c_i \cdot a_{m-1,i}$ in the form

$$c_i \cdot a_{m-1,i} = b_1 \cdot a_{m-1,1} + \cdots + b_{i-1} \cdot a_{m-1,i-1} + e$$

with $b_1, \ldots, b_{i-1} \in R$ and $e \in I \cap R$. Hence,

$$\begin{aligned} q'_i &:= c_i \cdot q_i - (b_1 \cdot q_1 \cdot x^{n_i - n_1} + \cdots + b_{i-1} \cdot q_{i-1} \cdot x^{n_i - n_{i-1}} + e \cdot x^{d+n_i+m-1}) \\ &= c_i \cdot ((a_{m-2,i} \cdot x^{m-2} + \cdots + a_{0,i}) \cdot x^{d+n_i} + g_i \cdot f) \\ &\quad - b_1 \cdot ((a_{m-2,1} \cdot x^{m-2} + \cdots + a_{0,1}) \cdot x^{d+n_i} + g_1 \cdot f \cdot x^{n_i - n_1}) - \cdots \end{aligned}$$

$$\begin{aligned} &-b_{i-1}\cdot((a_{m-2,i-1}\cdot x^{m-2}+\cdots+a_{0,i-1})\cdot x^{d+n_i}+g_{i-1}\cdot f\cdot x^{n_i-n_{i-1}})\\ &=h_i'\cdot x^{d+n_i}+g_i'\cdot f\in I, \end{aligned}$$

where

$$\begin{aligned} h_i' := {} & c_i\cdot(a_{m-2,i}\cdot x^{m-2}+\cdots+a_{0,i})-b_1\cdot(a_{m-2,1}\cdot x^{m-2}+\cdots+a_{0,1})-\cdots\\ & -b_{i-1}\cdot(a_{m-2,i-1}\cdot x^{m-2}+\cdots+a_{0,i-1}) \end{aligned}$$

and

$$g_i' := c_i\cdot g_i-b_1\cdot g_1\cdot x^{n_i-n_1}-\cdots-b_{i-1}\cdot g_{i-1}\cdot x^{n_i-n_{i-1}}.$$

Together with (7.11) we obtain that $\{n_i \mid i\in M'\}$ satisfies the induction hypothesis and the lemma is proved. □

Proof of Theorem 7.6. **(a)** Let $i\in\{s+1,\ldots,r\}$ and $j\in A$. As $\sqrt{I}$ is strongly unmixed and $(\sqrt{I}\cap R)\,R[x]=\sqrt{I}$ we obtain from Theorem 2.1

$$height(P_j+\langle x\rangle)=height(P_j)+1\le height(P_i).$$

As $I:x^\infty=I$ we have $x\notin P_i$ and therefore P_i is not a subideal of $P_j+\langle x\rangle$. Furthermore, $P_k\not\subseteq P_j+\langle x\rangle$ for $k\in\{1,\ldots,s\}\setminus A$. Let $f\in hull_A(I)$. By Matsumura (1970, p.2), we can choose a $g\in R[x]$ such that $g\notin\bigcup_{j\in A}(P_j+\langle x\rangle)$ and $g\cdot f\in I$. As $(P_j+\langle x\rangle)_{j\in A}$ are the associated primes of $hull_A(I+\langle x^n\rangle)$ for every natural number n we obtain $f\in hull_A(I+\langle x^n\rangle)$.

(b) By **(a)** and the definition of β,

$$hull_A(I)=\langle\{f\in hull_A(I)\mid deg(f)\le\beta\}\rangle\subseteq\langle\{f\in hull_A(I+\langle x^\alpha\rangle)\mid deg(f)\le\beta\}\rangle.$$

Let $f\in hull_A(I+\langle x^\alpha\rangle)$ with $deg(f)\le\beta$. Obviously, we can choose a $c\in R$ with $c\notin\bigcup_{j\in A}P_j$ and $c\cdot f\in I+\langle x^\alpha\rangle$. Hence, there exists an $h\in R[x]$ with $h\cdot x^\alpha+c\cdot f\in I$. By reducing $h\cdot x^\alpha+c\cdot f$ modulo the Gröbner basis G we obtain polynomials $h_1,\ldots,h_{\alpha-\beta}$ with $deg(h_i)<\beta$ and $h_i\cdot x^{\beta+i}+c\cdot f\in I$. Thus, the set $\{1,\ldots,\alpha-\beta\}$ satisfies the conditions in Lemma 7.2 and there exists a polynomial $p\in R[x]$ with $p(0)\notin\bigcup_{j\in A}P_j$ and $p\cdot f\in I$. As $p\notin\bigcup_{j\in A}P_j$ we have $f\in hull_A(I)$ and the theorem is proved. □

We can use Theorem 7.6 together with Lemma 7.1 and Theorem 7.2 for computing a non-trivial decomposition of I if I is not unmixed. But as we do not know the constant β in Theorem 7.6 we cannot use this result for deciding whether I is unmixed. This will be done by means of the following theorem.

Theorem 7.7. *Let $G=\{g_1,\ldots,g_k\}$ be a Gröbner basis of I and $m:=\max(\{deg(g_i)\mid i\in\{1,\ldots,k\}\})$. The following two conditions are equivalent:*

(a) *I is unmixed.*
(b) *There exists a natural number n with $\{f\in I+\langle x^n\rangle\mid deg(f)\le m\}\subseteq I$.*

Proof. (**a**) ⇒ (**b**) Obviously, $I=hull(I)$. Define $A:=\{1,\ldots,s\}$ and let n be a natural number greater than $m\cdot(\lambda(hull_A(I\cap R))+1)$. Then we obtain from the previous theorem

$$\{f\in I+\langle x^n\rangle\mid deg(f)\le m\}\subseteq\{f\in hull_A(I+\langle x^n\rangle)\mid deg(f)\le m\}\subseteq I.$$

(**a**) ⇐ (**b**) Let H be a Gröbner basis of $I+\langle x^n\rangle$ and $h\in H$. Assume that $h\notin I$. From

$\{f \in I + \langle x^n \rangle \mid deg(f) \leq m\} \subseteq I$ we obtain $m < d$, where $d := deg(h)$. We can write h in the form

$$h = \sum_{i=1}^{k} f_i g_i + f x^n,$$

where $f_1, \ldots, f_k, f \in R[x]$. Let $i \in \{1, \ldots, k\}$ and $a_0, \ldots, a_j \in R$ such that $f_i = a_j x^j + \cdots + a_0$. We define

$$f_i' := a_j x^j + a_{j-1} x^{j-1} + \cdots + a_{d-m} x^{d-m}, \quad h' := \sum_{i=1}^{k} f_i' g_i + f x^n.$$

Obviously, h' is divisible by x and $lm(h') = lm(h)$. Therefore, $(H \setminus \{h\}) \cup \{h'\}$ is a Gröbner basis of $I + \langle x^n \rangle$. Continuing this replacement process we obtain a

Gröbner basis H' of $I + \langle x^n \rangle$ whose elements are in I or divisible by x. (7.12)

Let the elements $h_1, \ldots, h_l$ of H' be ordered in such a way that there exists a $j \in \{0, \ldots, l\}$ with $h_1, \ldots, h_j \in I$ and $h_{j+1}, \ldots, h_l \notin I$.

Assume now that I is not unmixed. We choose an element g of minimal degree in the set $hull(I) \setminus I$. Let P be an associated prime ideal of $(\bigcap_{i=s+1}^{r} Q_i) + \langle x^n \rangle$. Then there exists an $i \in \{s+1, \ldots, r\}$ with $P_i \subset P$. Since P_i is an embedded prime of I with $height(P_i \cap R) = height(I \cap R)$ we have $height(P_i \cap R) < height(P_i)$. Together with Theorem 2.1 we obtain for every $j \in \{1, \ldots, r\}$

$$height(P_j \cap R) = height(P_i \cap R) = height(P_i) - 1 < height(P) - 1 \leq height(P \cap R).$$

Hence, by Matsumura (1970, p.2), there exists a $c \in R$ which is in $(\bigcap_{i=s+1}^{r} Q_i) + \langle x^n \rangle$ but not in $\bigcup_{j=1}^{r} P_j$. Therefore, $cg \in I + \langle x^n \rangle$ and $cg \notin I$. We write cg in the form

$$cg = \sum_{i=1}^{l} f_i h_i,$$

where $f_1, \ldots, f_l \in R[x]$ with $deg(f_i h_i) \leq deg(cg)$ for $i \in \{1, \ldots, l\}$. Furthermore, we define

$$g' := cg - \sum_{i=1}^{j} f_i h_i.$$

Then $g' \in hull(I) \setminus I$, $deg(g') \leq deg(g)$ and g' is divisible by x. From $I : x^\infty = I$ we deduce that the polynomial g'/x is an element of $hull(I) \setminus I$. This is a contradiction to the minimality of g. □

We are now ready to construct an algorithm which returns a non-trivial decomposition of the ideal I or the information that I is unmixed. Let G be a Gröbner basis of I and $m := \max(\{deg(g) \mid g \in G\})$.

We choose a natural number n and compute a Gröbner basis F of $I + \langle x^n \rangle$. If

$$\{f \in F \mid deg(f) \leq m\} \subseteq I \tag{7.13}$$

then I is unmixed. Otherwise we compute a Gröbner basis H of $hull_A(I + \langle x^n \rangle)$ for some $A \subseteq \{1, \ldots, s\}$. This is possible because the radical of $I + \langle x^n \rangle$ is strongly unmixed and $(\sqrt{I + \langle x^n \rangle} \cap R)\, R[x] \neq \sqrt{I + \langle x^n \rangle}$. We compute a Gröbner basis G_h of $I : h$ for every

$h \in H \setminus I$. If there exists an $f \in \bigcup_{h \in H \setminus I} G_h$ with $I \subset I : f^\infty \subset R[x]$ we compute a non-trivial decomposition

$$I = (I : f^\infty) \cap (I + \langle f^d \rangle)$$

using Theorem 7.2. Otherwise we repeat the whole process with a natural number $n' > n$.

Assume that I is unmixed. It follows from Theorem 7.7 that after finitely many repetitions the algorithm either returns a non-trivial decomposition of I or the information that I is unmixed.

Assume that I is not unmixed. It follows from the Theorems 7.6 and 7.7 that eventually a Gröbner basis H of $hull_A(I + \langle x^\alpha \rangle)$ is computed, where the natural number α and $A \subseteq \{1, \ldots, s\}$ have the following property: there exists a natural number β with

$$\langle \{ f \in hull_A(I + \langle x^\alpha \rangle) \mid deg(f) \leq \beta \} \rangle = hull_A(I).$$

As $hull_A(I) \neq I$ there exists an $h \in H$ which is in $hull_A(I)$ but not in I. By Lemma 7.1, there exists an f in the Gröbner basis G_h of $I : h$ such that $I \subset I : f^\infty \subset R[x]$. Hence, the algorithm returns a non-trivial decomposition

$$I = (I : f^\infty) \cap (I + \langle f^d \rangle)$$

using Theorem 7.2.

7.3. THE ALGORITHM IN PSEUDOCODE

We will now write down the unmixed decomposition algorithm in pseudocode.

As unmixed decompositions are computable in the ring R there exists an algorithm $\mathbf{unmixed\_dec}_R$ which computes for a finite subset F of R a set $\{F_1, \ldots, F_k\}$ of finite bases of unmixed ideals in R with $\langle F \rangle = \bigcap_{i=1}^k \langle F_i \rangle$. Hence, there exists a system of unmixed representations $(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$ in R such that S is the set of those finite subsets of R which generate unmixed ideals different from R. We apply Theorem 4.1 and obtain a system of unmixed representations

$$(\bar{S}, \overline{Rep}, \mathbf{decompose}_{R[x]}, \mathbf{split}_{R[x]})$$

in $R[x]$. The algorithm $\mathbf{decompose}_{R[x]}$ is now used for computing decompositions

$$I = I_1 \cap \cdots \cap I_l$$

such that each $\sqrt{I_i}$ is strongly unmixed.

quasi_unmixed(F)

Input: F, a finite subset of $R[x]$.

Output: $(\{H_1, \ldots, H_k\}, \{H_{k+1}, \ldots, H_l\})$, where each H_i is a Gröbner basis in $R[x]$ whose radical $\sqrt{H_i}$ is strongly unmixed and $\langle F \rangle = \langle H_1 \rangle \cap \cdots \cap \langle H_l \rangle$. Furthermore,

$$(\sqrt{H_i} \cap R)\, R[x] \neq \sqrt{H_i} \text{ for } i \leq k \text{ and } (\sqrt{H_i} \cap R)\, R[x] = \sqrt{H_i} \text{ for } i > k.$$

$\{C_1, \ldots, C_l\} := \mathbf{decompose}_{R[x]}(F)$
forall $i \in \{1, \ldots, l\}$ **do**
  if $C_i \not\subseteq R$ **then**

$g_i :=$ the only element in $C_i \setminus R$
$G_i :=$ Gröbner basis of $\langle C_i \rangle : lc(g_i)^\infty$
else
$G_i := C_i$
end
$m_i :=$ natural number with $\langle F \rangle + \langle G_i \rangle^{m_i} = \langle F \rangle + \langle G_i \rangle^{m_i+1}$
$G'_i :=$ Gröbner basis of $\langle F \rangle + \langle G_i \rangle^{m_i}$
end
return$((\{G'_i \mid C_i \not\subseteq R\}, \{G'_i \mid C_i \subseteq R\}))$

In the next step we formalize the decomposition strategy based on Theorem 7.5. We denote the concatenation of two tuples $a = (a_1, \ldots, a_i)$ and $b = (b_1, \ldots, b_j)$ by $a \circ b$, i.e.

$$a \circ b := (a_1, \ldots, a_i, b_1, \ldots, b_j).$$

hullA(G)

Input: G, a Gröbner basis of an ideal $I \subset R[x]$ whose radical is strongly unmixed.
Output: $(F_1, \ldots, F_r)$, where every F_i is a finite basis of an ideal $I_i \subset R[x]$ and $I = I_1 \cap \cdots \cap I_r$. The set F_1 is a Gröbner basis. If $r > 1$ then $I \subset I_i$ for every $i \in \{1, \ldots, r\}$. Furthermore,

(1) if I has an embedded prime P with $height(P \cap R) > height(I \cap R)$ then $r > 2$,
(2) if $(\sqrt{I} \cap R)\, R[x] \neq \sqrt{I}$ then I_1 is the intersection of some of the primary components of I with minimal height.

$m := \max(\{deg(g) \mid g \in G\})$
forall $j \in \{0, \ldots, m\}$ **do**
$L_j := \{lc(g) \mid g \in G,\ deg(g) \leq j\}$
$\{F_{j1}, \ldots, F_{jr_j}\} :=$ **unmixed_dec**$_R(L_j)$
end
$U := \bigcup_{j=0}^{m} \bigcup_{i=1}^{r_j} F_{ji}$
if there exists an $f \in U$ with $I \subset I : f^\infty \subset R[x]$ **then**
$f :=$ element of U with $I \subset I : f^\infty \subset R[x]$
$H :=$ Gröbner basis of $I : f^\infty$
$d :=$ natural number with $I : f^d = I : f^\infty$
return(**hullA**$(H) \circ (G \cup \{f^d\})$)
else
return$((G))$
end

The correctness of the following algorithm is based on the Theorems 7.6 and 7.7.

addx(G)

Input: G, a Gröbner basis of an ideal $I \subset R[x]$ such that

(1) $\sqrt{I}$ is strongly unmixed,
(2) $(\sqrt{I} \cap R)\, R[x] = \sqrt{I}$,

(3) $height(P \cap R) = height(I \cap R)$ for each associated prime P of I.

Output: $(F_1, \ldots, F_r)$, where every F_i is a finite basis of an ideal $I_i \subset R[x]$ and $I = I_1 \cap \cdots \cap I_r$. Furthermore,

(1) if $r = 1$ then I_1 is unmixed,
(2) if $r > 1$ then $I \subset I_i$ for every $i \in \{1, \ldots, r\}$.

if $I \subset I : x^\infty \subset R[x]$ **then**
  $H :=$ Gröbner basis of $I : x^\infty$
  $d :=$ natural number with $I : x^d = I : x^\infty$
  return$((H, G \cup \{x^d\}))$
else
  $m := \max(\{deg(g) \mid g \in G\})$
  $n :=$ arbitrary natural number
  $O := \emptyset$
  while $O = \emptyset$ **do**
    $F :=$ Gröbner basis of $I + \langle x^n \rangle$
    if $\{f \in F \mid deg(f) \leq m\} \subseteq I$ **then**
      $O := (G)$
    else
      $(H_1, \ldots, H_s) :=$ **hullA**(F)
      forall $h \in H_1 \setminus I$ **do**
        $G_h :=$ Gröbner basis of $I : h$
      end
      $U := \bigcup_{h \in H_1 \setminus I} G_h$
      if there exists an $f \in U$ with $I \subset I : f^\infty \subset R[x]$ **then**
        $f :=$ element of U with $I \subset I : f^\infty \subset R[x]$
        $H :=$ Gröbner basis of $I : f^\infty$
        $d :=$ natural number with $I : f^d = I : f^\infty$
        $O := (H, G \cup \{f^d\})$
      else
        $n := n + k$, where k is an arbitrary natural number
      end
    end
  end
  return(O)
end

Using the above subalgorithms we can now construct a procedure for computing unmixed decompositions of arbitrary ideals in $R[x]$.

unmixed_dec$_{R[x]}(F)$

Input: F, a finite subset of $R[x]$.

Output: $\{F_1, \ldots, F_r\}$, where every F_i is a finite basis of an unmixed ideal in $R[x]$ and $\langle F \rangle = \bigcap_{i=1}^{r} \langle F_i \rangle$.

$(\{G_1, \ldots, G_k\}, \{G_{k+1}, \ldots, G_l\}) := \mathbf{quasi\_unmixed}(F)$
forall $i \in \{1, \ldots, l\}$ **do**
$(G_{1i}, \ldots, G_{s_i i}) := \mathbf{hullA}(G_i)$
end
$J_1 := \{i \in \{k+1, \ldots, l\} \mid s_i > 1\}$
$J_2 := \{i \in \{k+1, \ldots, l\} \mid s_i = 1\}$
forall $i \in J_2$ **do**
$(H_{1i}, \ldots, H_{t_i i}) := \mathbf{addx}(G_i)$
end
$J_2' := \{i \in J_2 \mid t_i = 1\}$
$J_2'' := \{i \in J_2 \mid t_i > 1\}$
$O := \bigcup_{i=1}^{k} \{G_{1i}\} \cup \bigcup_{j=2}^{s_i} \mathbf{unmixed\_dec}_{R[x]}(G_{ji}) \cup$
$\bigcup_{i \in J_1} \bigcup_{j=1}^{s_i} \mathbf{unmixed\_dec}_{R[x]}(G_{ji}) \cup$
$\bigcup_{i \in J_2'} \{H_{1i}\} \cup$
$\bigcup_{i \in J_2''} \bigcup_{j=1}^{t_i} \mathbf{unmixed\_dec}_{R[x]}(H_{ji})$
return(O)

EXAMPLE 7.1. We will now use the techniques developed in this section for computing an unmixed decomposition of the ideal $I \subseteq \mathbf{Q}[x_1, x_2, x_3]$ generated by $F = \{f_1, f_2, f_3, f_4\}$, where

$$\begin{aligned} f_1 &:= x_1^3 x_2 + x_1^3 x_2 x_3 + x_1^2, \\ f_2 &:= x_1^4 x_2^4 - x_1 x_2, \\ f_3 &:= x_2^2 x_3^3 + 3x_2^2 x_3^2 + 3x_2^2 x_3 + 2x_2^2, \\ f_4 &:= x_1 x_3^2 - x_1 x_3 + x_2 x_3 - x_2. \end{aligned}$$

First we construct a system of unmixed representations

$$(\bar{S}, \overline{Rep}, \mathbf{decompose}_{\mathbf{Q}[x_1,x_2,x_3]}, \mathbf{split}_{\mathbf{Q}[x_1,x_2,x_3]})$$

in $\mathbf{Q}[x_1, x_2, x_3]$ as in Example 4.2. We compute $\mathbf{decompose}_{\mathbf{Q}[x_1,x_2,x_3]}(F)$ and obtain $\{C_1, C_2, C_3\}$, where

$$\begin{aligned} C_1 &:= \{x_3 + 2, x_2 - 2x_1, 2x_1^2 - 1\}, \\ C_2 &:= \{-x_1 x_2 x_3 - x_1 x_2 - 1, x_2^2 - x_1 x_2 - 1, 1 + x_1^2\}, \\ C_3 &:= \{x_2, x_1\}. \end{aligned}$$

Hence, $\sqrt{I} = \bigcap_{i=1}^{3} \overline{Rep}(C_i)$ and each $\overline{Rep}(C_i)$ is a strongly unmixed radical. By computing natural numbers j_1, j_2, j_3 with $I + \overline{Rep}(C_i)^{j_i} = I + \overline{Rep}(C_i)^{j_i+1}$ we obtain $I = I_1 \cap I_2 \cap I_3$, where

$$\begin{aligned} I_1 &:= \langle x_3 + 2, x_2 - 2x_1, 2x_1^2 - 1 \rangle, \\ I_2 &:= \langle x_3 - x_1 x_2, x_2^2 - x_1 x_2 - 1, 1 + x_1^2 \rangle, \\ I_3 &:= \langle x_1 x_3^2 - x_1 x_3 + x_2 x_3 - x_2, x_2^2, x_1 x_2, x_1^2 \rangle. \end{aligned}$$

As I_1 and I_2 are 0-dimensional and therefore unmixed it remains to compute an unmixed decomposition of I_3. We consider I_3 as an ideal in the univariate polynomial ring $R[x_3]$, where $R := \mathbf{Q}[x_1, x_2]$. As

$$\{x_1 x_3^2 - x_1 x_3 + x_2 x_3 - x_2, x_2^2, x_1 x_2, x_1^2\}$$

is a Gröbner basis of I_3 it is easy to see that

(1) $\sqrt{I_3} = \overline{Rep}(C_3)$ is strongly unmixed,
(2) $(\sqrt{I_3} \cap R)\, R[x_3] = \sqrt{I_3}$,
(3) $height(P \cap R) = height(I_3 \cap R)$ for each associated prime P of I_3,
(4) $I_3 : x_3^\infty = I_3$.

Hence, for deciding whether I_3 is unmixed we can use the criterion in Theorem 7.7:

$$I_3 \text{ is unmixed if and only if } \{h \in H \mid deg(h) \leq 2\} \subseteq I_3,$$

where H is a Gröbner basis of $I_3 + \langle x_3^n \rangle$ and $n \in \mathbf{N}$ is sufficiently large. We choose $n = 5$, compute a Gröbner basis

$$H := \{x_3^5, x_3^4 x_2, x_1 x_3 + x_2, x_2^2, x_1 x_2, x_1^2\}$$

of $I_3 + \langle x_3^n \rangle$ and obtain $\{h \in H \mid deg(h) \leq 2\} \not\subseteq I_3$. Therefore we now try to decompose I_3. If this does not work we know that n is not large enough and we have to repeat the whole process with $n > 5$.

Obviously, $I_3 + \langle x_3^n \rangle$ is a primary ideal with radical $\langle x_3, x_2, x_1 \rangle$. If I_3 is not unmixed and n has been chosen sufficiently large then, by Theorem 7.6, some element of

$$\{x_3^5, x_3^4 x_2, x_1 x_3 + x_2\} = H \setminus I_3$$

is in the primary component of I_3 which belongs to the isolated prime $\langle x_2, x_1 \rangle$. In this case a decomposition of I_3 can be obtained using Lemma 7.1. Therefore, we now compute Gröbner bases G_1, G_2, G_3 of the ideal quotients $I_3 : x_3^5$, $I_3 : x_3^4 x_2$ and $I_3 : (x_1 x_3 + x_2)$ and a Gröbner basis of $I_3 : f^\infty$ for each f in $G_1 \cup G_2 \cup G_3$. As $x_3 - 1$ is an element of the Gröbner basis of $I_3 : (x_1 x_3 + x_2)$ we compute

$$I_3 : (x_3 - 1)^\infty = \langle x_1 x_3 + x_2, x_2^2, x_1 x_2, x_1^2 \rangle.$$

Together with Theorem 7.2 it follows from

$$I_3 \subset I_3 : (x_3 - 1)^\infty \subset R[x_3] \text{ and } I_3 : (x_3 - 1)^\infty = I_3 : (x_3 - 1)$$

that $I_3 = I_3' \cap I_3''$ is a non-trivial decomposition of I_3, where

$$I_3' := \langle x_3 - 1, x_2^2, x_1 x_2, x_1^2 \rangle,$$
$$I_3'' := \langle x_1 x_3 + x_2, x_2^2, x_1 x_2, x_1^2 \rangle.$$

The ideal I_3' is 0-dimensional and therefore unmixed. As

$$\{x_3^5, x_3^4 x_2, x_1 x_3 + x_2, x_2^2, x_1 x_2, x_1^2\}$$

is a Gröbner basis of $I_3'' + \langle x_3^5 \rangle$ it immediately follows from Theorem 7.7 that I_3'' is unmixed. Hence,

$$\begin{aligned} I = {} & \langle x_3 + 2, x_2 - 2x_1, 2x_1^2 - 1 \rangle \cap \\ & \langle x_3 - x_1 x_2, x_2^2 - x_1 x_2 - 1, 1 + x_1^2 \rangle \cap \\ & \langle x_3 - 1, x_2^2, x_1 x_2, x_1^2 \rangle \cap \\ & \langle x_1 x_3 + x_2, x_2^2, x_1 x_2, x_1^2 \rangle \end{aligned}$$

is an unmixed decomposition of I.

8. Computing Primary Decompositions

We say that primary decompositions of ideals are computable in R if there exists an algorithm which computes for an arbitrary finite subset F of R finite bases $F_1, \ldots, F_r$ of primary ideals in R with

$$\langle F \rangle = \langle F_1 \rangle \cap \cdots \cap \langle F_r \rangle.$$

We say that associated (resp. isolated) primes of ideals are computable in R if there exists an algorithm which computes for an arbitrary finite subset F of R finite bases $F_1, \ldots, F_r$ of the associated (resp. isolated) prime ideals of $\langle F \rangle$.

Before we deal with primary decompositions we present an algorithm for computing isolated primes. As the computability of radicals is related to the computability of squarefree parts of polynomials the computability of isolated primes is related to the computability of factorizations of polynomials. Even the proofs of these two results are very similar.

THEOREM 8.1. *The following two conditions are equivalent if linear equations are solvable and isolated primes of ideals are computable in R.*

- **(a)** *For every number of variables n isolated primes of ideals are computable in the polynomial ring $R[x_1, \ldots, x_n]$.*
- **(b)** *For every number of variables n and every finite basis F of a prime ideal P in $R[x_1, \ldots, x_n]$ there exists an algorithm for expressing every non-constant element of the univariate polynomial ring $K(P)[x]$ as a product of irreducible polynomials.*

PROOF. For proving Theorem 8.1 it suffices to show that the following two conditions are equivalent.

- **(1)** Isolated primes of ideals are computable in the univariate polynomial ring $R[x]$.
- **(2)** For every finite basis F of a prime ideal P in R there exists an algorithm for expressing every non-constant element of $K(P)[x]$ as a product of irreducible polynomials.

We construct a system of prime representations $(S, Rep, \mathbf{decompose}_R, \mathbf{split}_R)$ in R: let S be the set of finite bases of prime ideals in R and define $Rep(A) := \langle A \rangle$. By assumption, we can compute for a finite subset F of R a set $\{F_1, \ldots, F_r\}$ of finite bases of the isolated primes of $\langle F \rangle$. Let $\mathbf{decompose}_R$ be the algorithm which returns for given F the set $\{F_1, \ldots, F_r\}$. Let $A \in S$ and $f \in R$. As linear equations are solvable in R we can decide whether $f \in \langle A \rangle$. Hence, the algorithm which returns $(\{A\}, \emptyset)$ if $f \in \langle A \rangle$ and $(\emptyset, \{A\})$ otherwise satisfies the specification of $\mathbf{split}_R$.

(**1**) $\Leftarrow$ (**2**) We apply Theorem 4.1 and obtain a system of prime representations $(\bar{S}, \overline{Rep}, \mathbf{decompose}_{R[x]}, \mathbf{split}_{R[x]})$ in $R[x]$. It is now easy to construct an algorithm which computes for an arbitrary finite subset F of $R[x]$ finite bases of the isolated prime ideals of $\langle F \rangle$: if $\emptyset = \mathbf{decompose}_{R[x]}(F)$ then F generates $R[x]$ and $\langle F \rangle$ has no isolated primes. Otherwise, $\mathbf{decompose}_{R[x]}$ computes $C_1, \ldots, C_r \in \bar{S}$ with

$$\sqrt{F} = \bigcap_{i=1}^{r} \overline{Rep}(C_i).$$

It immediately follows from Theorem 3.1 and Lemma 4.4 that we can compute a basis

F_i of the prime ideal $\overline{Rep}(C_i)$ for every $i \in \{1,\ldots,r\}$. As we can algorithmically decide whether $\langle F_i\rangle \subseteq \langle F_j\rangle$ we compute a subset $\{j_1,\ldots,j_s\}$ of $\{1,\ldots,r\}$ such that the prime ideals $\langle F_{j_1}\rangle,\ldots,\langle F_{j_s}\rangle$ are the minimal elements in $\{\langle F_1\rangle,\ldots,\langle F_r\rangle\}$. Obviously, $\langle F_{j_1}\rangle,\ldots,\langle F_{j_s}\rangle$ are the isolated primes of $\langle F\rangle$.

(**1**) $\Rightarrow$ (**2**) Let F be a finite basis of a prime ideal P in R, $f \in R[x]$ such that f^P is not a constant and let $g \in K(P)[x]$ be an irreducible factor of f^P. Let $I := \{h \in R[x] \mid g \text{ divides } h^P\}$. Obviously, $I \cap R = P$. By Lemma 4.1, I is an isolated prime of $\langle F \cup \{f\}\rangle$. Hence, we can find all irreducible factors of f^P in the following way:

Compute finite bases $F_1,\ldots,F_r$ of the isolated primes $P_1,\ldots,P_r$ of $\langle F\cup\{f\}\rangle$. W.l.o.g. assume that $P_i \cap R = P$ for $i \in \{1,\ldots,s\}$ and $P_i \cap R \neq P$ for $i \in \{s+1,\ldots,r\}$ for some $s \in \{1,\ldots,r\}$. Compute for $i \in \{1,\ldots,s\}$ the gcd $f_i \in K(P)[x]$ of the polynomials in $\{h^P \mid h \in F_i\}$. The f_is are the irreducible factors of f^P. □

Assume that Seidenberg's condition **(P)** holds for K and univariate polynomials can be factored over K. It is shown in Seidenberg (1974, p.291) that in this case **(P)** holds for $K(P)$ and univariate polynomials can be factored over $K(P)$, where P is an arbitrary prime ideal in a polynomial ring over K. We refer to van der Waerden (1930), Seidenberg (1973) and Seidenberg (1974) for explicitly given fields which do not have this factorization property.

We will now write down the algorithm for computing isolated primes in $R[x]$ in pseudocode. By our assumptions and Theorem 4.1 there exists a system of prime representations $(\bar{S}, \overline{Rep}, \mathbf{decompose}_{R[x]}, \mathbf{split}_{R[x]})$ in $R[x]$ such that $A \cap R$ is a finite basis of a prime ideal in R for every $A \in \bar{S}$. Using $\mathbf{decompose}_{R[x]}$ we can construct $\mathbf{iprime}_{R[x]}$:

$\mathbf{iprime}_{R[x]}(F)$

Input: F, a finite subset of $R[x]$.
Output: $\{G_1,\ldots,G_s\}$, a set of Gröbner bases of the isolated primes of $\langle F\rangle$.

$\{C_1,\ldots,C_r\} := \mathbf{decompose}_{R[x]}(F)$
forall $i \in \{1,\ldots,r\}$ **do**
  if $C_i \subseteq R$ **then**
    $F_i := C_i$
  else
    $f_i :=$ the only element in $C_i \setminus R$
    $F_i :=$ Gröbner basis of $\langle C_i\rangle : lc(f_i)^\infty$
  end
end
return$(\{F_{j_1},\ldots,F_{j_s}\})$, where $\langle F_{j_1}\rangle,\ldots,\langle F_{j_s}\rangle$ are minimal in $\{\langle F_1\rangle,\ldots,\langle F_r\rangle\}$

We now turn to the computation of primary decompositions.

THEOREM 8.2. *If linear equations are solvable and primary decompositions are computable in R and for any natural number n isolated primes of ideals are computable in $R[x_1,\ldots,x_n]$ then for any natural number n primary decompositions and associated primes of ideals are computable in $R[x_1,\ldots,x_n]$.*

PROOF. For proving this theorem it suffices to construct an algorithm which computes

primary decompositions and associated primes in the univariate polynomial ring $R[x]$. This can easily be done by modifying the unmixed decomposition algorithm developed in the previous section. Using $\mathbf{iprime}_{R[x]}$ we first modify **quasi_unmixed**.

quasi_primary(F)

Input: F, a finite subset of $R[x]$.
Output: $(\{H_1, \ldots, H_k\}, \{H_{k+1}, \ldots, H_l\})$, where each H_i is a Gröbner basis in $R[x]$ whose radical $\sqrt{H_i}$ is prime and $\langle F\rangle = \langle H_1\rangle \cap \cdots \cap \langle H_l\rangle$. Furthermore,

$$(\sqrt{H_i} \cap R)\, R[x] \neq \sqrt{H_i} \text{ for } i \leq k \text{ and } (\sqrt{H_i} \cap R)\, R[x] = \sqrt{H_i} \text{ for } i > k.$$

$\{G_1, \ldots, G_l\} := \mathbf{iprime}_{R[x]}(F)$
forall $i \in \{1, \ldots, l\}$ **do**
  $m_i :=$ natural number with $\langle F\rangle + \langle G_i\rangle^{m_i} = \langle F\rangle + \langle G_i\rangle^{m_i+1}$
  $G_i' :=$ Gröbner basis of $\langle F\rangle + \langle G_i\rangle^{m_i}$
end
$J := \{i \in \{1, \ldots, l\} \mid \langle G_i \cap R\rangle\, R[x] = \langle G_i\rangle\}$
return$((\{G_i' \mid i \in \{1, \ldots, l\} \setminus J\}, \{G_i' \mid i \in J\}))$

As primary decompositions are computable in the ring R there exists an algorithm $\mathbf{primary\_dec}_R$ which computes for a finite subset F of R a set $\{F_1, \ldots, F_r\}$ of finite bases of primary ideals such that $\langle F\rangle = \bigcap_{i=1}^r \langle F_i\rangle$. In **hullA** we only replace $\mathbf{unmixed\_dec}_R$ by $\mathbf{primary\_dec}_R$ and there are no changes in **addx**. We replace the algorithm **quasi_unmixed** by **quasi_primary** in $\mathbf{unmixed\_dec}_{R[x]}$ and obtain an algorithm $\mathbf{primary\_dec}_{R[x]}$ which satisfies the following specification.

Input: F, a finite subset of $R[x]$.
Output: $\{F_1, \ldots, F_r\}$, where every F_i is a finite basis of a primary ideal in $R[x]$ and $\langle F\rangle = \bigcap_{i=1}^r \langle F_i\rangle$.

As we can compute primary decompositions and isolated primes in $R[x]$ we can also compute associated primes in $R[x]$. Hence, the theorem is proved. □

Acknowledgements

I am grateful to Professor Erwin Engeler for creating an excellent working environment and to Dr. Stephane Collart and Dr. Daniel Mall for many helpful discussions.

References

Adams, W.W., Loustaunau, P. (1994). *An Introduction to Gröbner Bases*, Vol. 3. *Graduate Studies in Mathematics*, Providence, RI, AMS.

Alonso, M.E., Mora, T., Raimondo, M. (1990). Local decomposition algorithms. In *Proc. AAECC-8*, LNCS **508**, pp. 208–221. Tokyo, Japan, Springer.

Armendáriz, I., Solerno, P. (1995). On the computation of the radical of polynomial complete intersection ideals. In *Proc. AAECC-11*, pp. 106–119. Paris, France.

Atiyah, M.F., Macdonald, I.G. (1969). *Introduction to Commutative Algebra*. Reading, MA, Addison-Wesley.

Aubry, P., Lazard, D., Moreno Maza, M. (1998). On the theories of triangular sets. Submitted to *J. Symb. Comput.*

Aubry, P., Moreno Maza, M. (1998). Triangular sets for solving polynomial systems: a comparative implementation of four methods. Submitted to *J. Symb. Comput.*

Ayoub, C.W. (1982). The decomposition theorem for ideals in polynomial rings over a domain. *J. Algebra* **76**, 99–110.
Bayer, D., Galligo, A., Stillman, M. (1991). Gröbner bases and extension of scalars. In *Proc. Comput. Algebraic Geom. and Commut. Algebra*, pp. 198–215. Cortona, Italy, Cambridge University Press.
Bayer, D., Mumford, D. (1991). What can be computed in algebraic geometry? In *Proc. Comput. Algebraic Geom. and Commut. Algebra*, pp. 1–48. Cortona, Italy, Cambridge University Press.
Bayer, D., Stillman, M. (1992). Computation of Hilbert functions. *J. Symb. Comput.*, **14**, 31–50.
Becker, T., Weispfenning, V. (1993). *Gröbner Bases. A Computational Approach to Commutative Algebra*. Vol. 141. *Graduate Texts in Mathematics*. New York, Springer, p. 54.
Bigatti, A.M., Caboara, M., Robbiano, L. (1991). On the computation of Hilbert–Poincaré series. *J. AAECC*, **2**, 21–33.
Bigatti, A.M., Conti, P., Robbiano, L., Traverso, C. (1993). A "divide and conquer" algorithm for Hilbert-Poincaré series, multiplicity and dimension of monomial ideals. In *Proc. AAECC-10*, LNCS **673**, pp. 76–88. San Juan de Puerto Rico, Puerto Rico, Springer.
Böge, W., Gebauer, R., Kredel, H. (1986). Some examples for solving systems of algebraic equations by calculating Gröbner bases. *J. Symb. Comput.*, **2**, 83–98.
Brown, W.S., Traub, J.F. (1971). On Euclid's algorithm and the theory of subresultants. *J. ACM*, **18**, 505–514.
Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD thesis, University Innsbruck, Department of Mathematics, Innsbruck, Austria.
Buchberger, B. (1970). Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Mathematicae*, **4**, 374–383.
Buchberger, B. (1984). A critical-pair/completion algorithm for finitely generated ideals in rings. In *Symposium "Rekursive Kombinatorik"*, LNCS **171**, pp. 137–161. Münster, Germany, Springer.
Buchberger, B. (1987). Applications of Gröbner bases in non-linear computational geometry. In *Proc. Workshop on Scientific Software*, pp. 59–88. Minneapolis, Minnesota, IMA.
Chistov, A.L., Grigoryev, D.Y. (1983). Subexponential-time solving systems of algebraic equations I. Technical Report LOMI Preprints E-9-83, USSR Acad. of Sciences, Steklov Math. Institute, Leningrad Dept., Leningrad, USSR.
Chou, S.C. (1988). *Mechanical Geometry Theorem Proving*. Dordrecht, Reidel.
Chou, S.C., Gao, X.S. (1990). Ritt–Wu's decomposition algorithm and geometry theorem proving. In *Proc. CADE-10*, pp. 202–220. Kaiserslautern, Germany.
Chou, S.C., Schelter, W.F. (1986). Proving geometry theorems with rewrite rules. *J. Automated Reasoning*, **2**, 253–273.
Cohen, I.S. (1946). On the structure and ideal theory of complete local rings. *Trans. AMS*, **59**, 54–106.
Collins, G.E. (1967). Subresultants and reduced polynomial remainder sequences. *J. ACM*, **14**, 128–142.
Czapor, S.R. (1989). Solving algebraic equations: Combining Buchberger's algorithm with multivariate factorization. *J. Symb. Comput.*, **7**, 49–53.
Czapor, S.R., Geddes, K.O. (1986). On implementing Buchberger's algorithm for Gröbner bases. In *Proc. SYMSAC'86*, pp. 233–238. Waterloo, Canada.
Della Dora, J., Dicrescenzo, C., Duval, D. (1985). About a new method for computing in algebraic number fields. In *Proc. EUROCAL'85*, LNCS **204**, pp. 289–290. Linz, Austria, Springer.
Dicrescenzo, C., Duval, D. (1988). Algebraic extensions and algebraic closure in Scratchpad II. In *Proc. ISSAC'88*, LNCS **358**, pp. 440–446. Rome, Italy, Springer.
Eisenbud, D. (1995). *Commutative Algebra with a View Toward Algebraic Geometry*. Vol. 150. *Graduate Texts in Mathematics*. New York, Springer.
Eisenbud, D., Huneke, C., Vasconcelos, W. (1992). Direct methods for primary decomposition. *Inventiones Mathematicae*, **110**, 207–235.
Galligo, A., Traverso, C. (1989). Practical determination of the dimension of an algebraic variety. *Computer and Mathematics 89*, pp. 46-52. Springer.
Gallo, G., Mishra, B. (1990). Efficient algorithms and bounds for Wu–Ritt characteristic sets. In *Proc. MEGA'90, Progress in Mathematics* **94**, pp. 119–142. Livorno, Italy, Birkhäuser.
Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comput.*, **6**, 149–168.
Giusti, M. (1988). Combinatorial dimension theory of algebraic varieties. *J. Symb. Comput.*, **6**, 249–265.
Giusti, M., Heintz, J. (1990). Algorithmes – disons rapides – pour la décomposition d'une variété algébrique en composantes irréductibles et équidimentionnelles. In *Proc. MEGA'90, Progress in Mathematics* **94**, pp. 169–194. Livorno, Italy, Birkhäuser.
Gräbe, H.G. (1993). Two remarks on independent sets. *J. Algebraic Combin.*, **2**, 137–145.
Gräbe, H.G. (1995). Minimal primary decomposition and factorized Gröbner bases. Preprint.
Gröbner, W. (1970). *Algebraische Geometrie II*. Bibliographisches Institut Mannheim, Germany.
Hartshorne, R. (1977). *Algebraic Geometry*. Vol. 52, *Graduate Texts in Mathematics*. New York, Springer.

Hearn, A.C. (1979). Non-modular computation of polynomial gcds using trial division. In *Proc. EUROSAM'79*, LNCS **72**, pp. 227–239. Marseille, France, Springer.
Hermann, G. (1926). Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Annalen*, **95**, 736–788.
Kalkbrener, M. (1993). A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *J. Symb. Comput.*, **15**, 143–167.
Kalkbrener, M. (1994). Prime decompositions of radicals in polynomial rings. *J. Symb. Comput.*, **18**, 365–372.
Kalkbrener, M. (1995). A generalized Euclidean algorithm for geometry theorem proving. *Ann. Math. and Artificial Intelligence*, **13**, 73–95.
Kalkbrener, M., Sturmfels, B. (1995). Initial complexes of prime ideals. *Adv. Math.*, **116**, 365–376.
Kandri-Rody, A. (1985). Dimension of ideals in polynomial rings. In J. Avenhaus and K. Madlener, eds., *Proc. Combinatorial Algorithms in Algebraic Structures*, Otzenhausen, Germany.
Kaplansky, I. (1970). *Commutative Rings*. Boston, MA, Allyn and Bacon.
Kapur, D. (1986). Geometry theorem proving using Hilbert's Nullstellensatz. In *Proc. SYMSAC'86*, pp. 202–208. Waterloo, Canada.
Kapur, D., Wan, H.K. (1990). Refutational proofs of geometry theorems via characteristic set computation. In *Proc. ISSAC'90*, pp. 277–284. Tokyo, Japan, ACM Press.
Ko, H.P., Hussain, M.A. (1985). A study of Wu's method – a method to prove certain theorems in elementary geometry. In *Proc. of 1985 Congressus Numerantium*.
Kondrat'eva, M.V., Pankrat'ev, E.V. (1987). A recursive algorithm for the computation of the Hilbert polynomial. In *Proc. EUROCAL'87*, LNCS **378**, pp. 365–375. Leipzig, Germany, Springer.
Kredel, H. (1987). Primary ideal decomposition. In *Proc. EUROCAL'87*, LNCS **378**, pp. 270–281. Leipzig, Germany, Springer.
Kredel, H., Weispfenning, V. (1988). Computing dimension and independent sets for polynomial ideals. *J. Symb. Comput.*, **6**, 231–248.
Krick, T., Logar, A. (1991). An algorithm for the computation of the radical of an ideal in the ring of polynomials. In *Proc. AAECC-9*, LNCS **539**, pp. 195–205. New Orleans, Louisiana, Springer.
Krull, W. (1928). Primidealketten in allgemeinen Ringbereichen. *Sitzungsberichte Heidelberger Akad.* **7**.
Kutzler, B. (1988). Algebraic approaches to automated geometry theorem proving, PhD thesis, University Linz, RISC, Linz, Austria.
Kutzler, B., Stifter, S. (1986). Automated geometry theorem proving using Buchberger's algorithm. In *Proc. SYMSAC'86*, pp. 209–214. Waterloo, Canada.
Lazard, D. (1985). Ideal bases and primary decomposition: case of two variables. *J. Symb. Comput.*, **1**, 261–270.
Lazard, D. (1991). A new method for solving algebraic systems of positive dimension. *Discrete Applied Math.*, **33**, 147–160.
Lazard, D. (1992). Solving zero-dimensional algebraic systems. *J. Symb. Comput.*, **13**, 117–131.
Matsumura, H. (1970). *Commutative Algebra*. New York, W.A. Benjamin.
Mines, R., Richman, F., Ruitenburg, W. (1988). *A Course in Constructive Algebra*. New York, Springer.
Möller, H.M. (1988). On the construction of Gröbner bases using syzygies. *J. Symb. Comput.*, **6**, 345–360.
Möller, H.M. (1993). On decomposing systems of polynomial equations with finitely many solutions. *J. AAECC*, **4**, 217–230.
Möller, H.M., Mora, T. (1983). The computation of the Hilbert function. In *Proc. EUROCAL'83*, LNCS **162**, pp. 157–167. London, Springer.
Möller, H.M., Mora, F. (1987). Computational aspects of reduction strategies to construct resolutions of monomial ideals. In *Proc. AAECC-2*, LNCS **228**, pp. 182–197. Toulouse, Springer.
Mora, T., Robbiano, L. (1988). The Gröbner fan of an ideal. *J. Symb. Comput.*, **6**, 183–208.
Richman, F. (1974). Constructive aspects of Noetherian rings. *Proc. AMS*, **44**, 436–441.
Ritt, J.F. (1950). *Differential Algebra*. Vol. 33. *Colloquium Publications*. New York, AMS.
Robbiano, L. (1986). On the theory of graded structures. *J. Symb. Comput.*, **2**, 139–170.
Schaller, S.C. (1978). Algorithmic aspects of polynomial residue class rings, PhD thesis, University of Wisconsin-Madison, Department of Comp. Sci., Madison, WI.
Seidenberg, A. (1973). On the impossibility of some constructions in polynomial rings. In *Proc. Int. Cong. Geom.*, pp. 77–85. Milano, Italy.
Seidenberg, A. (1974). Constructions in algebra. *Trans. AMS*, **197**, 273–313.
Seidenberg, A. (1978). Constructions in a polynomial ring over the ring of integers. *Am. J. Math.*, **100**, 685–703.
Seidenberg, A. (1984). On the Lasker–Noether decomposition theorem. *Am. J. Math.*, **106**, 611–638.
Shimoyama, T., Yokoyama, K. (1994). Localization and primary decomposition of polynomial ideals. Technical Report ISIS-RR-94-10E, ISIS, Fujitsu, Numazu, Japan.
Shtokhamer, R. (1988). Lifting canonical algorithms from a ring R to the ring $R[x]$. *J. Symb. Comput.*, **6**, 169–182.

Spear, D. (1977). A constructive approach to ring theory. In *Proc. MACSYMA Users' Conference*, pp. 369–376. Berkeley, CA, The MIT Press.
Stoutemyer, D.R. (1985). Polynomial remainder sequence greatest common divisors revisited. In *Proc. Second RIKEN Int. Symp. on Symbolic and Algebraic Computation by Computers*, pp. 1–12. World Scientific.
Szanto, A. (1997). The computational complexity of the Wu-Ritt type unmixed decomposition of radical ideals. Preprint, Cornell University, Ithaca, New York.
Trinks, W. (1978). Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. *J. Number Theory*, **10**, 475–488.
van der Waerden, B.L. (1930). Eine Bemerkung über die Unzerlegbarkeit von Polynomen. *Math. Annalen*, **102**, 738–739.
van der Waerden, B.L. (1967). *Algebra II (in German)*. 5th edition. Berlin Heidelberg New York, Springer.
Wang, D. (1993). An elimination method for polynomial systems. *J. Symb. Comput.*, **16**, 83–114.
Wang, D. (1995). Elimination procedures for mechanical theorem proving in geometries. *Ann. Math. and Artificial Intelligence*, **13**, 1–24.
Winkler, F. (1990). Gröbner bases in geometry theorem proving and simplest degeneracy conditions. *Mathematica Pannonica*, **1**, 15–32.
Wu, W. (1978). On the decision problem and the mechanization of theorem proving in elementary geometry. *Scientia Sinica*, **21**, 157–179.
Wu, W. (1984). Basic principles of mechanical theorem proving in elementary geometries. *J. Sys. Sci. and Math. Sci.*, **4**, 207–235.
Wu, W. (1987). A zero structure theorem for polynomial equations solving. *MM Research Preprints*, **1**, 2–12.
Zacharias, G. (1978). Generalized Gröbner bases in commutative polynomial rings, Master's thesis, MIT, Dept. of Comp. Sci., Boston, MA.
Zariski, O., Samuel, P. (1975a). *Commutative Algebra I*. Vol. 28 of *Graduate Texts in Mathematics*. Berlin Heidelberg New York, Springer.
Zariski, O., Samuel, P. (1975b). *Commutative Algebra II*. Vol. 29 of *Graduate Texts in Mathematics*. Berlin Heidelberg New York, Springer.

Originally Received 6 August 1996
Accepted 19 June 1998