Prime decompositions of radicals in polynomial rings

MICHAEL KALKBRENER

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

In this paper we are concerned with the computation of prime decompositions of radicals in polynomial rings over a noetherian commutative ring R with identity. We show that prime decomposition algorithms in R can be lifted to $R[x]$ if for every prime ideal P in R univariate polynomials can be factored over the quotient field of the residue class ring R/P. In the proof of this result a lifting algorithm is constructed which can be considered as a generalization of the algorithm of Ritt and Wu.

1. Introduction

In the last twenty years several methods for computing primary decompositions of ideals in multivariate polynomial rings over fields (Seidenberg (1974), Lazard (1985), Kredel (1987), Eisenbud et al. (1992)), the integers (Seidenberg, 1978), factorially closed principal ideal domains (Ayoub (1982), Gianni et al. (1988)) and more general rings (Seidenberg, 1984) have been proposed. A related problem is the computation of the irreducible components of an algebraic variety or, equivalently, the computation of the prime ideals in the prime decomposition of a radical. A well-known method for performing this task in a multivariate polynomial ring over a field of characteristic zero is the Ritt-Wu algorithm based on the computation of characteristic sets (Ritt (1950), Wu (1984)). Another method for solving the same problem can be found in (Wang, 1993). Giusti and Heintz deal with irreducible and equidimensional decompositions of varieties given by polynomials in multivariate polynomial rings over infinite perfect fields (Giusti and Heintz, 1990). In Chistov and Grigor'ev (1983) an irreducible decomposition algorithm is presented and analyzed that works in multivariate polynomial rings over fields which are finitely generated over primitive fields. In the present paper we are concerned with the computation of prime decompositions of radicals in polynomial rings over noetherian commutative rings with identity.

The prime ideals computed by the Ritt-Wu algorithm are not represented by bases but by so-called irreducible ascending sets. We will not restrict ourselves to either one of these two possible ways of representing prime ideals but will use the following rather general concept. Let R be a noetherian commutative ring with identity, S a set of finite subsets of R and Rep a surjective function from S to $Spec(R)$, the set of prime ideals in R. We assume that for a given $A \in S$ we can algorithmically decide for every $f \in R$ whether $f \in Rep(A)$. Then $A \in S$ is called a representation of the prime ideal $Rep(A)$ and the pair (S, Rep) is called a system of representations in R.

Example: Let R be the multivariate polynomial ring $K[x_1, \ldots, x_n]$ over a field K

and S the set of those Gröbner bases with respect to a given ordering which generate prime ideals. We define the function Rep by $Rep(C) := Ideal(C)$ for every $C \in S$, where $Ideal(C)$ denotes the ideal generated by C if $C \neq \emptyset$ and $Ideal(\emptyset) := \{0\}$.

Another common way of representing prime ideals is by means of ascending sets: let S' be the set of irreducible ascending sets in $K[x_1, \ldots, x_n]$ (Wu, 1984) 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.

Throughout this paper let R be a noetherian commutative ring with identity and (S, Rep) a system of representations in R. We assume that R is explicitly given, i.e. that one can carry out the ring operations in R, and also that there exists an algorithm that computes for a finite subset F of R a (possibly empty) subset $\{C_1, \ldots, C_r\}$ of S such that

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

where $Radical(F)$ denotes the radical of $Ideal(F)$. It is an objective of this paper to investigate under which conditions this algorithm can be lifted to $R[x]$. A similar study has been done by Seidenberg in order to lift algorithms for computing primary decompositions of ideals from R to $R[x_1, \ldots, x_n]$ (see Seidenberg (1984)). Our main result is the following theorem.

THEOREM 1.1. *Assume that for every $C \in S$ there exists an algorithm for expressing every non-constant element of $K[x]$ as a product of irreducible polynomials, where K is the quotient field of the residue class ring $R/Rep(C)$. Then there exists a system of representations $(\bar{S}, \overline{Rep})$ in $R[x]$ and an algorithm that computes for a given finite subset F of $R[x]$ a subset $\{C_1, \ldots, C_r\}$ of $\bar{S}$ such that*

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

We can inductively use Theorem 1.1 to lift prime decomposition algorithms in R to multivariate polynomial rings over R if these polynomial rings satisfy the condition in Theorem 1.1 (see Seidenberg (1974) for a class of rings with this property).

For proving Theorem 1.1 we first construct a system of representations $(\bar{S}, \overline{Rep})$ in $R[x]$ which can be considered as a generalization of the concept of irreducible ascending sets. Then we construct the prime decomposition algorithm in $R[x]$. Despite its generality this algorithm has a very simple structure. The same elementary operations are used as in the Ritt-Wu algorithm: pseudodivision and factorization. Another method based on a similar strategy is the algorithm for computing equidimensional decompositions of varieties in Kalkbrener (1993). Compare also with Lazard (1991) and Wang (1993). Differences and similarities to existing algorithms as well as open problems regarding the complexity and the practical applicability of the presented algorithm are discussed in the last section of this paper.

2. Proof of Theorem 1.1

Let J be an ideal in R, f a polynomial in $R[x]$ and I an ideal in $R[x]$. The image of f in $(R/J)[x]$ is denoted by f^J, the ideal $\{f^J \mid f \in I\}$ in $(R/J)[x]$ by I^J and the leading coefficient of f by $lc(f)$. If J is prime the quotient field of the residue class ring R/J is denoted by $K(J)$.

First we construct a system of representations $(\bar{S}, \overline{Rep})$ in $R[x]$. Our approach can be considered as a generalization of the concept of irreducible ascending sets in Ritt (1950) and Wu (1984). It is based on the following lemma.

LEMMA 2.1. *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 $I^{I\cap R} = J \cap (R/I \cap R)[x]$, where J is the ideal in $K(I \cap R)[x]$ generated by $I^{I\cap R}$.*
(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*

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

PROOF. **(a)** $\Leftrightarrow$ **(b)**: Since

$$I^{I\cap R} \cap (R/I \cap R) = \{0\}, \tag{2.1}$$

the equivalence of **(a)** and **(b)** follows from Lemma 4.1 and Lemma 4.2 in Gianni et al. (1988).

(b) $\Rightarrow$ **(c)**: Let $q \in K(I \cap R)[x]$ be the polynomial that generates J. From (2.1) we obtain $I^{I\cap R} \neq (R/I \cap R)[x]$ and therefore $J \neq K(I \cap R)[x]$. Hence, q is either irreducible or zero. Let $f \in R[x]$. Then

$$f \in I \quad \text{iff} \quad f^{I\cap R} \in I^{I\cap R} \quad \text{iff} \quad f^{I\cap R} \in J \quad \text{iff} \quad f^{I\cap R} \in Ideal(\{q\}).$$

(c) $\Rightarrow$ **(b)**: J is prime because q generates J and q is irreducible or zero. Let $f \in R[x]$ with $f^{I\cap R} \in J$. Then $f^{I\cap R} \in Ideal(\{q\})$ and therefore $f \in I$ and $f^{I\cap R} \in I^{I\cap R}$. $\square$

We now define

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

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

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

Note that membership for $\overline{Rep}(B)$, $B \in \bar{S}$, can be algorithmically decided. Hence, it follows from Lemma 2.1 that $(\bar{S}, \overline{Rep})$ is a system of representations in $R[x]$.

It remains to construct a prime decomposition algorithm in $R[x]$. By assumption, there exist the following two algorithms.

primedec$_R$ (in: F; out: O)

Input: F, a finite subset of R.
Output: $O = \{C_1, \ldots, C_r\}$, a subset of S with

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

factor (in: C, f; out: $g_1, \ldots, g_r$)

Input: C, an element of S,
f, a polynomial in $R[x]$ with ${f^P} \neq 0$, where $P := Rep(C)$.
Output: $g_1, \ldots, g_r$, 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 $i \in \{1, \ldots, r\}$ and there exists a q in R with

$$q^P \cdot f^P = \prod_{i=1}^{r} {g_i}^P.$$

We have assumed that for a given $C \in S$ we can algorithmically decide for every $f \in R$ whether $f \in Rep(C)$. Hence, using pseudodivision we can easily construct an algorithm that satisfies the following specification.

gcd (in: C, F; out: g)

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 $Ideal(P \cup F)$ 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 $P := Rep(C)$.

Using these algorithms we construct **primedec**$_{R[x]}$:

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

It remains to show that this algorithm terminates and satisfies the following specification.

primedec$_{R[x]}$ (in: F; out: O)

Input: F, a finite subset of $R[x]$.
Output: $O = \{C_1, \ldots, C_r\}$, a subset of $\bar{S}$ with

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

Proof of termination of primedec$_{R[x]}$: Let F satisfy the input specification and let $C \in M$. If $f^{Rep(C)} = 0$ for every $f \in F$ then termination is obvious. Otherwise, it follows from the specification of **factor** that for every $i \in \{1, \ldots, r\}$ the leading coefficient of g_i is not in $Rep(C)$ and therefore not in $Ideal(F \cap R)$. Since R is noetherian **primedec**$_{R[x]}$ terminates. □

The correctness of the algorithm is based on the following decomposition mechanism. Let $L \subseteq R[x]$ be multiplicatively closed and I an ideal in $R[x]$. We define

$$I_L := \{g \in R[x] \mid f \cdot g \in I \text{ for some } f \in L\}.$$

It is easy to see that I_L is an ideal (van der Waerden, 1967, p. 139).

Lemma 2.2. *Let f be an element of $R[x]$, L the set $\{f^m \mid m$ a natural number$\}$ and I an ideal in $R[x]$. Then*

$$Radical(I) = Radical(I_L) \cap Radical(I \cup \{f\}).$$

Proof. Obviously,

$$Radical(I) \subseteq Radical(I_L) \cap Radical(I \cup \{f\}).$$

Let $g \in I_L \cap Ideal(I \cup \{f\})$. Then there exists a natural number m such that $f^m \cdot g \in I$ and an $h \in R[x]$ with $g - h \cdot f \in I$. Hence, $f^{m-1} \cdot g^2 - h \cdot f^m \cdot g \in I$ and therefore $f^{m-1} \cdot g^2 \in I$. In this way we obtain $g^{m+1} \in I$. Thus, $I_L \cap Ideal(I \cup \{f\}) \subseteq Radical(I)$. By Theorem 9 in (Zariski and Samuel, 1975, p. 147),

$$Radical(I) \supseteq Radical(I_L) \cap Radical(I \cup \{f\}). \quad \square$$

Lemma 2.3. *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*

$$Ideal(P \cup \{f\})_L = \overline{Rep}(C \cup \{f\}),$$

where $L := \{lc(f)^m \mid m$ a natural number$\}$.

Proof. Let $g \in R[x]$. If $g \in Ideal(P \cup \{f\})_L$ then f^P divides g^P in $K(P)[x]$ and therefore $g \in \overline{Rep}(C \cup \{f\})$. On the other hand, if $g \in \overline{Rep}(C \cup \{f\})$ then $h^P = 0$, where h denotes the pseudoremainder of g and f. Thus, $g \in Ideal(P \cup \{f\})_L$. □

Proof of correctness of primedec$_{R[x]}$: Let F satisfy the input specification. We will show correctness by induction.

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

Induction step: $Ideal(F \cap R) \neq R$. It follows from the specifications of **gcd** and **factor**, the definition of $\overline{Rep}$ and the induction hypothesis that

$$Radical(F) \subseteq \bigcap_{A \in O} \overline{Rep}(A).$$

It remains to show that for every prime ideal P with $Radical(F) \subseteq P$

$$\text{there exists an } A \in O \text{ with } \overline{Rep}(A) \subseteq P. \tag{2.2}$$

Obviously, there exists a $C \in M$ with $Rep(C) \subseteq P$. If $C \in O$ then (2.2) is obviously satisfied. Otherwise, there exists an $i \in \{1, \ldots, r\}$ with $g_i \in P$, where $g_1, \ldots, g_r := \mathbf{factor}(C, \mathbf{gcd}(C, F))$. By Lemma 2.2,

$$Radical(I) = Radical(I_L) \cap Radical(I \cup \{lc(g_i)\}),$$

where $I := Ideal(Rep(C) \cup \{g_i\})$ and $L := \{lc(g_i)^m \mid m \text{ a natural number}\}$. Therefore, by Lemma 2.3,

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

In the second case (2.2) follows from the induction hypothesis. □

3. Modifications

No implementation of $\mathbf{primedec}_{R[x]}$ has been made yet. Therefore, we know nothing about the practical applicability of this algorithm. In this context the following two problems are of importance. In general, $\mathbf{primedec}_{R[x]}$ does not compute a reduced prime decomposition of a given radical.

Example: Let R be the univariate polynomial ring $\mathbf{Q}[y]$ over the rationals $\mathbf{Q}$ and S the set

$$\{\{f\} \subseteq R \mid f = 0 \text{ or } f \text{ is irreducible in } R\}.$$

We define the function Rep by $Rep(C) := Ideal(C)$ for every $C \in S$. For the input set $\{yx^2+x+y\} \subseteq R[x]$ the following prime decomposition of the prime ideal $Radical(\{yx^2+x+y\})$ is computed by $\mathbf{primedec}_{R[x]}$:

$$Radical(\{yx^2 + x + y\}) = \overline{Rep}(\{yx^2 + x + y\}) \cap \overline{Rep}(\{y, x\}).$$

Obviously, the second component is superfluous.

From a computational point of view the development of variants of $\mathbf{primedec}_{R[x]}$ which compute as few superfluous components as possible is an important problem.

The algorithm $\mathbf{primedec}_{R[x]}$ is a recursive algorithm. It terminates because $Ideal(F_1 \cap R)$ is a proper subset of $Ideal(F_2 \cap R)$, where F_1 and F_2 are input sets of successive calls of $\mathbf{primedec}_{R[x]}$. Therefore, if F and G are finite subsets of $R[x]$ with

$$Radical(F) = Radical(G) \text{ but } Radical(F \cap R) \subset Radical(G \cap R)$$

then in general $\mathbf{primedec}_{R[x]}$ terminates faster with input G than with input F. Hence, the question arises whether the performance of $\mathbf{primedec}_{R[x]}$ can be improved by using an elimination method for preprocessing. For instance, if R is a polynomial ring

over a field we could compute $\mathbf{primedec}_{R[x]}(F \cup C)$ or $\mathbf{primedec}_{R[x]}(B)$ instead of $\mathbf{primedec}_{R[x]}(F)$, where C is a characteristic set of F (Wu, 1984) and B is a Gröbner basis of F with respect to a lexicographical ordering with x as the highest variable. If characteristic sets are used for preprocessing $\mathbf{primedec}_{R[x]}$ becomes very similar to the prime decomposition algorithm of Ritt and Wu (Wu, 1984).

Another algorithm based on a similar strategy can be found in Kalkbrener (1993). Instead of assuming that every radical in R can be decomposed into prime ideals consider rings which satisfy the following weaker condition:

There exist a set S of finite subsets of R, a function *Rep* from S to the set of radicals in R, an algorithm **decompose** that computes for a finite subset F of R elements $C_1, \ldots, C_r$ of S such that

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

and an algorithm **split** that computes for a given $A \in S$ and $f \in R$ elements $B_1, \ldots, B_r$, $C_1, \ldots, C_s$ of S with the properties

$$Rep(A) = \bigcap_{i=1}^{r} Rep(B_i) \cap \bigcap_{i=1}^{s} Rep(C_i)$$

and

$$f \in Rep(B_i) \text{ for } i = 1, \ldots, r \quad \text{and} \quad Rep(C_i) : f = Rep(C_i) \text{ for } i = 1, \ldots, s.$$

It is proved in Kalkbrener (1993) that multivariate polynomial rings over explicitly given fields satisfy the above condition. Furthermore, it is shown that the set S can be constructed in such a way that $Rep(C)$ is equidimensional for every $C \in S$ and therefore **decompose** computes equidimensional decompositions of radicals. The decomposition algorithm in Kalkbrener (1993) is similar to $\mathbf{primedec}_{R[x]}$. The main difference is that radicals are decomposed using algorithm **split** instead of factorization. A generalization of the results in Kalkbrener (1993) to multivariate polynomial rings over noetherian commutative rings with identity will be presented in a forthcoming paper.

The complexity of computing characteristic sets has been analyzed by Gallo and Mishra (1990). But we do not know the complexity of the prime decomposition algorithm of Ritt and Wu or the complexity of the method presented in this paper. We think that a complexity analysis of algorithms of this type and a comparison with the results in Chistov and Grigor'ev (1983) and Giusti and Heintz (1990) are challenging problems for future research.

Acknowledgement: I want to thank both referees for their detailed and helpful comments on an earlier version of this paper.

References

Ayoub, C.W. (1982). The decomposition theorem for ideals in polynomial rings over a domain. *J. Algebra* **76**, 99–110.

Chistov, A.L., Grigor'ev, D.Y. (1983). Subexponential-time solving systems of algebraic equations I, II. Technical Report LOMI Preprints E-9-83 and E-10-83, Steklov Math. Institute, Leningrad, USSR.

Eisenbud, D., Huneke, C., Vasconcelos, W. (1992). Direct methods for primary decomposition. *Inventiones Mathematicae* **110**, 207–235.

Gallo, G., Mishra, B. (1990). Efficient algorithms and bounds for Wu-Ritt characteristic sets. In *Proc. MEGA'90*, pp. 119–142.
Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comp.* **6**, 149–168.
Giusti, M., Heintz, J. (1990). Algorithmes – disons rapides – pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles. In *Proc. MEGA'90*, pp. 169–194.
Kalkbrener, M. (1993). A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *J. Symb. Comp.* **15**, 143-167.
Kredel, H. (1987). Primary ideal decomposition. In *Proc. EUROCAL'87*, pp. 270–281, Leipzig, Germany.
Lazard, D. (1985). Ideal bases and primary decomposition: Case of two variables. *J. Symb. Comp.* **1**, 261–270.
Lazard, D. (1991). A new method for solving algebraic systems of positive dimension. *Discrete Applied Math.* **33**, 147–160.
Ritt, J.F. (1950). *Differential Algebra*. Volume 33, AMS Colloquium Publications, New York.
Seidenberg, A. (1974). Constructions in algebra. *Trans. AMS* **197**, 273–313.
Seidenberg, A. (1978). Constructions in a polynomial ring over the ring of integers. *Amer. J. Math.* **100**, 685–703.
Seidenberg, A. (1984). On the Lasker-Noether decomposition theorem. *Amer. J. Math.* **106**, 611–638.
van der Waerden, B.L. (1967). *Algebra II* (in German). Springer, Berlin Heidelberg New York, 5. edition.
Wang, D. (1993). An elimination method for polynomial systems. *J. Symb. Comp.* **16**, 83–114.
Wu, W. (1984). Basic principles of mechanical theorem proving in elementary geometries. *J. Sys. Sci. and Math. Scis* **4**, 207–235.
Zariski, O., Samuel, P. (1975). *Commutative Algebra I*. Volume 28 of *Graduate Texts in Mathematics*, Springer-Verlag Heidelberg.