J. Symbolic Computation (2002) **34**, 451–459
doi:10.1006/jsco.2002.0571
Available online at http://www.idealibrary.com on IDEAL®

Computing the Primary Decomposition of Zero-dimensional Ideals

CHRIS MONICO†

Department of Mathematics, University of Notre Dame, Notre Dame, IN 46556-4618, U.S.A.

Let $\mathbb{K}$ be an infinite perfect computable field and let $I \subseteq \mathbb{K}[\underline{x}]$ be a zero-dimensional ideal represented by a Gröbner basis. We derive a new algorithm for computing the reduced primary decomposition of I using only standard linear algebra and univariate polynomial factorization techniques. In practice, the algorithm generally works in finite fields of large characteristic as well.

1. Introduction

By now there are several known algorithms for computing the primary decomposition of an ideal. We would like to mention the papers by Eisenbud *et al.* (1992) and by Gianni *et al.* (1988). The algorithms in these papers reduce the general problem of primary decomposition to primary decomposition of zero-dimensional ideals.

In this paper we present what we believe is a new algorithm for computing the primary decomposition of a zero-dimensional ideal. After presenting the algorithm, we will see that it has complexity which is relatively easy to determine as it requires no intermediate Gröbner basis computations nor an expensive "normal position" computation as in Becker and Weispfenning (1993). Finally, we give some timings which indicate that this algorithm, while relatively easy to implement, is only of practical interest if the vectorspace dimension of the quotient ring is small.

We now give the notations and conventions which will be used in this paper. Let $\mathbb{K}$ be a perfect field which admits efficient operations and factorization of polynomials in $\mathbb{K}[t]$. Computationally, we are considering the rationals $\mathbb{Q}$ and the Galois field $\mathbb{F}_q$ with q elements. Let $S = \mathbb{K}[x_1, \ldots, x_s]$ and let $I \subseteq S$ be a zero-dimensional ideal. Set $R := S/I$ and $n := \dim_{\mathbb{K}} R$. For $r \in R$,

$$\begin{aligned} m_r : R &\longrightarrow R \\ x &\longmapsto rx \end{aligned}$$

is the vector space endomorphism induced by multiplication by r.

The motivation for our algorithm is that if $I = Q_1 \cap \cdots \cap Q_c$ is a reduced primary decomposition then $Q_i = \langle I, u_i \rangle$ for some $u_i \in S$. In particular, our goal is to find $u_i \in Q_i$ such that $u_i(z) \neq 0$ for all $z \in \mathcal{V}(I) \setminus \mathcal{V}(Q_i)$, which will give the desired result. The method of finding such u_i is based on the observation that there is an intimate relationship between the primary components of I and the invariant factors of m_r.

†E-mail: cmonico@nd.edu

0747–7171/02/050451 + 09 $35.00/0

This relationship of m_r with the primary components of I has been studied, in the case where $\mathbb{K}$ is algebraically closed in Cox *et al.* (1998, Chapter 4.2).

When considering R as a $\mathbb{K}$-vector space we will always assume some fixed ordering of the standard monomials as a basis. M_r is the matrix associated with m_r with respect to this fixed basis and $p_r(t) \in \mathbb{K}[t]$ is the characteristic polynomial of M_r. We also call $p_r(t)$ the *characteristic polynomial of* r since it is independent of the choice of basis we made to get M_r. For $r \in R$ we will let $\tilde{r}$ denote a lift of r to S. For any ring T, T^* will denote the invertible elements.

If $I \subseteq S$ is an ideal and $f \in S$, we also use the standard notation $\langle I, f\rangle$ to denote the ideal $I + \langle f\rangle$.

When we refer to the variety $\mathcal{V}(I)$ of an ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_s]$, we are considering it as a subset of the algebraic closure, $\mathcal{V}(I) \subseteq \overline{\mathbb{K}}^s$, since $\mathbb{K}$ is not assumed algebraically closed.

In addition, we rely heavily on standard results about the decomposition of a linear transformation. For background, the reader is referred to Hungerford (1980) .

Let $\mathbb{K}(u) \supseteq \mathbb{K}$ be a finite dimensional algebraic extension and $\alpha, \beta \in \mathbb{K}(u)$. Recall that α and β are said to be *conjugates* of each other if there exists a monic irreducible polynomial $f(t) \in \mathbb{K}[t]$ such that $f(\alpha) = f(\beta) = 0$. Elements α and β are conjugates if and only if $\alpha = \sigma(\beta)$ for some $\sigma \in \mathrm{Aut}_{\mathbb{K}}\mathbb{K}(u)$.

REMARK 1.1. $p_r(r) = 0$ by the Cayley–Hamilton theorem, and, in particular, $p_{x_i}(x_i) \in I$. One may thus use this characteristic polynomial to find a univariate polynomial in I.

2. Decomposition of m_r

Suppose $I = Q_1 \cap \cdots \cap Q_c$ is a reduced primary decomposition of I. Set $R_i := S/Q_i$ and $n_i := \dim_{\mathbb{K}} R_i$ and consider the isomorphism

$$\begin{aligned} \delta : R &\longrightarrow R_1 \times \cdots \times R_c \\ s + I &\longmapsto (s + Q_1, \ldots, s + Q_c). \end{aligned}$$

Since each R_i is an n_i-dimensional $\mathbb{K}$-vector space, let $\mathcal{B}_i = \{e_{i1}, \ldots, e_{in_i}\}$ denote a basis. Then

$$\mathcal{B} = \bigcup_{i=1}^{c} \{(0_{R_1}, \ldots, 0_{R_{i-1}}, x, 0_{R_{i+1}}, \ldots, 0_{R_c}) | x \in \mathcal{B}_i\}$$

is a basis for $R_1 \times \cdots \times R_c$ as a $\mathbb{K}$-vector space. Since δ is an isomorphism, there exists a change of basis matrix $C \in \mathrm{GL}_n(\mathbb{K})$ to go from the standard monomial basis to $\mathcal{B}$. That is, if M is the matrix representation of an endomorphism of R relative to the standard monomial basis, CMC^{-1} is the matrix representing the same endomorphism with respect to $\mathcal{B}$.

For $r \in R$, $m_r \in \mathrm{End}(R)$ and $m'_r := \delta m_r \delta^{-1} \in \mathrm{End}(R_1 \times \cdots \times R_c)$. Furthermore, notice that m'_r is given by

$$\begin{aligned} m'_r : R_1 \times \cdots \times R_c &\longrightarrow R_1 \times \cdots \times R_c \\ (s_1 + Q_1, \ldots, s_c + Q_c) &\longmapsto (s_1\tilde{r} + Q_1, \ldots, s_c\tilde{r} + Q_c), \end{aligned}$$

where $\tilde{r}$ is a lift of r to S. In particular, for any $(0, \ldots, 0, s_i + Q_i, 0, \ldots, 0) \in R_1 \times \cdots \times R_c$, and $r \in R$ one has that

$$m'_r(0, \ldots, 0, s_i + Q_i, 0, \ldots, 0) = (0, \ldots, 0, s_i\tilde{r} + Q_i, 0, \ldots, 0),$$

whence R_i is an m'_r-invariant subspace. Thus if $M'_{i,r}$ is the matrix of $m'_r|_{R_i}$ relative to some fixed basis, there exists a basis of R relative to which m'_r has the matrix

$$M'_r = \begin{pmatrix} M'_{1,r} & & & \\ & M'_{2,r} & & 0 \\ & & \ddots & \\ & 0 & & \\ & & & M'_{c,r} \end{pmatrix}.$$

For a proof of this last fact, see, e.g. Hungerford (1980, Lemma VII 4.5). Let $p_{i,r}(t) \in \mathbb{K}[t]$ be the characteristic polynomial of $M'_{i,r}$ and $p_r(t) \in \mathbb{K}[t]$ the characteristic polynomial of M'_r. One then has

$$p_r(t) = \prod_{i=1}^{c} p_{i,r}(t).$$

Since similar matrices have the same characteristic polynomial, $p_r(t)$ is also the characteristic polynomial of M_r, hence of r as well. In particular, $p_r(t)$ has at least one irreducible factor for each primary component. We thus have the following lemma for an upper bound on the number of primary components of I:

LEMMA 2.1. *Let R be as above and $r \in R$. Suppose that $p_r(t) = f_1(t)^{j_1} \cdots f_m(t)^{j_m}$ with the f_i irreducible. Then the number of distinct primary ideals in a reduced primary decomposition of I is at most $\sum_{i=1}^{m} j_i$.*

Now, if $r_1, r_2 \in R$ with $\tilde{r}_1 + Q_i = \tilde{r}_2 + Q_i$, one has $\tilde{r}_1 - \tilde{r}_2 \in Q_i$. Whence,

$$\begin{aligned} m'_{r_1}(0, \ldots, 0, s + Q_i, 0, \ldots, 0) &= (0, \ldots, 0, s\tilde{r}_1 + Q_i, 0, \ldots, 0) \\ &= (0, \ldots, 0, s\tilde{r}_1 - s(\tilde{r}_1 - \tilde{r}_2) + Q_i, 0, \ldots, 0) \\ &= (0, \ldots, 0, s\tilde{r}_2 + Q_i, 0, \ldots, 0) \\ &= m'_{r_2}(0, \ldots, 0, s + Q_i, 0, \ldots, 0). \end{aligned}$$

So, to study $m'_r|_{R_i}$, it suffices to study the linear transformations m_r in the case where I is primary.

PROPOSITION 2.2. *Let $r \in (S/Q)^*$ with Q primary. Then $p_r(t) = f(t)^i$ for some irreducible $f \in \mathbb{K}[t]$.*

PROOF. Since S/Q is a local ring (of finite dimension over K), for any of its elements r, the subring $K[r]$ must be local since S/Q is integral over it. Now $K[r] \cong K[t]/\langle g(t) \rangle$, where g is the minimal polynomial of r. Since $g(t)$ is a power of an irreducible polynomial and it shares all the irreducible factors of $p_r(t)$, the latter must be the power of an irreducible polynomial. □

Suppose $I = Q_1 \cap \cdots \cap Q_c$ is a reduced primary decomposition as before and $R_i := S/Q_i$. Let

$$\begin{aligned} \pi_i : \quad R &\longrightarrow R_i \\ s + I &\longmapsto s + Q_i. \end{aligned}$$

Let $r \in R^*$ and $p_{i,r}(t)$ be the characteristic polynomial of $\pi_i(r) \in R_i$. We then have

$$p_r(t) = \prod_{i=1}^{c} p_{i,r}(t).$$

Observe that if the $p_{i,r}(t)$ are known, a simple application of the Chinese remainder theorem yields the following result.

PROPOSITION 2.3. *Let I, Q_i and $p_{i,r}(t)$ all be as above, and fix $i \in \{1, 2, \ldots, c\}$. Then*

1. $I = \langle I, p_{1,r}(\tilde{r})\rangle \cap \cdots \cap \langle I, p_{c,r}(\tilde{r})\rangle$.
2. *If $(p_{i,r}(t), p_{j,r}(t)) = 1$ for all $j \neq i$ then $Q_i = \langle I, p_{i,r}(\tilde{r})\rangle$.*

3. The Primary Decomposition Algorithm

We first show that the condition

$$(p_{i,r}(t), p_{j,r}(t)) = 1 \qquad \text{for all } i \neq j \tag{1}$$

is satisfied when $r \in R$ is a generic element. We will then give the algorithm.

LEMMA 3.1. *Suppose $(p_{i,r}(t), p_{j,r}(t)) \neq 1$ for some fixed i and j with $i \neq j$. If $\tilde{r}$ is a lift of r to S, $\tilde{r}(y)$ is a conjugate of $\tilde{r}(z)$ for all $y \in \mathcal{V}(Q_i), z \in \mathcal{V}(Q_j)$.*

PROOF. $(p_{i,r}(t), p_{j,r}(t)) \neq 1 \Rightarrow p_{i,r}(t) = f(t)^{m_i}$ and $p_{j,r}(t) = f(t)^{m_j}$ for some irreducible $f \in \mathbb{K}[t]$. Furthermore, since $p_{i,r}(\tilde{r}) \in Q_i$, we have $f(\tilde{r}) \in \mathrm{Rad}(Q_i)$, whence $f(\tilde{r})(y) = 0$ for all $y \in \mathcal{V}(Q_i)$. But then $f(\tilde{r})(y) = f(\tilde{r}(y)) = 0$. Similarly, $f(\tilde{r}(z)) = 0$ for all $z \in \mathcal{V}(Q_j)$. But since f is irreducible, $\tilde{r}(y)$ and $\tilde{r}(z)$ are conjugates of each other for all $y \in \mathcal{V}(Q_i), z \in \mathcal{V}(Q_j)$. □

LEMMA 3.2. (*Existence*) *Let c denote the number of primary components in a reduced primary decomposition of the zero-dimensional ideal I. If $|\mathbb{K}| > c$, there exists $r \in (S/I)^*$ such that $(p_{i,r}(t), p_{j,r}(t)) = 1$ for all $i \neq j$.*

PROOF. By the previous lemma, it suffices to show that there exists $r \in R^* = (S/I)^*$ such that $\tilde{r}(y)$ is not a conjugate of $\tilde{r}(z)$ for all $y \in \mathcal{V}(Q_i)$, $z \in \mathcal{V}(Q_j)$, $i \neq j$. For $1 \leq i \leq c$ there exists $r_i \in R$ such that $\tilde{r}_i(y) = 0$ for all $y \in \mathcal{V}(I) \setminus \mathcal{V}(Q_i)$ and $\tilde{r}_i(z) = 1$ for all $z \in \mathcal{V}(Q_i)$. By assumption, there exist non-zero elements, $a_1, \ldots, a_c \in \mathbb{K}$ that are pairwise distinct. Take $r = a_1 r_1 + \cdots a_c r_c$. Then evaluation of $\tilde{r}$ at any point in $\mathcal{V}(Q_i)$ is a_i. Furthermore, $\tilde{r}$ does not vanish on any point of $\mathcal{V}(I)$, whence $r \in R^*$. □

THEOREM 3.3. *Assume $|\mathbb{K}| > c$ and let $I = Q_1 \cap \cdots \cap Q_c$ be a reduced primary decomposition. Suppose $1 \leq i < j \leq c$ and $r \in R$ is a generic element. Then for all $z_i \in \mathcal{V}(Q_i)$, $z_j \in \mathcal{V}(Q_j)$, $\tilde{r}(z_i)$ and $\tilde{r}(z_j)$ are not conjugates over $\mathbb{K}$.*

PROOF. Throughout, when we say "conjugates" we mean conjugates over $\mathbb{K}$. If $c = 1$, there is nothing to show, so assume $c \geq 2$. Let $n = \dim_{\mathbb{K}} R$. Then there exists a bijection between elements of R and points in $\mathbb{K}^n$. We wish to show that

$$\{r \in R | r(z_i), r(z_j) \text{ are conjugates for some } i \neq j\}$$

identifies with an algebraic set under this bijection. Since $\mathcal{V}(I)$ is finite, it suffices to show that for each fixed i, j with $i \neq j$, and $z_i \in Q_i$, $z_j \in Q_j$

$$\{r \in R | r(z_i), r(z_j) \text{ are conjugates}\}$$

is algebraic. (Then, the first set is a finite union of sets of this latter form). Since i, j are fixed, we will assume $i = 1, j = 2$.

Fix $z_1 \in \mathcal{V}(Q_1), z_2 \in \mathcal{V}(Q_2)$ and let $\mathbb{F} \supseteq \mathbb{K}$ be the smallest field extension such that $z_1, z_2 \in \mathbb{F}^s$. Let $e_1, \ldots, e_n$ be the standard monomials in R. Set

$$C := \{(a_1, \ldots, a_n) \in \mathbb{K}^n | a_1 e_1(z_1) + \cdots + a_n e_n(z_1) \text{ and } a_1 e_1(z_2) + \cdots + a_n e_n(z_1) \text{ are conjugates}\}.$$

We now must show that C is a proper algebraic subset of $\mathbb{K}^n$. First note that, by the previous existence lemma, $C \neq \mathbb{K}^n$. Let $c_i = e_i(z_1), d_i = e_i(z_2) \in \mathbb{F}$ and

$$f_1(x_1, \ldots, x_n) = c_1 x_1 + \cdots + c_n x_n \in \mathbb{F}[x_1, \ldots, x_n],$$
$$f_2(x_1, \ldots, x_n) = d_1 x_1 + \cdots + d_n x_n \in \mathbb{F}[x_1, \ldots, x_n].$$

Then $C = \{y \in \mathbb{K}^n | f_1(y), f_2(y) \text{ are conjugates}\}$. Recall that $f_1(y)$ and $f_2(y)$ are conjugates if and only if $f_1(y) = \sigma(f_2(y))$ for some $\sigma \in \mathrm{Aut}_{\mathbb{K}}\mathbb{F}$. Since $\mathbb{F} \supseteq \mathbb{K}$ is a finite dimensional extension, $\mathrm{Aut}_{\mathbb{K}}\mathbb{F}$ is finite and we may write $\mathrm{Aut}_{\mathbb{K}}\mathbb{F} = \{\sigma_1, \ldots, \sigma_m\}$ and set $C_i = \{y \in \mathbb{K}^n | f_1(y) = \sigma_i(f_2(y))\}$. Then $C = C_1 \cup \cdots \cup C_m$. Since σ_i is a field isomorphism, we have

$$\sigma_i(f_2(y)) = \sigma_i(d_1)\sigma_i(y_1) + \cdots \sigma_i(d_n)\sigma_i(y_n).$$

Thus, if we set $f_{2,i}(x_1, \ldots, x_n) = \sigma_i(d_1)x_1 + \cdots \sigma_i(d_n)x_n$, we obtain

$$\sigma_i(f_2(y)) = f_{2,i}(\sigma_i(y_1), \ldots, \sigma_i(y_n)).$$

But since $\sigma_i \in \mathrm{Aut}_{\mathbb{K}}\mathbb{F}$ and $y_j \in \mathbb{K}$, we have $\sigma_i(y_j) = y_j$, whence $\sigma_i(f_2(y)) = f_{2,i}(y)$ for all $y \in \mathbb{K}^n$. We thus need to show that $C_i = \{y \in \mathbb{K}^n | f_1(y) - f_{2,i}(y) = 0\}$ is an algebraic subset of $\mathbb{K}^n$. For this, first consider

$$\tilde{C}_i = \{y \in \mathbb{F}^n | f_1(y) - f_{2,i}(y) = 0\}.$$

This is an algebraic subset of $\mathbb{F}^n$, and $C_i = \tilde{C}_i \cap \mathbb{K}^n$. But $C = C_1 \cup \cdots \cup C_m \subset \mathbb{K}^n$ is a proper subset, and so $C_i \subset \mathbb{K}^n$ is a proper subset. Hence, C_i is an algebraic subset of $\mathbb{K}^n$, and thus C is an algebraic subset of $\mathbb{K}^n$. □

Remark 3.4. In the above theorem, we did not assume $\mathbb{K}$ to be infinite but the result is rather weak in the case where $\mathbb{K}$ is finite. However, it may be possible to prove some probability bounds in the finite case.

We now have our primary decomposition for the case where $\mathbb{K}$ is infinite:

Algorithm. **Z-D Primary Decomposition:**
Input: Gröbner basis for a zero-dimensional ideal, $I \subset \mathbb{K}[x_1, \ldots, x_n] = S$, with $\mathbb{K}$ infinite.
Output: Elements $r_1, \ldots, r_c \in R$ such that $\langle I, \tilde{r}_1 \rangle \cap \cdots \cap \langle I, \tilde{r}_c \rangle$ is a reduced primary decomposition of I.

1. Fix a basis, $\{e_1, \ldots, e_n\}$, consisting of the standard monomials of $R = S/I$.

2. Choose a random element, $r \in R$, and calculate $p_r(t)$. If $t \mid p_r(t)$, r is not invertible, so repeat until $t \nmid p_r(t)$. (The generic element is invertible, so this will not happen often).
3. Compute the factorization of $p_r(t) = f_1(t)^{d_1} \cdots f_c(t)^{d_c}$ into irreducible components with $(f_i, f_j) = 1$ for $i \neq j$.
4. Calculate $r_i = f_i(r)^{d_i}$ for $1 \leq i \leq c$, and output the r_i.

REMARK 3.5. Recall that for the output to be correct, r must satisfy condition (1). While we showed that the generic r does satisfy this, we have no way to certify a particular r as suitable. Insisting on an invertible r is simply to insure we have not "accidentally" chosen a degenerate case, but it is not sufficient to prove correctness of the output. If a particular r is chosen that does not satisfy condition (1), the intersection of the output ideals will still equal the input ideal, but may not be a complete primary decomposition. In practice, this rarely seems to happen (i.e. it did not happen during any of the computations in Section 5).

REMARK 3.6. In step 4, $f_i(r)^{d_i} \in R$ should not be computed in the naive way (i.e. first computing $f_i(\tilde{r})^{d_i} \in S$, then reducing modulo I) since the number of terms will grow exponentially. Instead observe that the desired value lies in S/I, so one may use consecutive squaring reducing all intermediate results modulo I. Equivalently, one may compute a normal form of $f_i(T)^{d_i}$ with respect to the ideal $\langle T - r, I\rangle$ where T is a new variable with $T \gg$ the original variables.

4. Examples

At this point, we present the reader with two simple examples that can be easily verified by hand.

EXAMPLE 4.1. Consider $I = \langle x^2 - 2, y^2 - 2\rangle \subset \mathbb{Q}[x, y] = S$. S/I is a four-dimensional $\mathbb{Q}$-vector space with a basis given by the standard monomials $\{1, x, y, xy\}$. Let $r = 1 + x + y$, and we get the matrix representation of r, relative to this basis:

$$M_r = \begin{pmatrix} 1 & 2 & 2 & 0 \\ 1 & 1 & 0 & 2 \\ 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

which has characteristic polynomial

$$p_r(t) = (t^2 - 2t - 7)(t - 1)^2.$$

Taking $p_{1,r}(t) = (t^2 - 2t - 7)$ and $p_{2,r}(t) = (t - 1)^2$, we get

$$I = \langle I, p_{1,r}(r)\rangle \cap \langle I, p_{2,r}(r)\rangle = \langle x^2 - 2, y^2 - 2, xy - 2\rangle \cap \langle x^2 - 2, y^2 - 2, xy + 2\rangle.$$

EXAMPLE 4.2. Let $I = \langle x^2 + y + 1, 2xy + y\rangle$. A Gröbner basis for I is given by $I = \langle x^2 + y + 1, 4y^2 + 5y, 2xy + y\rangle$. Let $r = 1 + x + 2y$ and we get:

$$M_r = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 2 & -2 & -2 \end{pmatrix}$$

and characteristic polynomial

$$p_r(t) = (t+2)(t^2 - 2t + 2)$$

which gives primary components:

$$Q_1 = \langle I, 3 + x + 2y \rangle$$
$$Q_2 = \langle I, -8y \rangle.$$

Notice the complexity of these computations: given a Gröbner basis for I, computing a basis for S/I has complexity $O(n)$. Computing the matrix M_r, requires $O(n^3)$ field operations in the worst case. Computing the characteristic polynomial, $p_r(t)$, can be done using Hessenberg's algorithm, which requires $O(n^3)$ field operations. The time required to factor $p_r(t)$ is a complicated issue that we do not wish to get into in detail here except to mention that:

- Lenstra, Lenstra and Lovász (Lenstra *et al.*, 1982) have shown that polynomials in $\mathbb{Q}[t]$ can be factored with a deterministic polynomial time algorithm.
- If one assumes the generalized Riemann hypothesis (GRH), polynomials in $\mathbb{F}_p[t]$ can be factored with a deterministic polynomial time algorithm (Cohen, 1993). Not assuming GRH, factorization of such polynomials still seems to be very efficient in practice.

5. Timings

The algorithm described in this paper has been implemented in the primary decomposition library (Pfister *et al.*, 2002) of recent releases of SINGULAR (Greuel *et al.*, 2002). We obtained timings for the primary decomposition of seven ideals, using SINGULAR 2.0.3 for Windows on a 400 MHz Pentium II. Each primary decomposition was computed five times using the algorithm in this paper ("zerodec" in Pfister *et al.* (2002)) and five times using the algorithm of Gianni *et al.* (1988) ("primdecGTZ" in Pfister *et al.* (2002)), and the average timings are reported here. The net result seems to be that this algorithm is competitive with the general purpose algorithm in Gianni *et al.* (1988) when the vectorspace dimension of the quotient ring is small. However as the dimension grows, "primdecGTZ" drastically outperforms "zerodec". The dominant reason seems to be the amount of time required to compute the characteristic polynomial $p_r(t)$, which grows quickly ($O(d^3)$) with respect to the dimension, if the field is finite. The situation is even worse over $\mathbb{Q}$ since coefficient explosion also occurs. The first five ideals are the zero-dimensional examples from Pfister *et al.* (1999), and the last two were constructed to illustrate the effect of larger dimension. For consistency with the results there, all computations were performed over the field $\mathbb{F}_{32003}$ using the degree reverse lexicographical ordering. The "dimension" column gives the vectorspace dimension of the quotient ring. The "components" column gives the number of primary components in the primary decomposition. The last two columns give the timings of the corresponding SINGULAR library functions, as reported by the "rtime" value of the software.

1. Over $\mathbb{F}_{32003}[x, y, z]$:
   $x^2yz + xy^2z + xyz^2 + xyz + xy + xz + yz$, $x^2y^2z + xy^2z^2 + x^2yz + xyz + yz + x + z$,
   $x^2y^2z^2 + x^2y^2z + xy^2z + xyz + xz + z + 1$.

2. Over $\mathbb{F}_{32003}[a,b,c,d,e,f,g,h,k,o]$:
$o+1,\ k^4+k,\ hk,\ h^4+h,\ gk,\ gh,\ g^3+h^3+k^3+1,\ fk,\ f^4+f,\ eh,\ ef,$
$f^3h^3+e^3k^3+e^3+f^3+h^3+k^3+1,\ e^3g+f^3g+g,\ e^4+e,\ dh^3+dk^3+d,\ dg,$
$df,\ de,\ d^3+e^3+f^3+1,\ e^2g^2+d^2h^2+c,\ f^2g^2+d^2k^2+b,\ f^2h^2+e^2k^2+a.$

3. Over $\mathbb{F}_{32003}[x,y,z,t]$:
$y^2z+2xyt-2x-z,\ -x^3z+4xy^2z+4x^2yt+2y^3t+4x^2-10y^2+4xz-10yt+2,$
$2yzt+xt^2-x-2z,\ -xz^3+4yz^2t+4xzt^2+2yt^3+4xz+4z^2-10yt-10t^2+2.$

4. Over $\mathbb{F}_{32003}[a,b,c,d,e,f]$:
$a^2+d^2+2ce+2bf+a,\ 2ab+2de+2cf+b,\ b^2+2ac+e^2+2df+c,\ 2bc+2ad+2ef+d,$
$c^2+2bd+2ae+f^2+e,\ 2cd+2be+2af+f.$

5. Over $\mathbb{F}_{32003}[a,b,c,d,e]$:
$a+b+c+d+e,\ ab+bc+cd+de+ae,\ abc+bcd+abe+ade+cde,$
$abcd+abce+abde+acde+bcde,\ abcde-1.$

6. Over $\mathbb{F}_{32003}[u,v,w,x,y,z]$:
$u^3+vx^2+1,\ v^2+3yz+xw,\ w^2-3vz+y^2,\ x^2+xy-xz,\ y^3-1,\ z^2+u.$

7. Over $\mathbb{F}_{32003}[t,u,v,w,x,y,z]$:
$u^2+vx,\ v^2+3yz+1,\ w^2-3v+1,\ x^2+xy-xz,\ y^3-1,\ z^2+u,\ t^2-1.$

Ideal	Dimension	Components	primdecGTZ	zerodec
1	20	14	0.2	0.2
2	54	30	1.8	0.2
3	56	19	0.6	0.6
4	64	40	1.4	3.0
5	70	20	1.6	1.8
6	144	45	4.6	13.8
7	192	36	3.8	60.4

Acknowledgements

I would like to thank the anonymous referees for their valuable input which greatly improved the quality of this manuscript, as well as the SINGULAR group for taking the time to implement the algorithm described here. I was supported by a fellowship from the Center for Applied Mathematics at the University of Notre Dame. This work was also supported in part by NFS grant DMS-00-72383.

References

Becker, T., Weispfenning, V. (1993). *Gröbner Bases: A Computational Approach to Commutative Algebra*. New York, Springer.

Cohen, H. (1993). *A Course in Computational Algebraic Number Theory*. New York, Springer.

Cox, D., Little, J., O'Shea, D. (1998). *Using Algebraic Geometry*. New York, Springer.

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

Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comput.*, **6**, 149–167.

Greuel, G.-M., Pfister, G., Schönemann, H. (2002). SINGULAR 2.0.3. A computational algebra system for polynomial computations, Centre for Computer Algebra, University of Kaiserslautern, `http://www.singular.uni-kl.de`.

Hungerford, T. W. (1980). *Algebra*. New York, Springer.
Lenstra, H. W., Lenstra, A. K., Lovász, L. (1982). Factoring polynomials with rational coefficients. *Math. Ann.*, **261**, 515–534.
Pfister, G., Decker, W., Greuel, G. (1999). Primary decomposition: algorithms and comparisons. In Matzat, B., Greuel, G., Hiss, G. eds, *Algorithmic Algebra and Number Theory*, pp. 187–220. Berlin, Springer.
Pfister, G., Decker, W., Schönemann, H. (2002). `primdec.lib`. A SINGULAR 2.0.3 library for computing the primary decomposition and radical of ideals.

Received 8 May 2002
Accepted 6 August 2002