MATHEMATICS OF COMPUTATION
Volume 78, Number 265, January 2009, Pages 509–521
S 0025-5718(08)02115-7
Article electronically published on May 1, 2008

PRIMARY DECOMPOSITION OF ZERO-DIMENSIONAL IDEALS OVER FINITE FIELDS

SHUHONG GAO, DAQING WAN, AND MINGSHENG WANG

Abstract. A new algorithm is presented for computing primary decomposition of zero-dimensional ideals over finite fields. Like Berlekamp's algorithm for univariate polynomials, the new method is based on the invariant subspace of the Frobenius map acting on the quotient algebra. The dimension of the invariant subspace equals the number of primary components, and a basis of the invariant subspace yields a complete decomposition. Unlike previous approaches for decomposing multivariate polynomial systems, the new method does not need primality testing nor any generic projection, instead it reduces the general decomposition problem directly to root finding of univariate polynomials over the ground field. Also, it is shown how Gröbner basis structure can be used to get partial primary decomposition without any root finding.

1. Introduction

Let k be any field and I an ideal in the polynomial ring $k[x_1, \ldots, x_n]$. We are interested in computing a primary decomposition of I. Most approaches in the literature follow essentially two stages. In the first stage, the decomposition of I is reduced to the decomposition of a sequence of ideals that are zero-dimensional over rational function fields containing k. In the second stage, the decomposition of each zero-dimensional ideal is then reduced to factorization of (multivariate) polynomials. In the current paper, we are interested in the second stage, that is, developing a new algorithm for decomposition of zero-dimensional ideals.

We focus on the case when k has positive characteristic, say k contains a finite field $\mathbb{F}_q$. For fields with characteristic zero, one usually uses modular approaches that reduce the problem to fields of positive characteristic. In the following, k may be a finite field $\mathbb{F}_q$, or any finitely generated function field over $\mathbb{F}_q$, that is,

$$k \cong \mathbb{F}_q(t_1, \ldots, t_d)[y_1, \ldots, y_m]/J$$

where t_i's and y_i's are independent variables, $\mathbb{F}_q(t_1, \ldots, t_d)$ the rational function field with d variables over $\mathbb{F}_q$, and $J \subset \mathbb{F}_q(t_1, \ldots, t_d)[y_1, \ldots, y_m]$ a maximal ideal. Let $I \subset k[x_1, \ldots, x_n]$ be a zero-dimensional ideal. Then the current approaches use generic projection and reduce the decomposition of I to factorization of polynomials

Received by the editor December 1, 2006 and, in revised form, October 29, 2007.

2000 *Mathematics Subject Classification.* Primary 13P10, 68W30; Secondary 11Y16, 12Y05, 13P05.

Key words and phrases. Primary decomposition, primary ideals, quasi-primary ideals, Groebner bases, Frobenius map.

The work was done while the authors were visiting IMA at University of Minnesota in Fall 2006. Gao and Wan were supported in part by National Science Foundation (NSF), and Wang was partially supported by 973 Projects (2004CB318004) and NSFC (60573041).

in $k[t_1, \dots, t_d, z]$. It is well recognized that generic projections are expensive to compute and the polynomials from projections are usually "large" in certain sense. Hence the current implementations of primary decomposition in major computer algebra systems (including Maple, Magma, Macaulay 2, Singular, etc.) are quite slow even for small systems of polynomials. As remarked by Decker, Greuel and Pfister [5], finding an efficient algorithm for primary decomposition is a difficult task and still one of the big challenges for computational algebra and computational algebraic geometry. For more details of the current approaches in the literature, we refer the reader to the books [1, 14, 25] and the papers [22, 13, 7, 23, 12, 5, 21, 24, 27, 28, 29].

It is somewhat surprising to us that all the existing techniques for decomposing zero-dimensional ideals over finite fields so far do not generalize any of the known methods for factoring univariate polynomials over finite fields. It was pointed out in [26] that any formula for computing zeta functions over finite fields should be useful in decomposing the ideal. This naturally explains the three algorithms [26] for factoring univariate polynomials over finite fields: Berlekamp's algorithm [2] using the fixed points of the Frobenius map, Niederreiter's algorithm [18, 19] using solutions of certain differential equations (fixed points of Cartier's operator) and Wan's algorithm [26] using fixed points of Dwork's operator. It is thus very natural to try to extend each of the above three algorithms to the general multivariate case. In this paper, we extend Berlekamp's approach to zero-dimensional ideals over finite fields and explore some novel features resulting from the use of Gröbner basis. For higher dimensional ideals over finite fields, Berlekamp's approach does not seem to generalize, as there is no corresponding known formula for computing the zeta function of higher dimensional ideal using the Frobenius map (which only works for zero-dimensional ideals). However, we expect that the other two approaches (Niederreiter's approach and Wan's approach) should generalize to higher dimensional cases, since there are corresponding formulas for zeta functions in the higher dimensional cases.

Thus, our new method in this paper does not require any generic projection. Like Berlekamp's algorithm, the new method is based on the invariant subspace of the Frobenius map acting on the quotient algebra. The dimension of the invariant subspace equals the number of primary components, and a basis of the invariant subspace yields a complete decomposition. The method tells automatically whether a computed component is primary, hence no need for a separate procedure to test primality. Since our method needs no generic projection, it may take advantage of possible sparsity of polynomial systems especially when the systems have sparse Gröbner bases. We shall also show how Gröbner basis structure can be used to get Gröbner bases for primary components.

The paper is organized as follows. In Section 2, we present the basic theory that works for any field k containing a finite field. In Section 3, we show how to turn the theory into an algorithm when k is a finite field. A detailed example is presented to demonstrate the ideas. Finally, we make a few comments, especially on what needs to be done when k is a finitely generated rational function field.

2. Theory

In this section, we assume that k is any field containing $\mathbb{F}_q$. For basic notions in commutative algebra, especially on primary decomposition, we refer the reader to the books [1, 4, 6, 14].

An ideal $I \subset k[x_1, \dots, x_n]$ is called *quasi-primary* if $\sqrt{I}$ is a prime ideal, that is, if I has only one minimal component and all other components are embedded. For example, $I = \langle x^2, xy \rangle \subset k[x, y]$ is quasi-primary but not primary. In fact, $\sqrt{I} = \langle x \rangle$ and I has the primary decomposition

$$I = \langle x \rangle \cap \langle x^2, y \rangle = \langle x \rangle \cap \langle x^2, xy, y^m \rangle$$

where $m \geq 1$ and the second component is embedded on the first one. Our method is based on the following key lemma.

Lemma 2.1. *Let k be any field containing $\mathbb{F}_q$ as a subfield, and $Q \subset k[x_1, \dots, x_n]$ a quasi-primary ideal. Then, for any $g \in k[x_1, \dots, x_n]$,*

$$g^q \equiv g \pmod{Q} \tag{1}$$

iff there exists $\alpha \in \mathbb{F}_q$ such that

$$g \equiv \alpha \pmod{Q}. \tag{2}$$

Proof. Clearly, (2) implies (1). Assume (1) holds. Then

$$g^q - g \equiv \prod_{\alpha \in \mathbb{F}_q} (g - \alpha) \pmod{Q}.$$

That is, $\prod_{\alpha \in \mathbb{F}_q} (g - \alpha) \in Q \subseteq \sqrt{Q}$. Since $\sqrt{Q}$ is a prime ideal, there exists $\alpha \in \mathbb{F}_q$ such that $g - \alpha \in \sqrt{Q}$. Hence $(g - \alpha)^m \in Q$ for some integer m. Let $g_1 = g - \alpha$. Then $g_1^q \equiv g_1 \pmod{Q}$ and $g_1^m \equiv 0 \pmod{Q}$. If $m \leq q$, then $g_1 \equiv g_1^q \equiv 0 \pmod{Q}$, so (2) is satisfied. Suppose $m > q$. Write $m = qu + v$ where $0 \leq v < q$ and $u \geq 1$. Then

$$g_1^m \equiv (g_1^q)^u \cdot g_1^v \equiv g_1^u \cdot g_1^v = g_1^{u+v} \pmod{Q}.$$

Hence $g_1^{u+v} \equiv 0 \pmod{Q}$ and $u + v < uq + v = m$. If $u + v > q$, we can repeat this process until we find an integer $m_1 \leq q$ so that $g_1^{m_1} \equiv 0 \pmod{Q}$. Therefore we have $g_1 \equiv 0 \pmod{Q}$ as required. □

Now consider an arbitrary ideal $I \subseteq k[x_1, \dots, x_n]$. Suppose I has an irredundant primary decomposition

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_r \tag{3}$$

where $Q_i \in k[x_1, \dots, x_n]$ are primary ideals. In general, the components Q_i are not unique, but the number r depends only on I, not on the specific decomposition. Our goal is to determine r and find an irredundant primary decomposition as in (3).

For $g \in k[x_1, \dots, x_n]$, consider the equation

$$g^q \equiv g \pmod{I}. \tag{4}$$

Let $R = k[x_1, \dots, x_n]/I$ and define

$$G = \{g \in R \mid g \text{ satisfies (4)}\}. \tag{5}$$

Then G is an $\mathbb{F}_q$-linear subspace of R.

We hope that the dimension of G over $\mathbb{F}_q$ is equal to r, the number of primary components of I. Unfortunately, this is not true in general. For example, let $I = \langle xy \rangle \subset k[x, y]$, generated by one polynomial. Then $I = \langle x \rangle \bigcap \langle y \rangle$ has two primary components. But (4) has only the trivial solutions $g = \alpha$, $\alpha \in \mathbb{F}_q$, modulo I.

In the following, we assume that I is a zero-dimensional ideal with an irredundant primary decomposition as in (3). We note that the Q_i's are zero-dimensional and are uniquely defined by I. Most importantly, the Q_i's are pairwise coprime, that is, for each pair $i \neq j$,

$$Q_i + Q_j = \langle 1 \rangle = k[x_1, \ldots, x_n].$$

By the Chinese remainder theorem, there exist $E_1, \ldots, E_r \in k[x_1, \ldots, x_n]$ such that

$$E_i \equiv \begin{cases} 1 \mod Q_i, \\ 0 \mod Q_j, \quad j \neq i. \end{cases} \tag{6}$$

These E_i's are unique mod I and are linearly independent over $\mathbb{F}_q$. For $\lambda_i \in \mathbb{F}_q$, $1 \leq i \leq r$, let

$$g = \sum_{i=1}^{r} \lambda_i E_i \in k[x_1, \ldots, x_n].$$

Then $g^q \equiv \lambda_i^q \equiv \lambda_i \equiv g \pmod{Q_i}$, that is, $g^q - g \in Q_i$ for $1 \leq i \leq r$. Hence $g^q - g \in I$ and g is a solution to (4).

Conversely, if $g \in k[x_1, \ldots, x_n]$ satisfies (4), then $g^q \equiv g \pmod{Q_i}, 1 \leq i \leq r$. By the lemma above, $g \equiv \alpha_i \pmod{Q_i}$ for some $\alpha_i \in \mathbb{F}_q$. This implies that $g \equiv \sum_{j=1}^{r} \alpha_j E_j \pmod{Q_i}$ for $1 \leq i \leq r$, hence $g \equiv \sum_{j=1}^{r} \alpha_j E_j \pmod{I}$. We have proved the following theorem.

Theorem 2.2. *Let k be any field containing $\mathbb{F}_q$. Suppose $I \subset k[x_1, \ldots, x_n]$ is a zero-dimensional ideal with r primary components. Then the space G in* (5) *has dimension r over $\mathbb{F}_q$. Furthermore, suppose I is decomposed as in* (3)*, and $E_i \in k[x_1, \ldots, x_n]$ satisfies* (6)*. Then every $g \in G$ is of the form*

$$g \equiv \sum_{i=1}^{r} \lambda_i E_i \pmod{I} \tag{7}$$

where $\lambda_i \in \mathbb{F}_q$ for $1 \leq i \leq r$.

A solution g is called trivial if $g \equiv \lambda \pmod{I}$ for some $\lambda \in \mathbb{F}_q$. Next, we show how to get a proper decomposition of I from any nontrivial solution g.

Theorem 2.3. *Let $g \in k[x_1, \ldots, x_n]$ be any solution of* (4)*. Then*

$$I = \bigcap_{\lambda \in \mathbb{F}_q} \langle I, g - \lambda \rangle. \tag{8}$$

Furthermore, assume g is of the form (7) *and I has a primary decomposition as in* (3)*. Then*

$$\langle I, g - \lambda \rangle = \bigcap_{1 \leq i \leq r, \lambda_i = \lambda} Q_i.$$

Hence $\langle I, g - \lambda \rangle \neq \langle 1 \rangle$ or I iff $\lambda = \lambda_i$ for at least one but not all i.

Proof. Note that, for $1 \le i \le r$, $g \equiv \lambda_i E_i \equiv \lambda_i \pmod{Q_i}$. We have

$$\langle Q_i, g - \lambda \rangle = \langle Q_i, \lambda_i - \lambda \rangle = \begin{cases} \langle 1 \rangle, & \text{if } \lambda_i \ne \lambda, \\ Q_i, & \text{if } \lambda_i = \lambda. \end{cases}$$

Since the Q_i's are pairwise coprime, we have

$$\langle I, g - \lambda \rangle = \bigcap_{i=1}^{r} \langle Q_i, g - \lambda \rangle = \bigcap_{1 \le i \le r, \lambda_i = \lambda} \langle Q_i, g - \lambda \rangle = \bigcap_{1 \le i \le r, \lambda_i = \lambda} Q_i.$$

This completes the proof. □

Remark. We should mention that the following equation, which we used above,

$$\langle Q_1 \cap Q_2 \cap \cdots \cap Q_r, J \rangle = \langle Q_1, J \rangle \cap \langle Q_2, J \rangle \cap \cdots \cap \langle Q_r, J \rangle$$

does not hold for general ideals $Q_1, \dots, Q_r$ and J, but is true whenever the Q_i's are pairwise coprime.

When q is small, (8) can be computed by plugging in each value $\lambda \in \mathbb{F}_q$. When q is large, we need a better method to find all the λ_i that appear in g. Traditionally, this is handled by computing the characteristic polynomial $h(z)$ of g as a linear operator on the quotient algebra R, or by computing the minimal polynomial $h(z)$ of $g \bmod I$, i.e., the polynomial $h(z) \in \mathbb{F}_q[x]$ of smallest degree so that $h(g) \equiv 0 \pmod{I}$. Then all the λ_i are the roots of $h(z)$. We shall see in the next section that $h(z)$ can be computed via Gröbner basis technique that simultaneously gives Gröbner bases for all the components $\langle I, g - \lambda \rangle$.

Next we show how to tell if $\langle I, g - \lambda \rangle$ is primary. If it is not primary, then we want to know how many components it has.

Theorem 2.4. *Let B be any linear basis of G over $\mathbb{F}_q$. For $g \in G$ and $\lambda \in \mathbb{F}_q$, set*

$$I_\lambda = \langle I, g - \lambda \rangle$$

and

$$B_\lambda = B \bmod I_\lambda,$$

which means that reducing every element of B by I_λ, and getting rid of linearly dependent elements. Then B_λ is a linear basis over $\mathbb{F}_q$ for the solution space of (5) *with I_λ in place of I. Particularly, $|B_\lambda|$ is equal to the number of primary components of I_λ.*

Proof. Suppose $B = \{g_1, \dots, g_r\}$. Express g_j in the form (7):

$$g_j \equiv \sum_{i=1}^{r} \lambda_{ij} E_i \pmod{I}$$

where $\lambda_{ij} \in \mathbb{F}_q, 1 \le i \le r$. In other words,

$$(g_1, \dots, g_r) = (E_1, \dots, E_r)\Lambda,$$

where $\Lambda = (\lambda_{ij})$ is an $r \times r$ matrix. Since both g_i's and E_i's are bases for G, Λ has rank r.

For $g \in G$, write g as in (7). For $\lambda \in \mathbb{F}_q$, let $i_1, \dots, i_t$ be all the i, $1 \le i \le r$, such that $\lambda_i = \lambda$. By the previous theorem, $I_\lambda = \bigcap_{j=1}^{t} Q_{i_j}$ has t primary components. Let

$$G_\lambda := \{g \in R_1 | g^q \equiv g \pmod{I_\lambda}\},$$

where $R_1 = k[x_1, \ldots, x_n]/I_\lambda$. By Theorem 2.2, $\dim_{\mathbb{F}_q} G_\lambda = t$. In fact, let $\Lambda_{i_1 \cdots i_t}$ be the submatrix of Λ consisting of the rows indexed by $i_1, \ldots, i_t$. Then

$$(g_1, \ldots, g_r) \equiv (E_{i_1}, \ldots, E_{i_t})\Lambda_{i_1 \ldots i_t} \pmod{I_\lambda}.$$

Note that $\Lambda_{i_1,\ldots,i_t}$ has rank t, and by Theorem 2.2 $E_{i_1}, \ldots, E_{i_t}$ form a basis for G_λ over $\mathbb{F}_q$. Hence we have that $g_1, \ldots, g_r \pmod{I_\lambda}$ contains a basis for I_λ. As B_λ is obtained from them by deleting the dependent ones, we see that $|B_\lambda| = t$, the number of primary components of I_λ. □

Berlekamp's algorithm [2] is the special case when I is generated by one polynomial in the univariate polynomial ring $\mathbb{F}_q[x]$. Suppose $f \in \mathbb{F}_q[x]$ with

$$f = f_1^{e_1} f_2^{e_2} \cdots f_r^{e_r}$$

where $f_1, f_2, \ldots, f_r \in \mathbb{F}_q[x]$ are distinct irreducible. Then the factorization of f above is equivalent to the primary decomposition

$$\langle f \rangle = \langle f_1^{e_1} \rangle \cap \langle f_2^{e_2} \rangle \cap \cdots \cap \langle f_r^{e_r} \rangle.$$

The two theorems above immediately yield Berlekamp's algorithm (note that f does not need to be squarefree).

3. Implementation and Gröbner bases

In this section we first assume that k is a finite field. At the end of the section, we make some comments about the case when k is infinite. To convert the theory of the previous section into an algorithm, we need an explicit representation of ideals and linear bases of quotient algebras. We do this via Gröbner basis theory. For an ideal $I \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ given by an arbitrary set of generators, it is NP-hard to compute a Gröbner basis for I (for any term order). For large systems of polynomials, computing Gröbner bases is most likely the bottleneck of our approach (which is true for almost all the algorithms in the literature). In the following, we assume that a Gröbner basis for I is already known or computed for some term order. This assumption is reasonable for several applications. For example, in a Pham system, I is generated by polynomials of the form $x_i^{d_i} + f_i$ where $f_i \in k[x_1, \ldots, x_n]$ has total degree $< d_i$ for $1 \le i \le n$, so they form a Gröbner basis under a graded order. Our aim is to compute a primary decomposition of I.

Assume I is a zero-dimensional ideal in $\mathbb{F}_q[x_1, \ldots, x_n]$. Then $R = \mathbb{F}_q[x_1, \ldots, x_n]/I$ is a finite dimensional vector space over $\mathbb{F}_q$. Suppose $I = \langle f_1, \ldots, f_m \rangle$ where $f_1, \ldots, f_m$ form a Gröbner basis for I (for some term order). By Gröbner basis theory, the following set of monomials form a linear basis for R over $\mathbb{F}_q$:

$$B = (X^\alpha | \alpha \in \mathbb{N}^n, \text{ and } X^\alpha \text{ is not divisible by any } \mathrm{LT}(f_i), 1 \le i \le m),$$

where $\mathrm{LT}(f)$ denotes the leading term of f (we emphasize that $\mathrm{LT}(f)$ is a monomial without the corresponding coefficient of f), and for $\alpha = (i_1, \cdots, i_n) \in \mathbb{N}^n$,

$$X^\alpha = x_1^{i_1} \cdots x_n^{i_n}.$$

Here and hereafter $X = x_1, \ldots, x_n$ represents the list of variables. We order B as a row vector

$$B = (X^{\alpha_1}, \ldots, X^{\alpha_d}),$$

where d is the dimension of $R = \mathbb{F}_q[x_1, \ldots, x_n]/I$ over $\mathbb{F}_q$. Note that with any linear basis for R, one can perform addition and multiplication in R.

Now we turn the congruence equation (4) into an explicit linear system over $\mathbb{F}_q$. For $1 \le j \le n$, compute

$$(X^{\alpha_j})^q \equiv \sum_{i=1}^{d} c_{ij} X^{\alpha_i} \pmod{I},$$

where $c_{ij} \in \mathbb{F}_q$. For large q, $X^{\alpha_j q} \bmod I$ can be computed by the square and multiply method. Hence each $X^{\alpha_j q} \bmod I$ can be computed using $\mathcal{O}(n \log q)$ multiplications in R. Let $C = (c_{ij})$ be a $d \times d$ matrix over $\mathbb{F}_q$. Then the above equation can be written as

$$B^q = B \cdot C. \tag{9}$$

An element $g \in R$ can be represented as

$$g = B(a_1, \ldots, a_d)^T$$

where $a_i \in \mathbb{F}_q$ are unknowns. Then

$$g^q = B^q(a_1, \ldots, a_d)^T \equiv B \cdot C(a_1, \ldots, a_d)^T \pmod{I}.$$

Hence $g^q \equiv g \pmod{I}$ if and only if

$$(C - I)(a_1, \ldots, a_d)^T = 0, \tag{10}$$

where I is the $d \times d$ identity matrix. The equation (10) is equivalent to (4). One can compute a linear basis for G using any fast algorithm for solving linear systems.

Next let $g \in G$ be any non-trivial element and suppose $g = \sum_{i=1}^{r} \lambda_i E_i$ as in (7). We need to show how to find these λ_i's. Define

$$h(z) = \Pi(z - \lambda_i),$$

where the product runs over all distinct values of λ_i's, so $h(z)$ is squarefree. The following theorem is a special case of the structure theorem of Gröbner bases in [11]. For completeness, we give a self-contained proof here. Note that a Gröbner basis is called minimal if the leading term of each polynomial in the basis is not divisible by the leading term of any other polynomial in the basis.

Theorem 3.1. *Let $g = \sum_{i=1}^{r} \lambda_i E_i$ as in (7) and let $h(z)$ be as defined above. Let*

$$J_z = \langle I, z - g \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_n, z].$$

Then, under any elimination ordering with $x_1, \ldots, x_n > z$, any minimal Gröbner basis G_z of J_z has the following properties:

(a) *It contains the polynomial $h(z)$.*

(b) *For any polynomial f in G_z, viewed as a polynomial in $\mathbb{F}_q[z][x_1, \ldots, x_n]$, say*

$$f = u(z) \cdot X^{\alpha} + \cdots + (\textit{lower order terms}),$$

where X^{α} is the leading monomial and $u(z) \in \mathbb{F}_q[z]$ is the leading coefficient. Then $u(z) \mid h(z)$.

(c) *For any root λ of $h(z)$, the specialization G_λ of G_z is a Gröbner basis for $\langle I, \lambda - g \rangle$.*

Proof. For part (a), as $g \equiv \lambda_i \pmod{Q_i}$, we have

$$\langle Q_i, z - g \rangle = \langle Q_i, z - \lambda_i \rangle.$$

Since the Q_i's are pairwise coprime, we have

$$J_z = \bigcap_{i=1}^{r} \langle Q_i, z - g\rangle = \bigcap_{i=1}^{r} \langle Q_i, z - \lambda_i\rangle. \tag{11}$$

Hence $h(z) \in J_z$ and must be one of the polynomials in G_z.

For part (b), let $w(z) = \gcd(u(z), h(z))$. Suppose $u(z) \nmid h(z)$. Then $\ell_1 = \deg(w(z)) < \deg(u(z)) = \ell$. Let $s(z), t(z) \in \mathbb{F}_q[z]$ be such that $w(z) = s(z)u(z) + t(z)h(z)$. Define

$$w_1 := s(z) \cdot f + t(z)X^\alpha \cdot h(z) = w(z)X^\alpha + \cdots \in J_z.$$

Then $\mathrm{LT}(w_1) = X^\alpha z^{\ell_1} < \mathrm{LT}(f) = X^\alpha z^\ell$, and $\mathrm{LT}(w_1) \mid \mathrm{LT}(f)$. Since G_z is a Gröbner basis, there is a polynomial $g \in G_z$ such that $\mathrm{LT}(g) \mid \mathrm{LT}(w)$, hence $\mathrm{LT}(g) \mid \mathrm{LT}(f)$, contradictory to the assumption that G_z is minimal. Therefore, we must have $u(z) \mid h(z)$.

Finally, the proof of (c) is a little longer. Let $\{g_1, \ldots, g_t\}$ be any minimal Gröbner basis for the ideal $\langle I, \lambda - g\rangle \subseteq \mathbb{F}_q[X]$. Suppose

$$\mathrm{LT}(g_i) = X^{\alpha_i}, \quad 1 \le i \le t.$$

We show below that G_z contains polynomials $f_i \in G_z$, $1 \le i \le t$, of the form

$$f_i(X, z) = u_i(z)X^{\alpha_i} + \cdots \tag{12}$$

with $u(\lambda) \neq 0$, where $X^{\alpha_i} = \mathrm{LT}(f_i)$ and $u_i(z) \in \mathbb{F}_q[z]$ is the coefficient of X^α in $f(X, z)$. Hence $\mathrm{LT}(f_i(X, \lambda)) = X^{\alpha_i} = \mathrm{LT}(g_i)$. As $f_i(X, \lambda) \in \langle I, \lambda - g\rangle$ and $\{g_1, \ldots, g_t\}$ form a Gröbner basis, we conclude that $\{f_1(X, \lambda), \ldots, f_t(X, \lambda)\} \subseteq G_\lambda$ form a Gröbner basis for $\langle I, \lambda - g\rangle$ as claimed.

It remains to prove that f_i in (12) exists in G_z for each $1 \le i \le t$. Without loss of generality, we assume that $\lambda = \lambda_1$ and that $\lambda_1, \ldots, \lambda_v$ are the distinct values of $\lambda_1, \ldots, \lambda_r$. Let

$$w(z) = \prod_{j=2}^{v} (z - \lambda_j).$$

Note that

$$J_z = \langle I, z - g\rangle = \bigcap_{i=1}^{v} \langle I, \lambda_i - g, z - \lambda_i\rangle.$$

Since $g_i \in \langle I, \lambda - g, z - \lambda\rangle = \langle I, \lambda_1 - g, z - \lambda_1\rangle$, we have $w(z)g_i \in J_z$. By the standard division algorithm, there are polynomials $f_j \in G_z$ and $u_j \in \mathbb{F}_q[X, z]$, $1 \le j \le s$, such that

$$w(z)g_i(X) = u_1(X, z)f_1(X, z) + \cdots + u_s(X, z)f_s(X, z) \tag{13}$$

with $\mathrm{LT}(u_j f_j) \le \mathrm{LT}(w(z)g_i)$, $1 \le j \le s$. Since G_z is assumed to be a Gröbner basis under an elimination order with $X > z$, we also have that

$$\mathrm{LT}_X(u_j(X, z)f_j(X, z)) \le \mathrm{LT}_X(w(z)g_i(X)) = \mathrm{LT}_X(g_i(X)) = X^{\alpha_i}, \tag{14}$$

where $\mathrm{LT}_X(f)$ means the leading term of f as a polynomial in X. Now plugging $z = \lambda$ into (13), we get

$$w(\lambda)g_i(X) = u_1(X, \lambda)f_1(X, \lambda) + \cdots + u_s(X, \lambda)f_s(X, \lambda).$$

Note that (14) implies that

$$\mathrm{LT}(u_j(X, \lambda)f_j(X, \lambda)) \le \mathrm{LT}(w(\lambda)g_i) = \mathrm{LT}(g_i) = X^{\alpha_i}, \quad 1 \le j \le s.$$

There is at least one j such that $\mathrm{LT}(u_j(X,\lambda)f_j(X,\lambda)) = X^{\alpha_i}$, hence $\mathrm{LT}(f_j(X,\lambda))$ divides X^{α_i}.

By renaming $f_1,\ldots,f_s$ if needed, we may assume that $\mathrm{LT}(u_i(X,\lambda)f_i(X,\lambda)) = X^{\alpha_i}$, thus $\mathrm{LT}(f_i(X,\lambda))$ divides X^{α_i}. We claim that $\mathrm{LT}(f_i(X,\lambda)) = X^{\alpha_i}$. Otherwise, since $f_i(X,\lambda) \in \langle I, \lambda - g\rangle$ and $\{g_1,\ldots,g_t\}$ is a Gröbner basis for the latter, $\mathrm{LT}(f_i(X,\lambda))$ would be divisible by $\mathrm{LT}(g_\ell)$ for some $\ell \neq i$, hence $\mathrm{LT}(g_\ell)$ would divide $\mathrm{LT}(g_i)$, contradicting to the assumption that $\{g_1,\ldots,g_t\}$ is minimal. It follows that $\mathrm{LT}_X(f_i(X,z)) = X^{\alpha_i}$ and the coefficient of X^{α_i} in $f_i(X,z))$ is a polynomial $u_i(z) \in \mathbb{F}_q[z]$ such that $u_i(\lambda) \neq 0$. This proves that G_z has a polynomial of the form (12) for each $1 \leq i \leq t$. The proof is complete. □

Note that if G is a Gröbner basis for I under a term order σ, then $G \cup \{z - g\}$ is a Gröbner basis for J_z under the elimination order $z > x_1,\ldots,x_n$ with the x_i's ordered by σ. Hence the Gröbner basis G_z for J_z under the elimination order $x_1,\ldots,x_n > z$ can be computed by a change of term order using the algorithm in [8]. After G_z is computed, the Gröbner bases for the components $\langle I, \lambda - g\rangle$ are obtained from G_z by specializing z to the roots of the polynomial $h(z)$. Also, the leading coefficients $u(z)$ automatically give a partial factorization of $h(z)$.

Based on the above results, one can write an algorithm explicitly for computing primary decomposition for zero-dimensional ideals over $\mathbb{F}_q$. We shall not present the details of such an algorithm, instead we demonstrate below by giving a concrete example, which we hope is more helpful in understanding the ideas. Consider the ideal

$$I = \langle y^2 - xz, z^2 - x^2y, x + y + z - 1\rangle \subset \mathbb{F}_5[x,y,z].$$

One can use any term order in the following computation, but we happen to use lex order. Under the lex order with $x > y > z$, I has a Gröbner basis

$$\begin{aligned} G =& [x + y + z - 1, y^2 + 3y - 2z^4 + z^3 + 2z^2 + z, yz + 2y \\ &\qquad + 2z^4 - z^3 - z^2 - 2z, z^5 - z^4 + 3z^3 - z^2 + 2z], \end{aligned}$$

and the corresponding monomial basis for $R = \mathbb{F}_5[x,y,z]/I$ is

$$B = (z^4, z^3, z^2, z, y, 1).$$

The matrix C in (9) of the Frobenius map on R under this basis is

$$C = \begin{bmatrix} -2 & -1 & 1 & 1 & 1 & 0 \\ -1 & -1 & 2 & 2 & 0 & 0 \\ 2 & -1 & 2 & 1 & 0 & 0 \\ -1 & -2 & 2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The solution space of the linear equation system (10) has a basis with four elements:

$$\begin{aligned} (0,0,0,0,0,1) &\quad\longleftrightarrow\quad g_1 = 1, \\ (0,0,-1,1,0,0) &\quad\longleftrightarrow\quad g_2 = z - z^2, \\ (0,1,1,0,0,0) &\quad\longleftrightarrow\quad g_3 = z^2 + z^3, \\ (-2,1,0,0,0,0) &\quad\longleftrightarrow\quad g_4 = z^3 - 2z^4. \end{aligned}$$

Hence I has four primary components.

Choose $g = g_2 = z - z^2$ and let $J = \langle I, w - g\rangle \subseteq \mathbb{F}_5[x, y, z, w]$. A Gröbner basis G_w of J under the lex order with $x > y > z > w$ follows:

$$\begin{gathered} w^4 + w^3 + w^2 + w, \quad (w-2)z + 2w^3 + w^2, \quad z^2 - z + w, \\ (w+1)y + zw - z - w, \quad yz - 2yw - 2z^2w - 2z^2 + 2zw + 2z, \\ y^2 + yz + z^2 - z, \quad x + y + z - 1. \end{gathered}$$

The polynomial $h = w^4 + w^3 + w^2 + w$ has four different roots: $w = 0, -1, -2, 2$. Note that two of the roots can be seen from the leading coefficients $w-2$ and $w+1$. As the degree of h equals 4, the dimension of the solution space, we get a primary component for each of the roots. For example, if $w = 0$, then the above Gröbner basis becomes

$$G_0 = \{-2z, z^2 - z, y - z, yz + 3z^2 + 2z, y^2 + yz + z^2 - z, x + y + z - 1\}.$$

Deleting the redundant polynomials (i.e., those whose leading terms are divisible by the leading terms of other polynomials), we have

$$Q_1 = \langle G_0\rangle = \langle -2z, y - z, x + y + z - 1\rangle = \langle z, y, x - 1\rangle,$$

where the basis was reduced in the last equation. Similarly, for the other three components:

$$\begin{aligned} w = -1: &\qquad Q_2 = \langle z + 2, y^2 - 2y + 1, x + y + 2\rangle, \\ w = -2: &\qquad Q_3 = \langle z - 2, y - 1, x + 2\rangle, \\ w = 2: &\qquad Q_4 = \langle z^2 - z + 2, y + 2z + 1, x - z + 3\rangle. \end{aligned}$$

Then $I = Q_1 \cap Q_2 \cap Q_3 \cap Q_4$ is a primary decomposition.

In the above computation, we obtained all the primary components using only the solution g. In this case, we say g is separable for I. Note that g is separable iff the λ_i's in (7) are distinct, i.e., iff $h(z)$ has degree r. One can prove that when the field $\mathbb{F}_q$ is large relative to r, a random solution g is separable with high probability. In fact, Theorem 2.10 in [9] applies here directly and one has the following proposition.

Proposition 3.2. *The probability that a random solution $g \in G$ in* (5) *is separable, is at least* $1 - \frac{r(r-1)}{2q}$.

Next we show how to apply Theorem 2.4 when g is not separable. Suppose we happen to pick $g = g_3 = z^3 + z^2$. Then the Gröbner basis of $J = \langle I, w - g\rangle$ under the lex order with $x > y > z > w$ follows:

$$\begin{gathered} w^3 + 2w^2 + 2w, \quad z^3 + z^2 - w, \quad yz + 2y + 2z^2 + 2w^2, \\ (w-1)z - w^2 + w, \quad (w-1)y + 2w^2 + 3w, \\ y^2 + 3y - z^2 - z + 3w^2, \quad x + y + z - 1. \end{gathered}$$

The leading coefficient $w - 1$ gives the root $w = 1$ for $h = w^3 + 2w^2 + 2w$, and the other two roots of h are $w = 0, 2$. Note that $h(z)$ has degree $3 < r = 4$, so g is not separable for I.

Specializing w to 0, 1 and 2 in the above basis gives three components:

$$
\begin{aligned}
w=0:&\quad Q_1=\langle z,y,x-1\rangle\\
w=1:&\quad I_2=\langle x+y+z-1,y^2-2y-z^2-z-2,yz+2y+2z^2+2,z^3+z^2-1\rangle\\
w=2:&\quad Q_3=\langle z-2,y-1,x+2\rangle.
\end{aligned}
$$

For each of the components, we apply Theorem 2.4. We demonstrate this on I_2. Reduce the basis polynomials g_1, g_2, g_3, g_4 by I_2 to get

$$1,\ -z^2+z,\ 1,\ 2z^2+3z+3,$$

for which 1 and $-z^2+z$ are linearly independent over $\mathbb{F}_5$ and the other two polynomials are linearly dependent on them. Hence the solution space for I_2 in (5) has dimension $r=2$, or equivalently I_2 has two primary components.

To decompose I_2, we compute a Gröbner basis for the ideal $\langle I_2, w-(z-z^2)\rangle$:

$$
\begin{array}{llll}
w^2-w+3, & (w+3)z+2w+1, & yz+2y+2z+3w+2, & \\
z^2-z+w, & (w+1)y+z+2w+4, & y^2+3y+3z+w+3, & x+y+z-1.
\end{array}
$$

As the factors $w+1$ and $w+3$ appear as leading coefficients, -1 and $-3=2$ are roots of $h=w^2-w+3$. Plugging each of them back into this Gröbner basis gives two primary components of I_2 (after reduction):

$$Q_2=\langle z+2,y^2-2y+1,x+y+2\rangle,\quad Q_4=\langle z^2-z+2,y+2z+1,x-z+3\rangle.$$

They give the same decomposition of I as above.

Note that in the above example, Q_1, Q_3 and Q_4 are prime ideals but not Q_2. In fact, $\sqrt{Q_2}=\langle z+2,y-1,x-2\rangle$. Also, if we change the polynomial $x+y+z-1$ to $x+y+z$ in I and apply our algorithm to the modified ideal

$$I_1=\langle y^2-xz,z^2-x^2y,x+y+z\rangle\subset\mathbb{F}_5[x,y,z],$$

then $I_1=Q_5\cap Q_6$ where

$$Q_5=\langle z^2,y^2+yz,x+y+z\rangle,\quad Q_6=\langle z^2+z+1,y+z+1,x-1\rangle.$$

Note that $\sqrt{Q_5}=\langle x,y,z\rangle$ and $\sqrt{Q_6}=Q_6$. Hence Q_6 is a prime ideal but not Q_5. (Note that a primary ideal Q is a prime ideal iff $\sqrt{Q}=Q$.)

Our algorithm computes an irredundant primary decomposition of a zero-dimensional ideal over $\mathbb{F}_q$. If the associated primes are needed, one can simply compute the radicals of the primary ideals that appear in the decomposition.

Finally, when k is not a finite field, but a more general function field over $\mathbb{F}_q$ (or over $\mathbb{Q}$) as mentioned in the introduction, much more needs to be done. Equation (4) is a quasi-linear system over k, so not a finite linear system over $\mathbb{F}_q$ as k has infinite dimension as a vector space over $\mathbb{F}_q$. A practical approach is to use a modular method, that is, reduce by a maximal ideal and do Hensel lifting. This will convert the congruence equation (4) to a finite linear system over $\mathbb{F}_q$. The main problem is that, under a reduction at a prime ideal, a primary ideal may split into many primary ideals, so one needs to find the right combinations to get back to the original primary components. For polynomial factorization, which corresponds to the special case when I is generated by one polynomial, efficient algorithms were recently developed by van Hoeij [15] and Lecerf [16]. It is desirable to develop a similar theory for systems of multivariate polynomials. As mentioned in the introduction, the other two approaches are to use differential equations and Dwork's operators, which behave much better than the Frobenius operator in higher dimensional cases. For factoring bivariate polynomials, the paper [10] shows how to solve related quasi-linear systems over function fields. We hope to explore these approaches for general ideals in a future paper.

References

[1] T. Becker and V. Weispfenning, *Gröbner Bases, A Computational Approach to Commutative Algebra*, GTM 141, Springer, New York, 1993. MR1213453 (95e:13018)

[2] E.R. Berlekamp, "Factoring polynomials over finite fields", Bell System Technical J., 46(1967), 1853-1859. MR0219231 (36:2314)

[3] E.R. Berlekamp, "Factoring polynomials over large finite fields", Mathematics of Computation **24** (1970), 713-735. MR0276200 (43:1948)

[4] D. Cox, J. Little and D. O'Shea, *Using algebraic geometry*, Graduate Texts in Mathematics, 185, Springer-Verlag, New York, 1998. MR1639811 (99h:13033)

[5] W. Decker, G.-M. Greuel and G. Pfister, "Primary decomposition: algorithms and comparisons", Algorithmic algebra and number theory (Heidelberg, 1997), 187–220, Springer, Berlin, 1999. MR1672046 (99m:13049)

[6] D. Eisenbud, *Commutative algebra*, With a view toward algebraic geometry, Graduate Texts in Mathematics, 150, Springer-Verlag, New York, 1995. xvi+785 pp. MR1322960 (97a:13001)

[7] D. Eisenbud, C. Huneke and W. Vasconcelos, "Direct methods for primary decomposition", *Invent. Math.* **110** (1992), no. 2, 207–235. MR1185582 (93j:13032)

[8] J. Faugere, P. Gianni, D. Lazard and T. Mora, "Efficient computation of zero-dimensional Gröbner bases by change of ordering", *J. Symbolic Comput.* **16** (1993), 329-344. MR1263871 (94k:68095)

[9] S. Gao, "Factoring multivariate polynomials via partial differential equations", *Mathematics of Computation* **72** (2003), 801–822. MR1954969 (2003m:12014)

[10] S. Gao, Y. Guan and R. Heindl, "Factoring bivariate polynomials via Niederreiter's differential equation", in preparation.

[11] S. Gao, V. M. Rodrigues and J. Stroomer, "Gröbner basis structure of finite sets of points", preprint 2003.

[12] H.-G. Gräbe, "Minimal primary decomposition and factorized Gröbner bases", *Appl. Algebra Engrg. Comm. Comput.* **8** (1997), no. 4, 265–278. MR1464788 (98k:13031)

[13] P. Gianni, B. M. Trager and G. Zacharias, "Gröbner bases and primary decomposition of polynomial ideals", *J. Symbolic Comput.*, 6 (2-3), 1988, 149-167. MR988410 (90f:68091)

[14] G.-M. Greuel and G. Pfister, *A SINGULAR Introduction to Commutative Algebra*, Springer-Verlag 2002, xvii + 588 pp. MR1930604 (2003k:13001)

[15] M. van Hoeij, "Factoring polynomials and the knapsack problem", *Journal of Number Theory* **95** (2002), 167-189. MR1924096 (2003f:13029)

[16] G. Lecerf "Sharp precision in Hensel lifting for bivariate polynomial factorization", *Mathematics of Computation* **75** (2006), 921-933. MR2197000 (2007g:12008)

[17] C. Monico, "Computing the primary decomposition of zero-dimensional ideals", *J. Symbolic Comput.* **34** (2002), 451–459. MR1937469 (2003i:13036)

[18] H. Niederreiter, "A new efficient factorization algorithm for polynomials over small finite fields", *Appl. Alg. Eng. Comm. Comp.* **4** (1993), 81–87. MR1223850 (94h:11112)

[19] H. Niederreiter, "Factoring polynomials over finite fields using differential equations and normal bases", *Math. Comp.* **62** (1994), 819-830. MR1216262 (94g:11113)

[20] J.F. Ritt, *Differential algebra*. Dover Publications, Inc., New York, 1966 viii+184 pp. MR0201431 (34:1315)

[21] A. Sausse, "A new approach to primary decomposition", Computational Algebra and Number Theory (Milwaukee, WI, 1996). *J. Symbolic Comput.* **31** (2001), no. 1-2, 243–257. MR1806219 (2002k:13038)

[22] A. Seidenberg, "On the Lasker-Noether decomposition theorem", *American J. Math.* **106** (1984), 611-638. MR745143 (86b:03078)

[23] T. Shimoyama and K. Yokoyama, "Localization and primary decomposition of polynomial ideals", *J. Symbolic Comput.* **22** (1996), no. 3, 247–277. MR1427183 (98a:13038)

[24] A.K. Steel, "Conquering inseparability: Primary decomposition and multivariate factorization over algebraic function fields of positive characteristic", *J. Symbolic Comput.* **40** (2005), 1053-1075. MR2167699 (2006f:13023)

[25] W.V. Vasconcelos, *Computational methods in commutative algebra and algebraic geometry*, With chapters by David Eisenbud, Daniel R. Grayson, Jürgen Herzog and Michael Stillman. Algorithms and Computation in Mathematics, 2, Springer-Verlag, Berlin, 1998. xii+394 pp. MR1484973 (99c:13048)

[26] D. Wan, "Computing zeta functions over finite fields", *Contemporary Mathematics*, **225** (1999), 131-141. MR1650604 (99j:11073)

[27] D. Wang, "Decomposing algebraic varieties", Automated deduction in geometry (Beijing, 1998), 180–206, Lecture Notes in Comput. Sci., 1669, Springer, Berlin, 1999. MR1775951 (2001f:68144)

[28] Wen Jun Wu, "Basic principles of mechanical theorem proving in elementary geometries", *J. Systems Sci. Math. Sci.* **4** (1984), no. 3, 207–235. MR795000 (87g:03017)

[29] Wen Tsun Wu, *Mechanical theorem proving in geometries. Basic principles.* Translated from the 1984 Chinese original by Xiao Fan Jin and Dong Ming Wang. Texts and Monographs in Symbolic Computation. Springer-Verlag, Vienna, 1994. xiv+288 pp. MR1284925 (96a:68110)

Department of Mathematical Sciences, Clemson University, Clemson, South Carolina 29634-0975
E-mail address: sgao@math.clemson.edu

Department of Mathematics, University of California, Irvine, California 92697-3875
E-mail address: dwan@math.uci.edu

Information Security laboratory, Institute of Software, Chinese Academy of Sciences, Box 8718, Beijing 100080, People's Republic of China
E-mail address: mingsheng_wang@yahoo.com.cn