COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 59, No. 2 2010

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171–8501 JAPAN

A Note on Distinct Nilpotency Decomposition of Polynomial Ideals over Finite Fields

by

Kazuhiro YOKOYAMA

(Received September 29, 2010)
(Revised November 15, 2010)

1. Introduction

Efficient computation of the radical of an arbitrary ideal in a polynomial ring over a field of positive characteristic is very interesting problem as we have to resolve computational difficulty coming from "inseparability" which appears in many cases. There are several works on the subject and many of proposed methods are based on derivation. (See [7, 8, 11].) In [12] Matsumoto proposed an effective and efficient method in a different approach based on computation of *inverse image of Frobenius map*. Also, for further computation such as prime/primary decomposition, special efforts are done for solving such difficulty and, by using Matsumoto's method, a complete method for prime decomposition is established in [15, 13].

In this paper, we extend Matsumoto's method for further decomposition of polynomial ideals over finite fields without complicated procedures of prime decomposition. In more detail, we can utilize *inverse image of Frobenius map* very precisely to extract the intersection of all primary components which are prime by *basic ideal operations* such as ideal quotient and saturation. Moreover, by applying such computation repeatedly, we can obtain an interesting intermediate decomposition, where each *component* has different *degree of nilpotency*. Therefore, we call such an intermediate decomposition the *distinct nilpotency decomposition*.

Now we explain the new notion distinct nilpotency decomposition. Let p be a prime number and q a power of p. By $\mathbb{F}_q$ we denote the finite field of order q and by $\mathbb{F}_q[x_1, \ldots, x_n]$ we denote a polynomial ring over $\mathbb{F}_q$ in n variables $x_1, \ldots, x_n$.

We begin by defining *degree of nilpotency*.

DEFINITION 1.1 (Degree of Nilpotency). For an ideal I of $\mathbb{F}_q[x_1, \ldots, x_n]$, we denote its radical by $\sqrt{I}$. We define the *degree of nilpotency* of I as the smallest integer s such that x^s belongs to I for any element x in $\sqrt{I}$, and denote it by $\mathrm{nil}(I)$.

By Brownawell and Kollár, it is shown that the degree of nilpotency of an ideal J is bounded by d^n, where d is the maximum of total degrees of polynomials in a generating set of J. (See Theorem 9.2.1 in [14].)

REMARK 1.2. The definition of the degree of nilpotency is slightly different from the standard one. In [14], the degree of nilpotency of J is defined as the smallest integer s such that $\sqrt{J}^s \subset J$.

From now on, let I be an ideal of a polynomial ring $\mathbb{F}_q[x_1, \dots, x_n]$ and suppose that I has no embedded primary component and every primary component of I has a common *maximal* independent set. This assumption is not so special, since many cases in actual mathematical problems have such property and also during primary decomposition there appears such an ideal. See [9, 15, 13].

DEFINITION 1.3 (Distinct Nilpotency Decomposition). Let $\mathcal{S}(I)$ be the set of all irredundant primary components. We note that $\mathcal{S}(I)$ is determined uniquely for I. Also, when a subset $\mathcal{A}$ of $\mathcal{S}(I)$ is empty, we set $\bigcap_{Q\in\mathcal{A}} Q = \mathbb{F}_q[x_1, \dots, x_n]$.

(1) By $\mathcal{R}_0(I)$, we denote the set of all irredundant primary components of I which are prime, and we denote those intersection by $r_0(I)$, that is,

$$r_0(I) = \bigcap_{Q\in\mathcal{R}_0(I)} Q\,.$$

We call $r_0(I)$ the *radical part* of I. For each Q in $\mathcal{R}_0(I)$, its degree of nilpotency is 1.

For each $k \geq 1$, we denote by $\mathcal{R}_k(I)$ the set of all irredundant primary components Q such that $p^{k-1} < \mathrm{nil}(Q) \leq p^k$. Moreover, we denote those intersection by $r_k(I)$, that is,

$$r_k(I) = \bigcap_{Q\in\mathcal{R}_k(I)} Q\,.$$

(2) We define $\mathcal{N}R_k(I)$ by

$$\mathcal{N}R_k(I) = \mathcal{S}(I) \setminus \bigcup_{i=0}^{k} \mathcal{R}_i(I)\,.$$

Then, $\mathcal{N}R_k(I)$ consists of all irredundant primary components Q with $nil(Q) > p^k$. Moreover, we denote those intersection by $nr_k(I)$, that is,

$$nr_k(I) = \bigcap_{Q\in\mathcal{N}R_k(I)} Q.$$

When $k = 0$, $nr_0(I)$ is the intersection of all primary components which are non-prime, and we call it *the non-radical part* of I.

By definition, for each non-negative integer k, it follows that

$$I = \left(\bigcap_{i=0}^{k} r_i(I)\right) \cap nr_k(I)\,.$$

When $k = 0$, we have

$$I = r_0(I) \cap nr_0(I) \tag{1}$$

and we call the decomposition (1) the *radical part decomposition* of I.

(3) As the degree of nilpotency of each component Q is bounded, there exists a non-negative integer d such that

$$I = \bigcap_{i=0}^{d} r_i(I)\,. \tag{2}$$

We call the decomposition (2) the *distinct nilpotency decomposition* of I or the DND of I for short.

In this paper, we show that the DND of I can be computed by elementary ideal operations in a recursive manner as follows. Here by *computing an ideal* we mean *computing its Gröbner basis*.

(I) First the radical part decomposition (1) is computed. That is, $r_0(I)$ and $nr_0(I)$ are obtained by computation of *inverse image of Frobenius map* and *ideal quotient* computation.

(II) Beginning by $k = 0$, by applying the method for (I) repeatedly, $r_{k+1}(I)$ and $nr_{k+1}(I)$ are computed from $nr_k(I)$.

(III) When $nr_k(I) = r_{k+1}(I)$, that is, $\mathcal{NR}_{k+1}(I) = \emptyset$, the whole computation terminates. Then we have computed $r_0(I), \ldots, r_{k+1}(I)$ such that $I = \bigcap_{i=0}^{k+1} r_i(I)$ gives the DND of I.

The method proposed in the paper has the following features:

(1) During radical computation along with Matsumoto's method, we obtain the DND as an intermediate decomposition.

(2) Additional computations for the DND are only basic ideal operations (ideal quotient and saturation).

As the method does not require any additional "decomposition" based on *factorization*, DND computation may contribute a new approach to efficient and practical prime/primary decomposition of polynomial ideals over finite fields. Because, for prime decomposition of an ideal with positive dimension, we have to execute a special treatment for resolving computational difficulty derived from "inseparability". (See [15, 13] for details.) Also, when we consider the factorization of a polynomial over an algebraic extension of a rational function field, it corresponds to a primary decomposition of a corresponding ideal and the distinct nilpotency decomposition can be considered as a variant of the square-free decomposition which is computed in a very different approach.

2. Mathematical fundamentals

Here we provide necessary definitions and useful propositions for the DND computation. We begin by showing our setting.

Let p be a prime number and q a power of p. By $\mathbb{F}_q$ we denote the finite field of order q and by $\mathbb{F}_q[x_1, \ldots, x_n]$ we denote a polynomial ring over $\mathbb{F}_q$ in n variables $x_1, \ldots, x_n$. For simplicity, we write X for $\{x_1, \ldots, x_n\}$ and $\mathbb{F}_q[X]$ for $\mathbb{F}_q[x_1, \ldots, x_n]$. For a subset Y of X, we also write $\mathbb{F}_q[Y]$ and $\mathbb{F}_q(Y)$ for a polynomial ring over $\mathbb{F}_q$ in Y and a rational function field over $\mathbb{F}_q$ in Y, respectively.

SETTING: Let I be an ideal of $\mathbb{F}_q[x_1,\dots,x_n]$ and suppose that I has no embedded primary component and every primary component of I has a common *maximal independent set*. As to a maximal independent set, see [3] for its definition and computational details. In this case, the dimension of each primary component coincides with the cardinality of a common maximal independent set.

In the following, we denote the dimension of I by ℓ and fix a common maximal independent set Y. Then $\#Y = \ell$. Also, let $\mathcal{S}(I) = \{Q_1,\dots,Q_t\}$ the set of all irredundant primary components, where $Q_1,\dots,Q_s$ $(s \le t)$ are prime but $Q_{s+1},\dots,Q_t$ are not. When no component is prime, we set $s = 0$. Then the irredundant primary decomposition of I is given as follows:

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_t\,. \tag{3}$$

We denote by P_i the associated prime of Q_i, that is, $P_i = \sqrt{Q_i}$. Then for each Q_i, $i \le s$, $Q_i = P_i$ and for each Q_i, $s+1 \le i \le t$, $Q_i \ne P_i$.

By Definition 1.3, $\bigcap_{i=1}^{s} Q_i$ is the radical part $r_0(I)$ of I and $\bigcap_{i=s+1}^{t} Q_i$ is the non-radical part $nr_0(I)$ of I. We note that for a set $\mathcal{A}$ of ideals, if $\mathcal{A}$ is empty, we set $\bigcap_{J\in\mathcal{A}} J = \mathbb{F}_q[X]$.

FROBENIUS MAP: We define the Frobenius map which is an endomorphism of $\mathbb{F}_q[X]$ as follows:

$$\varphi_p : \mathbb{F}_q[X] \ni f(x_1,x_2,\dots,x_n) \mapsto f(x_1,x_2,\dots,x_n)^p \in \mathbb{F}_q[x]\,.$$

We note that φ_p is the composition of the following commutative endomorphisms φ_v and φ_c:

$$\varphi_v : \mathbb{F}_q[X] \ni f(x_1,x_2,\dots,x_n) \mapsto f(x_1^p,x_2^p,\dots,x_n^p) \in \mathbb{F}_q[X]\,,$$
$$\varphi_c : \mathbb{F}_q[X] \ni \sum a_{e_1,\dots,e_n} x_1^{e_1}\cdots x_n^{e_n} \mapsto \sum a_{e_1,\dots,e_n}^p x_1^{e_1}\cdots x_n^{e_n} \in F_q[X]\,.$$

That is, $\varphi_p = \varphi_v \circ \varphi_c = \varphi_c \circ \varphi_v$. If $q = p$, then φ_c is the identity map and $\varphi_p = \varphi_v$. Then, the inverse image of the Frobenius map plays a very important role for radical computation.

PROPOSITION 2.1 ([12]).
(1) $I \subseteq \varphi_p^{-1}(I) \subseteq \sqrt{I}$.
(2) *If* $I \ne \sqrt{I}$, *then* $I \ne \varphi_p^{-1}(I)$. *Otherwise*, $I = \varphi_p^{-1}(I)$.
(3) *There is a positive integer d such that* $\varphi_p^{-d}(I) = \sqrt{I}$.

The third statement of Proposition 2.1 can be shown by the finiteness of the following ascending chain:

$$I \subsetneq \varphi_p^{-1}(I) \subsetneq \varphi_p^{-2}(I) \subsetneq \cdots \subsetneq \varphi_p^{1-d}(I) \subsetneq \varphi_p^{-d}(I) = \sqrt{I}$$

To utilize $\varphi_p^{-1}(I)$ for the DND computation, we provide several lemmas and propositions in the sequent.

By a general property of maps, it follows that $\varphi_p^{-1}(A \cap B) = \varphi_p^{-1}(A) \cap \varphi_p^{-1}(B)$ for subsets A, B of $\mathbb{F}_q[X]$. By using this, we have the following.

LEMMA 2.2. *Corresponding to the primary decomposition* (3) *of I, we have the following decomposition*:

$$\varphi_p^{-1}(I) = \bigcap_{i=1}^{t} \varphi_p^{-1}(Q_i)\,.$$

In the following, we write $J^{(k)}$ for $\varphi_p^{-k}(J)$ for an ideal J and a positive integer k. Thus, $I^{(k)} = \varphi_p^{-k}(I)$ and $Q_i^{(k)} = \varphi_p^{-k}(Q_i)$. Then, for any positive integer k, Proposition 2.1 shows that $Q_i^{(1)} = Q_i$ for $1 \le i \le s$, and $Q_i^{(1)} \supsetneq Q_i$ for $s+1 \le i \le t$.

IDEAL QUOTIENT AND SATURATION: Next we provide necessary properties related ideal quotient and saturation. We recall the definition of saturation in a general setting. Let I_1, I_2 be ideals of a noetherian domain R. Then, we have the following ascending chain of ideals:

$$I_1 = (I_1 : I_2^0) \subset (I_1 : I_2) \subset (I_1 : I_2^2) \subset \cdots ,$$

where we set $I_2^0 = R$. Then there exists a positive integer d such that

$$(I_1 : I_2^{d-1}) \subsetneq (I_1 : I_2^d) = (I_1 : I_2^{d+1}) = \cdots . \tag{4}$$

DEFINITION 2.3. For a positive integer d satisfying the formula (4), $(I_1 : I_2^d)$ is called the saturation of I_1 with respect to I_2, and denoted by $(I_1 : I_2^\infty)$.

As to ideal quotient, the following related to primary ideals is very useful. (See Page 82 of [14].)

LEMMA 2.4. *Let P be a prime ideal of a noetherian ring and Q a P-primary ideal. Also, let J be an ideal of R. Then the quotient $(Q : J)$ of Q by J is determined as follows*:

(1) *If $J \not\subset P$, then $(Q : J) = Q$.*
(2) *If $J \subset Q$, then $(Q : J) = R$.*
(3) *If $J \subset P$ and $J \not\subset Q$, then $(Q : J)$ is a P-primary ideal properly containing Q.*

Proof. The statements (1) and (2) can be proved directly by the definition of "primary ideal".

Now we consider the case (3) where $J \subset P$ and $J \not\subset Q$. We remark that $Q \neq P$, as $J \not\subset Q$.

First we show that $(Q : J) \subset P$. If not, there is an element f in $(Q : J) \setminus P$. But, as $fJ \subset Q$, $fg \in Q$ for any element g of J. Since Q is a primary ideal, it implies that $g \in Q$ and thus $J \subset Q$. This is a contradiction.

Next we show that $(Q : J) \supsetneq Q$. By the definition of ideal quotient, it is clear that $(Q : J) \supset Q$. Thus, we show that $(Q : J) \neq Q$. As Q is a P-primary ideal, there exists a positive integer k such that $P^k \subset Q$, which implies $J^k \subset Q$. Then there exists a positive integer d such that $J^d \subset Q$ but $J^{d-1} \not\subset Q$. For such d, by the definition of ideal quotient, we have $J^{d-1} \subset (Q : J)$. As $J^{d-1} \not\subset Q$, it follows that $(Q : J) \neq Q$.

Finally we show that $(Q : J)$ is a P-primary ideal. Suppose that $fg \in (Q : J)$ but $f \notin (Q : J)$ for some elements f, g. Then $fgJ \subset Q$ but $fJ \not\subset Q$, which means that there is an element h in J such that $fgh \in Q$ but $fh \notin Q$. By the definition of primary ideal, it follows that $g^m \in Q \subset (Q : J)$ for sufficiently large m, which shows that $(Q : J)$ is a primary ideal. As $P = \sqrt{Q} \subset \sqrt{(Q : J)} \subset P$, $(Q : J)$ is a P-primary ideal. □

LEMMA 2.5. *For each primary component Q_i and a positive integer k, $Q_i^{(k)}$ is a P_i-primary ideal. Moreover, if $Q_i \neq P_i$, then $Q_i^{(k)} \supsetneq Q_i$ and $(Q_i : Q_i^{(k)})$ is also a P_i-primary ideal properly containing Q_i.*

Proof. For simplicity, we set $Q = Q_i$, $Q^{(k)} = Q_i^{(k)}$, and $P = \sqrt{Q}$. As $Q \subset Q^{(k)} \subset \sqrt{Q}$ by Proposition 2.1, we have $\sqrt{Q^{(k)}} = P$.

First we show that $Q^{(k)}$ is a P-primary ideal. For $a, b \in \mathbb{F}_q[X]$, suppose that $ab \in Q^{(k)}$. Then $a^{p^k} b^{p^k} \in Q$, as $Q^{(k)} = \varphi_p^{-k}(Q) = \{g \in \mathbb{F}_q[X] \mid \varphi_p(g) = g^{p^k} \in Q\}$. If $a \notin P$, then $a^{p^k} \notin P$, and $b^{p^k} \in Q$, since Q is a primary ideal. Thus, we have $b \in \varphi_p^{-k}(Q) = Q^{(k)}$ and $Q^{(k)}$ is shown to be a P-primary ideal.

Next we show that $Q^{(k)} \supsetneq Q$ and $(Q : Q^{(k)})$ is a P-primary ideal, if $Q \neq P$. By Proposition 2.1, if $Q \neq P$, $Q^{(k)}$ is containing Q properly. Thus, using Lemma 2.4, it can be shown that $(Q : Q^{(k)})$ is a P-primary ideal properly containing Q, since Q and $Q^{(k)}$ are P-primary ideal, and $Q^{(k)} \subset P$ and $Q^{(k)} \not\subset Q$. □

EXTENSION AND CONTRACTION: Now we consider *extension* and *contraction* with respect to $\mathbb{F}_q(Y)[X \setminus Y]$, where Y is the fixed common maximal independent set. As Q_i and $Q_i^{(k)}$ are P_i-primary ideal, those have Y as a common maximal independent set. Thus, $I^{(k)}$ has also Y as its maximal independent set.

Then we consider those extensions as ideals of $\mathbb{F}_q(Y)[X \setminus Y]$ and contractions of such extensions. Here we use the following notation:

For an ideal J of $\mathbb{F}_q[X]$, we denote by J^e the *extension* of J, which is the ideal of $\mathbb{F}_q(Y)[X \setminus Y]$ generated by J. Also, for an ideal $\hat{J}$ of $\mathbb{F}_q(Y)[X \setminus Y]$, we denote by $\hat{J}^c$ the *contraction* of $\hat{J}$, which is defined as $\hat{J} \cap \mathbb{F}_q[X]$.

LEMMA 2.6. *Let J, L be ideals of $\mathbb{F}_q[X]$ and J', L' ideals of $\mathbb{F}_q(Y)[X \setminus Y]$. Then, we have $(J \cap L)^e = J^e \cap L^e$, $(JL)^e = J^e L^e$, $(J : L)^e = (J^e : L^e)$ and $(J' \cap L')^c = J'^c \cap L'^c$.*

Moreover, if $J^{ec} = J$ and $L^{ec} = L$ hold, then we have $(J \cap L)^{ec} = (J \cap L)$, $(J : L)^{ec} = (J : L)$ and $(J : L^k)^{ec} = (J : L^k)$ for every positive integer k, which implies $(J : L^\infty)^{ec} = (J : L^\infty)$.

Proof. Since $\mathbb{F}_q(Y)[X \setminus Y]$ can be considered as the ring of fractions of $\mathbb{F}_q[X]$ with respect to $\mathbb{F}_q[Y] \setminus \{0\}$, that is, $\mathbb{F}_q(Y)[X \setminus Y] = (\mathbb{F}_q[Y] \setminus \{0\})^{-1}\mathbb{F}_q[X]$, it can be show by using properties of rings of fractions that $(J \cap L)^e = J^e \cap L^e$, $(JL)^e = J^e L^e$ and $(J : L)^e = (J^e : L^e)$. (See Proposition 3.11 and Corollary 3.15 in [2].) Also, by a general property of contraction, we have $(J' \cap L')^c = J'^c \cap L'^c$.

Next we consider the case where $J^{ec} = J$ and $L^{ec} = L$ hold. By general properties of contraction, we have $(J \cap L) \subset (J \cap L)^{ec}$, and $(J : L) \subset (J : L)^{ec}$. But, we also have

$$(J \cap L)^{ec} = (J^e \cap L^e)^c = J^{ec} \cap L^{ec} = J \cap L\,,$$
$$(J : L)^{ec} = (J^e : L^e)^c \subset (J^{ec} : L^{ec}) = (J : L)\,.$$

Thus, we obtain $(J \cap L)^{ec} = J \cap L$ and $(J : L)^{ec} = (J : L)$. For an integer $k \geq 2$, since $(J : L^k) = ((J : L^{k-1}) : L)$, we can show $(J : L^k)^{ec} = (J : L^k)$ by using induction argument on k. □

Since Y is a common maximal independent set, I^e and $I^{(1)^e}$ are 0-dimensional ideal of $\mathbb{F}_q(Y)[X \setminus Y]$ and each P_i^e is a maximal ideal. Moreover, by the one-to-one correspondence of primary components (see Proposition 3.11 and Proposition 4.8 in [2]), $P_i^e \neq P_j^e$ for $i \neq j$ and $Q_i{}^e$, $(Q_i^{(1)})^e$ are P_i^e-primary ideals. We also notice that if $i \neq j$, $Q_i{}^e \not\subset P_j$ and $(Q_i^{(1)})^e \not\subset P_j$.

Lemma 2.7. *For each Q_i and a positive integer k, we have $Q_i^{ec} = Q_i$, $Q_i^{(k)^{ec}} = Q^{(k)}$ and $(Q_i : Q_i^{(k)})^{ec} = (Q_i : Q_i^{(k)})$. Moreover, we have $I^{ec} = I$ and $(I^{(k)})^{ec} = I^{(k)}$.*

Proof. By Lemma 2.5, Q_i and $Q_i^{(k)}$ are P_i-primary ideals. Therefore, those have Y as a common maximal independent set and we have $Q_i^{ec} = Q_i$ and $(Q_i^{(k)})^{ec} = Q^{(k)}$. (See Proposition 4.8 in [2].) Also by Lemma 2.6, we also have $(Q_i : Q_i^{(k)})^{ec} = (Q_i : Q_i^{(k)})$, and moreover, we have $I^{ec} = I$ and $I^{(k)^{ec}} = I^{(k)}$, since $I = \bigcap_{i=1}^t Q_i$ and $I^{(k)} = \bigcap_{i=1}^t Q_i^{(k)}$. □

Now we show three propositions which are used for the DND computation in the next section.

Proposition 2.8. *Suppose that Q_i' is a P_i-primary ideal and $Q_i \subset Q_i'$ for each i. Then $(Q_i : Q_i')$ contains Q_i properly, and if $Q_i \neq Q_i'$, then $(Q_i : Q_i')$ is a P_i-primary ideal. Otherwise, that is, if $Q_i = Q_i'$, then $(Q_i : Q_i') = \mathbb{F}_q[X]$. Moreover, we have*

$$\left(I : \bigcap_{i=1}^{t} Q_i'\right) = \bigcap_{i=1}^{t} (Q_i : Q_i') = \bigcap_{i : Q_i \neq Q_i'} (Q_i : Q_i').$$

Proof. By Lemma 2.4, it follows that $(Q_i : Q_i')$ contains Q_i properly, and if $Q_i \neq Q_i'$, then $(Q_i : Q_i')$ is a P_i-primary ideal. If $Q_i = Q_i'$, then we have $(Q_i : Q_i') = \mathbb{F}_q[X]$.

Since Q_i' is a P_i-primary ideal, Q_i' has Y as a maximal independent set and thus we have $(Q_i')^{ec} = Q_i'$. (See the proof of Lemma 2.7.) Then, by Lemma 2.6, we have

$$\left(\bigcap_{i=1}^{t} Q_i'\right)^{ec} = \bigcap_{i=1}^{t} Q_i', \quad \text{and} \quad (I : \bigcap_{i=1}^{t} Q_i')^{ec} = \left(I : \bigcap_{i=1}^{t} Q_i'\right).$$

Now we evaluate $(I : \bigcap_{i=1}^t Q_i')^e$ as follows. By Lemma 2.6, we have $(I : \bigcap_{i=1}^t Q_i')^e = (I^e : (\bigcap_{i=1}^t Q_i')^e)$. Moreover, we have

$$\left(\bigcap_{i=1}^{t} Q_i'\right)^{e} = \bigcap_{i=1}^{t} Q_i'^{\,e}.$$

Since $Q_i'^e$ is a $P_i{}^e$-primary ideal and $P_i{}^e$ is maximal, it follows that $Q_i'^e$ and $Q'_j{}^e$ are comaximal for $i \neq j$. Then, by Chinese remainder theorem, we have

$$\bigcap_{i=1}^t Q_i'^e = \prod_{i=1}^t Q_i'^e\,.$$

By Lemma 2.6 and using properties of ideal quotient (see Exercise 1.12 in [2]), we also have

$$\left(I : \bigcap_{i=1}^t Q'_i\right)^e = \left(\bigcap_{i=1}^t Q_i{}^e : \prod_{j=1}^t Q'_j{}^e\right) = \bigcap_{i=1}^t \left(Q_i{}^e : \prod_{j=1}^t Q'_j{}^e\right).$$

For each $(Q_i{}^e : \prod_{j=1}^t Q'_j{}^e)$, by using general properties of ideal quotient, we have

$$\left(Q_i{}^e : \prod_{j=1}^t Q'_j{}^e\right) = ((\cdots((Q_i{}^e : Q'_1{}^e) : Q'_2{}^e)\cdots) : Q'_t{}^e)\,. \tag{5}$$

By changing the order of evaluation of the ideal quotient by each $Q'_j{}^e$ in (5) so that the ideal quotient by $Q_i'^e$ is evaluated lastly, we obtain

$$\left(Q_i{}^e : \prod_{j=1}^t Q'_j{}^e\right) = (Q_i{}^e : Q_i'^e)\,,$$

as $(Q_i^e : Q'_j{}^e) = Q_i^e$ for $j \neq i$ by Lemma 2.4. We note that $Q'_j{}^e \not\subset P_i^e$ for $j \neq i$.

Since $Q_i^{ec} = Q_i$ and $Q_i'^{ec} = Q'_i$, it follows that if $Q_i = Q'_i$, then we have $Q_i{}^e = Q_i'^e$ and

$$(Q_i{}^e : Q_i'^e) = \mathbb{F}_q(Y)[X \setminus Y]\,. \tag{6}$$

Also, if $Q_i \subsetneq Q'_i$, then we have $Q_i{}^e \subsetneq Q_i'^e$ and

$$P_i^e \supset (Q_i{}^e : Q_i'^e) \supsetneq Q_i{}^e\,, \tag{7}$$

by Lemma 2.4. Thus, gathering the results (6) and (7) in the above, we obtain

$$\left(I : \bigcap_{i=1}^t Q'_i\right)^e = \bigcap_{i=1}^t (Q_i{}^e : Q_i'^e) = \bigcap_{i:Q_i \neq Q'_i} (Q_i{}^e : Q_i'^e)\,. \tag{8}$$

Next we evaluate the contraction of of (8). Then we have

$$\left(I : \bigcap_{i=1}^t Q'_i\right)^{ec} = \left(\left(I : \bigcap_{i=1}^t Q'_i\right)^e\right)^c = \left(\bigcap_{i:Q_i \neq Q'_i} (Q_i{}^e : Q_i'^e)\right)^c = \bigcap_{i:Q_i \neq Q'_i} (Q_i{}^e : Q_i'^e)^c$$

by Lemma 2.6. Since $(Q_i{}^e : Q_i'^e)^c = (Q_i : Q'_i)^{ec} = (Q_i : Q'_i)$, we have

$$\left(I : \bigcap_{i=1}^t Q'_i\right) = \left(I : \bigcap_{i=1}^t Q'_i\right)^{ec} = \bigcap_{i=1}^t (Q_i : Q'_i) = \bigcap_{i:Q_i \neq Q'_i} (Q_i : Q'_i)\,.$$

□

We can extend Proposition 2.8 as follows.

PROPOSITION 2.9. *Suppose that Q'_i is a P_i-primary ideal and $Q_i \subset Q'_i$ for each i. Let $\lambda_0 = \{1, 2, \dots, t\}$ and λ_1, λ_2 subsets of λ_0. Then we have $(\bigcap_{i\in\lambda_1} Q_i : \bigcap_{i\in\lambda_2} Q'_i)^{ec} = (\bigcap_{i\in\lambda_1} Q_i : \bigcap_{i\in\lambda_2} Q'_i)$ and*

$$\left(\bigcap_{i\in\lambda_1} Q_i : \bigcap_{i\in\lambda_2} Q'_i\right) = \left(\bigcap_{i\in\lambda_1\setminus\lambda_2} Q_i\right) \cap \left(\bigcap_{i\in\lambda_1\cap\lambda_2 : Q_i\neq Q'_i} (Q_i : Q'_i)\right).$$

Proof. We consider non-empty λ_1 and λ_2. We use the same argument used in the proof of Proposition 2.8. Since Y is a common maximal independent set of all Q_i and Q'_i, $Q_i{}^{ec} = Q_i$ and $Q'^{ec}_i = Q'_i$. By Lemma 2.6, we have

$$\left(\bigcap_{i\in\lambda_1} Q_i : \bigcap_{i\in\lambda_2} Q'_i\right)^{ec} = \left(\bigcap_{i\in\lambda_1} Q_i : \bigcap_{i\in\lambda_2} Q'_i\right).$$

Then we evaluate $(\bigcap_{i\in\lambda_1} Q_i : \bigcap_{i\in\lambda_2} Q'_i)^e$. By the argument used in the proof of Proposition 2.8, it follows that

$$\left(\bigcap_{i\in\lambda_1} Q_i : \bigcap_{i\in\lambda_2} Q'_i\right)^{e} = \bigcap_{i\in\lambda_1}\left(Q_i^e : \prod_{j\in\lambda_2} Q'^{\,e}_j\right).$$

On the other hand, each $(Q_i^e : \prod_{j\in\lambda_2} Q'^{\,e}_j)$ can be evaluated in the same manner as in the proof of Proposition 2.8 as follows:

$$\left(Q_i^e : \prod_{j\in\lambda_2} Q'^{\,e}_j\right) = \begin{cases} Q_i^e & (i \in \lambda_1 \setminus \lambda_2)\,, \\ \mathbb{F}_q(Y)[X \setminus Y] & (i \in \lambda_1 \cap \lambda_2,\ Q_i = Q'_i)\,, \\ (Q_i^e : Q'^{e}_i) & (i \in \lambda_1 \cap \lambda_2,\ Q_i \neq Q'_i)\,. \end{cases}$$

Thus, we obtain

$$\left(\bigcap_{i\in\lambda_1} Q_i : \bigcap_{i\in\lambda} Q'_i\right)^{e} = \left(\bigcap_{i\in\lambda_1\setminus\lambda_2} Q_i^e\right) \cap \left(\bigcap_{i\in\lambda_1\cap\lambda_2 : Q_i\neq Q'_i} (Q_i^e : Q'^{e}_i)\right).$$

To evaluate its contraction, we can apply the argument in the proof of Proposition 2.8 and obtain

$$\left(\bigcap_{i\in\lambda_1} Q_i : \bigcap_{i\in\lambda} Q'_i\right) = \left(\bigcap_{i\in\lambda_1} Q_i : \bigcap_{i\in\lambda} Q'_i\right)^{ec} = \left(\bigcap_{i\in\lambda_1\setminus\lambda_2} Q_i\right) \cap \left(\bigcap_{i\in\lambda_1\cap\lambda_2 : Q_i\neq Q'_i} (Q_i : Q'_i)\right).$$

□

Replacing ideal quotient with saturation in Proposition 2.9, we have the following.

PROPOSITION 2.10. *Suppose that Q'_i is a P_i-primary ideal and $Q_i \subset Q'_i$ for each i. Let $\lambda_0 = \{1, 2, \dots, t\}$ and λ_1, λ_2 subsets of λ_0. Then the saturation of $\bigcap_{i\in\lambda_1} Q_i$ with respect to $\bigcap_{i\in\lambda_2} Q'_i$ coincides with $\bigcap_{i\in\lambda_1\setminus\lambda_2} Q_i$. That is, we have*

$$\left(\bigcap_{i\in\lambda_1} Q_i : (\bigcap_{i\in\lambda_2} Q'_i)^{\infty}\right) = \bigcap_{i\in\lambda_1\setminus\lambda_2} Q_i\,.$$

Proof. We set $I_1 = \bigcap_{i\in\lambda_1} Q_i$ and $I_2 = \bigcap_{i\in\lambda_2} Q'_i$. Then, as shown in the proof of Proposition 2.9, we have $I_1^{ec} = I_1$, $I_2^{ec} = I_2$ and $(I_1 : I_2^k)^{ec} = (I_1 : I_2^k)$ for any positive integer k by using Lemma 2.6.

When $k = 1$, in Proposition 2.9 we have shown

$$(I_1 : I_2) = \Bigg(\bigcap_{i\in\lambda_1\setminus\lambda_2} Q_i\Bigg) \cap \Bigg(\bigcap_{i\in\lambda_1\cap\lambda_2 : Q_i\neq Q'_i} (Q_i : Q'_i)\Bigg).$$

For each positive integer k, by using the fact that $(I_1 : I_2^k) = ((I_1 : I_2^{k-1}) : I_2)$ and applying the argument in the proof of Proposition 2.9 repeatedly, it follows that

$$(I_1 : I_2^k) = \Bigg(\bigcap_{i\in\lambda_1\setminus\lambda_2} Q_i\Bigg) \cap \Bigg(\bigcap_{i\in\lambda_1\cap\lambda_2 : Q_i\neq Q'_i} (Q_i : Q_i'^k)\Bigg).$$

Consider the case $Q_i \neq Q'_i$. Since Q_i and $Q_i'^k$ are P_i-primary ideals, there exists a positive integer d_i such that $P_i^{d_i} \subset Q_i$ and we have $Q_i'^{d_i} \subset Q_i$. Thus, for any integer $k \geq d_i$ we obtain

$$(Q_i : Q_i'^k) = \mathbb{F}_q[X].$$

Finally, for sufficiently large k it follows that

$$(I_1 : I_2^k) = \bigcap_{i\in\lambda_1\setminus\lambda_2} Q_i,$$

which implies $(I_1 : I_2^\infty) = \bigcap_{i\in\lambda_1\setminus\lambda_2} Q_i$. □

3. Distinct Nilpotency Decomposition

In this section, we show a concrete method for the DND for a given ideal. We begin by showing a method for the radical part decomposition which can be considered as the first step of the DND.

3.1. Computation of Radical Part Decomposition

The radical part decomposition of I, that is, computation of $r_0(I)$ and $nr_0(I)$, can be done by computation of one "inverse image of Frobenius map", that of two ideal quotients and that of one saturation.

PROPOSITION 3.1. *$(I : I^{(1)}) = \bigcap_{i=s+1}^t (Q_i : Q_i^{(1)})$ and $(I : I^{(1)})^{ec} = (I : I^{(1)})$ hold.*

Proof. By Lemma 2.7 and Lemma 2.6, we have $(I : I^{(1)})^{ec} = (I : I^{(1)})$. Also, by Lemma 2.5, we have ${Q_i}^{(1)} = Q_i = P_i$ for $1 \leq i \leq s$ and ${Q_i}^{(1)} \supsetneq Q_i$ for $s+1 \leq i \leq t$. Then by replacing Q'_i with $Q_i^{(1)}$ in Proposition 2.8, where $Q'_i = Q_i$ for $1 \leq i \leq s$ and $Q'_i \neq Q_i$ for $s+1 \leq i \leq t$, it follows that

$$(I : I^{(1)}) = \bigcap_{i=s+1}^{t} (Q_i : Q_i^{(1)}) .$$

□

Next we set $J_1(I) = (I : I^{(1)})$ and consider the saturation of I with respect to $J_1(I)$.

THEOREM 3.2. *$(I : J_1(I)^\infty)$ coincides with $r_0(I)$.*

Proof. By Lemma 2.5 $(Q_i : {Q_i}^{(1)})$ is a P_i-primary ideal properly containing Q_i for $s + 1 \leq i \leq t$. By setting $\lambda_1 = \{1, 2, \dots, t\}$, $\lambda_2 = \{s + 1, \dots, t\}$ and $Q'_i = (Q_i : Q_i^{(1)})$ for $s + 1 \leq i \leq t$ in Proposition 2.10, we have

$$(I : J_1(I)^\infty) = \bigcap_{i=1}^{s} Q_i = r_0(I) .$$

□

Once we have obtained $r_0(I)$, we can compute $nr_0(I)$ by ideal quotient computation.

THEOREM 3.3. *$nr_0(I)$ coincides with $(I : r_0(I))$.*

Proof. As $r_0(I) = \bigcap_{i=1}^{s} Q_i$, we have $r_0(I)^{ec} = r_0(I)$ by Lemma 2.6. Then, also by Lemma 2.6, we have $(I : r_0(I))^{ec} = (I : r_0(I))$. Setting $\lambda_1 = \{1, 2, \dots, t\}$, $\lambda_2 = \{1, \dots, s\}$ and $Q'_i = Q_i$ for $1 \leq i \leq s$ in Proposition 2.9, it follows that

$$(I : r_0(I)) = \left(\bigcap_{i=1}^{s}(Q_i : Q_i)\right) \cap \left(\bigcap_{i=s+1}^{t} Q_i\right) = \bigcap_{i=s+1}^{t} Q_i = nr_0(I) .$$

□

Also by using a similar argument as in the proof of Theorem 3.3 based on Proposition 2.9, we have the following.

PROPOSITION 3.4. *$\varphi_p^{-1}(nr_0(I))$ coincides with $(I^{(1)} : r_0(I))$.*

Following our notation, we write $nr_0(I)^{(1)}$ for $\varphi_p^{-1}(nr_0(I))$. Although this ideal does not appear in the DND of I, it can be used effectively for computation of the DND.

Thus, it is shown that the radical part decomposition of I can be done by computation of one "inverse image of Frobenius map", that of two ideal quotients and that of one saturation. Applying this computation repeatedly, we have a total method for computing the DND.

3.2. Computation of DND

Here we show that the DND of I can be computed by applying the method in the previous subsection for the radical part decomposition repeatedly. For describing our method, we redefine $\mathcal{R}_k(I)$ in a different form.

LEMMA 3.5. *For each positive integer k, $\mathcal{R}_k(I)$ consists of all primary component Q_i such that $\varphi_p^{1-k}(Q_i) \neq P_i$ and $\varphi_p^{-k}(Q_i) = P_i$.*

Proof. Consider a primary component Q_i in $\mathcal{R}_k(I)$. By the definition of $\mathcal{R}_k(I)$, g^{p^k} belongs to Q_i for any element g in $P_i = \sqrt{Q_i}$ and there exists some element h in P_i such that $h^{p^{k-1}} \notin Q_i$. This implies that $P_i \subset \varphi_p^{-k}(Q_i)$ but $P_i \not\subset \varphi_p^{-k+1}(Q_i)$. Since $\varphi_p^{-k}(Q_i)$ is a P_i-primary ideal by Lemma 2.5, we have $P_i = \varphi_p^{-k}(Q_i)$.

It can be shown in a similar manner that for any primary component Q_i such that $P_i \subset \varphi_p^{-k}(Q_i)$ but $P_i \not\subset \varphi_p^{-k+1}(Q_i)$, Q_i belongs to $\mathcal{R}_k(I)$. □

Now we consider the radical part decomposition of I described in the previous subsection as the *first round* of recursive structure of the DND computation. Then we will show the second round and k-th round in the below. We denote $\varphi_p^{-k}(nr_0(I))$ by $nr_0(I)^{(k)}$.

SECOND ROUND: By Lemma 2.2 we have

$$nr_0(I)^{(1)} = \bigcap_{i=s+1}^{t} \varphi_p^{-1}(Q_i) = \bigcap_{i=s+1}^{t} Q_i^{(1)},$$

$$nr_0(I)^{(2)} = \bigcap_{i=s+1}^{t} \varphi_p^{-2}(Q_i) = \bigcap_{i=s+1}^{t} Q_i^{(2)}.$$

Now we let $J_2(I) = (nr_0(I)^{(1)} : nr_0(I)^{(2)})$.

PROPOSITION 3.6. *$J_2(I) = \bigcap_{i\in\{s+1,\ldots,t\}:Q_i^{(1)}\neq Q_i^{(2)}}(Q_i^{(1)} : Q_i^{(2)})$ and $J_2(I)^{ec} = J_2(I)$ hold.*

Proof. By Lemma 2.5, $Q_i^{(1)}$ is a P_i-primary ideal. Also by Proposition 2.1, $Q_i^{(1)} = P_i$ holds if and only if $Q_i^{(1)} = Q_i^{(2)}$.

Now we consider the radical part decomposition of $nr_0(I)^{(1)}$. Then, we can apply Proposition 2.9, where we replace Q_i and Q_i' with $Q_i^{(1)}$ and $Q_i^{(2)}$, respectively, and set $\lambda_1 = \lambda_2 = \{s+1, \ldots, t\}$ to show the statements of the proposition. □

We remark that for computation $nr_0(I)^{(1)}$ we can do it efficiently by $nr_0(I)^{(1)} = (I^{(1)} : r_0(I))$. (See Proposition 3.4.) Also, $nr_0(I)^{(2)}$ can be computed by the inverse image of the Frobenius map of $nr_0(I)^{(1)}$, that is, $nr_0(I)^{(2)} = \varphi_p^{-1}(nr_0(I))^{(1)}$.

Next we consider the saturation of $nr_0(I)$ with respect to $J_2(I)$. Then, by Proposition 2.10, we have the following.

PROPOSITION 3.7. *$(nr_0(I) : J_2(I)^\infty) = \bigcap_{i\in\{s+1,\ldots,t\}:Q_i^{(1)}=P_i} Q_i$ and $(nr_0(I) : J_2(I)^\infty)^{ec} = (nr_0(I) : J_2(I)^\infty)$ hold.*

By Propositions 3.6 and 3.7 and Lemma 3.5, we can compute the decomposition $nr_0(I) = r_1(I) \cap nr_1(I)$ as follows:

THEOREM 3.8. *$r_1(I)$ coincides with $(nr_0(I) : J_2(I)^\infty)$ and $nr_1(I)$ coincides with $(nr_0(I) : r_1(I)) = (nr_0(I) : r_1(I)^\infty)$.*

Proof. By Proposition 3.7, $(nr_0(I) : J_2(I)^\infty)$ is the intersection of primary components Q_i such that $\varphi_p^{-1}(Q_i) \neq P_i$ and $\varphi_p^{-2}(Q_i) = P_i$. Then, by Lemma 3.5, those components Q_i belong to $\mathcal{R}_1(I)$, that is, the degree of nilpotency $nil(Q_i)$ is greater than 1 but not greater than p. Thus, we have $r_1(I) = (nr_0(I) : J_2(I)^\infty)$.

Also by Proposition 2.9, $nr_1(I)$ coincides with the saturation of $nr_1(I)$ with respect to $r_1(I)$. □

By the same argument as in Proposition 3.4, we have the following on $nr_1(I)^{(2)}(= \varphi_p^{-2}(nr_1(I)))$.

PROPOSITION 3.9. *$\varphi_p^{-2}(nr_1(I))$ coincides with $(nr_0(I)^{(2)} : r_1(I))$.*

As $nr_0(I)^{(2)}$ and $r_1(I)$ are already computed, we obtain $nr_1(I)^{(2)}$ by ideal quotient of already computed ideals. By this way, we may avoid unnecessary computation of inverse image of Frobenius map. See Remark 4.2 for computational aspect.

$(K-1)$-TH ROUND: For each positive integer k, we can compute the decomposition $nr_{k-1}(I) = r_k(I) \cap nr_k(I)$ by the same manner as in the second round.

Now we assume that $nr_{k-1}(I) = r_k(I) \cap nr_k(I)$ is already computed for some $k \geq 1$. We denote $\varphi_p^{-k-1}(nr_k(I))$ and $\varphi_p^{-k-2}(nr_k(I))$ by $nr_k(I)^{(k+1)}$ and $nr_k(I)^{(k+2)}$, respectively. Then, by Lemma 2.2, we have

$$\begin{aligned} nr_k(I)^{(k+1)} &= \bigcap_{Q_i \in \mathcal{N}R_k(I)} \varphi_p^{-k-1}(Q_i) = \bigcap_{Q_i \in \mathcal{N}R_k(I)} Q_i^{(k+1)} \\ nr_k(I)^{(k+2)} &= \bigcap_{Q_i \in \mathcal{N}R_k(I)} \varphi_p^{-k-2}(Q_i) = \bigcap_{Q_i \in \mathcal{N}R_k(I)} Q_i^{(k+2)}. \end{aligned}$$

Also we set $J_{k+2}(I) = (nr_k(I)^{(k+1)} : nr_k(I)^{(k+2)})$.

Corresponding to Proposition 3.6, we have the following proposition by using the same argument as in used in the proof of Proposition 3.6.

PROPOSITION 3.10. *$J_{k+2}(I) = \bigcap_{Q_i \in \mathcal{N}R_k(I) : Q_i^{(k+1)} \neq Q_i^{(k+2)}} (Q_i^{(k+1)} : Q_i^{(k+2)})$ and ${J_{k+2}}^{ec} = J_{k+2}$ hold.*

Proof. By Lemma 2.5, $Q_i^{(k+1)}$ is a P_i-primary ideal and also $Q_i^{(k+1)} = P_i$ if and only if $Q_i^{(k+1)} = Q_i^{(k+2)}$.

Now we consider the radical part decomposition of $n_k(I)^{(k+1)}$. Samely as in the proof of Proposition 3.6, we can apply Proposition 2.9, where we replace Q_i and Q_i' with $Q_i^{(k+1)}$ and $Q_i^{(k+2)}$, respectively, and set $\lambda_1 = \lambda_2 = \{i \mid Q_i \in \mathcal{N}R_k(I)\}$. □

Also, corresponding to Proposition 3.7, we have the following saturations with respect to $J_{k+2}(I)$.

PROPOSITION 3.11. *$(nr_k(I) : J_{k+2}(I)^{\infty}) = \bigcap_{Q_i \in \mathcal{N}R_k(I) Q_i^{(k+1)} = P_i} Q_i$ and $(nr_0(I) : J_{k+2}(I)^{\infty})^{ec} = (nr_0(I) : J_{k+2}(I)^{\infty})$ hold.*

By Propositions 3.11, $(nr_0(I) : J_{k+2}(I)^{\infty})$ is the intersection of primary components Q_i of I such that $\varphi_p^{-k}(Q_i) \neq P_i$ and $\varphi_p^{-k-1}(Q_i) = P_i$. Then, by Lemma 3.5, those components Q_i belongs to $\mathcal{R}_{k+1}(I)$, that is, $nil(Q_i)$ is greater than p^k but not greater than p^{k+1}. Thus, we have $r_{k+1}(I) = (nr_0(I) : J_{k+2}(I)^{\infty})$ and the following corresponding to Theorem 3.8. (From $r_{k+1}(I)$, we can compute $nr_{k+1}(I)$ by saturation computation.)

THEOREM 3.12. *$r_{k+1}(I)$ coincides with $(nr_k(I) : J_{k+2}(I)^{\infty})$ and $nr_{k+1}(I)$ coincides with $(nr_k(I) : r_{k+1}(I)) = (nr_k(I) : r_{k+1}(I)^{\infty})$*

Thus, we can compute the decomposition $nr_k(I) = r_{k+1}(I) \cap nr_{k+2}(I)$ by ideal quotient and saturation. When $nr_k(I) = r_{k+1}(I)$ holds, the whole computation is completed and we have the DND of I:

$$I = r_0(I) \cap \cdots \cap r_{k+1}(I)\,.$$

As to $nr_{k+1}(I)^{(k+2)}(= \varphi_p^{-k-2}(nr_{k+1}(I)))$, we also compute it by ideal quotient of already computed ideals as the same manner as in Proposition 3.9.

PROPOSITION 3.13. *$\varphi_p^{-k-2}(nr_{k+1}(I))$ coincides with $(nr_k(I)^{(k+2)} : r_{k+1}(I))$.*

4. Computational Details and Examples

In this section, we give computational details on inverse image of Frobenius map, ideal quotient and saturation and some examples for making the details of the method very clear.

4.1. Inverse Frobenius Map and Ideal Quotient

We begin by showing a concrete method for inverse image of Frobenius map.

INVERSE IMAGE OF FROBENIUS MAP: Computation of the inverse image of Frobenius map ϕ_p consists of that of ϕ_v and that of ϕ_c, as $\phi_p^{-1}(L) = \phi_c^{-1}(\phi_v^{-1}(L)) = \phi_v^{-1}(\phi_c^{-1}(L))$ for an ideal L of $\mathbb{F}_q[X]$. Here we show a method given in [12].

For computation of the inverse image of ϕ_v of an ideal L, we provide new n variables $y_1, \dots, y_n$ and consider ideals of a polynomial ring $\mathbb{F}_q[X \cup Y]$ in $2n$ variables, where we set $Y = \{y_1, \dots, y_n\}$. In $\mathbb{F}_q[X \cup Y]$ we consider the ideal $F(L)$ which is generated by $L \cup \{x_1^p - y_1, x_2^p - y_2, \dots, x_n^p - y_n\}$. (Actually $F(L)$ is generated by a given generating set of L and $\{x_1^p - y_1, x_2^p - y_2, \dots, x_n^p - y_n\}$.) Moreover, we fix an *elimination order* $\prec$ with $\{y_1, \dots, y_n\} \prec\prec \{x_1, \dots, x_n\}$. Then we have the following. (See Chapter 2 in [1] or [12].)

PROPOSITION 4.1. *The elimination ideal $\mathbb{F}_q[Y] \cap F(L)$ coincides with the ideal $\varphi_v^{-1}(L)$ with y_i replaced by x_i for each i. Moreover, for a Gröbner basis G_0 of $F(L)$ with respect to the elimination order $\prec$, $G_0 \cap \mathbb{F}_q[Y]$ with y_i replaced by x_i is a Gröbner basis of $\varphi_v^{-1}(L)$.*

For computation of the inverse image of ϕ_c of an ideal L, we use the property that the restriction $\phi_c|_{\mathbb{F}_q}$ of ϕ_c on $\mathbb{F}_q$ is a field automorphism and its inverse can be computed easily as follows:

$$(\phi_c|_{\mathbb{F}_q})^{-1} : \mathbb{F}_q \ni \alpha \mapsto \alpha^{q/p} \in \mathbb{F}_q\,.$$

We note that $\alpha^q = \alpha$ for any α in $\mathbb{F}_q$. Then, we have

$$\phi_c^{-1} : \mathbb{F}_q[X] \ni \sum a_{e_1,\dots,e_n} x_1^{e_1} \cdots x_n^{e_n} \mapsto \sum a_{e_1,\dots,e_n}^{q/p} x_1^{e_1} \cdots x_n^{e_n} \in \mathbb{F}_q[X]\,.$$

Thus, for a given generator $\{g_1, \dots, g_m\}$ of L, $\phi_c^{-1}(L)$ is computed as an ideal generated by $\{\phi_c^{-1}(g_1), \dots, \phi_c^{-1}(g_m)\}$.

REMARK 4.2. As to the computational efficiency of the inverse image of Frobenius map φ_p^{-d}, the size p^d effects very much. When d becomes large, its computation becomes very difficult. However, even though d increases during the DND computation, ideals for which inverse images are computed become "large", which means those Gröbner basis computation tend to be efficiently done. Moreover, during the DND computation, for each k-th round, we can utilize the ideal $nr_k^{(k+1)}(I)$, which can be computed by ideal quotient of already computed ideals, for computation of the inverse image $\varphi_p^{-k-2}(nr_k(I))$, since $\varphi_p^{-k-2}(nr_k(I)) = \varphi_p^{-1}(nr_k^{(k+1)}(I))$.

IDEAL QUOTIENT: Next we show two typical methods for ideal quotient. (See [14, 10] for details.)

For two ideals I_1, I_2 of $\mathbb{F}_q[X]$, the ideal quotient $(I_1 : I_2)$ can be computed by the following methods. Here we assume that I_2 is generated by $H = \{h_1, \ldots, h_s\}$, that is, $I_2 = \langle H\rangle = \langle h_1, \ldots, h_s\rangle$.

(Method 1) As I_2 is generated by H, it follows that

$$(I_1 : I_2) = \bigcap_{i=1}^{s}(I_1 : h_i) \tag{9}$$

Then, the computation of the ideal quotient can be reduced to that of ideal intersection and that of *ideal quotient in special case*, that is, "ideal quotient by principal ideal". See [14, 10] for computational details on ideal intersection.

Thus, we assume that I_2 is a principal ideal generated by a polynomial h. Then, it is easily shown that a generating set of the ideal $I_1 \cap \langle h\rangle$ is of form $\{g_1 h, \ldots, g_t h\}$. From this generating set, we have $(I_1 : h) = \langle g_1, \ldots, g_t\rangle$.

(Method 2) We can compute the ideal quotient more simply. Let y be a new variable and consider a polynomial ring $\mathbb{F}_q[X \cup \{y\}]$ in $n + 1$ variables. Also we set

$$h = h_1 + h_2 y + \cdots + h_s y^{s-1}\,. \tag{10}$$

Then, we have

$$(I_1 : I_2) = (I \cdot \mathbb{F}_q[X \cup \{y\}] : h) \cap \mathbb{F}_q[X]\,,$$

where $I \cdot \mathbb{F}_q[X \cup \{y\}]$ is the ideal of $\mathbb{F}_q[X \cup \{y\}]$ generated by I. Thus, the computation the ideal quotient $(I_1 : I_2)$ is reduced to that of *ideal quotient in special case* and that of *elimination ideal*.

In fact, we first compute the ideal quotient $(I \cdot \mathbb{F}_q[X \cup \{y\}] : h)$ by Method 1, and then we compute its elimination ideal with respect to an elimination order $X \prec\prec \{y\}$.

REMARK 4.3. In the ideal intersection computation in (9) we can omit $(I_1 : h_i)$ if $h_i \in I_1$, since $(I_1 : h_i) = \mathbb{F}_q[X]$ holds for such a case. Also, for construction (10) of h, we can omit all elements $h_i \in I_1$, by which we have a smaller expression of h and improve the efficiency of the computation $(I_1 : I_2)$.

There are cases where such omissions appear. Especially, in algebraic factorization of polynomials, which is considered as a special type of prime decomposition, ideals contain a prime ideal which describes an algebraic extension over a rational function field as those elimination ideals. For such ideals, there are many common elements in their generating sets which are corresponding to generators for the common prime ideal, and we can omit those for ideal quotient computation. See Example 2 for such a case.

SATURATION: Finally we show some typical methods for saturation. (See [3, 10, 14] for details.)

(Method 3) First we show a special method for a saturation with respect to an element (a principal ideal). In this case, the computation of saturation can be reduced to that of elimination ideal.

Suppose that I_2 is a principal ideal generated by a polynomial h. Then, providing a new variable z, we consider a polynomial ring $\mathbb{F}_q[X \cup \{z\}]$ in $n+1$ variables, and its ideal $\hat{I}_1$ generated by I_1 and $zh-1$. That is, $\hat{I}_1 = \langle I_1 \cup \{zh-1\}\rangle$. Then, it can be shown that $\hat{I}_1 \cap \mathbb{F}_q[X] = (I_1 : h^\infty)$.

Now we show two general methods for saturation.

(Method 4) We compute the saturation $(I_1 : I_2^\infty)$ by repeating corresponding ideal quotient computation as follows: Compute the ascending chain of ideal quotients till it stops, that is, $(I_1 : I_2^d) = (I_1 : I_2^{d+1})$ holds.

$$I_1 = (I_1 : I_2^0) \subset (I_1 : I_2) \subset (I_1 : I_2^2) = ((I_1 : I_2) : I_2) \subset \cdots$$

Then, by the definition of *saturation*, we have $(I_1 : I_2^d) = (I_1 : I_2^\infty)$.

(Method 5) We compute the saturation at once by using the same idea used in Method 2. Suppose that I_2 is generated by $H = \{h_1, \dots, h_s\}$. Then we introducing new variables y, z and consider a polynomial ring $\mathbb{F}_q[X \cup \{y, z\}]$ in $n+2$ variables. Let h be a polynomial expressed in the formula (10). Then we have

$$(I_1 : I_2^\infty) = (\langle I \cup \{z-h\}\rangle : z^\infty) \cap \mathbb{F}_q[X]\,.$$

Thus, for computation of $(\langle I \cup \{z-h\}\rangle : z^\infty)$, we apply Method 3 and by elimination ideal computation, we obtain $(\langle I \cup \{z-h\}\rangle : z^\infty) \cap \mathbb{F}_q[X]$.

4.2. Examples

Here we give two examples for making computational behaviors of proposed method clear.

EXAMPLE 1. First we show a simpler case, where the given ideal is principal. In this case, each primary component is also principal and its degree of nilpotency coincides with the multiplicity of its generator.

Suppose that an ideal I is generated by a polynomial f in $\mathbb{F}_3[x, y, z]$ and

$$f = (x^2+y+z)^3(x+2y+z^2)(x^2y+zx+y^3)^2$$

In order to make our computation very clear, for each principal ideal, its generator is written *in a factorized form*.

Then, $I^{(1)}$ is computed by the method based on elimination ideal computation and its reduced Gröbner basis consists of one element g, where

$$g = (x^2+y+z)(x+2y+z^2)(x^2y+zx+y^3)\,.$$

We note that $I^{(1)} = I^{(2)}$ in this case and $\langle g\rangle$ coincides with the radical $\sqrt{I}$.

By Method 1, we compute the reduced Gröbner basis of the ideal quotient $J_1(I) = (I : I^{(1)}) = (\langle f\rangle : \langle g\rangle)$. Then the Gröbner basis consists of one element h, where

$$h = (x^2+y+z)^2(x^2y+zx+y^3)\,.$$

The polynomial h coincides with the division of f by g.

Also by Method 3, we compute the radical part $r_0(I)$ by saturation computation $(I : J_1^\infty)$ and its Gröbner basis consists of one element k, where

$$k = x + 2y + z^2 .$$

Then $r_0(I) = \langle x + 2y + z^2 \rangle$.

Finally, by Method 1, we compute the reduced Gröbner basis of the non-radical part of I and

$$nr_0(I) = \langle (x + 2y + z^2)^2 (x^2 + y + z)^3 \rangle .$$

As $I^{(1)} = I^{(2)} = \sqrt{I}$, we also have $r_1(I) = nr_0(I)$.

EXAMPLE 2. Next we show an example which related to algebraic factoring.

Algebraic Factoring Problem: We consider an extension field K of a rational function field $\mathbb{F}_q(Y)$ by $K \cong \mathbb{F}_q(Y)[X]/P$, where X, Y are set of variables with $X \cap Y = \emptyset$ and P is a maximal ideal of $\mathbb{F}_q(Y)[X]$. Then, for a given polynomial $f(t)$ in $K[t]$, where t is also a new variable, we want to factor $f(t)$ over K.

This problem can be reduced to that of primary decomposition of the ideal I of $\mathbb{F}_q[X \cup Y \cup \{t\}]$ which is generated by $P \cap \mathbb{F}_q[X \cup Y]$ and $f(t)$, where we consider $f(t)$ as a polynomial in $X \cup Y \cup \{t\}$ over $\mathbb{F}_q$ by removing the denominator, if necessary. Thus, the DND of $I = \langle P \cup \{t\} \rangle$ is an intermediate decomposition of I.

Now consider $\mathbb{F}_3$, $Y = \{y_1, y_2\}$, $X = \{x_1, x_2\}$ and $P = \langle x_1^3 - y_1, x_2^9 - y_2 \rangle$. Moreover, let $f(t) = (t^3 - y_1)(t^9 - y_2)(t^3 + t - x_1)$. In fact $f(t)$ can be expressed by $(t - x_1)^3 (t - x_2)^9 (t^3 + t - x_1)$ as a polynomial in t over K.

REMARK 4.4. We note that, for polynomials $g(t), h(t)$ in $\mathbb{F}_3[X \cup Y \cup \{t\}]$, the ideal quotient $(\langle P \cup \{g(t)\} \rangle : h(t))$ can be considered as the division of $g(t)$ by $h(t)$ over $K = \mathbb{F}_3(Y)[X]/P$, and there is a polynomial $k(t)$ in $\mathbb{F}_3[X \cup Y \cup \{t\}]$ such that $(\langle P \cup \{g(t)\} \rangle : h(t)) = \langle P \cup \{k(t)\} \rangle$. For this $k(t)$, $f(t) = g(t)k(t)$ over K.

Now we compute the DND of the ideal

$$I = \langle x_1^3 - y_1, x_2^9 - y_2, (t^3 - y_1)(t^9 - y_2)(t^3 + t - x_1) \rangle$$

of $\mathbb{F}_3[y_1, y_2, x_1, x_2, t]$. By the method based on elimination ideal, we have

$$I^{(1)} = \langle x_1^3 - y_1, x_2^9 - y_2, (t - x_1)(t^3 - x_2^3)(t^3 + t - x_1) \rangle .$$

Then by Method 2 in the previous subsection, we have

$$(I : I^{(1)}) = (I : x_1^3 - y_1) \cap (I : x_2^9 - y_2) \cap (I : (t - x_1)(t^3 - x_2^3)(t^3 + t - x_1)) .$$

By Remark 4.3, the first two ideal quotients can be omitted and thus, we apply Method 1 for computing

$$J_1(I) = (I : (t - x_1)(t^3 - x_2^3)(t^3 + t - x_1)).$$

Then, $I \cap \langle (t - x_1)(t^3 - x_2^3)(t^3 + t - x_1) \rangle$ is generated by 3 elements which are divisible by $(t - x_1)(t^3 - x_2^3)(t^3 + t - x_1))$ and from those, we have

$$J_1(I) = \langle x_1^3 - y_1, x_2^9 - y_2, (t - x_2)^6 (t - x_1)^2 \rangle .$$

By Remark 4.4, $(I : (t - x_1)(t^3 - x_2^3)(t^3 + t - x_1))$ can be considered as the division of $f(t)$ by $(t - x_1)(t^3 - x_2^3)(t^3 + t - x_1)$ over $K = \mathbb{F}_3(Y)[X]/P$.

Then, we obtain the radical part $r_0(I)$ of I by $r_0(I) = (I : J_1^\infty)$, which is computed by elimination technique described in Method 3. Also by Remark 4.3, as the reduced Gröbner basis of I and that of J_1 have the first two elements in common, we omit those and thus, the saturation $(I : J_1^\infty)$ coincides with $(I : (t - x_2)^\infty (t - x_1)^\infty)$ and we can apply Method 3 for its computation. The computed reduced Gröbner basis of $r_0(I)$ consists of one element $t^3 + t - x_1$ and thus

$$r_0(I) = \langle x_1^3 - y_1, x_2^9 - y_2, t^3 + t - x_1 \rangle .$$

The non-radical part $nr_0(I)$ of I is computed by the ideal quotient $(I : r_0(I))$. But, samely as in the computation of $J_1(I)$, we have

$$(I : r_0(I)) = (I : x_1^3 - y_1) \cap (I : x_2^9 - y_2) \cap (I : t^3 + t - x_1) = (I : t^3 + t - x_1) .$$

Thus, its computation is done by Method 1 and we obtain

$$nr_0(I) = \langle x_1^3 - y_1, x_2^9 - y_2, (t^3 - y_1)(t^9 - y_2) \rangle = \langle x_1^3 - y_1, x_2^9 - y_2, (t - x_1)^3 (t - x_2)^9 \rangle .$$

In the second round, we have

$$\begin{aligned} nr_0(I)^{(1)} &= \langle x_1^3 - y_1, x_2^9 - y_2, (t - x_1)(t - x_2)^3 \rangle , \\ nr_0(I)^{(2)} &= \langle x_1^3 - y_1, x_2^9 - y_2, (t - x_1)(t - x_2) \rangle . \end{aligned}$$

Then, in a similar way as in the first round, we have

$$\begin{aligned} J_2(I) &= \langle x_1^3 - y_1, x_2^9 - y_2, (t - x_2)^2 \rangle , \\ r_1(I) &= (nr_0(I) : J_2(I)^\infty) = (nr_0(I) : (t - x_2)^\infty) \\ &= \langle x_1^3 - y_1, x_2^9 - y_2, (t - x_1)^3 \rangle . \end{aligned}$$

Finally, we obtain

$$nr_1(I) = (nr_0(I) : r_1(I)) = (nr_0(I) : (t - x_1)^3) = \langle x_1^3 - y_1, x_2^9 - y_2, (t - x_2)^9 \rangle .$$

And, by computation of $\varphi_3^{-2}(nr_1(I))$, we have $r_2(I) = nr_1(I)$.

5. Concluding Remarks

In this paper we have shown that an intermediate decomposition of an ideal named *distinct nilpotency decomposition (DND)* related to degree of nilpotency can be computed by combining computation of inverse image of Frobenius map and that of basic ideal operations such as ideal quotient and saturation. The notion *distinct nilpotency decomposition* and its computation are derived by revisiting Matsumoto's method [12] for computation of the radical of an ideal based on computation of inverse image of Frobenius map. The method for the DND proposed in the paper has the following features;

(1) During radical computation along with Matsumoto's method, we obtain the DND as an intermediate decomposition.

(2) Additional computations for the DND are only basic ideal operations (ideal quotient and saturation).

As the method does not require any additional decomposition based on *factorization*, DND computation may contribute a new approach to efficient and practical prime/primary decomposition of polynomial ideals over finite fields. Because, for prime decomposition of such an ideal, when its dimension is positive, we have to execute a special treatment for resolving computational difficulty derived from "inseparability". Thus, it is expected that for many cases, we can avoid such a special treatment, which should contribute the total efficiency. Also, the prime part decomposition, which is considered as the first step of the DND, is efficiently computable and it is useful for obtaining primary components which are prime at once.

Although certain interesting property is given and *possible effectiveness* of the DND is discussed in the paper, the proposed method is merely shown to be *executable* on real computer. Therefore, as further works, the efficiency and the practicality of the DND computation should be examined both in theory and practice. To do so, improving the computational efficiency of basic ideal operations such as ideal quotient, saturation and inverse image of Frobenius map, used in the DND is very important and analysis on finding certain classes of ideals for which the DND can be efficiently applied is highly required.

Acknowledgments. The authors would like to thank Mr. Xiaoliang Li for motivating the author to revisit Matsumoto's method and for stimulating discussions.

References

[1] Adams, W. W., Loustaunau, P. (1994). *An Introduction to Gröbner Bases*. Graduate Studies in Mathematics **3**, American Mathematical Society.

[2] Atiyah, M. F., MacDonald, I. G.(1969). *Introduction to Commutative Algebra*. Addison-Wesley, Reading.

[3] Becker, T., Weispfenning, V. (1993). *Gröbner Bases*. Springer-Verlag, New York.

[4] Caboara, M., Conti, P., Traverso, C. (1997). Yet another ideal decomposition algorithm. in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-12). Lecture Notes in Computer Science* **1255**, 39–54.

[5] Decker, D., Greuel, G.-M., Pfister, P. (1999). Primary decomposition: algorithms and comparisons. in *Algorithmic Algebra and Number Theory*, Springer, 187–220.

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

[7] Fortuna E., Gianni P., Trager B. (2002). Derivations and radicals of polynomial ideals over fields of arbitrary characteristic. *J. Symb. Comp.* **33**, 609–625.

[8] Gianni, P., Trager, B. (1996). Square-free algorithms in positive characteristic. *Appl. Alg. in Eng. Comm. and Comp*, **7**, 1–14.

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

[10] Greuel, G.-M., Pfister, P. (2002). *A Singular Introduction to Commutative Algebra*. Springer-Verlag, Berlin.

[11] Kemper, G. (2002). The calculation of radical ideals in positive characteristic. *J. Symb. Comp.* **34**, 229–238.

[12] Matsumoto, R. (2001). Computing the radical of an ideal in positive characteristic. *J. Symb. Comp.* **32**, 263–271.

[13] Noro, M., Yokoyama, K. (2004). Implementation of prime decomposition of polynomial ideals over small finite fields. *J. Symb. Comp.*, **38**, 1227–1246.

[14] Vasconcelos, V. (1998). *Computational Methods in Commutative Algebra and Algebraic Geometry*. Algorithms and Computation in Mathematics **2**, Springer-Verlag, Berlin.

[15] Yokoyama, K. (2002). Prime decomposition of polynomial ideals over finite fields. in *Mathematical Software (Proceedings of ICMS2002)*, World Scientific, 217–227.

Department of Mathematics
Rikkyo University
Nishi Ikebukuro, Toshima-ku
Tokyo, 171-8501, Japan
e-mail: kazuhiro@rikkyo.ac.jp