Proceedings of the Risa Consortium
1997 pp. 11– pp. 33

Factoring Polynomials over Algebraic Extension Fields

Masayuki Noro *

HPC Research Center, FUJITSU LABORATORIES LIMITED

Kazuhiro Yokoyama †

HPC Research Center, FUJITSU LABORATORIES LIMITED

(RECEIVED 1997/7/14 REVISED 1997/11/20)

1. Introduction

We give a new method for factoring polynomials over successive extension fields over the field $\mathbb{Q}$ of rational numbers based on factorization of the norms of polynomials originally proposed by Trager [15], and apply it for computing the splitting fields of integral polynomials. In [3] we showed that using non square-free norms of polynomials improves the total efficiency of the factorizations, especially, in the computation of the splitting fields. However, in this method we cannot avoid factoring square-free norms of polynomials to guarantee the correctness of the computation, which often becomes the most dominant step in the whole. Here, to improve the efficiency of factoring square-free norms, we generalize a technique used for factoring polynomial over simple extension by Encarnación [6, 7] to work over successive extension fields. Moreover, we also extend the technique for factorization of non-square-free norms of polynomials. Combining these two improvements and other precise devices, we obtain a new method which seems practical for actual problems.

In more detail, in methods based on Trager's algorithm, the factorization of a given uni-variate polynomial f over an extension field K is reduced to the factorization of a polynomial over $\mathbb{Q}$ which is the norm of a certain polynomial derived from f. However,

*noro@para.flab.fujitsu.co.jp

†yokoyama@para.flab.fujitsu.co.jp

it tends to be very hard to factorize this norm polynomial by the ordinary Berlekamp-Hensel method, since the norm polynomial tends to have many modular factors, and thus many candidates on combinations of modular factors to be tested by trial-division. (See an estimation on the average number of modular factors of norm polynomials in [8].) To resolve this combinatorial explosion, we provide an effective criterion for valid combinations based on useful information on the decomposition of the residue class rings over the finite field corresponding to the extension field K. In [6, 7], Encarnación gave such a criterion for square-free norms of polynomials over simple extension fields.

To obtain a practical method, we give a discussion on each part of the method and we examine the quality of the method by experiment. Especially, for several algebraic factorization problems related to splitting fields the new method can compute the results much faster than the method in [3].

The paper is organized as follows. In Section 2 we provide mathematical basis on algebraic factorization and its related subjects. In section 3 we show algorithms based on criteria for valid combinations, and in Section 4 we give details on parts of algorithms. We apply the method for computing splitting fields of polynomials in Section 5, and show its efficiency by experiments on examples in Section 6. In Section 7, we discuss future works.

2. Mathematical Background

We provide necessary notions and properties related to factorization of polynomials over extension fields. Here we denote by $\mathbb{Q}$, $\mathbb{Z}$ and $GF(p)$ the field of rational numbers, the ring of rational integers and the finite field of order p, respectively. We denote by $\mathbb{Z}_p$ the ring of integers localized by a prime p, i.e. $\mathbb{Z}_p = \{a/b \mid a, b \in \mathbb{Z},\ p \not| \ b\}$, and the natural projection from $\mathbb{Z}_p$ to $GF(p)$ by ϕ_p. We use the same symbol ϕ_p for its extension from polynomial rings over $\mathbb{Z}_p$ to those over $GF(p)$. For a finite extension of fields K/F, we denote the norm of an element β in K and a polynomial f over K by $\mathrm{N}_{K/F}(\beta)$ and $\mathrm{N}_{K/F}(f)$, respectively.

From now on, we express an extension field K over $\mathbb{Q}$ as follows: Let α_i, $i = 1, \ldots, n$, be algebraic numbers such that $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ and let $K_0 = \mathbb{Q}$, $K_i = K_{i-1}(\alpha_i)$ for $1 \leq i \leq n$. Then $K_i = \mathbb{Q}(\alpha_i, \cdots, \alpha_1)$ and $K = K_n$. We assign each α_i to a variable x_i for $i = 1, \ldots, n$. For simplicity, we write $X_i = \{x_i, \ldots, x_1\}$ for $i < n$ and $X = \{x_n, \ldots, x_1\}$. Then K is represented by the residue class ring of the polynomial ring $\mathbb{Q}[X]$ factored by the kernel $\mathcal{M}$ of a ring-epimorphism from $\mathbb{Q}[X]$ to K which sends $g(x_n,\ldots,x_1)$ to $g(\alpha_n,\ldots,\alpha_1)$ for each g in $\mathbb{Q}[X]$. A *successive extension representation* of K uses the reduced Gröbner base of $\mathcal{M}$ with respect to the lexicographic order $<$ such that $x_1 < \cdots < x_n$. For each α_i, its (monic) minimal polynomial $m_{0,i}(x)$ over K_{i-1} can be treated as a polynomial in x over $\mathbb{Q}[\alpha_{i-1},\cdots,\alpha_1]$ and so by replacing α_j with x_j for $j = 1,\ldots,i-1$ and x with x_i, we have a polynomial $m_i(x_i,\ldots,x_1)$ over $\mathbb{Q}$. Then $\{m_1(x_1),\ldots,m_n(x_n,\ldots,x_1)\}$ is the reduced Gröbner base of $\mathcal{M}$ with respect to $<$, which we denote by $\mathcal{G}$. And moreover,

$$K_i = \mathbb{Q}[X_i]/(\mathcal{M} \cap \mathbb{Q}[X_i]),$$
$$\mathcal{M} \cap \mathbb{Q}[X_i] = \mathrm{Id}_{\mathbb{Q}[X_i]}(m_i,\cdots,m_1),$$

where $\mathrm{Id}_R(F)$ denotes the ideal generated by a set F in a ring R. The set $\mathcal{B} = \{x_n^{e_n}\cdots x_1^{e_1} \mid 0 \leq e_i < \deg_{x_i}(m_i)\}$ is a linear base of the *residue class ring* K over $\mathbb{Q}$ and so $[K : \mathbb{Q}] = \prod_{i=1}^n deg_{x_i}(m_i)$. The representative of each residue class is the unique normal form of elements in the class with respect to $\mathcal{G}$. That is, for a polynomial g, its normal form $\mathrm{NF}_{\mathcal{G}}(g)$ with respect to $\mathcal{G}$ represents the residue class containing g.

Now we fix a prime p such that every m_i belongs to $\mathbb{Z}_p[X]$. We call such a prime *a lucky* prime for $\mathcal{M}$. Then the ideal $Id_{GF(p)[X]}(\phi_p(m_1),\ldots,\phi_p(m_n))$ is 0-dimensional and equal to $\phi_p(\mathcal{M} \cap \mathbb{Z}_p[X])$. (See [12] for details on the luckiness.) Here we write $\mathcal{M}_p = \mathrm{Id}_{\mathbb{Z}_p[X]}(m_1,\cdots,m_n)$ and $\bar{\mathcal{M}} = \mathrm{Id}_{GF(p)[X]}(\bar{m_1},\cdots,\bar{m_n})$. We denote by $\mathrm{disc}(h)$ the discriminant of h for a univariate polynomial h.

2.1. lucky primes and minimal polynomials

First we give necessary notions and properties in a slightly general setting. (See [14] and [17].) Let $\mathcal{I}$ be a 0-dimensional ideal in $F[X]$, where F is a field.

Definition 1

For each $g \in F[X]$, the map $M_{g,\mathcal{I}}$ which multiplies each element in $F[X]/\mathcal{I}$ by g is a linear map on $F[X]/\mathcal{I}$. We call the minimal (characteristic) polynomial of $M_{g,\mathcal{I}}$ the minimal (characteristic) polynomial of g with respect to $\mathcal{I}$ *and denote it by $Min_{g,\mathcal{I}}$ ($Cha_{g,\mathcal{I}}$) (respectively).*

Lemma 2

(1) *The set of all distinct irreducible factors of $Min_{g,\mathcal{I}}$ over F coincides with that of $Cha_{g,\mathcal{I}}$.*

(2) *If $\mathcal{I}$ is a radical ideal, then $Min_{g,\mathcal{I}}$ is square-free for every $g \in F[X]$. Conversely, if $Min_{x_i,\mathcal{I}}$ is square-free for every x_i, then $\mathcal{I}$ is a radical ideal.*
(3) *If $\mathcal{I}$ is a maximal ideal in $F[X]$, then $Min_{g,\mathcal{I}}$ is irreducible over F for every $g \in F[X]$. Thus, $Cha_{g,\mathcal{I}}$ coincides with $Min_{g,\mathcal{I}}$ or its power.*

Lemma 3

(Chinese remainder theorem) *Suppose that $\mathcal{I}$ is expressed as $\mathcal{I} = \cap_{i=1}^{s}\mathcal{I}_i$ for ideals $\mathcal{I}_i$ such that* $\mathrm{Id}(\mathcal{I}_i, \mathcal{I}_j) = F[X]$ *if $i \neq j$. Then $F[X]/\mathcal{I} \cong \oplus_{i=1}^{s} F[X]/\mathcal{I}_i$. Consequently, for $g \in F[X]$, $Cha_{g,\mathcal{I}} = \prod_{i=1}^{s} Cha_{g,\mathcal{I}_i}$ and $Min_{g,\mathcal{I}} = \mathrm{LCM}(Min_{g,\mathcal{I}_1}, \ldots, Min_{g,\mathcal{I}_s})$.*

We return to our setting. Since the fixed prime p is a lucky prime, $\mathcal{M} \cap \mathbb{Z}_p[X] = \mathcal{M}_p$ and $\phi_p(\mathcal{M}_p) = \bar{\mathcal{M}}$. Moreover, since every $m_i \in \mathcal{G}$ belongs to $\mathbb{Z}_p[X]$, $\mathrm{NF}_{\mathcal{G}}(g)$ belongs to $\mathbb{Z}_p[X]$ for every $g(X) \in \mathbb{Z}_p[X]$. So, we have the natural embeddings: $\mathbb{Z}_p[X]/\mathcal{M}_p \subset \mathbb{Q}[X]/\mathcal{M}$. (See details in [12].) We consider minimal polynomials of variables. From now on, we write h_i for $Min_{x_i,\mathcal{M}}$ for $1 \leq i \leq n$. From the matrix representation of the map $M_{x_i,\mathcal{M}}$ with respect to the linear base $\mathcal{B}$, we can see that the representation is a matrix over $\mathbb{Z}_p$. Thus, its minimal polynomial and its characteristic polynomial are polynomials over $\mathbb{Z}_p$ and hence $h_i \in \mathbb{Z}_p[X]$. Moreover, we have the following linear map on $GF(p)[X]/\bar{\mathcal{M}}$:

$$M_{x_i,\bar{\mathcal{M}}} : GF(p)[X]/\bar{\mathcal{M}} \ni \bar{g} \rightarrow x_i\bar{g} \in GF(p)[X]/\bar{\mathcal{M}}.$$

Proposition 4

If $p \not| \mathrm{disc}(h_i(x))$ for every i, then $\phi_p(h_i)$ is the minimal polynomial of x_i with respect to $\bar{\mathcal{M}}$ and it is square-free for every i. Consequently, $\bar{\mathcal{M}}$ is a radical ideal.

Proof. Let M_i be the matrix representation of the linear map $M_{x_i,\mathcal{M}}$. Then $h_i(M_i) = 0$, $\phi_p(h_i)(\phi_p(M_i)) = 0$ and $\phi_p(M_i)$ coincides with the matrix representation of the map $M_{x_i,\bar{\mathcal{M}}}$ with respect to the same linear base $\mathcal{B}$. From this, the minimal polynomial $\bar{h}_i$ of $\phi_p(M_i)$ is a factor of $\phi_p(h_i)$. On the other hand,

$$Cha_{x_i,\mathcal{M}}(t) = det(tI - M_i)$$
$$Cha_{x_i,\bar{\mathcal{M}}} = \phi_p(Cha_{x_i,\mathcal{M}}) = det(tI - \phi_p(M_i)).$$

From Lemma 2 (1), irreducible factors of $\phi_p(Cha_{x_i,\mathcal{M}})$ are also those of $\bar{h}_i$. Then, the square-freeness of $\phi_p(h_i)$ implies $\bar{h}_i = \phi_p(h_i)$. ∎

Definition 5

If a lucky prime p satisfies the condition in Proposition 4, we say that p is radically lucky *for $\mathcal{M}$.*

From now on we suppose that the fixed prime p is radically lucky for $\mathcal{M}$ and that we have the following prime decomposition:

$$\bar{\mathcal{M}} = \cap_{i=1}^{s} \bar{\mathcal{M}}_i. \tag{1}$$

We denote by $\bar{L}_i$ the extension field $GF(p)[X]/\bar{\mathcal{M}}_i$ for each i. Let $\bar{\mathcal{G}}_j$ be the reduced Gröbner base of $\bar{\mathcal{M}}_j$ with respect to the lexicographic order $<$ for each j. Then

$$\bar{\mathcal{G}}_j = \{\bar{m}_{j,1}(x_1), \ldots, \bar{m}_{j,n}(x_n, \ldots, x_1)\}. \tag{2}$$

For each i, $GF(p)[X_i]/\mathrm{Id}_{GF(p)[X_i]}(\bar{m}_{j,1}, \ldots, \bar{m}_{j,i})$ is an extension field, over which $\bar{m}_{j,i+1}$ is an irreducible factor of $\bar{m}_{i+1}$.

2.2. norms and characteristic polynomials

We recall relations between the norms of polynomials and the characteristic polynomials. (We omit easy proofs.) Consider an element g in K. Here, by the expression of K, we regard g as a polynomial $g(x_1, \ldots, x_n)$. Then,

$$\mathrm{N}_{K/\mathbb{Q}}(g) = \mathrm{res}_{x_1}(\cdots \mathrm{res}_{x_n}(g, m_n) \cdots m_1),$$

where res_x denotes the resultant with respect to x. This coincides with the constant term of $Cha_{g,\mathcal{M}}$. Moreover, $Min_{g,\mathcal{M}}$ coincides with the minimal polynomial of g over $\mathbb{Q}$, and $Min_{g,\mathcal{M}}(g) = Cha_{g,\mathcal{M}}(g) = 0$.

Next consider a polynomial $g(y)$ over K monic with respect to y. Then $g(y)$ is regarded as a polynomial in $\mathbb{Q}[y, X]$ and

$$\mathrm{N}_{K/\mathbb{Q}}(g(y)) = \mathrm{res}_{x_1}(\cdots \mathrm{res}_{x_n}(g(y), m_n) \cdots m_1).$$

Let $\mathcal{I} = \mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{M}, g(y))$. Then $\{m_1, \ldots, m_n, g\}$ is the reduced Gröbner base of $\mathcal{I}$ with respect to the lexicographic order $<_y$ such that $x_1 <_y \cdots <_y x_n <_y y$ and

$$\mathrm{N}_{K/\mathbb{Q}}(g) = Cha_{y,\mathcal{I}}.$$

Moreover, if g belongs to $\mathbb{Z}_p[y, X]$, then p is a lucky prime for $\mathcal{I}$ and the following decomposition holds:

$$\bar{\mathcal{I}} = \cap_{i=1}^{s} \bar{\mathcal{I}}_i,$$

where $\bar{\mathcal{I}} = \mathrm{Id}_{GF(p)}(\bar{\mathcal{M}}, \phi_p(g))$ and $\bar{\mathcal{I}}_i = \mathrm{Id}_{GF(p)}(\bar{\mathcal{M}}_i, \phi_p(g))$. By Lemma 3, we have

$$\phi_p(\mathrm{N}_{K/\mathbb{Q}}(g)) = \prod_{i=1}^{s} Cha_{y,\bar{\mathcal{I}}_i} = \prod_{i=1}^{s} \mathrm{N}_{\bar{L}_i/GF(p)}(\phi_p(g)).$$

3. Factoring Polynomials over Extension Fields

Now we use the same notation as in Section 2. and consider a square-free polynomial $f(y, X)$ in y over K, which is monic with respect to y and belonging to $\mathbb{Z}_p[y, X]$. Let $\mathcal{I} = \mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{M}, f(y, X))$. By Section 2.2., $\mathcal{I}$ is 0-dimensional and p is a lucky prime for $\mathcal{I}$. Moreover, we have

Lemma 6

$\mathcal{I}$ is a radical ideal.

Proof. We note that a 0-dimensional ideal is a radical ideal if and only if the number of distinct zeros of the ideal coincides with the linear dimension of the residue class ring factored by the ideal. The number of distinct zeros of $\mathcal{M}$ coincides with $\dim_{\mathbb{Q}}(\mathbb{Q}[X]/\mathcal{M}) = \prod_{i=1}^{n} \deg_{x_i}(m_i)$. Since $\mathcal{M}$ is a maximal ideal, each zero of $\mathcal{M}$ is conjugate to each other by the action of the Galois group of the Galois closure of K over $\mathbb{Q}$. From this and the square-freeness of $f(y, X)$ over $\mathbb{Q}[X]/\mathcal{M}$, $f(y, \beta_1, \ldots, \beta_n)$ is square-free for any zero $(\beta_1, \ldots, \beta_n)$ of $\mathcal{M}$. Thus, the number of distinct zeros of $\mathcal{I}$ coincides with $\deg_y(f) \prod_{i=1}^{n} \deg_{x_i}(m_i) = \dim_{\mathbb{Q}} \mathbb{Q}[y, X]/\mathcal{I}$ and so $\mathcal{I}$ is radical. ∎

3.1. separating elements and decomposition of ideals

Separating elements play important roles for factorization. (See [2] or [17].)

Definition 7

We call a polynomial $g(y, X) \in \mathbb{Q}[y, X]$ a separating element *for $\mathcal{I}$, if for any pair (β, β') of distinct zeros of $\mathcal{I}$, $g(\beta) \neq g(\beta')$. Since $\mathcal{I}$ is a radical ideal, this condition is equivalent to the condition that $Min_{g,\mathcal{I}} = Cha_{g,\mathcal{I}}$.*

By [4], $g(y, X)$ is a separating element of $\mathcal{I}$ if and only if $\mathcal{J} = \mathrm{Id}_{\mathbb{Q}[z,y,X]}(\mathcal{I}, z - g(y, X))$ is in *normal position* with respect to z.

Proposition 8

Suppose that $Min_{g,\mathcal{I}}$ is factorized over $\mathbb{Q}$ as $Min_{g,\mathcal{I}} = \prod_{i=1}^{r} H_i$. Then,

$$\mathcal{I} = \cap_{i=1}^{r} \mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{I}, H_i(g(y, X))).$$

If $g(y, X)$ is a separating element, the decomposition gives the prime decomposition of $\mathcal{I}$.

Proof. We use similar arguments as in Lemma 8.5, 8.6 in [4]. It is clear that $\mathcal{I} \subset \cap_{i=1}^{r} \mathrm{Id}(\mathcal{I}, H_i(g))$. Then we show the inverse inclusion. Suppose that h belongs to $\cap_{i=1}^{r} \mathrm{Id}(\mathcal{I}, H_i(g))$. Then, for each i, h can be written as $q_i H_i(g) + s_i$ for some $q_i \in \mathbb{Q}[y, X]$ and $s_i \in \mathcal{I}$ and so $h\tilde{H}_i(g)$ belongs to $\mathcal{I}$, where $\tilde{H}_i = Min_{g,\mathcal{I}}/H_i$. Since $H_1, \ldots, H_r$ are pairwise prime univariate polynomials, $\gcd(\tilde{H}_1, \ldots, \tilde{H}_r) = 1$ and there are univariate polynomials $P_1, \ldots, P_r$ such that $1 = P_1\tilde{H}_1 + \cdots + P_r\tilde{H}_r$. Therefore, we have $h = P_1(g)\tilde{H}_1(g)h + \cdots + P_r(g)\tilde{H}_r(g)h$, and h belongs to $\mathcal{I}$. Next we show that if g is a separating element, then each $\mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{I}, H_i(g))$ is a maximal ideal. Assume, to the contrary, that $\mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{I}, H_i(g))$ has distinct prime divisors. Then the minimal polynomial of g with respect to each component must be a factor of H_i. The fact that g is a separating element implies that those minimal polynomials differ from each other and contradicts the irreducibility of H_i. ∎

The prime decomposition of $\mathcal{I}$ corresponds to the factorization of f. Let $\mathcal{I}_1, \ldots, \mathcal{I}_r$ be prime divisors of $\mathcal{I}$. Since each $\mathcal{I}_i$ is a maximal ideal and $\mathbb{Q}[y, X]/\mathcal{I}_i$ is an extension of K, the reduced Gröbner base of $\mathcal{I}_i$ with respect to $<_y$ consists of $\mathcal{G}$ and one polynomial, say f_i, which is monic with respect to y and irreducible over K. Considering zeros of f_i, f_i is an irreducible factor of f over K. Conversely, the irreducibility of f_i over K implies the maximality of the ideal $\mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{I}, f_i)$. Thus, we have

Lemma 9

There is a one to one correspondence between the set of all prime divisors of $\mathcal{I}$ and that of all irreducible factors of f over K.

Since $K(= \mathbb{Q}[X]/\mathcal{M})$ can be embedded in $\mathbb{Q}[y, X]/\mathcal{I}$ and in each $\mathbb{Q}[X]/\mathcal{I}_i$, we have the following on the GCD computation over K. Here we assume that GCDs of univariate polynomials over fields are monic.

Lemma 10

For a univariate polynomial $G(y)$ over $\mathbb{Q}$,

$$\mathrm{GCD}(f, G) \text{ over } K = \prod_{i; G(y) \in \mathcal{I}_i} f_i.$$

Proof. Since $\mathcal{I}$ is a 0-dimensional radical ideal and each $\mathcal{I}_i$ is a maximal ideal, the ideal $\mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{M}, f(y, X), G(y))$ is expressed as

$$\mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{M}, f(y, X), G(y)) = \cap_{i=1}^{r} \mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{I}_i, G(y)).$$

Also by the maximality of each $\bar{\mathcal{I}}_i$, $\mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{I}_i, G(y)) = \mathcal{I}_i$, i.e. $G(y) \in \mathcal{I}_i$, or $\mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{I}_i, G(y)) = \mathbb{Q}[y, X]$, i.e. $G(y) \notin \mathcal{I}_i$. Seeing the common roots between $G(y)$ and $f(y)$ over K and using the irreducibility of each f_i over K, $G(y) \in \mathcal{I}_i$ if and only if f_i divides $\mathrm{GCD}(f, G)$ over K. As $\mathrm{GCD}(f, G)$ is a factor of f, we have $\mathrm{GCD}(f, G) = \prod_{i;G(y)\in\mathcal{I}_i} f_i$. ∎

3.2. factorization of f

Let $F = \mathrm{N}_{K/\mathbb{Q}}(f)$, that is, $F(y) = Cha_{y,\mathcal{I}} = \mathrm{res}_{x_1}(\cdots \mathrm{res}_{x_n}(f(y, X), m_n) \cdots, m_1)$. Assume that y is a separating element for $\mathcal{I}$. Let $F_1, \ldots, F_r$ be all the irreducible factors of F over $\mathbb{Q}$. Then for each F_i, $\mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{I}, F_i)$ is a maximal ideal. Therefore, by changing indices, we can assume that $\mathcal{I}_i = \mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{I}, F_i)$, to which the irreducible factor f_i of f corresponds. By Lemma 10

$$f_i = \mathrm{GCD}(f(y), F_i(y)) \text{ over } K.$$

When y is not a separating element, we search for a separating element as follows:

Proposition 11

(See details in [17].) *For all but finitely many linear sums $z = a_1x_1 + \cdots + a_nx_n$ with $a_1, \ldots, a_n \in \mathbb{Z}$, $y + z$ are separating elements for $\mathcal{I}$.*

For each $\mathbb{Z}$-linear sum z of X, we have

$$\begin{aligned} F_z(y) &= \mathrm{N}_{K/\mathbb{Q}}(f(y - z)) = Cha_{y+z,\mathcal{I}}(y) \\ &= \mathrm{res}_{x_1}(\cdots \mathrm{res}_{x_n}(f(y - z, X), m_n) \cdots, m_1). \end{aligned}$$

Then, $y + z$ is a separating element if and only if F_z is square-free. Suppose that F_z is square-free. Then each of its irreducible factors is the characteristic polynomial $Cha_{y+z,\mathcal{I}_i}$ of $y + z$ with respect to some prime divisor $\mathcal{I}_i$. By the argument as above, it follows that

$$f_i(y - z) = \mathrm{GCD}(Cha_{y+z,\mathcal{I}_i}(y), f(y - z)) \text{ over } K.$$

This gives the theoretical base for factorization using norms proposed originally by Trager.

3.3. factorization of F

Without loss of generality, we assume that y is a separating element for $\mathcal{I}$. Usually we use some method based on Berlekamp-Hensel algorithm to factorize $F(= \mathrm{N}_{K/\mathbb{Q}}(f))$ over $\mathbb{Q}$, however, we often meet difficulty. Because $\deg(F)$ is much greater than $\deg(f)$ and F

tends to have many modular factors. Thus, we provide an efficient *criterion* for detecting invalid combinations of modular factors.

Fix a prime p which is radically lucky for $\mathcal{I}$. Then $m_1, \dots, m_n, f \in \mathbb{Z}_p[y, X]$ and $\phi_p(h_1), \dots, \phi_p(h_n)$, $\phi_p(F)$ are square-free.

Proposition 12

For each irreducible factor $g(y)$ of $f(y)$ over K, $g(y, X) \in \mathbb{Z}_p[y, X]$.

Proof. Since $m_i \in \mathbb{Z}_p[X]$ for every i, there are algebraic integers β_i's such that $\beta_i = k_i\alpha_i$ for some integer $k_i \not\equiv 0 \pmod p$. Moreover, for each root γ of $g(y, \alpha_1, \dots, \alpha_n)$, $k\gamma$ is an algebraic integer for some integer $k \not\equiv 0 \pmod p$. Then, it follows that for each coefficient c of $g(y, X)$, $k_c c$ is an algebraic integer for some integer $k_c \not\equiv 0 \pmod p$. Meanwhile, for the ring R of algebraic integers in K,

$$R \subset \frac{1}{D^d}\mathbb{Z}[\beta_1, \dots, \beta_n],$$

where $D = \prod_{i=1}^n \mathrm{N}_{K_i/\mathbb{Q}}(\mathrm{disc}(\beta_i))$ and some positive integer d. (Cf. Abbott [1] or Proposition 1 in [10].) Since the square-freeness of $\phi_p(h_i)$ implies $\mathrm{N}_{K_i/\mathbb{Q}}(\mathrm{disc}(\alpha_i)) \not\equiv 0 \pmod p$, $\mathrm{N}_{K_i/\mathbb{Q}}(\mathrm{disc}(\beta_i)) \not\equiv 0 \pmod p$ and $D \not\equiv 0 \pmod p$. Thus, we have

$$R \subset \frac{1}{E}\mathbb{Z}[\alpha_1, \dots, \alpha_n],$$

for some $E \not\equiv 0 \pmod p$. Thus, for each coefficient c of $g(y, X)$, $k_c c \in \mathbb{Z}_p[X]$ and $c \in \mathbb{Z}_p[X]$. ∎

Proposition 12 holds for any prime q which is radically lucky for $\mathcal{M}$ and $f \in \mathbb{Z}_q[X]$.

Now we compute the prime decomposition of $\bar{\mathcal{M}}$ and use the same notation as in Section 2.. (In Section 4., we will show details on the prime decomposition of $\bar{\mathcal{M}}$.) So we assume the decomposition (1) and for each component $\bar{\mathcal{M}}_i$, its Gröbner base $\bar{\mathcal{G}}_i$ with respect to $<$ is given as (2). Let $\bar{\mathcal{I}} = \mathrm{Id}_{GF(p)[y,X]}(\bar{\mathcal{M}}, \phi_p(f))$ and $\bar{L}_i = GF(p)/\bar{\mathcal{M}}_i$ for each i. Regarding $\phi_p(f)$ as a polynomial over $\bar{L}_i$, we compute the norm $\mathrm{N}_{\bar{L}_i/GF(p)}(\phi_p(f))$ by

$$\mathrm{N}_{\bar{L}_j/GF(p)}(\phi_p(f)) = \mathrm{res}_{x_1}(\cdots \mathrm{res}_{x_n}(\phi_p(f), \bar{m}_{j,n}) \cdots \bar{m}_{j,1}).$$

Next we factorize $\mathrm{N}_{\bar{L}_j/GF(p)}(\phi_p(f))$ over $GF(p)$ and let $\bar{\mathcal{F}}_j$ be the set of all its irreducible factors over $GF(p)$ for each i, $1 \le i \le s$. Since

$$\phi_p(F) = \prod_{i=1}^{s} \mathrm{N}_{\bar{L}_i/GF(p)}(\phi_p(f)),$$

the set $\bar{\mathcal{F}}$ of all irreducible factors of $\phi_p(F)$ is expressed as the disjoint union $\bar{\mathcal{F}} = \bar{\mathcal{F}}_1 \cup \cdots \cup \bar{\mathcal{F}}_s$.

Theorem 13

Let $\bar{S}$ be a subset of $\bar{\mathcal{F}}$. If the product of all elements in $\bar{S}$ is the modular image $\phi_p(G)$ of some true factor G of F, then the following relation holds:

$$\frac{\deg(G)}{[K:\mathbb{Q}]} = \deg_y(g) = \frac{\sum_{\bar{g}\in\bar{\mathcal{F}}_j\cap\bar{S}} \deg(\bar{g})}{[\bar{L}_j : GF(p)]} \quad \text{for } 1 \le j \le s, \tag{3}$$

where $g = \mathrm{GCD}(f, G)$ over K.

Proof. From the relation $G = \mathrm{N}_{K/\mathbb{Q}}(g)$, we have

$$\phi_p(G) = \prod_{i=1}^{s} \mathrm{N}_{\bar{L}_i/\mathbb{Q}}(\phi_p(g)),$$

and so

$$\deg_y(g)[K:\mathbb{Q}] = \deg(G) = \sum_{i=1}^{s} [\bar{L}_i : GF(p)] \deg_y(g). \tag{4}$$

Then, by the definition of $\mathcal{F}_i$, we have

$$\mathrm{N}_{\bar{L}_i/\mathbb{Q}}(\phi_p(g)) = \prod_{\bar{g}\in\bar{\mathcal{F}}_i\cap\mathcal{S}} \bar{g},$$

$$\deg_y(g)[\bar{L}_i : GF(p)] = \sum_{\bar{g}\in\bar{\mathcal{F}}_i\cap\mathcal{S}} \deg(\bar{g}). \tag{5}$$

Combining Equations (4) and (5), we have Equation (3). ∎

Theorem 13 gives a generalization of Encarnación 's criterion for successive extension fields. Here we present an algorithm with the criterion.

Algorithm 1 [Factorization of norms of polynomials]

Inputs: A successive extension $K/\mathbb{Q}$, a square-free polynomial $f(y)$ over K and the norm $F = \mathrm{N}_{K/Q}(f)$.

Outputs: All irreducible factors of F over $\mathbb{Q}$.

Assumption: K is given by a residue class ring $\mathbb{Q}[X]/\mathcal{M}$, where $\mathcal{M}$ is given by its Gröbner base $\mathcal{G}$, and F is square-free.

(i) Choose a prime p radically lucky for $\mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{M}, f)$.

(ii) Compute the prime decomposition of $\bar{\mathcal{M}}$, where $\bar{\mathcal{M}} = \mathrm{Id}_{GF(p)[X]}(\phi_p(\mathcal{G}))$. Let $\bar{\mathcal{M}}_j$, $j = 1, \ldots, s$, be prime divisors of $\bar{\mathcal{M}}$.

(iii) For each $\bar{\mathcal{M}}_j$, compute the set $\bar{\mathcal{F}}_j$ of all irreducible factors of $\mathrm{N}_{\bar{L}_j/GF(p)}(\phi_p(f))$, where $\bar{L}_j = GF(p)[X]/\bar{\mathcal{M}}_j$.

(iv) Find each irreducible factor of F by *lifting up and trial-division* only applying for the modular factors which satisfy Equation (3).
(v) Return all irreducible factors of F found in (iv).

3.4. non-square-free norms and their factorization

Although the factorization of the norm of a non-separating element does not give the prime decomposition of the ideal $\mathcal{I}$, it often gives some intermediate decomposition of $\mathcal{I}$ and some non-trivial factorization of f. Using these intermediate decompositions, we can improve the total efficiency of the factorization. (See [3] and [11].) Here, we give a criterion for valid combinations of modular factors of non-square-free norms. We assume that y is not a separating element. Suppose that the norm $F = \mathrm{N}_{K/\mathbb{Q}}(f)$ is factorized as

$$F = \prod_{i=1}^{r} F_i^{e_i}.$$

where each F_i is an irreducible factor of F over $\mathbb{Q}$. As $\mathcal{I}$ is a radical ideal and $Min_{y,\mathcal{I}} = \prod_{i=1}^{r} F_i$, we have

$$\mathcal{I} = \cap_{i=1}^{r} \mathrm{Id}(\mathcal{I}, F_i(y))$$

by Proposition 8. Let $\hat{f}_i = \mathrm{GCD}(F_i, f)$ over K for each i. By Lemma 10, we have a factorization of f,

$$f = \prod_{i=1}^{r} \hat{f}_i.$$

Now we show the procedure for this intermediate factorization. First we consider the square-free decomposition:

$$F = \prod_{i=1}^{u} G_i^{E_i},$$

where $E_1 < \cdots < E_u$ and G_i is the product of factors of F with multiplicity E_i for each i. Letting $\tilde{f}_i = \mathrm{GCD}(G_i, f)$ over K, the factorization of f is reduced to those of $\tilde{f}_i$'s. In this case, $\mathrm{N}_{K/\mathbb{Q}}(\tilde{f}_i) = G_i^{E_i}$ and $\deg(\tilde{f}_i) = E_i \deg(G_i)/[K : \mathbb{Q}]$.

Considering each $\tilde{f}_i$ instead of f, we can assume that $F = S^E$ with $E > 0$ without loss of generality. Then $S = Min_{y,\mathcal{I}}(y)$ and $\mathrm{Id}_{\mathbb{Q}[X]}(\mathcal{M}, f, S) = \mathcal{I}$.

Now choose a prime p radically lucky for $\mathcal{I}$. This can be done by testing the square-freeness of $\phi_p(h_i)$, $1 \le i \le n$ and $\phi_p(S)$ for randomly generated primes p. Then Proposition 12 holds for p. Compute the prime decomposition of $\bar{\mathcal{M}}$:

$$\bar{\mathcal{M}} = \cap_{i=1}^{s} \bar{\mathcal{M}}_i,$$

and let $\bar{L}_i = GF(p)[X]/\bar{\mathcal{M}}_i$ for each i. Then we factorize $\mathrm{N}_{\bar{L}_i/GF(p)}(\phi_p(f))$ over $GF(p)$ for each i. Let $\bar{\mathcal{F}}_i$ be the set of all distinct irreducible factors of $\mathrm{N}_{\bar{L}_i/GF(p)}(\phi_p(F))$ for each i. Since

$$\phi_p(S)^E = \phi_p(F) = \prod_{i=1}^{s} \mathrm{N}_{\bar{L}_i/GF(p)}(\phi_p(f))$$

the set $\bar{\mathcal{F}}$ of all distinct irreducible factors of $\phi_p(f)$ is obtained by gathering distinct factors from $\bar{\mathcal{F}}_1, \ldots, \bar{\mathcal{F}}_s$. For each $\bar{g}$ in $\bar{\mathcal{F}}$, we denote by $e_i(\bar{g})$ the multiplicity of $\bar{g}$ in $\mathrm{N}_{\bar{L}_i/GF(p)}(\phi_p(f))$. Thus, $e_i(\bar{g}) = 0$ if $\bar{g}$ does not divide $\mathrm{N}_{\bar{L}_i/GF(p)}(\phi_p(f))$.

Theorem 14

Let $\bar{T}$ be a subset of $\bar{\mathcal{F}}$. If the product of all elements in $\bar{T}$ is the modular image $\phi_p(T)$ of some true factor T of S, then the following relation holds:

$$\frac{\Sigma_{\bar{g}\in\bar{T}} e_i(\bar{g}) \deg(\bar{g})}{[\bar{L}_i : GF(p)]} = \frac{E \deg(T)}{[K : \mathbb{Q}]} \quad \text{for } 1 \le i \le s, \tag{6}$$

and $E \deg(T)/[K : \mathbb{Q}] = \deg_y(\mathrm{GCD}(T, f))$. Moreover, for each $\bar{g}$ in $\bar{T}$, $\Sigma_{i=1}^{s} e_i(\bar{g}) = E$.

Proof. It suffices to show the theorem for each irreducible factor T of S. Let $f_1, \ldots, f_r$ be all irreducible factors of f over $\mathbb{Q}$. Since each $\mathcal{I}_i = \mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{M}, f_i)$ is a maximal ideal, the minimal polynomial $Min_{y,\mathcal{I}_i}$ is irreducible and the characteristic polynomial $Cha_{y,\mathcal{I}_i}$, which coincides with $\mathrm{N}_{K/\mathbb{Q}}(f_i)$, is equal to $Min_{y,\mathcal{I}_i}$ or its power. Thus, by changing indices, we can assume that $\mathrm{N}_{K/\mathbb{Q}}(f_i) = T^{e_i}$ for $i = 1, \ldots, u$, $u \le r$ and T does not divide $\mathrm{N}_{K/\mathbb{Q}}(f_i)$ for $u < i$. Then $e_i \deg(T) = \deg(f_i)[K : \mathbb{Q}]$ for $1 \le i \le u$ and

$$E \deg(T) = [K : \mathbb{Q}] \sum_{i=1}^{u} \deg_y(f_i). \tag{7}$$

By seeing modular images,

$$\phi_p(T)^{e_i} = \prod_{j=1}^{s} \mathrm{N}_{\bar{L}_j/GF(p)}(\phi_p(f_i))$$
$$\phi_p(T)^{E} = \prod_{j=1}^{s} \mathrm{N}_{\bar{L}_j/GF(p)}(\phi_p(f_1) \cdots \phi_p(f_u)).$$

On the other hand, we have

$$\mathrm{N}_{\bar{L}_j/GF(p)}(\phi_p(f)) = \prod_{\bar{g}\in\bar{\mathcal{F}}} \bar{g}^{e_j(\bar{g})},$$

and so

$$\mathrm{N}_{\bar{L}_j/GF(p)}(\phi_p(f_1 \cdots f_u)) = \prod_{\bar{g}\in\bar{T}} \bar{g}^{e_j(\bar{g})}. \tag{8}$$

Counting the degrees of both side of Equation (8), we obtain

$$[\bar{L}_j : GF(p)] \sum_{i=1}^{u} \deg_y(f_i) = \sum_{\bar{g} \in \bar{T}} e_j(\bar{g}) \deg(\bar{g}). \tag{9}$$

Combining Equations (9) and (7), we obtain Equation (6). Since $f_1 \cdots f_u = \mathrm{GCD}(T, f)$ over K by considering common roots, we have $E \deg(T) = [K : \mathbb{Q}]\mathrm{GCD}(T, f)$. ∎

Theorem 14 gives a criterion for valid combinations of modular factors for non-square-free norms, by which we can suppress "combinatorial explosion" efficiently. When $E = 1$, Theorem 14 gives Theorem 13, because $\bar{e}_i(\bar{g}) = 1$ or 0 and there is no common factor between $\mathrm{N}_{\bar{L}_i/GF(p)}(\phi_p(f))$ and $\mathrm{N}_{\bar{L}_j/GF(p)}(\phi_p(f))$ for $i \neq j$.

Algorithm 2 [Factorization of norms of polynomials]

Inputs: A successive extension $K/\mathbb{Q}$, a square-free polynomial $f(y)$ over K and the square free part S of $F = \mathrm{N}_{K/Q}(f)$.

Outputs: All irreducible factors of F over $\mathbb{Q}$.

Assumption: K is given by a residue class ring $\mathbb{Q}[X]/\mathcal{M}$, where $\mathcal{M}$ is given by its Gröbner base $\mathcal{G}$, and $F = S^E$.

(i) Choose a prime p radically lucky for $\mathrm{Id}_{\mathbb{Q}[y,X]}(\mathcal{M}, f, S)$.

(ii) Compute the prime decomposition of $\bar{\mathcal{M}}$, where $\bar{\mathcal{M}} = \mathrm{Id}_{GF(p)}(\phi_p(\mathcal{G}))$ and let $\bar{\mathcal{M}}_i$, $i = 1, \ldots, s$, be prime divisors of $\bar{\mathcal{M}}$.

(iii) For each $\bar{\mathcal{M}}_j$, compute the set $\bar{\mathcal{S}}_j$ of pairs of each irreducible factor and its multiplicity in $\mathrm{N}_{\bar{L}_j/GF(p)}(\phi_p(f))$, where $\bar{L}_j = GF(p)[X]/\bar{\mathcal{M}}_j$.

(iv) Find each irreducible factor of S by *lifting up and trial-division* only applying for the modular factors which satisfy Equation (6).

(v) Return all irreducible factors of F found in (iv).

Remark 1

If S is irreducible over $\mathbb{Q}$, the factorization of S means nothing, since it cannot say the irreducibility of f. So it is desirable to check such a case before trial-division. The following gives a quick-test for such a case.

Lemma 15

If some $\bar{\mathcal{F}}_i$ consists of one element, then S is irreducible.

Remark 2

The criteria given here may work efficiently when the norm F has many modular factors over $GF(p)$, especially the number of irreducible factors of $\phi_p(F)$ is much greater than $\deg_y(f)$. In this case, $\bar{\mathcal{M}}$ has non-trivial prime decomposition. Let us consider an ideal *case: F is irreducible but $\bar{\mathcal{M}}$ has s prime divisors $\bar{\mathcal{M}}_1, \ldots, \bar{\mathcal{M}}_s$ and each $\bar{\mathcal{F}}_i$ has t irreducible factors. (Then $\phi_p(F)$ has st irreducible factors.) The number of combinations of modular factors to be tested is 2^{ts-1} without the criterion, which is reduced to $1/2({}_tC_1{}^s + \cdots + {}_tC_{t-1}{}^s)$ ($<< 2^{(s-1)t}$) with the criterion. Such a case occurs in the computation of splitting field of integral polynomials. (See Section 5. and examples in Section 6..)*

However, when F has a few modular factors or $\bar{\mathcal{M}}$ is still a maximal ideal, the criteria do not work well and the additional computation for the prime decomposition of $\bar{\mathcal{M}}$ harm the efficiency. Thus, for practical implementation, if the factorization problem is not related to splitting field computation, it seems better to decide the usage of the criteria after counting the number of modular factors.

4. Remarks on Other Steps

In Section 3. we give an improvement for factoring the norms of polynomials. However, as pointed out in [3], to obtain practical implementation, we must improve the efficiency of the steps; (a) the computation of the norm F and (b) GCD(F_i, f) for each irreducible factors F_i of F. Moreover, we have to give an efficient method for the decomposition of the ideal $\bar{\mathcal{M}}$. Here we give brief discussion on those. (We use the same notations as in the previous sections.)

4.1. computing the norms

When the extension degree $N = [K : \mathbb{Q}]$ is large, *interpolation* techniques work quite efficiently to compute $F(y) = \mathrm{N}_{K/\mathbb{Q}}(f(y))$. We provide $nN+1$ integers $a_0, \ldots, a_{nN}$, where $n = \deg_y(f(y))$, and compute

$$F(a_i) = \mathrm{N}_{K/\mathbb{Q}}(f(a_i)) = \mathrm{res}_{x_1}(m_1, \cdots \mathrm{res}_{x_n}(m_n, f(a_i)) \cdots)$$

for each a_i. From $\{F(a_0), \ldots, F(a_{nN})\}$, we construct $F(y)$ by Chinese remainder theorem. Moreover, by using enough numbers of primes, we can compute $F(a_i)$ by the modular images $\phi_p(F(a_i)) = \mathrm{res}_{x_1}(\bar{m}_1, \cdots \mathrm{res}_{x_n}(\bar{m}_n, \phi_p(f(a_i))) \cdots)$. We will show some further technique on interpolation for F in Section 5.3..

4.2. GCD computation

There are efficient methods for GCD computation over extension fields based on modular technique ([10],[6]). In our case, since we can detect the luckiness of each prime from the degree of the modular GCD, we can take advantage of *early detection.* (For each irreducible factor F_i of F, we already know the degree of $\mathrm{GCD}(F_i, f)$ from $\deg(F_i)$.)

We use a method based on Gröbner base with modular technique [12] in the implementation. As mentioned in Section 3.1., $\mathrm{GCD}(F_i, f)$ over K appears as an element in the Gröbner base of $Id_{\mathbb{Q}[y,X]}(\mathcal{M}, F_i, f)$ with respect to $<_y$ and other elements are elements of the *given* Gröbner base of $\mathcal{M}$. In the method, we execute similar computations as the method in Langemyr [10] but we use "recover of rational numbers from their modular residue," (see [6]) without estimate on the size of coefficients. Although we do not provide necessary number of primes in advance, it terminates at the step before the size of the product of used primes exceeds the bound estimated in [10].

4.3. decomposition of ideals over finite fields

Here we give a concrete method used in our implementation. To take advantage of the successive expression of extension fields, we employ "successive decomposition:" We factorize $\bar{m}_1(x_1)$ and then factorize $\bar{m}_2(x_2, x_1)$ over extension fields obtained by irreducible factors of $\bar{m}_1(x_1)$ and so on. By these recursive procedures, the problem is reduced to the factorization of polynomials over extension fields. To simplify the implementation, we change the expression of fields from successive one to simple one. This change does not harm the efficiency, since there is no coefficient growth over finite fields. Then we apply an efficient existing method for factoring polynomials over simple extension fields over finite fields. Of course, we can also apply Berlekamp's algorithm directly to the residue class ring factored by the given ideal (see [13]).

We give more details. Suppose that $\bar{\mathcal{M}} \cap GF(p)[X_i] = \mathrm{Id}_{GF(p)[X_i]}(\bar{m}_1, \ldots, \bar{m}_i)$ is decomposed as

$$\bar{\mathcal{M}} \cap GF(p)[X_i] = \cap_{j=1}^{r_i} \bar{\mathcal{M}}_j^{(i)},$$

where $\bar{\mathcal{M}}_j^{(i)}$ is a maximal ideal in $GF(p)[X_i]$ for each i. Then the decomposition of $\mathrm{Id}_{GF(p)[X_{i+1}]}(\bar{m}_1, \ldots, \bar{m}_{i+1})$ is reduced to that of each component $\mathrm{Id}_{GF(p)[X_{i+1}]}(\bar{\mathcal{M}}_j^{(i)}, \bar{m}_{i+1})$, which comes from the factorization of $\bar{m}_{i+1}$ over $GF(p)[X_i]/\bar{\mathcal{M}}_j^{(i)}$. To express $GF(p)/\bar{\mathcal{M}}_j^{(i)}$, we employ a simple extension expression by its primitive element β. Let $\bar{g}_j(y)$ be the minimal polynomial of β over $GF(p)$. Then there are univariate polynomials $h_{1,j}, \ldots, h_{i,j}$ such that

$$\bar{\mathcal{M}}_j^{(i)} = GF(p)[X_i] \cap Ideal_{GF(p)[y,X_i]}(x_1 - h_{1,j}(y), \ldots, x_i - h_{i,j}(y), \bar{g}_j(y)).$$

By replacing $x_1, \ldots, x_i$ with $h_{1,j}(y), \ldots, h_{i,j}(y)$, respectively, $\bar{m}_{i+1}$ becomes a polynomial in $(GF(p)[y]/\mathrm{Id}(g_j(y)))[x_{i+1}]$. The following gives the procedure in general setting:

Algorithm 3 [change of expression]

Input: an irreducible polynomial $a(t) \in GF(p)[t]$ and an irreducible polynomial $b(s,t) \in GF(p)[t,s]$ over $GF(p)[t]/Id(a(t))$.

Output: an irreducible polynomial c over $GF(p)$ such that $GF(p)[s,t]/Id(b(s,t),a(t)) \cong GF(p)[u]/Id(c(u))$ and expressions $s = h_s(u)$, $t = h_t(u)$ of s, t.

(1) Find an irreducible polynomial $c(u) \in GF(p)[u]$ such that $\deg(c) = \deg_s(b(s,t))\deg(a)$.

(2) Find a root $h_t(u)$ of $a(t)$ over $GF(p)[u]/(c(u))$.

(3) Find a root $h_s(u)$ of $b(s, h_t(u))$ over $GF(p)[u]/(c(u))$.

In the current implementation, we find c from randomly generated polynomials of the specified degree. Of course, to improve efficiency, we can apply existing efficient methods. (See a survey [9].) Since we find each root as a linear factor at Step 2 and 3, these steps can be done efficiently.

By applying Algorithm 3 to "successive decomposition" recursively, we obtain the decomposition of $\bar{\mathcal{M}}$ after a number of algebraic factorizations over simple extension fields.

5. Computing Splitting Fields

As a special case of factorization of polynomials over extension fields, we consider the splitting field of an integral polynomial. We consider the following. (See details in [3] and [18].)

Let $f(x)$ be a monic and irreducible integral polynomial of degree n and let $\alpha_1, \ldots, \alpha_n$ be all roots of f. We denote the splitting field of f and the Galois group of f by K_f and G_f, respectively. By assigning a variable x_i to each α_i, there is the unique maximal ideal $\mathcal{M}i$ of $\mathbb{Q}[X]$ such that $K_f \cong \mathbb{Q}[X]/\mathcal{M}$ and we identify K_f with $\mathbb{Q}[X]/\mathcal{M}$. Thus, to compute the splitting field K_f is to compute a Gröbner base of $\mathcal{M}$. Especially, the reduced Gröbner base $\mathcal{G}$ with respect to the lexicographic order $<$ can be computed by sequentially factoring polynomials over extension fields and $\mathcal{G}$ takes the form of $\{f_1(x_1), f_2(x_2, x_1), \ldots, f_n(x_n, \ldots, x_1)\}$. Then for each i, $\mathbb{Q}[X_i]/\mathcal{M}_i \cong \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$, where $\mathcal{M}_i = \mathrm{Id}_{\mathbb{Q}[X_i]}(f_1, \ldots, f_i)$. We denote the extension field by K_i. In more detail, $f_1 = f$ and each f_{i+1} is the irreducible factor of g_{i+1} over K_i such that $f_{i+1}(\alpha_{i+1}, \ldots, \alpha_1) = 0$, where g_{i+1} is the irreducible factor of $f(x)/((x - x_1)\cdots(x - x_{i-1}))$ over K_{i-1} such that

$g_{i+1}(\alpha_{i+1}, \alpha_{i-1}, \ldots, \alpha_1) = 0$.

5.1. lucky primes

In the computation of K_f, we factorize g_{i+1} over K_i successively from $i = 1$ to some k until we have a complete factorization of f. In each i-th step, we consider the ideal $\mathcal{J} = \mathrm{Id}_{\mathbb{Q}[X_{i+1}]}(f_1, \ldots, f_i, g_{i+1}(x_{i+1} - z))$ for some $z = c_1x_1 + \cdots + c_ix_i$, where $c_1, \ldots, c_i \in \mathbb{Z}$. Since a prime p divides none of $\mathrm{N}_{K_i/\mathbb{Q}}(\mathrm{disc}(\alpha_i))$'s if and only if p does not divide $\mathrm{disc}(f)$, we have the following criterion for the luckiness of primes.

Lemma 16

A prime p is radically lucky for $\mathcal{M}_i$ if and only if p does not divide $\mathrm{disc}(f)$. *Moreover, if a prime p is radically lucky for $\mathcal{M}_i$, then p is also lucky for $\mathcal{J}$ and* $\mathrm{Id}_{GF(p)}(\phi_p(f_1), \ldots, \phi_p(f_i), \phi_p(g_z))$ *is radical.*

Among all lucky primes, the following are useful for our computation; (1) primes p such that $\phi_p(f)$ has small splitting field over $GF(p)$ and (2) primes p such that $\phi_p(f)$ has large splitting field over $GF(p)$. Here, "small" means $E << \deg(f)$ and "large" means $E \geq \deg(f)$, where E is the extension degree of the splitting field $K_{\phi_p(f)}$ of $\phi_p(f)$. We denote the set of primes in (1) by $\mathcal{P}_0$ and that in (2) by $\mathcal{P}_1$. By Chebotarev's density theorem, the ratio of primes such that $K_{\phi_p(f)} = GF(p)$ is $1/|G_f|$ and so the ratio of primes in $\mathcal{P}_0$ is at least $1/|G_f|$, and that in $\mathcal{P}_1$ is expected much larger than $1/|G_f|$ for many cases. (But, $\mathcal{P}_1$ can be empty.) Primes in $\mathcal{P}_0$ seem useful for computation of the norms and primes in $\mathcal{P}_1$ seem useful for factoring the norms of polynomials.

5.2. efficiency of the criteria

First we explain the efficiency of the criteria. At each i-th step, we choose a radically lucky prime p and decompose $\bar{\mathcal{M}}_i$ to $\cap_{j=1}^{r_i} \bar{\mathcal{M}}_j^{(i)}$. Then each $\bar{L}_j^{(i)} = GF(p)[X_i]/\bar{\mathcal{M}}_j^{(i)}$ is a subfield of the splitting field $K_{\phi_p(f)}$ of $\phi_p(f)$. On the other hand, Chevotarev's density theorem says the following:

Proposition 17

For a radically lucky prime p, the Galois group of $\phi_p(f)$ is isomorphic to a cyclic subgroup of G_f.

Thus, except the case where G_f is cyclic, there is a big difference between the order of G_f and that of its cyclic subgroup, and so every $\bar{L}_j^{(i)}$ tends to be small, which implies that $\bar{\mathcal{M}}_i$

tends to have many prime divisors.

Next we remark on the choice of p. The splitting field $K_{\phi_p(f)}$ *controls* the number of irreducible factors of $\phi_p(G)$, where $G = \mathrm{N}_{K_i/\mathbb{Q}}(g_{i+1}(x_{i+1} - z))$. Because, the degree of each irreducible factor of $\phi_p(G)$ coincides with the extension degree of the field obtained by adjoining a root of $\phi_p(G)$ to $GF(p)$, which is also a subfield of $K_{\phi_p(f)}$. Therefore, to make the number of irreducible factors of $\phi_p(G_z)$ smaller, we must choose p so that $K_{\phi_p(f)}$ has large extension degree. Although this may decrease the number of prime divisors of $\bar{\mathcal{M}}_i$, it shall decrease the number of combinations of modular factors for trial-division in total. So, we suggest to use primes in $\mathcal{P}_1$ for factorization of G.

5.3. norm computation

We give a method for computing norms by using primes in $\mathcal{P}_0$, which seems suited for our case. (The method is not used in the current implementation. So its practical efficiency must be checked in the next work.)

Select k primes in $\mathcal{P}_0$. We write $\mathcal{L}$ for the set of such primes. For each $p \in \mathcal{L}$ we have

$$\phi_p(f) = (x - a_{p,1}) \cdots (x - a_{p,n}),$$

where $a_{p,1}, \ldots, a_{p,n} \in K_{\phi_p(f)}$. Let $\bar{\mathcal{J}}_{i,p} = \mathrm{Id}_{GF(p)[X_{i+1}]}(\phi_p(f_1), \ldots, \phi_p(f_i), \phi_p(g_z))$, where $g_z = g_{i+1}(x_{i+1} - z)$, and set $R_p = \{a_{p,1}, \ldots, a_{p,n}\}$. Then we can show the following easily.

Lemma 18

The set $\mathcal{V}_{i,p}$ of all zeros of the ideal $\bar{\mathcal{J}}_{i,p}$ consists of all vectors $(b_1, \ldots, b_{i+1})$, where $b_1, \ldots, b_{i+1} \in R_p$, such that $\phi_p(f_1)(b_1) = 0, \ldots, \phi_p(f_i)(b_i, \ldots, b_1) = 0$ and
$\phi_p(g_z)(b_{i+1}, \ldots, b_1) = 0$.

Let $G = \mathrm{N}_{K_f/\mathbb{Q}}(g_z)$. Then each root of $\phi_p(G)$ can be written as $b_{i+1} + \phi_p(c_1)b_1 + \cdots + \phi_p(c_i)b_i$, where $(b_1, \ldots, b_{i+1}) \in \mathcal{V}_{i,p}$. As $\phi_p(G) = \mathrm{res}_{x_1}(\cdots \mathrm{res}_{x_i}(\phi_p(f_i), \phi_p(g_z)) \cdots)$, $\phi_p(G)$ coincides with

$$\prod_{(b_1, \ldots, b_{i+1}) \in \mathcal{V}_{i,p}} (x_{i+1} - b_{i+1} - \phi_p(c_1)b_1 - \cdots - \phi_p(c_i)b_i).$$

Let $M = 2(1 + \sum_{j=1}^{i} |c_i|) max\{|\alpha_1|, \ldots, |\alpha_n|\}$, $N_i = [K_i : \mathbb{Q}]$ and $m = \deg_{x_{i+1}}(g_z) = \deg_{x_{i+1}}(g_{i+1})$. By the relation between coefficients and roots, the absolute value of each coefficient of G is bounded by $M^{N_i m}$. Then,

Lemma 19

By choosing $\mathcal{L}$ such that $\prod_{p\in\mathcal{L}} p \geq 2M^{N_i m}$, we can construct G from $\{\phi_p(G) \mid p \in \mathcal{L}\}$ by Chinese remainder theorem.

Remark 3

Using $\mathcal{P}_0$, we can compute $\phi_p(\mathrm{GCD}(H, g_z))$ for each factor H of G over $\mathbb{Q}$ as follows: Let $\mathcal{W}_{H,p} = \{(b_1, \ldots, b_{i+1}) \in \mathcal{V}_{i,p} \mid H(b_{i+1} + \phi_p(c_1)b_1 + \cdots + \phi_p(c_i)b_i) = 0\}$. By counting number of zeros, we can show that there exists a vector $C = (c_{k_1,\ldots,k_{i+1}})_{0\leq k_j<n_j;1\leq j\leq i+1}$ over $GF(p)$ uniquely such that for every $(b_1, \ldots, b_{i+1}) \in \mathcal{W}_{H,p}$

$$b_{i+1}^{n_{i+1}} + \sum_{0\leq k_j<n_j;1\leq j\leq i+1} c_{k_1,\ldots,k_{i+1}} b_1^{k_1} \cdots b_{i+1}^{k_{i+1}} = 0,$$

and we can compute C by solving linear equations. (Here, we set $n_j = \deg_{x_j}(f_j)$ for $j \leq i$ and $n_{i+1} = \deg(\mathrm{GCD}(H, g_z))$ tentatively.) Then,

$$\begin{aligned}&\phi_p(\mathrm{GCD}(H, g_z)) \\ &= x_{i+1}^{n_{i+1}} + \sum_{0\leq k_j<n_j;1\leq j\leq i+1} c_{k_1,\ldots,k_{i+1}} x_1^{k_1} \cdots x_{i+1}^{k_{i+1}}.\end{aligned}$$

Hence, by computing $\phi_p(\mathrm{GCD}(H, g_z))$ for enough number of primes in $\mathcal{P}_0$, we can construct $\mathrm{GCD}(H, g_z)$ by Chinese remainder theorem. Since we do not have a good coefficient bound for factors of g_z over K_i, it seems better to make good use of trial division. For a method using Hensel construction, see Section 5.3 in [18].

6. Experiments and Remarks

We tested the efficiency of the proposed method for several examples where we met heavy combinatorial explosion in our previous experiments. We implemented the method on a computer algebra system *Risa/Asir* [11] and compared the timings on those examples on a PC with P6-200MHz CPU. First we show two typical examples, where the criteria worked very efficiently.

Example 1 (computation of splitting field)

Consider $f = x^7 - 7x + 3$ whose Galois group is isomorphic to $PSL(2, 3)$, a simple group of order 168. In the authors' previous method in [3], which uses a simple criterion *hint* on the degrees of candidates, the whole computation took 1060 seconds. But it took 287.5 seconds by the new method.

In [3], the most time-consuming step was verification of the irreducibility of a polynomial of degree 4 over $K = \mathbb{Q}(\alpha_1, \alpha_2)$, where $f_2(x) = f(x)/(x - \alpha_1)$, $f(\alpha_1) = 0$ and $f_2(\alpha_2) = 0$. This is checked by testing the irreducibility of the norm $F(x) = \mathrm{N}_{K/\mathbb{Q}}(f(x + \alpha_2 - 2\alpha_1))$ over $\mathbb{Q}$, whose degree is 168. Although F is irreducible, F has many modular factors and so we meet combinatorial explosion in ordinary Berlekamp-Hensel algorithms. $\phi_5(F)$ has 24 irreducible factors of degree 7 and we have to check 2^{23} combinations for trial division and also check 1.4×10^6 combinations even with *hint* criterion ([3]). However, the ideal $\mathrm{Id}(\phi_p(f_1), \phi_p(f_2))$ has 6 prime divisors, each of which gives an extension field of degree 7, and 24 factors of F are divided to 6 subsets consisting of 4 factors. With the criterion in Theorem 13, we have only to check ${}_4C_1^6 + {}_4C_2^6$ (about 50,000) combinations. Thus, on a PC, this step was completed in 92 seconds by the new method. Since the author's previous method took 852 seconds for this step, we succeeded in making the computation 9 times faster.

Example 2 (coincidence of two splitting fields given by Prof. McKay)
Let $f = x^6 + 2x^5 + 3x^4 + 4x^3 + 5x^2 + 6x + 7$ and $g = x^5 - 3x^4 - 2x^3 - 122x^2 + 325x + 577$. (See [5] for f.) Both have the Galois group isomorphic to S_5. To prove that the splitting field K_f of f coincides with that K_g of g, we factorize f over K_g into linear factors. Since $\deg(g) = 5$, the splitting field K_g is easily expressed as $\mathbb{Q}(\alpha_4, \ldots, \alpha_1)$, where $\alpha_4, \ldots, \alpha_1$ are distinct 4 roots of g. In the experiment, the complete factorization of f over K_g was completed in 700 seconds.

First we factorize f over a subfield $L = \mathbb{Q}(\alpha_3, \alpha_2, \alpha_1)$. The norm $\mathrm{N}_{K_g/\mathbb{Q}}(f(x - \alpha_3 - \alpha_2 + \alpha_1))$ is the square of a polynomial F_1 of degree 180. By the factorization with the criterion in Theorem 14, F_1 has divided two irreducible factors F_2, F_3, where $\deg(F_2) = 60$ and $\deg(F_3) = 120$. Then by GCD with f over L, f divided to two factors f_2 and f_3, where $\deg(f_2) = 2$ and $\deg(f_3) = 4$.

Then we factorize f_3 over L. The norm $\mathrm{N}_{L/\mathbb{Q}}(f_3(x - \alpha_3 + \alpha_2 - \alpha_1))$ is square-free factorized as $F_4^2 F_5$, where $\deg(F_4) = 60$ and $\deg(F_5) = 120$, which give a non-trivial factorization $f_3 = f_4 f_5$ over L, where $\deg(f_4) = \deg(f_5) = 2$. Thus, we have 3 factors f_2, f_4, f_5 of degree 2 over L.

Finally we factorize them over K_g. Then for $i = 2, 4, 5$, the norm $\mathrm{N}_{K_g/\mathbb{Q}}(f_i(x - \alpha_4 - \alpha_3 + \alpha_2 + \alpha_1))$ is square-free factorized as $h_{1,i}^2 h_{2,i}$, where $\deg(h_{1,i}) = 60$ and $\deg(h_{2,i}) = 120$. As $[K_g : \mathbb{Q}] = 120$, we can conclude that f_2, f_4, f_5 are factorized to linear factors over K_g.

Thus, f is split over K_g, which implies that $K_g = K_f$.

For factoring F_1, we choose 11 as a lucky prime. Then $\phi_{11}(F_1)$ has 30 irreducible factors of degree 6 and the modular image of the maximal ideal has 11 prime divisors, from which we can construct 9 extension fields of extension degree 6 and two of extension degree 3. Without the criterion in Theorem 14, even if we know the degrees of irreducible factors, we have to check ${}_{30}C_{10}$ (more than 3×10^7) combinations for finding F_2 in the worst case, and even if we change the shift to have a square-free norm and factorize it with the criterion in Theorem 13, we have to check ${}_6C_2^9 3^2$ (more than 3×10^{11}) combinations in the worst case, which implies that the factorization is very hard on a computer. However, with the criterion in Theorem 14, we have only to check ${}_6C_2^4 3^2$ (less than 500,000) combinations for trial-division. Thus the computation was completed in 181 seconds.

Next we give a brief comparison with the method by Weinberger & Rothschild [16]. With respect to finding valid combinations of modular factors, the criterion by Encarnación has heavy relation to their method; there is one to one correspondence between modular factors handled by the method by Trager with Encarnación's criterion and those by the method by Weinberger & Rothschild in factorization over a simple extension field. If we extend Weinberger & Rothschild's method to successive extension case, the criterion in Theorem 13 shall correspond to this extended method. However, its description and estimations on the size of coefficients of true factors shall be much complicated. Moreover, the criterion in Theorem 14 for non square-free norms cannot be applied to the extended method. These points support certain superiority of the method proposed here. Detailed comparison, both in theory and in practice, should be done in the next study.

7. Conclusion

In the paper, we propose a new method for factoring polynomials over successive extension fields over $\mathbb{Q}$ based on factorization of the norms of polynomials originally proposed by Trager, and apply it for computing the splitting fields of integral polynomials. To improve the efficiency of factoring square-free norms, we generalize a technique used for factoring polynomial over simple extension by Encarnación and we also extend the technique for factorization of non-square-free norms of polynomials. Combining these two improvements and other precise devices, we obtain a new method which seems practical for actual problems. By experiments on typical examples, the quality/ability of the method is examined.

Finally, we mention future works. Since the criteria require additional computation for prime decomposition of ideals over finite fields, we need further experiment to find a smart decision on whether we use the criteria and execute additional computation for practical implementation. And study on practical efficiency of methods using the LLL algorithm for factoring norms is also important. Moreover, there are two additional works:
(1) The problem discussed here can be considered as a special case of prime decomposition of 0-dimensional radical ideals over $\mathbb{Q}$, where all computations are done with respect to the lexicographic order. In [13], the authors had generalized Encarnación's criterion for ideals with respect to *block orderings* in theory. So, the practical efficiency of the criterion for prime decomposition should be tested.
(2) For computing the splitting fields efficiently, it is better to combine the information of their Galois groups, and conversely, certain algebraic factorizations are required for computing the Galois groups. (See [3] and [18].) Thus, for practical implementation, *integration* of different approaches (methods) is quite important. Since the criteria work quite efficiently in the case, it should contribute to *practically best* integration.

References

[1] Abbott, J. A., Factorization of polynomials over algebraic number fields. PhD thesis, University of Bath (1989).

[2] Alonso, M.E., Becker, E., Roy, M.F., Wörmann, T., *Zero's, multiplicities and idempotents for zero dimensional systems.* presented at MEGA'94, also in Progress in Mathematics 143, Birkhäser Verlag, 1996, 1-15.

[3] Anai, H. Noro, M, Yokoyama, K., *Computation of the splitting fields and the Galois groups of polynomials.* presented at MEGA'94, also in Progress in Mathematics 143, Birkhäuser Verlag, 1996, 29-50.

[4] Becker T., Weispfenning V., Gröbner bases. Springer-Verlag, 1993.

[5] McKay, J., *On computing discriminants.* Amer. Math. Montly, 94 (1987), 523-527.

[6] Encarnación, M., J., Faster algorithms for reconstructing rationals, computing polynomial GCDs, and factoring polynomials. Ph.D. Thesis, RISC-Linz, 1995.

[7] Encarnación, M., J., *Factoring polynomials over algebraic number fields via norms.* in Proc. ISSAC '97, ACM Press, 1997, 265-270.

[8] Encarnación, M., J., *The average number of modular factors in Trager's polynomial factorization algorithm.* in Proc. ISSAC '97, ACM Press, 1997, 278-281.

[9] Kaltofen, E., *Polynomial factorization 1987-1991.* in LATIN '92, L.N.Comp.Sci. 583, Springer Verlag, 1992, 294-313.

[10] Langemyr, L., *Algorithms for a multiple algebraic extension II.* in AAECC-9, L. N. Comp. Sci. 539, Springer Verlag, 1991, 224-233.

[11] Noro M., Takeshima T., *Risa/Asir -a computer algebra system.* in Proc. ISSAC '92, ACM Press, 1992, 387-396.

[12] Noro M., Yokoyama K., New methods for the change-of-ordering in Gröbner basis computation. Research Report ISIS-RR-95-8E, 1995.

[13] Noro M., Yokoyama K., Prime decomposition of radical ideals and algebraic factorization of polynomials. Research Report ISIS-RR-96-8E, 1996.

[14] Seidenberg, A., *Constructions in algebra.* Trans. Amer. Math. Soc. 197 (1974), 272-313.

[15] Trager, B.M., *Algebraic factoring and rational function integration.* in Proc. SYMSAC '76, ACM Press, 1976, 219-226.

[16] Weinberger, P. J., Rothschild, L. P., Factoring polynomials over algebraic number fields. ACM Trans. Math. Softw, 2/4 (1976), 335-350.

[17] Yokoyama K., Noro M., Takeshima T., *Solution of systems of algebraic equations and linear maps on residue class rings.* J. Symbolic Computation, 14 (1992), 399-417.

[18] Yokoyama, K., *A modular method for computing the Galois groups of polynomials.* presented at MEGA '96 and also in J. Pure and Applied Algebra, 117 & 118 (1997), 617-636.