SCIENCE CHINA
Mathematics

• ARTICLES •

June 2013 Vol. 56 No. 6: 1155–1168
doi: 10.1007/s11425-013-4586-0

An efficient algorithm for factoring polynomials over algebraic extension field

SUN Yao[1,2] & WANG DingKang[2,*]

[1]*SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2]*KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing* 100190*, China*
Email: sunyao@iie.ac.cn, dwang@mmrc.iss.ac.cn

Received September 9, 2011; accepted June 18, 2012; published online March 30, 2013

Abstract An efficient algorithm is proposed for factoring polynomials over an algebraic extension field defined by a polynomial ring modulo a maximal ideal. If the maximal ideal is given by its Gröbner basis, no extra Gröbner basis computation is needed for factoring a polynomial over this extension field. Nothing more than linear algebraic technique is used to get a characteristic polynomial of a generic linear map. Then this polynomial is factorized over the ground field. From its factors, the factorization of the polynomial over the extension field is obtained. The algorithm has been implemented in Magma and computer experiments indicate that it is very efficient, particularly for complicated examples.

Keywords algorithm, factorization, algebraic extension field

MSC(2010) 12Y05, 13P10, 13P15, 33F10

Citation: Sun Y, Wang D K. An efficient algorithm for factoring polynomials over algebraic extension field. Sci China Math, 2013, 56: 1155–1168, doi: 10.1007/s11425-013-4586-0

1 Introduction

Factorization of polynomials over algebraic extension fields has been widely investigated and there are polynomial-time algorithms for factoring multivariate polynomial over algebraic number field [1, 2, 6, 13, 16, 25].

Factorization over algebraic extension fields is needed for irreducible decomposition of algebraic variety by using characteristic set method [29, 30]. In [26, 27], Wang and Lin proposed a very good algorithm for factoring multivariate polynomials over algebraic fields obtained from successive extensions of the filed of rational numbers. This problem has been further investigated by Li and Yuan in [17, 31]. Li's algorithm decomposes ascending chain into irreducible ones directly and Yuan's algorithm follows Trager's method (see [25]). Their methods involve the computation of characteristic set, Gröbner basis or resultant of multivariate polynomial system and all these computations are quite expensive. Rouillier's approach can also deduce an algorithm for the same aim (see [23]). All the above algorithms are probabilistic, and if the characteristic of the ground field is 0, the algorithms terminate in finite steps with probability 1 (see [8, 27]). Besides, Steel gave his factorization method in another way when the characteristic of the field is positive and he concentrated on how to conquer the ground inseparability (see [24]).

The main purpose of the current paper is to present an efficient algorithm to solve the following factorization problem:

*Corresponding author

Let k be a perfect computable field and $k[x_1,\ldots,x_n]$ the polynomial ring in indeterminate $\{x_1,\ldots,x_n\}$ with coefficients in k. Let $I \subset k[x_1,\ldots,x_n]$ be a maximal ideal such that $\mathrm{K} = k[x_1,\ldots,x_n]/I$ is indeed an algebraic extension field of k. For a polynomial $f \in \mathrm{K}[y]$, we will derive a new efficient algorithm for factoring f over the field K.

The above problem can be converted to univariate polynomial factorization over the ground field k by using a generic linear map. If the maximal ideal I is represented by its Gröbner basis for any admissible order, no extra Gröbner basis computation is needed in the new algorithm. The new algorithm can check whether a factor of f is irreducible during the factorization process. For those reducible factors, the new algorithm will factor them further.

In [19], Monico proposed a new approach for computing a primary decomposition of a zero-dimensional ideal. This idea also plays an important role in the new proposed algorithm. However, Monico's algorithm is not complete, i.e., the components in the output of Monico's algorithm cannot be assured to be primary. Our new algorithm overcomes this flaw when applying Monico's idea to the above factorization problem, i.e., the irreducible factors can be verified without extra computations.

Noro and Yokoyama presented algorithms for computing prime decomposition of radical ideals and factorization of polynomials over algebraic extension field in [20–22]. Let $\sigma : k[x_1,\ldots,x_n] \to \mathrm{K}$ be the canonical map $\sigma(c) = [c]$ for all $c \in k[x_1,\ldots,x_n]$, where $[c]$ denotes the residue class $c + I$. This map can be extended (coefficient wise) to $\sigma : k[x_1,\ldots,x_n,y] \to K[y]$. Let $J = I + \langle h\rangle$, where $\sigma(h) = f$ (it is easy to check that J is well-defined). A polynomial in $k[x_1,\ldots,x_n,y]$ is said to be a separating element for $J \subset k[x_1,\ldots,x_n,y]$, if the evaluations of this polynomial as a function on any two distinct zeros of J are not equal. In Noro and Yokoyama's algorithm, if the polynomial y is a separating element for J, then a factorization of f is obtained by factoring the norm of f over the ground field; otherwise, variable substitutions are made to y, i.e., update y by $y + c_1x_1 + \cdots + c_nx_n$, where c_i are constants in k, and then check whether y is a separating element for ideal after variable substitution. Notice that such variable substitution is very expensive if the degree of f in y is high. In our algorithm, such variable substitutions will be avoided by computing the characteristic polynomial or minimal polynomial of some linear map.

This paper is organized as follows. Some necessary preliminaries are given in Section 2. In Section 3, we show how the problem of polynomial factorization over algebraic extension field, which is proposed in [26,27,29,30], can be transformed to a univariate factorization problem. A new algorithm for factoring polynomials over algebraic extension field is presented in Section 4. Examples and comparisons appear in Sections 5 and 6 respectively. Finally, we conclude this paper in Section 7.

2 Preliminaries

Let k be a perfect field which admits efficient operations and factorization of univariate polynomials. Let R be a multivariate polynomial ring over the field k and Q an ideal of R. Let $\mathcal{A}_k(Q) = R/Q$ denote the quotient ring.

Since we can add elements of $\mathcal{A}_k(Q)$ and multiply elements with scalars in k, $\mathcal{A}_k(Q)$ has the structure of a vector space over the field k. Furthermore, if Q is zero-dimensional, then $\mathcal{A}_k(Q)$ is a finite-dimensional vector space.

Given a polynomial $r \in R$, we define a map m_r from $\mathcal{A}_k(Q)$ to itself by multiplication:

$$\begin{aligned} m_r :\ & \mathcal{A}_k(Q) \to \mathcal{A}_k(Q), \\ & [g] \mapsto [rg], \end{aligned}$$

where $[g]$ denotes the residue class in $\mathcal{A}_k(Q)$ of the polynomial $g \in R$.

Here are the main properties of the map m_r.

Proposition 2.1. *Let $r \in R$. Then*

(1) *m_r is a linear map from $\mathcal{A}_k(Q)$ to $\mathcal{A}_k(Q)$.*

(2) *$m_r = m_g$ holds exactly when $r - g \in Q$. In particular, m_r is the zero map exactly when $r \in Q$.*

(3) *Let q be a univariate polynomial over k. Then $m_{q(r)} = q(m_r)$.*

(4) *If* $\mathrm{Chp}(m_r)$ *is the characteristic polynomial of* m_r*, then* $\mathrm{Chp}(m_r)(r) \in Q$.

Proof. For the proofs of parts (1), (2) and (3), please see [4]. For the part (4), since $\mathrm{Chp}(m_r)$ is the characteristic polynomial of the linear map m_r, $\mathrm{Chp}(m_r)(m_r) = 0$ by Cayley-Hamilton theorem. According to part (3), it follows that $m_{\mathrm{Chp}(m_r)(r)} = \mathrm{Chp}(m_r)(m_r) = 0$. Thus, $\mathrm{Chp}(m_r)(r)$ belongs to the ideal Q by part (2). □

Proposition 2.2. *If* Q *is a maximal ideal of* R*, then the* minimal *polynomial of* m_r *is irreducible over* k.

Proof. Assume R is the polynomial ring $k[x_1, \ldots, x_n]$. Let $\langle Q, z - r\rangle$ be the ideal generated by Q and $z - r$ over the polynomial ring $k[x_1, \ldots, x_n, z]$, where z is a new indeterminate. Since Q is a maximal ideal in $k[x_1, \ldots, x_n]$, it follows that $\langle Q, z - r\rangle$ is also a maximal ideal in $k[x_1, \ldots, x_n, z]$ and so is the ideal $\langle Q, z - r\rangle \cap k[z]$.

To study the ideal $\langle Q, z - r\rangle \cap k[z]$, let g be the monic generator of the principal ideal $\langle Q, z - r\rangle \cap k[z]$. Substitute the indeterminate z by r in g, then $g(r) \in \langle Q, z - r\rangle \cap k[x_1, \ldots, x_n] = Q$, which means $g(m_r) = m_{g(r)} = 0$ by Proposition 2.1. Since $\langle Q, z - r\rangle \cap k[z]$ is maximal in $k[z]$, g is irreducible over k, and hence g is the minimal polynomial of m_r. □

Since the characteristic polynomial and minimal polynomial of a linear map will be used quite frequently in this paper, we use the notations $\mathrm{Chp}_{\mathcal{A}_k(Q)}(m_r)$ and $\mathrm{Mp}_{\mathcal{A}_k(Q)}(m_r)$ to denote the characteristic polynomial and the minimal polynomial of m_r in $\mathcal{A}_k(Q)$ respectively. Sometime we use $\mathrm{Chp}(m_r)$ and $\mathrm{Mp}(m_r)$ for short, if no confusion occurs.

The following proposition, which is a basic conclusion from standard linear algebra, illustrates the relationship between *minimal* polynomial and *characteristic* polynomial.

Proposition 2.3. *The minimal polynomial* $\mathrm{Mp}_{\mathcal{A}_k(Q)}(m_r)$ *and characteristic polynomial* $\mathrm{Chp}_{\mathcal{A}_k(Q)}(m_r)$ *share the same irreducible factors.*

Thus we have an instant corollary of Proposition 2.2.

Corollary 2.4. *If* Q *is a maximal ideal of* R*, then the* characteristic *polynomial* $\mathrm{Chp}_{\mathcal{A}_k(Q)}(m_r)$ *is a power of a polynomial which is irreducible over* k.

With the above propositions, next we study more properties about $\mathrm{Chp}_{\mathcal{A}_k(Q)}(m_r)$.

Now suppose that Q is a zero-dimensional radical ideal of R and Q has a minimal prime decomposition:

$$Q = Q_1 \cap \cdots \cap Q_t,$$

where each Q_i is a prime ideal of R.

We define the linear map $m_{r,i}$ in the same fashion as m_r. Denote $\mathcal{A}_k(Q_i) = R/Q_i$ for $i = 1, \ldots, t$, and consider the linear maps:

$$\begin{aligned} m_{r,i}:\ & \mathcal{A}_k(Q_i) \to \mathcal{A}_k(Q_i), \\ & [g] \mapsto [rg], \end{aligned}$$

where $[g]$ denotes the residue class in $\mathcal{A}_k(Q_i)$ of the polynomial $g \in R$.

The following proposition proposed by Monico [19] describes the relationship between the characteristic polynomials of m_r and $m_{r,i}$'s.

Proposition 2.5. *Let* $\mathrm{Chp}_{\mathcal{A}_k(Q)}(m_r)$, $\mathrm{Chp}_{\mathcal{A}_k(Q_i)}(m_{r,i})$ *be the characteristic polynomials of* $m_r, m_{r,i}$ *respectively. Then*

$$\mathrm{Chp}_{\mathcal{A}_k(Q)}(m_r) = \mathrm{Chp}_{\mathcal{A}_k(Q_1)}(m_{r,1}) \cdots \mathrm{Chp}_{\mathcal{A}_k(Q_t)}(m_{r,t}).$$

3 Factorization of polynomials over algebraic extension field

In this section, we will discuss the main ideas about the new factorization method. First of all, we need some new notations. Throughout this section, let $R = k[x_1, \ldots, x_n]$ and $R_y = k[x_1, \ldots, x_n, y]$. Please

note that the notation R represents a general multivariate polynomial ring in the last section, while in this section R denotes the specific polynomial ring $k[x_1, \ldots, x_n]$. I is a *maximal* ideal in R and I_y is the ideal generated by I over the polynomial ring R_y. Since I is a maximal ideal, the quotient ring R/I is indeed a field. For convenience, we denote $\mathrm{K} = R/I$, which is a finite extension field of k. Remark that the quotient ring R_y/I_y is not a field, as I_y is not a maximal ideal in R_y any more.

The ring $\mathrm{K}[y]$, which is a polynomial ring over K with the indeterminate y, is a principal ideal domain, so each polynomial f in $\mathrm{K}[y]$ has a unique factorization over K. What we will do next is to give an efficient algorithm to calculate the factorization of f in $\mathrm{K}[y]$.

In order to exploit the properties of I, we should connect the ring R_y and $\mathrm{K}[y]$. Consider the canonical map:

$$\begin{aligned} \sigma :\ & R \to \mathrm{K} = R/I, \\ & c \mapsto [c], \end{aligned}$$

which sends a polynomial $c \in R$ to $[c] \in \mathrm{K}$. And σ extends canonically onto R_y by applying σ coefficient-wise. By definition, $\sigma(g) = 0$ if and only if $g \in I_y$ for any $g \in R_y$.

Conversely, given an element $c \in \mathrm{K}$, we say a polynomial $d \in R$ is a *lift* of c if $\sigma(d) = c$. Similarly, we say $h \in R_y$ is a *lift* of $g \in \mathrm{K}[y]$ if $\sigma(h) = g$ holds. Clearly, an element $c \in \mathrm{K}$ (or $g \in \mathrm{K}[y]$) may have infinite distinct lifts, as the map σ is not injective. Pay attention that, the lifts of $g \in \mathrm{K}[y]$ may have different degrees in y.

Since $\mathrm{K} = k(\alpha_1, \ldots, \alpha_n) = k[\alpha_1, \ldots, \alpha_n]$, the elements in K have polynomial forms in the letters $\alpha_1, \alpha_2, \ldots, \alpha_n$, i.e., for $g \in \mathrm{K}[y]$, g has the following form:

$$g = \sum_{i=0}^{d} c_i(\alpha) y^i,$$

where $c_i(\alpha) \in k[\alpha_1, \ldots, \alpha_n]$ for $i = 0, \ldots, d$. Let $h = \sum_{i=0}^{d} c_i(x) y^i$, where $c_i(x) \in k[x_1, \ldots, x_n]$ such that $\sigma(c_i(x)) = c_i(\alpha)$. It is easy to check $\sigma(h) = g$, and we call h a *natural lift* of g.

Let F be a set of polynomials in R_y, the ideal generated by F over R_y is denoted by $\langle F \rangle_{R_y}$ as usual.

In the rest of this paper, we always make the following assumptions:

- f is a square-free polynomial in $\mathrm{K}[y]$ and $h \in R_y$ is a lift of f.
- $Q = \langle I, h \rangle_{R_y} \subset R_y$ and $\mathcal{A}_k(Q) = R_y/Q$.
- For $r \in R_y$, the linear map m_r is defined from $\mathcal{A}_k(Q)$ to $\mathcal{A}_k(Q)$ as in the last section.
- $f = f_1 \cdots f_t$ is an irreducible factorization of f over K and h_i is a lift of f_i.
- $m_{r,i}$ is the linear map defined from $\mathcal{A}_k(Q_i)$ to $\mathcal{A}_k(Q_i)$, where $\mathcal{A}_k(Q_i) = R_y/Q_i$ and $Q_i = \langle I, h_i \rangle_{R_y}$ for $i = 1, \ldots, t$.
- $\mathrm{Chp}_{\mathcal{A}_k(Q)}(m_r)$, $\mathrm{Chp}_{\mathcal{A}_k(Q_i)}(m_{r,i}) \in k[\lambda]$ are the characteristic polynomials of m_r and $m_{r,i}$ respectively. We use $\mathrm{Chp}(m_r), \mathrm{Chp}(m_{r,i})$ for short, if no confusion occurs.

Now it is time to describe the main ideas of the new algorithm for factoring f over $\mathrm{K}[y]$. The following lemma builds a relation between the factorization of a square-free polynomial and the minimal decomposition of a radical ideal.

Lemma 3.1. *$Q = \langle I, h \rangle_{R_y} \subset R_y$ is a radical ideal and*

$$Q = Q_1 \cap \cdots \cap Q_t$$

is a minimal prime decomposition of Q, where $Q_i = \langle I, h_i \rangle_{R_y}$ for $i = 1, \ldots, t$.

Proof. First, we begin by showing the definition of $Q = \langle I, h \rangle_{R_y}$ is well defined. Suppose h' is another lift of f in R_y. Then it suffices to show the two ideals $Q = \langle I, h \rangle_{R_y}$ and $Q' = \langle I, h' \rangle_{R_y}$ are identical. By the definition of lift, we have $\sigma(h) = f = \sigma(h')$. Since σ is a homomorphism map, it follows that $\sigma(h - h') = 0$, which means $h - h' \in I_y$ and hence $Q = Q'$. Similarly, Q_i's are also well defined for the same reasons.

Next, we prove $Q = \langle I, h\rangle_{R_y}$ is a radical ideal of R_y. If $g^m \in Q$ for some positive integer m, then g^m has an expression $g^m = t + sh$, where $t \in I_y$ and $s \in R_y$. Since σ is a homomorphism map, we have

$$\sigma(g)^m = \sigma(g^m) = \sigma(t) + \sigma(s)\sigma(h) = \sigma(s)f,$$

which means $f \mid \sigma(g)^m$. Since f is a square-free polynomial as assumed, $f \mid \sigma(g)^m$ implies $f \mid \sigma(g)$. Let $\sigma(g) = bf$, $b \in \mathrm{K}[y]$ and $a \in R_y$ be a lift of b. Since h is a lift of f, it follows that $\sigma(g) = \sigma(a)\sigma(h)$, which means $\sigma(g - ah) = 0$ and hence $g - ah \in I_y$. So $g \in Q$, which shows Q is a radical ideal.

Similarly, it is easy to show Q_i is a prime ideal by using the property that f_i is irreducible over K (hence square-free), and the proof is omitted here.

Finally, we finish this proof by showing the Q_i's constitute a minimal prime decomposition of Q.

On one hand, we have $f \mid \sigma(g)$ for any $g \in Q$. It follows that $f_i \mid \sigma(g)$ for $i = 1, \ldots, t$. Then g belongs to each Q_i as discussed above and hence lies in the intersection of these Q_i's.

On the other hand, given $g \in Q_1 \cap \cdots \cap Q_t$, it is easy to see that $f_i \mid \sigma(g)$ for all $i = 1, 2, \ldots, t$. Since f_i's are irreducible factors of f and coprime with each other, it follows that $f = f_1 f_2 \cdots f_t \mid \sigma(g)$, which means there exists $a \in R_y$ such that $\sigma(g) = \sigma(a)f$ and hence $g - ah \in I_y$. Thus, $g \in Q$.

We have now proved that

$$Q = Q_1 \cap \cdots \cap Q_t.$$

As f_i and f_j are distinct irreducible factors of f whenever $i \neq j$, then $h_i \notin Q_j$ and $h_j \notin Q_i$, which indicates the above decomposition is minimal. □

The following theorem is the main theorem of this paper which provides a new method for factoring polynomials over algebraic extension fields.

Theorem 3.2 (Main theorem)**.** *With the notations defined as earlier, if the characteristic polynomial* $\mathrm{Chp}(m_r)$ *has an irreducible factorization*:

$$\mathrm{Chp}(m_r) = q_1^{m_1} \cdots q_s^{m_s},$$

where q_i *is irreducible over* k *and* $q_i \neq q_j$ *whenever* $i \neq j$*, then* $\gcd(f, \sigma(q_i(r))) \neq 1$ *and*

$$f = c \prod_{i=1}^{s} \gcd(f, \sigma(q_i(r))),$$

where c *is constant in* K *and* $\gcd(g_1, g_2)$ *is the monic greatest common divisor of* g_1 *and* g_2 *for any* $g_1, g_2 \in \mathrm{K}[y]$*. Furthermore, if* $m_i = 1$*, then* $\gcd(f, \sigma(q_i(r)))$ *is irreducible over* K.

Proof. For convenience, suppose f is monic. In this case, $c = 1$.

Since f is square-free and $f = f_1 \cdots f_t$ is an irreducible factorization of f as assumed, $Q = \langle I, h\rangle_{R_y}$ is a radical ideal and $Q_i = \langle I, h_i\rangle_{R_y}$'s are prime ideals by Lemma 3.1. Furthermore, Q has a minimal prime decomposition $Q = Q_1 \cap \cdots \cap Q_t$. We also have $\mathrm{Chp}(m_r) = \mathrm{Chp}(m_{r,1}) \cdots \mathrm{Chp}(m_{r,t})$ by Proposition 2.5.

Since $\mathrm{Chp}(m_{r,i}) \in k[\lambda]$ is the characteristic polynomial of $m_{r,i}$, substituting λ in $\mathrm{Chp}(m_{r,i})$ by the expression of $r \in R_y$, it follows that $\mathrm{Chp}(m_{r,i})(r) \in Q_i = \langle I, h_i\rangle_{R_y}$ by Proposition 2.1. That is, there exist $a \in I_y$ and $b \in R_y$ such that $\mathrm{Chp}(m_{r,i})(r) = a + bh_i$. Applying σ to both sides of equation, we get $\sigma(\mathrm{Chp}(m_{r,i})(r)) = \sigma(a) + \sigma(b)\sigma(h_i) = \sigma(b)f_i$, which means $f_i \mid \sigma(\mathrm{Chp}(m_{r,i})(r))$. This shows that f_i is a nontrivial common divisor of f and $\sigma(\mathrm{Chp}(m_{r,i})(r))$ for $1 \leqslant i \leqslant t$.

By Corollary 2.4, each $\mathrm{Chp}(m_{r,i})$ must be a power of an irreducible polynomial in $k[\lambda]$. Notice that $\mathrm{Chp}(m_r) = \mathrm{Chp}(m_{r,1}) \cdots \mathrm{Chp}(m_{r,t}) = q_1^{m_1} \cdots q_s^{m_s}$, which implies that for each j there exists at least one $\mathrm{Chp}(m_{r,i})$ such that $\mathrm{Chp}(m_{r,i}) \mid q_j$. So $\gcd(f, \sigma(q_j(r))) \neq 1$ for $1 \leqslant j \leqslant s$.

We have already shown that $f_i \mid \sigma(\mathrm{Chp}(m_{r,1})(r)) \cdots \sigma(\mathrm{Chp}(m_{r,t})(r)) = \sigma(q_1(r))^{m_1} \cdots \sigma(q_s(r))^{m_s}$. Since f_i is irreducible over K, then there exists a j where $1 \leqslant j \leqslant s$, such that $f_i \mid \sigma(q_j(r))$. As assumed, $f_1, \ldots, f_t$ are distinct factors of the square-free polynomial f. It follows that

$$f = f_1 \cdots f_t \Big| \prod_{i=1}^{s} \gcd(f, \sigma(q_i(r))). \tag{3.1}$$

For each i, $\gcd(f, \sigma(q_i(r)))$ is square-free since f itself is square-free.

Since q_i and q_j are co-prime in $k[\lambda]$ whenever $i \neq j$, then there exist $a, b \in k[\lambda]$ such that $aq_i + bq_j = 1$. Substituting λ by the expression of r, the equality still holds for $a(r)q_i(r) + b(r)q_j(r) = 1$. Applying σ to both sides of equation, we have $\sigma(a(r))\sigma(q_i(r)) + \sigma(b(r))\sigma(q_j(r)) = 1$, which implies $\sigma(q_i(r))$ and $\sigma(q_j(r))$ are co-prime in K[y] and hence $\gcd(f, \sigma(q_i(r)))$ and $\gcd(f, \sigma(q_j(r)))$ are co-prime as well. Therefore, $\prod_{i=1}^{s} \gcd(f, \sigma(q_i(r)))$ is square-free, which indicates

$$\prod_{i=1}^{s} \gcd(f, \sigma(q_i(r))) \mid f, \tag{3.2}$$

since $\gcd(f, \sigma(q_i(r))) \mid f$ for $1 \leqslant i \leqslant s$.

From (3.1) and (3.2), we have $f = \prod_{i=1}^{s} \gcd(f, \sigma(q_i(r)))$. The first part of theorem is proved.

Particularly, if $m_k = 1$ for some k, the equation $q_1^{m_1} \cdots q_s^{m_s} = \mathrm{Chp}(m_{r,1}) \cdots \mathrm{Chp}(m_{r,t})$ shows q_k divides only one $\mathrm{Chp}(m_{r,i})$. Then we have $\mathrm{Chp}(m_{r,i}) = q_k$ and $\mathrm{Chp}(m_{r,i})$ is co-prime with other $\mathrm{Chp}(m_{r,j})$ whenever $i \neq j$. With a similar discussion, it is easy to show $\sigma(\mathrm{Chp}(m_{r,i})(r))$ and $\sigma(\mathrm{Chp}(m_{r,j})(r))$ are co-prime in K[y] whenever $i \neq j$. Clearly, $\gcd(f, \sigma(\mathrm{Chp}(m_{r,i})(r))) = \gcd(f, \sigma(q_k(r)))$ is a factor of f and we also know $f_i \mid \gcd(f, \sigma(\mathrm{Chp}(m_{r,i})(r)))$ as discussed earlier. Therefore, if there exists f_j such that $f_i \neq f_j$ and $f_j \mid \gcd(f, \sigma(\mathrm{Chp}(m_{r,i})(r)))$, then $\sigma(\mathrm{Chp}(m_{r,i}))$ and $\sigma(\mathrm{Chp}(m_{r,j}))$ will have a nontrivial common divisor f_j. This contradiction implies $\gcd(f, \sigma(q_k(r))) = f_i$ and hence irreducible over K. □

Then we have two immediate corollaries of the main theorem.

Corollary 3.3. *If* $\mathrm{Chp}(m_r)$ *is square-free, suppose* $\mathrm{Chp}(m_r) = q_1 \cdots q_s$ *is an irreducible factorization of* $\mathrm{Chp}(m_r)$ *over* k*, then*

$$f = c \prod_{i=1}^{s} \gcd(f, \sigma(q_i(r)))$$

is an irreducible factorization of f *over* K*, where* c *is constant in* K.

Corollary 3.4. *If* $\mathrm{Chp}(m_r)$ *is irreducible over* k*, then* f *is irreducible over* K.

Corollary 3.3 indicates that if we are lucky enough to get a square-free $\mathrm{Chp}(m_r)$, then we can obtain the complete factorization of f directly; otherwise, by the main Theorem 3.2, we will get some factors of f, which can be factored in a further step.

The most important contribution of the main theorem is that we are able to check which factor of f is irreducible by simply investigating whether m_i is 1, which ensures the method provided in this paper is a complete method for factoring polynomials in K[y].

4 Algorithm for factorization

In this section, we will present the algorithm for factorization over algebraic extension field based on the main Theorem 3.2. Before doing that, we discuss some algorithmic details first.

Given a polynomial $f \in \mathrm{K}[y]$, it is usually not square-free. So in order to apply the main theorem, we can factor the square-free part of f first and deduce a factorization of f afterwards, which is not very difficult no matter the field K is characteristic 0 or not. In the new algorithm, the gcd computation over algebraic extension field is necessary, and many algorithms have been proposed for this purpose [10,14,18].

In case the *characteristic* polynomial $\mathrm{Chp}(m_r)$ is difficult to compute, we can calculate the *minimal* polynomial $\mathrm{Mp}(m_r)$ instead with the following observation.

Proposition 4.1. *If the* characteristic *polynomial* $\mathrm{Chp}(m_r)$ *is square-free, then the* minimal *polynomial* $\mathrm{Mp}(m_r)$ *and the* characteristic *polynomial* $\mathrm{Chp}(m_r)$ *are identical.*

Proof. It is an easy corollary of Proposition 2.3. □

Conversely, if the minimal polynomial has lower degree than its characteristic polynomial, then the characteristic polynomial is not square-free. Many methods can be used for computing the minimal polynomial, such as the famous FGLM method (see [7]).

Now, it is time to present the algorithm for factorization over algebraic extension field.

Algorithm 1 — Factorization

Input: f, a square-free monic polynomial in $\mathrm{K}[y]$.

Output: the factorization of f in $\mathrm{K}[y]$.

begin
  $r\leftarrow$ a random polynomial in $k[x_1,\ldots,x_n,y]$
  $\mathrm{Chp}(m_r)\leftarrow$ the characteristic polynomial of the linear map m_r
  factorize $\mathrm{Chp}(m_r)$ over k and obtain $\mathrm{Chp}(m_r)=q_1^{m_1}\cdots q_s^{m_s}$
  for i **from** 1 **to** s **do**
    $f_i\leftarrow\gcd(f,\sigma(q_i(r)))$
    if $m_i=1$ $\quad\#f_i$ is irreducible
      then $g_i\leftarrow f_i$
      else $g_i\leftarrow$Factorization(f_i)
    end if
  end for
  return $g_1g_2\cdots g_s$
end

Remark 4.2. The computation of $\mathrm{Chp}(m_r)$ is an important step of the above algorithm. According to the method provided in [4], $\mathrm{Chp}(m_r)$ is easy to compute if the Gröbner basis of $Q=\langle I,h\rangle_{R_y}$ is known, where h is a nature lift of f. Fortunately, if f is monic in $\mathrm{K}[y]$, the Gröbner basis of Q can be constructed directly, since $\{G,h\}$ is a Gröbner basis of $\langle I,h\rangle_{R_y}$ with the elimination monomial order $y\succ x$, where G is a Gröbner basis of I.

The correctness of the above algorithm is ensured by the main Theorem 3.2. So it remains to discuss the termination.

First, we will show $\mathrm{Chp}(m_r)$ is square-free with a fairly high probability for a random chosen $r\in R_y$. Clearly, if $\mathrm{Chp}(m_r)$ is square-free, then the algorithm terminates immediately by Corollary 3.3.

Proposition 4.3. *If the characteristic of k is 0, then the probability that the characteristic polynomial $\mathrm{Chp}(m_r)$ is square-free for a random $r\in R_y$ is 1.*

Proof. The technique of the proof draws lessons from [19].

Since $Q=\langle I,h\rangle_{R_y}$ is a zero-dimensional radical ideal, the quotient ring $\mathcal{A}_k(Q)=R_y/Q$ has finite dimension as a vector space. Let $d=\dim_k(\mathcal{A}_k(Q))$. According to the basic algebraic geometry, we know the variety $V(Q)$ has d distinct points, say $z_1,\ldots,z_d$, in an extension field of k.

Notice that $\mathrm{Chp}(m_r)\in k[\lambda]$ is square-free if and only if $r(z_i)\neq r(z_j)$ whenever $i\neq j$, which is a direct consequence of Theorem 4.5 in [4]. Therefore, consider the following set:

$$C=\{r\mid \mathrm{Chp}(m_r)\text{ is not square-free}\}=\{r\mid \exists\, z_i,z_j\in V(Q)\text{ with }z_i\neq z_j\text{ such that }r(z_i)=r(z_j)\}.$$

Since $V(Q)$ has finite points, it only suffices to show the set

$$C_{ij}=\{r\mid r(z_i)=r(z_j)\text{ and }z_i\neq z_j\}$$

is an algebraic set.

Let $\{e_1,\ldots,e_d\}$ be the standard monomial basis of $\mathcal{A}_k(Q)$. Thus, $[r]=a_1e_1+\cdots+a_de_d$, where $a_i\in k$ for $i=1,\ldots,d$. So C_{ij} also has an isomorphic form:

$$\tilde{C}_{ij}=\{(a_1,\ldots,a_d)\in k^d\mid a_1e_1(z_i)+\cdots+a_de_d(z_i)=a_1e_1(z_j)+\cdots+a_de_d(z_j)\text{ and }z_i\neq z_j\}.$$

According to [4, Subsection 2.4], z_i is uniquely determined by the vector $(e_1(z_i), \ldots, e_d(z_i))$. Therefore, $z_i \neq z_j$ implies

$$(e_1(z_i), \ldots, e_d(z_i)) \neq (e_1(z_j), \ldots, e_d(z_j)),$$

and hence $(e_1(z_i) - e_1(z_j), \ldots, e_d(z_i) - e_d(z_j))$ is a nonzero vector.

Thus $\tilde{C}_{ij}$ is a proper algebraic set in k^d. Consequently, C is isomorphic to a proper algebraic set of k^d. Since the characteristic of k is 0, the probability that a random $r \in R_y$ belongs to the set C is 0, which completes the proof. □

In order to simplify the computation, we usually prefer r in a linear form. The following corollary shows $\mathrm{Chp}(m_r)$ is also square-free with a high probability for a randomly chosen *linear* r.

Corollary 4.4. *If the characteristic of k is 0, then the probability that the characteristic polynomial $\mathrm{Chp}(m_r)$ is square-free for a random* linear *$r \in R_y$ is also* 1.

Proof. The proof is in the same fashion as Proposition 4.3. The only difference is that r has a *linear* expression $r = by + a_1x_1 + \cdots + a_nx_n$. Then the set $C_{ij} = \{r \mid r(z_i) = r(z_j) \text{ and } z_i \neq z_j\}$ is isomorphic to a proper algebraic set of k^{n+1}, which completes the proof. □

There are some tricks for choosing a linear r so as to speed up the algorithm. For example, the variable y needs to appear in the expression of r and we usually set the coefficient of y as 1; also, if the variable x_i happens to be a leading power product of some polynomial in the Gröbner basis of I, then this variable x_i is not needed in r, as it can be reduced afterwards.

Although the probability that the characteristic polynomial $\mathrm{Chp}(m_r)$ is square-free for a random (linear) $r \in R_y$ is 1, it is not sufficient to show the algorithm terminates all the time. However, the following proposition indicates that if we select r in a special fashion, the algorithm terminates in finite steps.

Proposition 4.5. *If the characteristic of k is 0, then we can find an $r \in R_y$ such that $\mathrm{Chp}(m_r)$ is square-free in finite steps.*

Proof. In fact, according to the proof of Proposition 4.3, the set C is the union of all C_{ij} for $i \neq j$, where C_{ij} is isomorphic to the set $\{(a_1, \ldots, a_d) \in k^d \mid a_1(e_1(z_i) - e_1(z_j)) + \cdots + a_d(e_d(z_i) - e_d(z_j)) = 0 \text{ and } z_i \neq z_j\}$. Thus, C is isomorphic to the solution set of a polynomial equation $F(a_1, \ldots, a_d) = 0$, while the total degree of F is at most $d(d-1)/2$. Let $d_i = \deg_{a_i} F(a_1, \ldots, a_d)$ for $i = 1, \ldots, d$ and $D = \{(a_1, \ldots, a_d) \mid a_i \text{ is an integer}, 0 \leqslant a_i \leqslant d_i \text{ and } 1 \leqslant i \leqslant d\}$. Since $F \neq 0$, F cannot vanish on all the points of D. So there must exist $(a'_1, \ldots, a'_d) \in D$ such that $F(a'_1, \ldots, a'_d) \neq 0$. Then $r = a'_1e_1 + \cdots + a'_de_d$ is the r such that $\mathrm{Chp}(m_r)$ is square-free. As the cardinality of D is finite, this r can be constructed within finite steps. □

Therefore, in each recursive call of Factorization(f_i), if we choose a different r in the above fashion, the algorithm must terminate in finite steps.

5 A rough complexity analysis

At last, we say something about the complexity of the new algorithm. The complexity of this algorithm contains three parts:

(1) Given a Gröbner basis G of I, then the set $\{G, h\}$ is a Gröbner basis of $Q = \langle I, h\rangle_{R_y}$ as discussed earlier, so computing a basis for $\mathcal{A}_k(Q)$ has complexity $O(D)$, where D is the dimension of the linear space $\mathcal{A}_k(Q)$.

(2) Computing the matrix of m_r requires $O(D^3)$ field operations in the worst case. Computing the characteristic polynomial $\mathrm{Chp}(m_r)$ requires $O(D^3)$ field operations.

(3) Factorizing the univariate polynomial $\mathrm{Chp}(m_r)$ has been studied by many researchers, and more details can be found in [3, 15].

As a result, by using this new algorithm, the problem of factoring polynomials over algebraic extension field can be transformed to the factorization of univariate polynomials over the ground field in polynomial time.

6 A complete example

In this section, we illustrate the new algorithm through a complete example.

Example 6.1. Given a maximal ideal $I = \langle x_1^2 + 1, x_2^2 + x_1\rangle \subset \mathbb{Q}[x_1, x_2]$, where $\mathbb{Q}$ is the rational field. Then the extension field is $\mathrm{K} = \mathbb{Q}[x_1, x_2]/I$. Notice that $\{x_1^2 + 1, x_2^2 + x_1\}$ is already a Gröbner basis of I for the lexicographic order with $x_2 \succ x_1$.

We are going to factor the polynomial

$$f = y^3 + (\alpha_1\alpha_2 - 2\alpha_1 - \alpha_2)y^2 + (\alpha_1\alpha_2 + 2\alpha_2 - 2)y + \alpha_1 - \alpha_1\alpha_2 \in \mathrm{K}[y],$$

where $\alpha_i = [x_i] \in \mathrm{K}$.

Since f is square-free and monic in $\mathrm{K}[y]$,

$$h = y^3 + (x_1x_2 - 2x_1 - x_2)y^2 + (x_1x_2 + 2x_2 - 2)y + x_1 - x_1x_2 \in R_y$$

is a natural lift of f. Thus, $\{x_1^2 + 1, x_2^2 + x_1, h\}$ is a Gröbner basis of the ideal $Q = \langle I, h\rangle_{\mathbb{Q}[x_1,x_2,y]}$ for the lexicographic order with $y \succ x_2 \succ x_1$.

According to the new algorithm, we need to choose a random polynomial $r \in R_y = \mathbb{Q}[x_1, x_2, y]$ first. Here $r = x_1 + 2x_2 + y$ is selected. Let $\mathcal{A}_k(Q) = \mathbb{Q}[x_1, x_2, y]/Q$, which is a vector space over $\mathbb{Q}$ with a monomial basis

$$B = [1, x_2, x_1, x_1x_2, y, x_2y, x_1y, x_1x_2y, y^2, x_2y^2, x_1y^2, x_1x_2y^2]^{\mathrm{T}}.$$

Next, compute the matrix M of the linear map m_r w.r.t. B. Then

$$m_r(B) = MB,$$

where M is a 12×12 matrix,

$$M = \begin{pmatrix}
0 & 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & -2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
-1 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\
2 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & -2 & 1 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 2 & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 0 & -1 & 1 & 2 & -2 & 0 & -1 & 0 & 3 & 3 & -1\\
1 & 0 & 0 & -1 & -1 & 2 & 2 & 0 & -1 & 0 & -3 & 3\\
1 & -1 & 0 & 0 & 0 & 1 & 2 & -2 & -3 & 1 & 0 & 3\\
0 & 1 & 1 & 0 & -2 & 0 & -1 & 2 & 3 & -3 & -1 & 0
\end{pmatrix}$$

The characteristic polynomial of this matrix is

$$\begin{aligned}\mathrm{Chp}(m_r) &= \lambda^{12} + 26\lambda^{10} - 116\lambda^9 + 371\lambda^8 - 2064\lambda^7 + 6802\lambda^6 - 17916\lambda^5 + 49922\lambda^4\\ &\quad - 109088\lambda^3 + 155984\lambda^2 - 134592\lambda + 55872\\ &= (\lambda^4 + 10\lambda^2 - 12\lambda + 18)(\lambda^4 + 8\lambda^2 - 72\lambda + 97)(\lambda^4 + 8\lambda^2 - 32\lambda + 32).\end{aligned}$$

The next step is to substitute λ by the expression of r in each factor of $\mathrm{Chp}(m_r)$. For example, $q_1 = \lambda^4 + 10\lambda^2 - 12\lambda + 18$ becomes

$$q_1(r) = (x_1 + 2x_2 + y)^4 + 10(x_1 + 2x_2 + y)^2 - 12(x_1 + 2x_2 + y) + 18.$$

And

$$\sigma(q_1(r)) = (\alpha_1 + 2\alpha_2 + y)^4 + 10(\alpha_1 + 2\alpha_2 + y)^2 - 12(\alpha_1 + 2\alpha_2 + y) + 18 \in \mathrm{K}[y].$$

In the following, we compute the gcd of f and $\sigma(q_1(r))$. Finally obtain

$$\gcd(f, \sigma(q_1(r))) = y + \alpha_1\alpha_2.$$

Since $m_1 = 1$, $y + \alpha_1\alpha_2$ is an irreducible factor of f by Theorem 3.2. Similarly, since $m_2 = m_3 = 1$, the other irreducible factors of f can be obtained from $q_2 = \lambda^4 + 8\lambda^2 - 72\lambda + 97$ and $q_3 = \lambda^4 + 8\lambda^2 - 32\lambda + 32$:

$$\gcd(f, \sigma(q_2(r))) = y - \alpha_1 - \alpha_2, \quad \gcd(f, \sigma(q_3(r))) = y - \alpha_1.$$

As a result, we get a complete factorization of $f \in \mathrm{K}[y]$:

$$f = (y + \alpha_1\alpha_2)(y - \alpha_1 - \alpha_2)(y - \alpha_1).$$

In the above procedure, $\mathrm{Chp}(m_r)$ is square-free, so we obtain a complete factorization of f directly. However, what if $\mathrm{Chp}(m_r)$ is not square-free?

For example, if $r = -\frac{3}{2}x_1 - \frac{1}{2}x_2 + y$ is selected at the beginning, then we repeat the above steps.

The monomial basis B does not change, but the matrix varies and the characteristic polynomial becomes

$$\begin{aligned}\mathrm{Chp}(m_r) &= \lambda^{12} + \frac{7}{2}\lambda^{10} - \frac{7}{2}\lambda^9 + \frac{113}{8}\lambda^8 - \frac{3}{2}\lambda^7 + \frac{33}{4}\lambda^6 + \frac{41}{4}\lambda^5 + \frac{273}{64}\lambda^4 + \frac{67}{16}\lambda^3 + \frac{467}{128}\lambda^2 + \frac{169}{128}\lambda + \frac{89}{512}\\ &= \left(\lambda^4 + \frac{5}{2}\lambda^2 - \frac{9}{2}\lambda + \frac{89}{8}\right)\left(\lambda^4 + \frac{1}{2}\lambda^2 + \frac{1}{2}\lambda + \frac{1}{8}\right)^2.\end{aligned}$$

Let $q_1 = \lambda^4 + \frac{5}{2}\lambda^2 - \frac{9}{2}\lambda + \frac{89}{8}$ and $q_2 = \lambda^4 + \frac{1}{2}\lambda^2 + \frac{1}{2}\lambda + \frac{1}{8}$. Since $m_1 = 1$, we can get an irreducible factor of f by Theorem 3.2:

$$\gcd(f, \sigma(q_1(r))) = y + \alpha_1\alpha_2.$$

While the other factor q_2 only leads to a reducible factor of f:

$$\gcd(f, \sigma(q_2(r))) = y^2 - (2\alpha_1 + \alpha_2)y + \alpha_1\alpha_2 - 1,$$

which needs to be factored further.

Let $f' = y^2 - (2\alpha_1 + \alpha_2)y + \alpha_1\alpha_2 - 1$ and $h' = y^2 - (2x_1 + x_2)y + x_1x_2 - 1 \in R_y$ is a natural lift of f'. Next $r' = -2x_1 - 2x_2 + y$ is chosen. And the monomial basis of $\mathbb{Q}[x_1, x_2, y]/\langle I, h'\rangle_{\mathbb{Q}[x_1,x_2,y]}$ is

$$B' = [1, x_2, x_1, x_1x_2, y, yx_2, yx_1, yx_1x_2]^{\mathrm{T}}.$$

Notice the length of B' is 8, which is smaller than the previous one. Thus an 8×8 matrix is constructed and the characteristic polynomial is

$$\begin{aligned}\mathrm{Chp}(m_{r'}) &= \lambda^8 + 4\lambda^6 + 20\lambda^5 + 23\lambda^4 + 40\lambda^3 + 102\lambda^2 + 100\lambda + 34\\ &= (\lambda^4 + 2\lambda^2 + 16\lambda + 17)(\lambda^4 + 2\lambda^2 + 4\lambda + 2) = q_1'q_2'.\end{aligned}$$

Since $m_1' = m_2' = 1$, we obtain two irreducible factors of f':

$$\gcd(f', \sigma(q_1'(r'))) = y - \alpha_1 \quad \text{and} \quad \gcd(f', \sigma(q_2'(r'))) = y - \alpha_1 - \alpha_2.$$

Combined with the factor we got earlier, f has a complete factorization in $\mathrm{K}[y]$:

$$f = (y + \alpha_1\alpha_2)(y - \alpha_1)(y - \alpha_1 - \alpha_2).$$

The new algorithm can also perform well when the ground field k is a finite field. However, if we consider the factorization when the ground field is a finite field, according the proof of Proposition 4.3, we will have a lower probability to find an r such that $\mathrm{Chp}(m_r)$ is square-free, especially when the cardinality of k is small.

7 Timings

We have implemented the new algorithm both for the case $k = \mathbb{Q}$ and for finite fields in *Magma*. Since Wang's algorithm can only work for fields of characteristic 0. In order to be fair, the examples are randomly generated over the ground field $k = \mathbb{Q}$.

We tested the examples in appendix both for *cfactor* which is an implementation of Wang's algorithm and for *efactor* which is an implementation of the new algorithm. The timings in the following table are obtained from a computer (Windows XP, CPU Core2 Duo 2.66GHz, Memory 2GB).

We should mention that *cfactor* is implemented in *Maple* 7, since *cfactor* only can work correctly for *Maple* 7, while *efactor* is implemented in *Magma*. For the input of the new algorithm, the maximal ideal can be expressed by its Gröbner basis for any admissible order, generally for a total degree order. And for the input of Wang's algorithm, the maximal ideal has to be its irreducible ascending set, which is equivalent to a lexicographic Gröbner basis. Notice that a Gröbner basis with lexicographic order usually has larger coefficients than that with a total degree order.

In the third column of Table 1, $h^{(i)}$ is a lift of $f^{(i)}$. From Table 1, we can see that the new algorithm is much more efficient than Wang's, especially for complicated examples.

By analyzing Wang's algorithm and the new algorithm, we think there are three main reasons that make the new algorithm more efficient than Wang's. First, in Wang's algorithm, the variable y in f, which is to be factored, needs to be replaced by a linear combination of a new variable y' and the x_i's. This leads to the expansions of the coefficients as well as the terms of f when the degree of f in y is big. Second, the modulo map by a Gröbner basis, which sends a polynomial into its remainder, is a ring homomorphism, which speeds up the new algorithm. But in Wang's algorithm, the pseudo-remainder map does not hold this property. Last and the most important, the complexity of computing the characteristic polynomial of m_r is polynomial time for any given r. However, the complexity of computing the characteristic set in Wang's algorithm is exponential. Besides, any new technique for calculating the characteristic polynomial will speed up the new algorithm as well.

8 Conclusions and future work

In this paper, we present a new method for factoring polynomials over an algebraic extension field and this algorithm performs pretty good for characteristic 0 systems as well as finite field systems. Compared with Monico's primary decomposition method, the new algorithm is complete and the irreducible factors can be verified without extra computations. The new algorithm surely terminates within finite steps if the linear map in each recursive call of the algorithm is selected in a special fashion. And in most cases, the proposed

Table 1 Comparation with Wang's algorithm

	R_y	$\dim_k R_y/\langle I^{(i)}, h^{(i)}\rangle_{R_y}$	cfactor (sec.)	efactor (sec.)
$f^{(1)}$	$\mathbb{Q}[x_1, x_2, y]$	16	0.032	0.000
$f^{(2)}$	$\mathbb{Q}[x_1, x_2, x_3, y]$	28	0.110	0.031
$f^{(3)}$	$\mathbb{Q}[x_1, x_2, x_3, x_4, y]$	48	12.171	0.734
$f^{(4)}$	$\mathbb{Q}[x_1, x_2, x_3, x_4, y]$	32	9.109	0.328
$f^{(5)}$	$\mathbb{Q}[x_1, x_2, x_3, x_4, y]$	64	245.531	4.313
$f^{(6)}$	$\mathbb{Q}[x_1, x_2, x_3, x_4, x_5, y]$	32	44.359	1.297
$f^{(7)}$	$\mathbb{Q}[x_1, x_2, x_3, x_4, x_5, y]$	48	91.500	9.719
$f^{(8)}$	$\mathbb{Q}[x_1, x_2, x_3, x_4, x_5, y]$	48	377.327	11.469
$f^{(9)}$	$\mathbb{Q}[x_1, x_2, x_3, x_4, x_5, y]$	80	2011.375	63.578
$f^{(10)}$	$\mathbb{Q}[x_1, x_2, x_3, x_4, x_5, x_6, y]$	64	> 2h	96.344

algorithm terminates in few loops, as the characteristic polynomial of a generic linear map is square-free with probability 1. Moreover, the total complexity of this new algorithm can be controlled in a reasonable degree.

However, when the characteristic of ground field is 0, the expansion of coefficients is unavoidable. The situation is better in finite field. Therefore, a natural idea emerges. That is we can factor the polynomials in finite field first, and lift the factorization to characteristic 0 afterwards. We also notice that Gao [9] gave an efficient algorithm for computing the primary decomposition over finite fields, which may help to improve the new algorithm in finite field and hence benefits our future work.

Acknowledgements This work was supported by National Key Basic Research Project of China (Grant No. 2011CB302400), National Natural Science Foundation of China (Grant Nos. 10971217, 60970152 and 61121062) and IIE'S Research Project on Cryptography (Grant No. Y3Z0013102).

References

1 Abbott J A, Bradford R J, Davenport J H. A remark on factoritation. ACM Sigsam Bull, 1985, 19: 31–33 & 37
2 Abbott J A, Davenport J H. Polynomial factorization: An exploration of Lenstra's algorithm. In: Lecture Notes in Computer Science, vol. 378. New York: Springer, 1989, 391–402
3 Cohen H. A Course in Computational Algebraic Number Theory. New York: Springer, 1993
4 Cox D, Little J, O'Shea D. Using Algebraic Geometry, 2nd ed. New York: Springer, 2004
5 Encarnacion M J. Computing gcds of polynomials over algebraic number fields. J Symb Comput, 1995, 20: 299–313
6 Encarnacion M J. Factoring polynomials over algebraic number fields via norms. In: Proc of ISSAC 97. New York: ACM Press, 1997, 265–270
7 Faugère J, Gianni P, Lazard D, et al. Efficient computation of zero-dimensional Gröbner bases by change of ordering. J Symb Comput, 1993, 16: 329–344
8 Gao X S, Chou S C. On the theory of resolvents and its applications. Syst Sci Math Sci, 1999, 12: 17–30
9 Gao S H, Wan D Q, Wang M S. Primary decomposition of zero-dimensional ideals over finite fields. Math Comp, 2009, 78: 509–521
10 Hoeij M V, Monagan M. Algorithms for polynomial GCD computation over algebraic function fields. In: Proc of ISSAC 2004. New York: ACM Press, 2004, 297–304
11 Kaltofen E. Factorization of Polynomials. In: Buchberger B, Collins G E, Loos R, eds. Computer Algebra: Symbolic and Algebraic Computation. Wien-New York: Springer-Verlag, 1982, 95–113
12 Kaltofen E. Polynomial Factorization 1982–1986. In: Chudnovsky D V, Jenks D R, eds. Computers in Mathematcis. New York-Basel: Marcel Dekker, 1990, 285–209
13 Landau S. Factoring polynomial over algebraic number fields. SIAM J Comput, 1985, 184–195
14 Langemyr L, McCallum S. The computation of polynomial greatest common divisors over an algebraic number field. J Symb Comput, 1989, 8: 429–448
15 Lenstra H W, Lenstra A K, Lovasz L. Factoring polynomials with rational coefficients. Math Ann, 1982, 261: 515–534
16 Lenstra A K. Factoring multivariate polynomials over algebraic number fields. SIAM J Comput, 1987, 16: 591–598
17 Li B H. An algorithm to decompose a polynomial ascending set into irreducible ones. Acta Anal Funct Appl, 2005, 7: 97–105
18 Maza M M, Rioboo R. Polynomial Gcd computations over towers of algebraic extensions. In: Lecture Notes in Computer Science, vol. 948. Proceeding of 11th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. New York: Springer, 1995, 365–382
19 Monico C. Computing the primary decomposition of zero-dimensional ideals. J Symb Comput, 2002, 34: 451–459
20 Noro M, Yokoyama K. Prime decomposition of radical ideals and algebraic factorization of polynomials. Research Report ISIS-RR-96-8E, 1996
21 Noro M, Yokoyama K. Factoring polynomials over algebraic extension fields. J Inform Sci Res, 1997, 9: 11–33
22 Noro M, Yokoyama K. Implementation of prime decomposition of polynomial ideals over small finite fields. J Symb Comput, 2004, 38: 1227–1246
23 Rouillier F. Solving zero-dimensional polynomail systems through the Rational Univariate Representation. Rapport de recherche INRIA 3426, 1998
24 Steel A. Conquering inseparability: Primary decomposition and multivariate factorization over algebraic function fields of positive characteristic. J Symb Comput, 2005, 40: 1053–1075
25 Trager B M. Algebraic factoring and rational function integration. In: Proceedings of the third ACM Symposiumon Symbolic and algebraic Computation. New York: ACM Press, 1976, 219–226

26 Wang D M. A method for factoring multivariate polynomials over successive algebraic extension fields. Preprint RISC-Linz. Austria: Johannes Kepler University, 1992
27 Wang D M, Lin D D. A method for factoring multivariate polynomials over successive algebraic extension fields. In: Mathematics and Mathematics-Mechanization. Jinan: Shandong Education Press, 2000, 138–172
28 Wang P S. Factoring multivariate polynomial over algebraic number fields. Math Comp, 1978, 32: 1215–1231
29 Wu W T. Basic Principles of Mechanical Theorem Proving in Geometries (Part on Elementary Geometries, in Chinese). Beijing: Science Press, 1984
30 Wu W T. Basic principles of mechanical theorem proving in elementary geometries. J Syst Sci Math Sci, 1984, 4: 207–235; J Autom Reasoning, 1986, 2: 221–252
31 Yuan C M. Generalized Trager's factorization algorithm over successive extension fields. J Syst Sci Math Sci, 2006, 26: 533–540

Appendix: Examples in timings

1. $f^{(1)} = (y+\alpha_1)(y-2\alpha_2)(y^2+\alpha_1+\alpha_2)$, $I^{(1)} = (x_1+x_2^2, 1+x_1^2-x_2x_1) \subset \mathbb{Q}[x_1,x_2]$.
2. $f^{(2)} = (y+\alpha_1\alpha_3+\alpha_2+\alpha_1)(y-2\alpha_2^2+\alpha_3^2+1)(y^2+\alpha_1\alpha_2+\alpha_3)$,
$I^{(2)} = (x_1^2-x_2x_1+x_3x_1-x_1-x_2, x_1^2-x_3x_1+x_1-x_2^2-x_3x_2-x_2+x_3^2, -1+x_1^2+x_3x_1+x_1-x_2^2-x_2+x_3^2-x_3) \subset \mathbb{Q}[x_1,x_2,x_3]$.
3. $f^{(3)} = (y+\alpha_1)(y-2\alpha_4)(y+\alpha_2+\alpha_3)$,
$I^{(3)} = (x_1^2+x_3x_1-x_1x_4+x_2^2-x_2+x_3x_4-x_4^2-x_4, x_1^2+x_2x_1-x_1x_4+x_2^2+x_3x_2+x_2+x_4^2-x_4, 1+x_2x_1-x_3x_1+x_1x_4+x_1+x_2^2-x_3x_2+x_2x_4-x_2+x_3^2+x_3x_4-x_4^2, x_1^2+x_2x_1+x_3x_1+x_1x_4-x_2^2+x_3x_2-x_2+x_3^2-x_3x_4-x_4^2+x_4) \subset \mathbb{Q}[x_1,x_2,x_3,x_4]$.
4. $f^{(4)} = (y-2\alpha_4^2+\alpha_3\alpha_1+\alpha_2+1)(y+\alpha_2^2+\alpha_3\alpha_4+\alpha_1\alpha_3+2)$,
$I^{(4)} = (-1-x_1^2+x_3x_1+x_2^2-x_3x_2+x_3^2-x_3x_4+x_4^2+x_4, 1+x_2x_1+x_3x_1+x_1-x_3x_2-x_2x_4+x_2-x_3^2-x_3x_4-x_3, 1+x_3x_1+x_1x_4+x_1+x_2^2+x_2x_4-x_2-x_3-x_4^2, x_1^2+x_2x_1+x_3x_1+x_1x_4-x_1-x_2x_4-x_3^2+x_3x_4-x_3+x_4^2+x_4) \subset \mathbb{Q}[x_1,x_2,x_3,x_4]$.
5. $f^{(5)} = (y^2+(\alpha_1+\alpha_4\alpha_2)y+\alpha_3\alpha_4+\alpha_2)(y^2+(\alpha_1\alpha_3-\alpha_4)y+\alpha_3+\alpha_2\alpha_4\alpha_1)$,
$I^{(5)} = (-1+2x_1^2-x_2x_1+2x_3x_1-x_1x_4+x_2^2+x_2x_3+2x_2x_4-2x_3^2+2x_3x_4-x_3-x_4, x_1^2-2x_1x_4-x_1+2x_2^2+x_2x_3+2x_2x_4-x_2-x_3x_4+x_3-2x_4^2+2x_4, 2-2x_1^2+2x_2x_1+x_3x_1+2x_1+2x_2x_3+x_2x_4-x_3^2-2x_3-2x_4^2, 2x_1^2-x_2x_1-x_3x_1-x_1x_4-x_2^2+x_2x_3-x_2x_4-2x_2+2x_3^2-2x_3x_4+x_3+x_4^2+2x_4) \subset \mathbb{Q}[x_1,x_2,x_3,x_4]$.
6. $f^{(6)} = (y+\alpha_1+\alpha_3\alpha_4+\alpha_2\alpha_5)(y+\alpha_2\alpha_5+2-\alpha_3+\alpha_4)$,
$I^{(6)} = (2-x_1^2+x_1x_2-2x_3x_1+2x_4x_1-2x_1+2x_2^2+x_2x_3+2x_2x_5+2x_3^2+x_3x_4-x_3-2x_4x_5-2x_4+2x_5, 1-x_1^2-x_1x_2-x_3x_1-x_1x_5+x_1-x_2^2-2x_2x_3+2x_2x_4-2x_2x_5+x_2+x_3^2+2x_3x_4-x_3-2x_4^2-x_4x_5+x_4+2x_5^2, 1-2x_1^2-2x_1x_2-2x_3x_1-x_4x_1-x_1x_5+x_2^2+2x_2x_3-2x_2x_4+x_2x_5-2x_2-x_3^2-2x_3x_4+2x_3x_5-2x_3-2x_4^2+x_4x_5+2x_5^2+x_5, x_1^2-x_1x_2-x_3x_1-x_4x_1+2x_1+2x_2^2+x_2x_3+2x_2+2x_3x_5+x_4^2-x_4+2x_5^2-x_5, x_2-2x_4+x_5-1) \subset \mathbb{Q}[x_1,x_2,x_3,x_4,x_5]$.
7. $f^{(7)} = (y+\alpha_1+\alpha_3\alpha_4)(y-\alpha_2\alpha_5)(y-\alpha_3+\alpha_4)$,
$I^{(7)} = (1-2x_3x_1+x_4x_1+2x_1x_5+x_1-2x_2^2-x_2x_3+2x_2x_4+2x_2x_5-2x_2-x_3^2-2x_3x_4+2x_3x_5+x_3+x_4^2+2x_4x_5+x_4-x_5^2-2x_5, 1-2x_1^2+2x_1x_2-2x_3x_1-2x_4x_1+2x_1x_5-2x_1+x_2^2+2x_2x_3+x_2x_4+2x_2x_5-2x_2+2x_3^2-x_3x_4+2x_3x_5+2x_3+2x_4^2-x_4x_5-2x_5^2+x_5, -x_1^2-x_1x_2-x_3x_1+x_4x_1-2x_1x_5+2x_1-x_2^2+2x_2x_3-x_2x_4+2x_2x_5+2x_2-2x_3^2+2x_3x_4-x_3x_5-x_3-x_4^2+2x_4x_5+2x_4-2x_5^2+2x_5, -1-2x_1^2+2x_1x_2-x_3x_1-x_4x_1+x_1x_5+x_1+2x_2x_3+x_2x_4+x_2x_5+2x_2+x_3x_4+x_3-2x_4^2-x_4+x_5^2-x_5, x_2-x_3+x_4-x_5+1) \subset \mathbb{Q}[x_1,x_2,x_3,x_4,x_5]$.
8. $f^{(8)} = (y^2+(\alpha_1-\alpha_2\alpha_4)y+\alpha_2\alpha_5+\alpha_3+\alpha_5)(y+\alpha_3\alpha_5+\alpha_2\alpha_4\alpha_3)$,
$I^{(8)} = (2+x_1^2+2x_2x_1+x_3x_1+2x_1x_4-2x_1x_5+2x_1-x_2^2+2x_3x_2+2x_4x_2+2x_2x_5-x_2-2x_3x_4+x_3x_5+x_3-x_4^2-x_4x_5-x_4+x_5^2-2x_5, 1-x_1^2+2x_2x_1-x_3x_1+2x_1x_4+2x_1x_5-2x_1+2x_2^2-x_3x_2-x_4x_2-x_2x_5+2x_2+2x_3^2-2x_3x_4+2x_3x_5-2x_4^2+2x_4x_5-x_4-x_5^2+x_5, 1+2x_2x_1+x_3x_1+x_1x_4+2x_1x_5+x_2^2+x_4x_2-2x_2x_5-x_3^2+x_3x_4-x_3x_5-x_3+x_4x_5-x_4+x_5^2-x_5, x_1^2+2x_2x_1+2x_3x_1+2x_1x_4+x_1x_5-2x_1+2x_2^2+x_3x_2+2x_4x_2-2x_2-2x_3^2+2x_3x_4-2x_3-2x_4^2-x_4x_5+x_5^2, x_1-2x_2-2x_3+2x_4+x_5-2) \subset \mathbb{Q}[x_1,x_2,x_3,x_4,x_5]$.

9. $f^{(9)}=(y^2+(\alpha_1-\alpha_2\alpha_4)y+\alpha_2\alpha_5+\alpha_3+\alpha_5)(y^2+y(1+\alpha_3-\alpha_2+\alpha_3\alpha_5)+\alpha_4+\alpha_3-\alpha_1\alpha_5)(y+\alpha_3\alpha_5+\alpha_2\alpha_4\alpha_3)$,
$I^{(9)}=I^{(8)}\subset\mathbb{Q}[x_1,x_2,x_3,x_4,x_5]$.

10. $f^{(10)}=(y+\alpha_1+\alpha_2+\alpha_6+\alpha_3\alpha_4+\alpha_2\alpha_5\alpha_6)(y+\alpha_2\alpha_6-\alpha_1\alpha_5+2-\alpha_3+\alpha_4)$,
$I^{(10)}=(-1+2x_1^2+x_1x_2+2x_1x_3-x_1x_4+x_1x_5-2x_1x_6+2x_1-x_2^2+x_3x_2+2x_4x_2-2x_2+x_3^2-2x_3x_5+2x_3x_6-2x_4^2-x_4x_5+2x_4x_6+x_4-2x_5x_6-2x_5+x_6^2+2x_6,-2x_1^2-x_1x_5-2x_1-2x_2^2+x_3x_2-x_4x_2-x_2x_6-x_3^2+2x_4x_3+2x_3x_5-x_3+2x_4^2-2x_4-x_5^2-x_5x_6+x_5+2x_6^2,-1+x_4-x_5+x_6+x_5x_6-2x_4x_6+2x_4x_5-2x_3x_6+x_3x_5+x_4x_3-x_2x_6+2x_2x_5+x_3x_2-x_1x_6-x_1x_5-2x_1x_4-x_1x_3-x_1x_2+2x_2-2x_1^2+x_2^2+2x_3^2-x_4^2+x_5^2+x_6^2,2-x_1^2-2x_1x_3-2x_1x_4-2x_1x_5+x_1x_6+x_1-x_3x_2+2x_4x_2-2x_2x_6-x_2+2x_3^2-x_4x_3+2x_3x_5+x_3x_6+x_3+x_4^2+x_4x_5-x_4-2x_5^2+2x_5x_6+x_5-x_6,x_1x_2-2x_1x_4-x_1x_5-x_1x_6-x_1-x_3x_2-2x_4x_2-2x_2x_5-2x_2x_6-x_3^2-x_4x_3-2x_3x_5-2x_3x_6-x_3-2x_4x_5-2x_4x_6-2x_4-x_5^2+2x_5x_6-x_5+2x_6^2+x_6,-2x_1+x_2+x_3-2x_4+2x_5+x_6-2)\subset\mathbb{Q}[x_1,x_2,x_3,x_4,x_5,x_6]$.