Vol. 34 No. 11 Transactions of Information Processing Society of Japan Nov. 1993

Regular Paper

Factorization of Noncommutative Polynomials

KAZUYOSHI MORI † and SABUROU IIDA ††

Two factorization methods of a polynomial with noncommutative multiplication are proposed. One of the methods factorizes a noncommutative polynomial by computing coefficients of factors as factorization by constructing and solving several equations. We call this the naïve method. This is simple, but does not factorize efficiently. To do this efficiently, an alternative method is proposed, which is called the constant term method. This factorizes a noncommutative polynomial in one of two ways according to its constant term. If the constant term of a polynomial is zero, the polynomial is factorized by classifying its monomials based on the leftmost and rightmost variables and by linear combinations of polynomials. An irreducible factor is obtained from this factorization. If its constant term is not zero, first, the constant term is reduced to zero by linear transformations of variables and an extension of the coefficient field, and then, the polynomial is factorized in the same manner as when a constant term is zero. After that, by computing the least common multiple, an irreducible factor over the original domain is obtained from irreducible factors over the extension field. This method, however, cannot be applied to noncommutative polynomials whose constant terms cannot be reduced to zero. To factorize such noncommutative polynomials, the former method is used. It is shown that the latter method is faster than the former. In the two proposed methods, factorizations over a finite field are not used explicitly, comparing with the factorization algorithms for usual commutative polynomials.

1. Introduction

Factorization algorithms of commutative polynomials have been well researched and developed. Such algorithms, however, cannot factorize polynomials whose multiplications are not commutative ; *e.g.*, polynomials whose variables represent matrices. In this paper, we propose two factorization methods for polynomials with noncommutative multiplication.

One of the methods factorizes a polynomial by simply computing coefficients of factors as factorization by constructing and solving several equations (Subsection 3.1). We call this the naïve method. This is simple, but does not factorize efficiently. To do so efficiently, an alternative one is proposed, which is called the constant term method (Subsection 3.2). This method factorizes a polynomial in one of two ways according to its constant term. When a polynomial with a zero constant term is given, it is factorized into four factors including an irreducible one by classifying monomials of the given polynomial based on the leftmost and rightmost variables and by linear combinations of polynomials (Subsection 3.2.1). On the other hand, for a polynomial with a nonzero constant term, the following procedure will be applied : first reducing a constant term to zero by linear transformations of variables and an extension of the coefficient field, then carrying out the factorization over the extension field as a polynomial with a zero constant term, and finally computing the least common multiple to obtain an irreducible factor over the original domain from the irreducible factors over the extension field (Subsection 3.2.2). An irreducible factorization is obtained by repeatedly applying them (Subsection 3.2.3). However, the method for reducing a constant term to zero cannot be applied to noncommutative polynomials whose constant terms cannot be reduced to zero. In order to factorize these polynomials, we employ the naïve method.

In general, there may exist multiple irreducible factorizations of a polynomial. In this paper, we confine ourselves to obtaining one

† Department of Information & Computer Sciences, Toyohashi University of Technology
†† School of Computer & Cognitive Sciences, Chukyo University

factorization because in the worst case, the number of irreducible factorizations increases exponentially with respect to the degree of the polynomial.

This paper is organized as follows. Section 2 presents preliminaries and fundamental results, Section 3 two factorization methods, Section 4 some examples, and Section 5 conclusions and comments.

2. Preliminaries

2.1 Definitions

Noncommutative polynomials are similar to usual polynomials except that variables in a term are not commutative.

Let a number field $\mathcal{K}$ be a coefficient domain and $\mathcal{X}$ a finite set of variables. Since we are interested in actual implementation and practical use of algorithms on computers, the operations such as addition, multiplication, and factorization of $\mathcal{K}$ should be able to be implemented on computers.

A term is defined as a free product of finite variables, including an empty product represented by 1, a monomial as the product of an element of $\mathcal{K}$ (called a coefficient) and a term, and a noncommutative polynomial as the sum of finite monomials, including an empty sum represented by 0. The sum and product of noncommutative polynomials are defined in an obvious manner, *e.g.*, $(\sum_i a_i t_i)(\sum_j b_j u_j) = \sum_{i,j} a_i b_j t_i u_j$, where a_i and b_j are coefficients, t_i and u_j are terms, and $t_i u_j$ is also a term. A noncommutative polynomial is also called a string polynomial or a free associative $\mathcal{K}$-algebra [Ref. 1), p. 418].

Let $\mathcal{K}\langle\mathcal{X}\rangle$ denote the set of noncommutative polynomials over $\mathcal{K}$ with variable set $\mathcal{X}$. The set $\mathcal{K}\langle\mathcal{X}\rangle$ is a noncommutative ring, and $\mathcal{K}$ as a commutative subring of $\mathcal{K}\langle\mathcal{X}\rangle$ is the center of $\mathcal{K}\langle\mathcal{X}\rangle$. This obviously is not a Euclidean domain, and for the factorization of polynomials, we cannot employ Berlekamp's method[2] and its various refinements (cf. Ref. 3)) using factorizations over finite fields.

We will assume in the rest of this paper that 'a polynomial' means a noncommutative polynomial to avoid repetitious expressions.

The *degree* $\deg(t)$ of a term t is an integer n, if $t = X_{s(1)} X_{s(2)} \cdots X_{s(n)}$, where $X_{s(i)} \in \mathcal{X}$. In particular, $\deg(t) = 0$, if $t = 1$. Although this degree is also called 'total degree,' or 'length,' we will call it simply 'degree' in this paper. The degree $\deg(m)$ of a monomial m is defined as the degree of its term, and the degree $\deg(P)$ of a polynomial P as the maximal degree of monomials with nonzero coefficients in P.

A monomial with degree 0 is called a constant term. A polynomial P is said to be *zct* if the constant term of P is zero. Otherwise, P is said to be *nzct*.

Each of the polynomials $P_1, P_2, \cdots, P_n$ is called a factor of a polynomial P, if $P = P_1 P_2 \cdots P_n$ ($n \geq 1$). A polynomial is irreducible, if there are no factors in $\mathcal{K}\langle\mathcal{X}\rangle - \mathcal{K}$ except itself, or *reducible*. A polynomial is said to be factorized, if it is represented by $P_1 P_2 \cdots P_n$. When each factor of a polynomial belongs to $\mathcal{K}\langle\mathcal{X}\rangle - \mathcal{K}$ and is irreducible, then the polynomial is said to be irreducibly factorized and such factorization is called irreducible factorization.

Polynomials P_l and P_r are called left and right factors of a polynomial P, respectively, if $P = P_l P_r$. We will also say that P_l left-divides P and P_r *right-divides* P, and denote the right and left factors P_r and P_l by $P \backslash P_l$ and P / P_r, respectively (*i.e.*, $P_r = P \backslash P_l$ and $P_l = P / P_r$ hold).

In order to exclude the uncertainty of polynomials with respect to a unit multiple of $\mathcal{K}$, like 'monic' of commutative polynomials, we assume that the coefficient of the leading term of a polynomial or a factor is 1, if it does not lose generality. The leading term is defined by an appropriate ordering, for example, 'total degree, then lexicographic' [Ref. 4), p. 71]. The coefficient of the leading term is also called the leading coefficient.

We note that a polynomial may have two or more irreducible factorizations while that of a commutative polynomial is unique up to a unit multiple. For example, for $X, Y \in \mathcal{X}$, a polynomial $XYX + X$ has two irreducible factorizations; $(XY+1)X$ and $X(YX+1)$. In the worst case, the number of irreducible factorizations increases exponentially with respect to the degree. Since we are interested in efficient algorithms and wish to avoid exponential computing time, if possible, for practical use, we will attempt to obtain only one irreducible factorization.

Replacement will be specified by square

brackets and slash '[/]'. For example, an expression '$A[B/C]$' represents replacement of C by B in A. Subscripts l and r usually mean left and right factors, respectively, of an original polynomial or a certain polynomial. If those subscripts are sequentially arranged, they will be interpreted from left to right. For example, P_l represents a left factor of P, P_{lr} a right factor of P_l, and P_{lrl} a left factor of P_{lr}.

As an example of noncommutative polynomials, let $\mathcal{K}$ be the rational number field $\mathbb{Q}$, $\mathcal{X}=\{X, Y\}$, $P_1=Y^2X-2XY+2X+3Y$, and $P_2=XY^2X+X^2+XY+YX+1$. Polynomial P_2 appeared in [Ref. 5), Expression (5.9)]. Then P_1, $P_2\in\mathbb{Q}\langle\mathcal{X}\rangle$, $\deg(P_1)=3$, $\deg(P_2)=4$, P_1 is *zct*, and P_2 is *nzct*. $P_1P_2=Y^2X^2Y^2X-2XYXY^2X+2X^2Y^2X+3YXY^2X+Y^2X^3+Y^2X^2Y+Y^2XYX-2XYX^2-2XYXY-2XY^2X+2X^3+2X^2Y+2XYX+3YX^2+3YXY+4Y^2X-2XY+2X+3Y$. $2P_1+P_2=XY^2X+2Y^2X+X^2-3XY+YX+4X+6Y+1$. Both P_1 and P_2 are irreducible over $\mathbb{Q}$. However, P_2 is reducible over $\mathbb{Q}(i)$. There are two irreducible factorizations of P_2 over $\mathbb{Q}(i)$; $P_2=(XY+iX+1)(YX-iX+1)=(XY-iX+1)(YX+iX+1)$. This shows that, as in the case of commutative polynomials, irreducibility depends on the coefficient domain.

2.2 Euclidean algorithm

We define a common multiple and a common divisor of polynomials. If $P_{l1}P_{r1}=P_{l2}P_{r2}$, $P_{l1}P_{r1}$ and $P_{l2}P_{r2}$ are called common right multiples of P_{l1} and P_{l2}, or common left multiples of P_{r1} and P_{r2}, where P_{l1}, P_{l2}, P_{r1}, and P_{r2} are polynomials. If there are some polynomials P_{l1} and P_{l2} such that $P_1=P_{l1}P_r$ and $P_2=P_{l2}P_r$, P_r is called *a* common right divisor of polynomials P_1 and P_2. A common left divisor is similarly defined.

A least common left multiple lclm(P_1, P_2) is a common left multiple of P_1 and P_2 and a right factor of any common left multiple of P_1 and P_2. A greatest common right divisor gcrd(P_1, P_2) is a common right divisor of P_1 and P_2 such that any common right divisor of P_1 and P_2 is a right factor of gcrd(P_1, P_2). A least common right multiple lcrm, and a greatest common left divisor gcld are similarly defined. They have the following property.

Proposition 2.1 *Each of* lclm, lcrm, gcld, *and* gcrd *is unique up to a unit multiple.*

Proof. We carry out the proof for only lclm and gcrd.

Suppose there exist two lclm's of polynomials P_1 and P_2, say $P_{l1}P_1$ and $P_{l2}P_1$. Because $P_{l2}P_1$ right-divides $P_{l1}P_1$ and vice versa by the definition of lclm, $P_{l1}P_1=uP_{l2}P_1$ for some $u\in\mathcal{K}$.

Suppose there exist two gcrd's of P_1 and P_2, say P_{r1} and P_{r2}. Similarly as above, P_{r2} right-divides P_{r1} and vice versa, and so $P_{r1}=uP_{r2}$ for some $u\in\mathcal{K}$. □

Each of lclm, lcrm, gcrd, and gcld is unique by our convention.

When there exist polynomials P_{l1}, P_{l2}, P_{r1}, and P_{r2} such that $P_{l1}P_{r1}=P_{l2}P_{r2}$, Cohn[5] found a Euclidean algorithm which computes the least common left and right multiples lclm(P_{r1}, P_{r2}) and lcrm(P_{l1}, P_{l2}), and the greatest common left and right divisors gcld(P_{l1}, P_{l2}) and gcrd(P_{r1}, P_{r2}). The algorithm is given in [Ref. 1), p. 419] and shown in **Fig. 1**. In the algorithm of Fig. 1, the relation $v_2=0$ can be used instead of $u_1=0$ in Step 2.1, and we can find such Q that $v_1=Qv_2+R'$ and $\deg(v_2)>\deg(R')$ instead of Step 3.1. If only lcrm(P_{l1}, P_{l2}) or gcld(P_{l1}, P_{l2}) are required, the variables v_1, v_2, z, and z' need not be calculated. Conversely, when only lclm(P_{r1}, P_{r2}) and gcrd(P_{r1}, P_{r2}) are required, the variables u_1, u_2, w, and w' need not be calculated.

2.3 Coefficient domain and irreducibility

In this subsection, we describe irreducibility of polynomials over $\mathcal{K}$ and over an extension field of $\mathcal{K}$.

Let α be a root of a minimal polynomial P_m with degree d_m over $\mathcal{K}$ and $\mathcal{K}_m$ the minimal splitting field of P_m. There are d_m conjugates of α. Let $\alpha_0, \alpha_1, \ldots, \alpha_{d_m-1}$ denote the conjugates of α, and C be $\{\alpha_0, \alpha_1, \ldots, \alpha_{d_m-1}\}$.

Let P be a polynomial over $\mathcal{K}_m$, which is irreducible over $\mathcal{K}$. Then P may be reducible

Algorithm : Euclidean algorithm

Input. Polynomials P_{l1}, P_{l2}, P_{r1}, and P_{r2} such that $P_{l1}P_{r1}=P_{l2}P_{r2}$.
Output. gcld(P_{l1}, P_{l2}), lcrm(P_{l1}, P_{l2}), gcrd(P_{r1}, P_{r2}), and lclm(P_{r1}, P_{r2}).

1. (Initialization)
1.1 $(u_1, u_2, v_1, v_2) \leftarrow (P_{l1}, P_{l2}, P_{r1}, P_{r2})$;
1.2 $z \leftarrow w \leftarrow 1$; $z' \leftarrow w' \leftarrow 0$;
2. (Check)
2.1 if $u_1 = 0$ then
2.2 return lcrm$(P_{l1}, P_{l2}) = P_{l1}w$; gcld$(P_{l1}, P_{l2}) = u_2$;
lclm$(P_{r1}, P_{r2}) = z'P_{r1}$; gcrd$(P_{r1}, P_{r2}) = v_1$;
3. (Division)
3.1 Find Q and R such that
$u_2 = u_1Q + R$ and $\deg(u_1) > \deg(R)$;
3.2 $(w, w', z, z', u_1, u_2, v_1, v_2)$
$\leftarrow (w' - wQ, w, z', z - Qz', u_2 - u_1Q, u_1, v_2, v_1 - Qv_2)$;
3.3 goto 2. ;

Fig. 1 Euclidean algorithm.

over $\mathcal{K}_m$ (*e.g.*, P_2 in the example of Subsection 2.1). Suppose that P is factorized as $P=P_lP_r$, where P_l and P_r are the left factor and irreducible right factor of P over $\mathcal{K}_m$, respectively. Then, each polynomial $P_r[\alpha_i/\alpha]$ for $\alpha_i \in C$ is also an irreducible right factor over $\mathcal{K}_m$.

Let C' be a set of α_i's such that all $P_r[\alpha_i/\alpha]$'s are distinct for $\alpha_i \in C'$. There are (d_m/n) conjugates α_j's, including α_i, such that $P_r[\alpha_i/\alpha]=P_r[\alpha_j/\alpha]$, where n is the number of elements of C'. By the fundamental theorem on symmetric polynomials, P is equal to the lclm of all $P_r[\alpha_i/\alpha]$'s of $\alpha_i \in C'$. It follows that C' is a minimal set among subsets of C such that $\mathrm{lclm}_{\alpha_i \in C'}(P_r[\alpha_i/\alpha])=P$.

Symmetrically, $P=\mathrm{lcrm}_{\alpha_i \in C''}(P_l[\alpha_i/\alpha])$ also holds, where C'' is a set of conjugates of α such that all irreducible left factors $P_l[\alpha_i/\alpha]$'s are distinct for $\alpha_i \in C''$. This C'' is a minimal set such that the equality holds.

In Subsection 3.2.2, we will compute an ir reducible factor over $\mathcal{K}$ from the lclm of irreducible factors over $\mathcal{K}_m$. This corresponds to finding C'.

3. Factorization

In this section, we present two factorization methods. First, in Subsection 3.1, the naïve method is presented. Next, in Subsection 3.2, the constant term method is presented.

3.1 Naïve method

The naïve method is a trivial one and its implementation is simple.

Let P be a polynomial with degree d_l+d_r, and P_l and P_r left and right factors of P with degrees d_l and d_r, respectively $(P=P_lP_r)$. Let $P=\sum_i a_i t_i$, $P_l=\sum_j b_j u_j$, and $P_r=\sum_k c_k v_k$, where a_i, b_j, and c_k are coefficients, t_i, u_j, and v_k are terms, and the values of a_i and t_i are known. By our convention, the leading coefficients of P, P_l, and P_r are equal to 1. A polynomial P is factorized by solving the following equations for b_j and c_k:

$$a_i=\sum_{t_i=u_jv_k} b_jc_k. \qquad (3.1)$$

Expression (3.1) is referred as a decomposition equation of degrees (d_l, d_r) or simply a decomposition equation.

The degrees of terms u_j and v_k arc less than or equal to d_l and d_r, respectively, and these terms are chosen from left and right parts of t_i, *i.e.*, the sets of u_j and v_k are determined by $\{u_j\}=\{t|t_i=tt' \text{ for some term } t', a_i\neq 0, \deg(t)\leq d_l\}$, and $\{v_k\}=\{t|t_i=t't \text{ for some term } t', a_i\neq 0, \deg(t)\leq d_r\}$. In order to solve the decomposition equations, we can employ, for example, computation of the Gröbner basis and factorization of commutative univariate polynomials over $\mathcal{K}$. If there are solutions of the decomposition equations of degrees (d_l, d_r) over $\mathcal{K}$, it indicates that P is factorized into the left and right factors with degrees d_l and d_r, respectively. If P is factorized into P_l and P_r such that the degree of P_l is minimized, then P_l is an irreducible left factor over $\mathcal{K}$. By repeatedly finding such left factors, P will be irreducibly factorized.

We note, in this method, the need to construct and solve the decomposition equations for every degree in order to irreducibly factorize a polynomial. In the worst case, for an irreducible polynomial, we must construct the decomposition equations, attempt to solve them, and then fail to solve them for every degrec. Finally, it is found to be irreducible. The rest of this section is devoted to the constant term method which avoids such inefficient factorizing.

3.2 Constant term method

The constant term method is composed of two parts. One part, described in Subsection 3.2.1, is for polynomials with zero constant terms, and the other, described in Subsection 3.2.2, for those with nonzero constant terms. Irreducible factorization of the constant term method is described in Subsection 3.2.3.

3.2.1 Factorization of *zct* polynomials

Let P be a *zct* polynomial.

In this subsection, we show how to factorize P into four factors as $P=P_{ll}P_{lrl}P_{lrr}P_r$, where P_{lrr} is irreducible over $\mathcal{K}$ and *zct*. In **Fig. 2**, the configuration of this factorization is shown; each rectangle represents a factor, and numbers in square brackets represent the steps of the factorization procedure described below.

Step 1: We first factorize P as $P=P_lP_r$, where

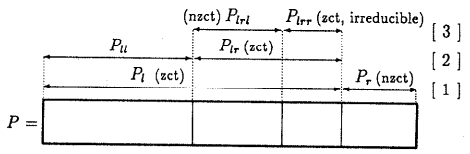


Fig. 2 Configuration of the factorization of a *zct* polynomial.

P_r is *nzct* and of the maximal degree ($\deg(P_l) > 0$ and $\deg(P_r) \geq 0$). The uniqueness of P_l and P_r is shown below.

Lemma 3.1 *The factors P_l and P_r are unique up to a unit multiple.*

Proof. If there were two such right factors as P_r, then there would exist the lclm of these factors. It is *nzct* again and its degree is greater than that of original factors, which is a contradiction. □

Thus, they are unique by our convention.

We classify P according to the leftmost variables. Let $P = \sum_{X_i \in \mathcal{X}_l} c_i X_i P_i$ ($P_i \neq 0$, $\mathcal{X}_l \subseteq \mathcal{X}$, $c_i \in \mathcal{K} - \{0\}$), where the leading coefficient of each P_i is equal to 1. Each P_i is uniquely determined. Since P is *zct*, P_r is a right factor of each P_i. We will find P_r from P_i's.

Lemma 3.2 *If P_i defined above is nzct and right-divides P, then such P_i is equal to P_r.*

Proof. Trivial by Lemma 3.1. □

Lemma 3.2 shows that P is factorized into $P_l (= P/P_i)$ and $P_r (= P_i)$ if the maximal degree is 1 in the monomials with the leftmost variable X_i of P_l. As a special case, P is factorized into P_l and P_r by finding P_i, if $\deg(P_l) = 1$.

If P_i is *zct* or does not right-divide P, P_r is a right factor of P_i again, and the degree of P_i is decreased by one comparing with that of P. Now, suppose that each P_i is *zct* or does not right-divide P. As an induction hypothesis, we assume that a *zct* polynomial can be factorized into a *zct* left factor and an *nzct* right one with the maximal degree among *nzct* right factors, where the degree of the *zct* left factor is less than that of P_l.

If P_i is *zct*, P_i is factorized into such left and right factors, say P_{il} and P_{ir}, respectively, by the hypothesis ($P_i = P_{il}P_{ir}$). If P_i is *nzct*, let $P_{il} = 1$ and $P_{ir} = P_i$.

Lemma 3.3 *There is a relation between P_r and P_{ir}'s as follows:*

$$P_r = \mathrm{gcrd}_{X_i \in \mathcal{X}_l}(P_{ir}). \tag{3.2}$$

Proof. Since P_r is a right factor of each P_{ir}, P_r is a right factor of $\mathrm{gcrd}_{X_i \in \mathcal{X}_l}(P_{ir})$. The degree of P_r is the maximal in the *nzct* right factors of P. We have therefore $P_r = \mathrm{gcrd}_{X_i \in \mathcal{X}_l}(P_{ir})$. □

In particular, if P_{ir} right-divides P, then $P_{ir} = P_r$ and P is factorized into $P_l (= P/P_{ir})$ and $P_r (= P_{ir})$.

If $P_{i_1 r} = P_{i_2 r}$ for any X_{i_1} and $X_{i_2} (\in \mathcal{X}_l)$, then every P_{ir} is equal to P_r. So, we assume that $P_{i_1 r} \neq P_{i_2 r}$ for some X_{i_1} and X_{i_2}. If the gcrd of $P_{i_1 r}$ and $P_{i_2 r}$ can be computed, we can compute expression (3.2). When there do not exist P_{l1} and P_{l2} such that $P_{l1}P_{i_1 r} = P_{l2}P_{i_2 r}$, the Euclidean algorithm mentioned in Subsection 2.2 cannot be applied to them due to its condition. Nevertheless, the following discussion shows the possibilities of its computation.

For $P_{i_1 r}$ and $P_{i_2 r}$, we choose a and $b \in \mathcal{K}$ which satisfy the expression

$$aP_{i_1 r} + bP_{i_2 r} \tag{3.3}$$

is *zct* and its leading coefficient is equal to 1. We obtain *nzct* right factor, say P'_r, with the maximal degree among *nzct* right factors from expression (3.3) by the hypothesis. Factor P'_r also contains P_r as a right factor. In contrast with P'_r, let P'_l be the left factor of expression (3.3) (*i.e.*, $aP_{i_1 r} + bP_{i_2 r} = P'_l P'_r$). Then both gcrd's of P'_r and $P_{i_1 r}$, and of P'_r and $P_{i_2 r}$ are equal to that of $P_{i_1 r}$ and $P_{i_2 r}$ as follows.

Lemma 3.4 *Both* $\mathrm{gcrd}(P'_r, P_{i_1 r}) = \mathrm{gcrd}(P_{i_1 r}, P_{i_2 r})$ *and* $\mathrm{gcrd}(P'_r, P_{i_2 r}) = \mathrm{gcrd}(P_{i_1 r}, P_{i_2 r})$ *hold.*

Proof By the construction of P'_r, $\mathrm{gcrd}(P_{i_1 r}, P_{i_2 r})$ is a common right factor of P'_r and $P_{i_1 r}$. $\mathrm{Gcrd}(P'_r, P_{i_1 r})$ is also a common right factor of $P_{i_1 r}$ and $P_{i_2 r}$. It follows that $\mathrm{gcrd}(P_{i_1 r}, P_{i_2 r}) = \mathrm{gcrd}(P'_r, P_{i_1 r})$. In the same manner, $\mathrm{gcrd}(P'_r, P_{i_2 r}) = \mathrm{gcrd}(P_{i_1 r}, P_{i_2 r})$ holds.

If P'_r right-divides both $P_{i_1 r}$ and $P_{i_2 r}$, $P'_r = \mathrm{gcrd}(P_{i_1 r}, P_{i_2 r})$. Otherwise, suppose that $\deg(P_{i_1 r}) \geq \deg(P_{i_2 r})$. Since $\deg(P'_r) \leq \deg(P_{i_1 r})$, we can finally obtain the gcrd of $P_{i_1 r}$ and $P_{i_2 r}$ by applying the above argument to $P_{i_2 r}$ and P'_r.

As we have indicated above the computation of $\mathrm{gcrd}(P_{i_1 r}, P_{i_2 r})$, P_r is obtained by expression (3.2), and P_l is obtained by P/P_r. Consequently, any *zct* polynomial is factorized into a *zct* left factor and an *nzct* right one with the maximal degree among *nzct* right factors.

In **Fig. 3**, we show the algorithm '*nzrf*' obtained from the above argument, whose name stands for '*nzct* right factor.' The input of *nzrf* is a *zct* polynomial P and *nzrf* returns the *nzct* right factor P_r with the maximal degree among *nzct* right factors of P. The variable Q represents a list of P_i's. Functions car and cdr return the head element of a list and the rest, respectively. A function ct returns a constant term of a polynomial. The input of the subalgorithm

Algorithm : Factorization algorithm 1 (*nzrf*)

Input. *Zct* polynomial P.
Output. *Nzct* right factor P_r with the maximal degree.

1. (Initialization)
1.1 $Q \leftarrow \{P_i \mid P = \sum_{X_i \in \mathcal{X}_i} c_i X_i P_i, P_i \neq 0, \mathcal{X}_l \subseteq \mathcal{X}, c_i \in \mathcal{K} - \{0\},$ Leading coefficient of P_i is 1$\}$;
1.2 $P_r \leftarrow \mathrm{car}(Q)$; $Q \leftarrow \mathrm{cdr}(Q)$;
1.3 if $\mathrm{ct}(P_r) = 0$ then
1.4 $P_r \leftarrow nzrf(P_r)$;
2. (Check)
2.1 if P_r right-divides P then
2.2 return P_r ;
3. (Gcrd)
3.1 $P'_r \leftarrow \mathrm{car}(Q)$; $Q \leftarrow \mathrm{cdr}(Q)$;
3.2 if $\mathrm{ct}(P'_r) = 0$ then
3.3 $P'_r \leftarrow nzrf(P'_r)$;
3.4 $P_r \leftarrow gcrd'(P_r, P'_r)$;
3.5 goto 2. ;

Subalgorithm : Special gcrd algorithm (*gcrd'*)

Input. *Nzct* polynomials P_1 and P_2.
Output. Greatest common right divisor of P_1 and P_2.
4.1 If $\deg(P_1) < \deg(P_2)$ then $(P_1, P_2) \leftarrow (P_2, P_1)$;
4.2 If P_2 right-divides P_1 then
4.3 return P_2 ;
4.4 $P_r \leftarrow nzrf(aP_1 + bP_2)$
where $aP_1 + bP_2$ is *zct*, its leading coefficient is 1, and $a, b \in \mathcal{K}$;
4.5 return $gcrd'(P_2, P_r)$;

Fig. 3 Factorization algorithm *nzrf* for a *zct* polynomial.

gcrd' is two *nzct* polynomials and their greatest common right divisor is returned. At Step 4.4 in this algorithm, when *nzrf* is applied to $aP_1 + bP_2$, $\deg(P) > \deg(aP_1 + bP_2)$ holds. At Step 4.5, when *gcrd'* is recursively called, $\deg(P_1) > \deg(P_r)$ holds. We described above that first all P_{lr}'s are obtained and then their gcrd is computed. The algorithm, however, examines whether the gcrd of two polynomials right-divides P in order to omit unnecessary computation at Step 2.

Step 2: We now show how to find a right factor of P_l, say P_{lr}, with the maximal degree among the right factors which contain just one *zct* irreducible factor. Let P_{ll} be a left factor of P_l in contrast with P_{lr} such that $P_l = P_{ll}P_{lr}$. If there is one *zct* irreducible factor in P_l, P_{ll} will be equal to 1. Otherwise, any right factor of P_{ll} will be *zct*.

The factors P_{ll} and P_{lr} are unique up to a unit multiple, similarly to Lemma 3.1. This is proven below.

Lemma 3.5 *The factors P_{ll} and P_{lr} are unique up to a unit multiple.*

Before proving the lemma above we prove the lemma below.

Lemma 3.6 *Let P_l and P_r be zct irreducible factors of a polynomial P such that P_lP_r is also a factor of P. Then, there do not exist polynomials P'_l and P'_r with degree one or more such that $P_lP_r = P'_lP'_r$ except $P_l = P'_l$ and $P_r = P'_r$.*

Proof. Suppose such P'_l and P'_r exist. By Ref. 5), Corollary 3 of Theorem 4.1, $P_l = f_{n+1}(a_1, \ldots, a_{n+1})$, $P_r = f_n(a_n, \ldots, a_1)$, $P'_l = f_n(a_1, \ldots, a_n)$, and $P'_r = f_{n+1}(a_{n+1}, \ldots, a_1)$ hold for some integer n and polynomials $a_1, \ldots, a_{n+1}$. We show below such n and $a_1, \ldots, a_{n+1}$ do not exist by induction.

For $n=1$, assume both $f_1(a_1)$ and $f_2(a_1, a_2)$ are *zct*. Both expanded formulas are a_1 and a_1a_2+1, respectively. If a_i is *zct*, a_1a_2+1 is not *zct*. Therefore, both $f_1(a_1)$ and $f_2(a_1, a_2)$ are not *zct*.

Next, as induction hypothesis, we assume both $f_{i-1}(a_1, \ldots, a_{i-1})$ and $f_i(a_1, \ldots, a_i)$ are not *zct*. Then, both $f_i(a_1, \ldots, a_i)$ and $f_{i+1}(a_1, \ldots, a_{i+1})$ are not *zct* as shown below. Suppose both are *zct*. This means that $f_{i+1}(a_1, \ldots, a_{i+1}) = f_i(a_1, \ldots, a_i)\, a_{i+1} + f_{i-1}(a_1, \ldots, a_{i-1})$ is *zct* and its first part $f_i(a_1, \ldots, a_i)\, a_{i+1}$ is also *zct*. It follows $f_{i-1}(a_1, \ldots, a_{i-1})$ is *zct*, which is a contradiction. □

Proof of Lemma 3.5. Suppose there exist two polynomials, say P_{lr1} and P_{lr2}, as P_{lr}. Each of them includes one *zct* irreducible right factor. By Lemma 3.6, the *zct* irreducible factor of P_{lr1} is equal to that of P_{lr2}. If $P_{lr1} \neq P_{lr2}$, then lclm (P_{lr1}, P_{lr2}) exists and its degree is greater than $\max(\deg(P_{lr1}), \deg(P_{lr2}))$. Although the lclm satisfies the condition to be P_r, this is a contradiction.

By the uniqueness of P_{lr}, that of P_{ll} is trivial. □

We describe below how P_l is factorized as $P = P_{ll}P_{lr}$. We classify P_l according to the rightmost variables. *Let* $P_l = \sum_{X_i \in \mathcal{X}_r} c_i P_{li} X_i$ ($P_{li} \neq 0$, $\mathcal{X}_r \subseteq \mathcal{X}$, $c_i \in \mathcal{K} - \{0\}$), where the leading coefficient of each P_{li} is equal to 1. Fix an arbitrary variable $X_i (\in \mathcal{X}_r)$ and the corresponding polynomial P_{li}. This P_{li} contains P_{ll} as a left factor, because any right factor of P_l is *zct*.

If the maximal degree of the terms with the rightmost variable X_i in P_{lr} is equal to 1, then P_{li} must left-divide P_l, $P_{ll} = P_{li}$, and $P_{lr} = P_l \backslash P_{ll}$. In particular, P_l is factorized into $P_{ll} (= P_{li})$ and $P_{lr} (= P_l \backslash P_{ll})$ by finding P_{li}'s, if $\deg(P_{lr}) = 1$. As an induction hypothesis, we now assume that a polynomial, any right factor of which is *zct*, can be factorized into left and right factors such

that the right one is of the maximal degree among the right factors which contain one *zct* irreducible factor, if the degree of such right factor is less than $\deg(P_{lr})$.

In the case when P_{li} is *nzct*, there exists just one *zct* irreducible factor in P_l. Hence, $P_{lr}=P_l$ and $P_{ll}=1$ hold.

In the case when P_{li} is *zct*, *nzrf* can be applied to P_{li}.

Lemma 3.7 *The expression* $P_{li}/nzrf(P_{li})$ *contains* P_{ll} *as a left factor.*

Proof. Polynomial P_{li} contains P_{ll} as a left factor.

When $P_{ll}=1$, this lemma is trivial. So, we assume in the rest of this lemma, P_{ll} is *zct*. If $P_{li}\backslash P_{ll}$ is *nzct*, $P_{li}/nzrf(P_{li})$ is equal to P_{ll} by Lemma 3.5. Otherwise, there exist *zct* factors placed to the right of P_{ll} in P_{li}. So, $P_{li}/nzrf(P_{li})$ contains P_{ll} as a left factor again. □

If $P_{li}/nzrf(P_{li})$ left-divides P_l, then P_{ll} is equal to $P_{li}/nzrf(P_{li})$. Otherwise, by the hypothesis, $P_{li}/nzrf(P_{li})$ can be factorized into the left and right factors such that the right one is of the maximal degree among the right factors containing one *zct* irreducible factor. It follows that P_{ll} is found by inductively repeating the above argument until it is found that either P_l contains only one *zct* irreducible factor, or the left factor, corresponding to $P_{li}/nzrf(P_{li})$, left-divides P_l. Then, P_{lr} is obtained by $P_l\backslash P_{ll}$. Consequently, any P_l can be factorized into P_{ll} and P_{lr}.

In **Fig. 4**, we show the algorithm '*zrf*' obtained from the above argument. This requires a *zct* polynomial P_l whose any right factor is *zct*, and returns P_{ll} and P_{lr}. This name stands for '*zct* right factor' in contrast with *nzrf*.

Step 3: We will obtain *nzct* left factor, say P_{lrl}, and *zct* irreducible right factor, say P_{lrr}, of P_{lr} ($P_{lr}=P_{lrl}P_{lrr}$), by applying to P_{lr} the algorithm *nzlf* which is reversal of the left and right sides of *nzrf*. This *nzlf* stands for '*nzct* left factor' in contrast with *nzrf*.

In **Fig. 5**, we show the algorithm '*decom1*' obtained from the above argument. This requires a *zct* polynomial P and returns a list of four factors $(P_{ll}, P_{lrl}, P_{lrr}, P_r)$, where P_r, P_{lrr}, P_{lrl}, and P_{ll} are the *nzct* right factor of the maximal degree, the *zct* irreducible factor, the *nzct* factor placed to the left of P_{lrr}, and the remaining left factor, respectively. The labels 1., 2., and 3. in Fig. 5 correspond to the steps in this subsection and the numbers in square brackets of Fig. 2.

Algorithm : Factorization algorithm 2 (*zrf*)
Input. *Zct* polynomial P_l whose any right factor is *zct*.
Output. Left and right factors of P_l such that the right factor is of the largest degree among the right factors which contain one *zct* irreducible factor.

1. (Initialization)
1.1 $P_{l0} \leftarrow P_l$;
2. (Classification)
2.1 fix P_i' such that $P_l = \sum_{X_i \in \mathcal{X}} c_i P_i' X_i$, $c_i \in \mathcal{K} - \{0\}$, and leading coefficient of P_i' is 1. ;
3. (Check1)
3.1 if $ct(P_i') \neq 0$ then
3.2 return $(1, P_{l0})$;
4. (Check2)
4.1 $P_{ll} \leftarrow P_i'/nzrf(P_i')$;
4.2 if P_{ll} left-divides P_{l0} then
4.3 return $(P_{ll}, P_{l0}\backslash P_{ll})$;
4.4 $P_l \leftarrow P_{ll}$,
4.5 goto 2. ;

Fig. 4 Factorization algorithm *zrf* for a *zct* polynomial.

Algorithm : Factorization algorithm 3 (*decom1*)
Input. *Zct* polynomial P.
Output. List of four factors such that 2nd one from the right is *zct* and irreducible.

1. (*nzrf*)
1.1 $P_r \leftarrow nzrf(P)$; $P_l \leftarrow P/P_r$;
2. (*zrf*)
2.1 $(P_{ll}, P_{lr}) \leftarrow zrf(P_l)$;
3. (*nzlf*)
3.1 $P_{lrl} \leftarrow nzlf(P_{lr})$; $P_{lrr} \leftarrow P_{lr}\backslash P_{lrl}$;
3.2 return $(P_{ll}, P_{lrl}, P_{lrr}, P_r)$;

Fig. 5 Factorization algorithm *decom1* for a *zct* polynomial.

3.2.2 Factorization of *nzct* polynomials

Let f_c be a natural homomorphic mapping from noncommutative polynomials $\mathcal{K}\langle\mathcal{X}\rangle$ to commutative ones $\mathcal{K}[\mathcal{X}]$, which simply interprets addition and multiplication operators of $\mathcal{K}\langle\mathcal{X}\rangle$ as those of $\mathcal{K}[\mathcal{X}]$.

Some polynomials are mapped into $\mathcal{K}$ by f_c, for example $3X^2Y-XYX-2YX^2+1$. Since such polynomial will be not easy to factorize by the method mentioned in Subsection 3.2.1, we apply the naïve method mentioned in Subsection 3.1. Otherwise, as we will show below, the polynomial can be converted into a *zct* one by linear transformations of some variables and the extension of the coefficient field, and it is applied the factorization method mentioned in Subsection 3.2.1. An irreducible factor over $\mathcal{K}$ is constructed from the factors over the extension field by computing the lclm. As a result, three factors over $\mathcal{K}$ will be obtained, whose central one is irreducible over $\mathcal{K}$.

In **Fig. 6**, the configuration of this factoriza-

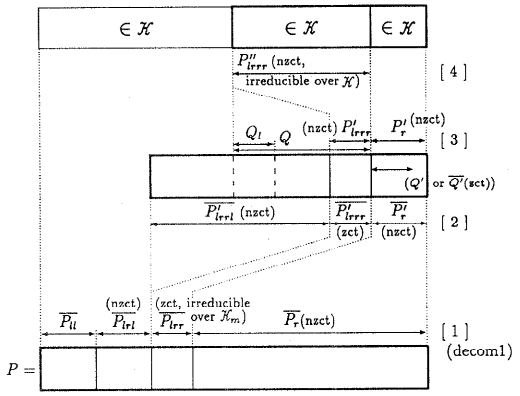


Fig. 6 Configuration of the factorization of an *nzct* polynomial.

tion for an *nzct* polynomial is shown. The lowest rectangle with thick lines represents a given polynomial to be factorized. Each rectangle represents a factor. Numbers in square brackets represent the steps of the factorization procedure described below. Dotted lines represent the correspondences between factors. Symbol '$\in\mathcal{K}$' in a rectangle indicates that the coefficients of the corresponding factor belong to $\mathcal{K}$.

Step 1: If an *nzct* polynomial is not mapped into $\mathcal{K}$ by f_c, a polynomial including univariate monomials is obtained from the *nzct* polynomial by linearly transforming some variables X_i into $X_i+c_i(c_i\in\mathcal{K})$. We assume, without loss of generality, that there exist univariate monomials in a given *nzct* polynomial P. Let P_X be a univariate polynomial, including a constant term, in P and X its variable. Since P_X is univariate, P_X is equivalent to a commutative polynomial over $\mathcal{K}$. Therefore, it is possible to factorize P_X over $\mathcal{K}$. Let P_{X0} be an irreducible factor over $\mathcal{K}$ of P_X and α a root of P_{X0}. From the practical viewpoint, P_{X0} should be chosen to minimize the degree of P_{X0}. Suppose that P is a polynomial over $\mathcal{K}(\alpha)$. Then by a linear transformation of X into $X+\alpha$ in P, a polynomial $P[X+\alpha/X]$ over $\mathcal{K}(\alpha)$ will be *zct*. To simplify notation in the rest of this subsection, we denote a transformation of X into $X+\alpha$ by an overline of a polynomial, like $\overline{P}$ instead of $P[X+\alpha/X]$. Applying the algorithm *decom1* mentioned in Subsection 3.2.1 to $\overline{P}$ over $\mathcal{K}(\alpha)$, the factors $\overline{P_{ll}}$, $\overline{P_{lrl}}$, $\overline{P_{lrr}}$, and $\overline{P_r}$ will be obtained, where $\overline{P_{ll}}$, $\overline{P_{lrl}}$, $\overline{P_{lrr}}$, and $\overline{P_r}$ over $\mathcal{K}$ (α) correspond to P_{ll}, P_{lrl}, P_{lrr}, and P_r defined in Subsection 3.2.1. In particular, when an irreducible polynomial P_{X0} is linear, it can be factorized using linear transformation of a variable only over $\mathcal{K}$.

We note that the constant terms of *nzct* polynomials which are mapped into $\mathcal{K}$ by f_c cannot be reduced to zero by linear transformations of variables. Indeed, no univariate monomials will appear in such polynomials whose variables are linearly transformed. This is the reason why the constant term method cannot be applied to them.

It is shown below how an irreducible factor over $\mathcal{K}$ is obtained from an irreducible factor over $\mathcal{K}(\alpha)$. We will retain the notations of C, C', d_m, and $\{\alpha_0, \ldots, \alpha_{d_m-1}\}$ in Subsection 2.3, but P_{X0} denotes the minimal polynomial of α and $\mathcal{K}_m$ the minimal splitting field of P_{X0}.

Spep 2: There is one *zct* irreducible factor in $\overline{P_{lrr}}\ \overline{P_r}$. In some factorization, such factor is $\overline{P_{lrr}}$. We, however, obtain the rightmost *zct* irreducible factor from $\overline{P_{lrr}}\ \overline{P_r}$ using *nzrf* and *nzlf*. Let $\overline{P'_{lrrl}}=nzlf\,(\overline{P_{lrr}}\ \overline{P_r})$, $\overline{P'_r}=nzrf\,(\overline{P_{lrr}}\ \overline{P_r}\backslash\overline{P'_{lrrl}})$, and $\overline{P'_{lrrr}}=(\overline{P_{lrr}}\ \overline{P_r}\backslash\overline{P'_{lrrl}})/\overline{P'_r}$; *i.e.*, $\overline{P_{lrr}}\ \overline{P_r}=\overline{P'_{lrrl}}\ \overline{P'_{lrrr}}\ \overline{P'_r}$ holds, both $\overline{P'_{lrrl}}$ and $\overline{P'_r}$ are *nzct*, and $\overline{P'_{lrrr}}$ is the rightmost *zct* irreducible factor of $\overline{P_{lrr}}\ \overline{P_r}$.

Step 3: The factor P'_r is a right factor of P over $\mathcal{K}$. This is shown below.

Theorem 3.1 *The factor P'_r is a right factor of P over $\mathcal{K}$.*

Proof. This is proven by showing that $P_{ll}P_{lrl}P'_{lrrl}P'_{lrrr}$ belongs to $\mathcal{K}\langle\mathcal{X}\rangle$, because P belongs to $\mathcal{K}\langle\mathcal{X}\rangle$. Suppose $P_{ll}P_{lrl}P'_{lrrl}P'_{lrrr}$ does not belong to $\mathcal{K}\langle\mathcal{X}\rangle$. Then, let Q be the right factor of $P_{ll}P_{lrl}P'_{lrrl}P'_{lrrr}$ against the maximal-degree left factor over $\mathcal{K}$. The right factor Q belongs to $\mathcal{K}_m\langle\mathcal{X}\rangle$, not $\mathcal{K}\langle\mathcal{X}\rangle$. Let Q_l be an irreducible left factor of Q over $\mathcal{K}_m$. As mentioned in Subsection 2.3, an irreducible factor over $\mathcal{K}$ is the lcrm of $Q_l[\alpha_i/\alpha]$'s for $\alpha_i\in C$. For the existence of P'_{lrrr} as an irreducible right factor of Q over $\mathcal{K}_m$, there exist a minimal set C_Q of conjugates and a conjugate α_j of α such that $\mathrm{lcrm}_{\alpha_i\in C_Q}(Q_l[\alpha_i/\alpha])=Q/P'_{lrrr}$ and $\mathrm{lcrm}_{\alpha_i\in C_Q\cup\{\alpha_j\}}(Q_l[\alpha_i/\alpha])=Q$. There also exists a conjugate α_k, satisfying $Q/P'_{lrrr}\neq\mathrm{lcrm}_{\alpha_i\in C_Q\cup\{\alpha_k\}}(Q_l[\alpha_i/\alpha])\neq Q$, in the set $C-(C_Q\cup\{\alpha_j\})$. Let

$$A_1=\mathrm{lcrm}_{\alpha_i\in C_Q\cup\{\alpha_k\}}(Q_l[\alpha_i/\alpha])\backslash(Q/P'_{lrrr}),\quad\text{and}\qquad(3.4)$$

$$B_1 = \mathrm{lcrm}_{\alpha_i \in C_0 \cup \{\alpha_j, \alpha_k\}}(Q_l[\alpha_i/\alpha]) \backslash Q. \quad (3.5)$$

Then, there exists such a B_2 that $P'_{lrrr}B_1 = A_1B_2$ by Ref. 5), Corollary 3 of Theorem 4.1. Since the constant terms of $\overline{P'_{lrrr}}$ and $\overline{B_2}$ are equal each other, $\overline{B_2}$ is *zct*. This contradicts the construction of $\overline{P'_{lrrr}}$, which is the rightmost *zct* irreducible factor of $\overline{P_{lrr}}\,\overline{P_r}$. Therefore, $P_{ll}P_{lrl}P'_{lrrl}P'_{lrrr}$ and P'_r belong to $\mathcal{K}\langle X\rangle$. □

Step 4: The irreducible factor, placed to the left of P'_r, over $\mathcal{K}$ is obtained by calculating the lclm over $\mathcal{K}_m$. Although there are computer utilities to express all conjugates of α in terms of an algebraic number, for example the "Algebraic Number Fields" package[6] of REDUCE, we will consider that a conjugate is not expressed in terms of an algebraic number. In the rest of this subsection, we deal symbolically with the conjugates rather than algebraic numbers. We describe below how to obtain an irreducible factor without expressing conjugates of α in terms of an algebraic number.

Let P'_{lrrrX} be the sum of univariate monomials with a variable X of P'_{lrrr} including constant term, and d_X be $\deg(P'_{lrrrX})$. We note that when all $P'_{lrrrX}[\alpha_i/\alpha]$'s for some α_i's ($\subseteq C$) are distinct even if each α_i is expressed in terms of an algebraic number, then the multiplication of them is equal to the least common multiple. The expression $\prod_{\alpha_i \in C} P'_{lrrrX}[\alpha_i/\alpha]$ is symmetric for $\alpha_i \in C$ and belongs to $\mathcal{K}$ by the fundamental theorem on symmetric polynomials. Let $\prod_{\alpha_i \in C} P'_{lrrrX}[\alpha_i/\alpha] = F^e$ where F is a factor in $\mathcal{K}[X]$ and e is the multiplicity of F (e is an large as possible). We can find F and e by calculating the square-free decomposition. Obviously, P_{X0} is a factor of F.

Let n denote the number of elements of C'. Then, nd_X needs to be a multiple of the degree of F ($\deg(F) = d_X d_m/e$), and obviously $n \leq d_m$ holds. Therefore, n is a multiple of d_m/e, $1 \leq n \leq d_m$. If the conjugates are expressed in terms of an algebraic number, then all coefficients of the multiplication of n distinct $P_{lrrrX}[\alpha_i/\alpha]$'s for $\alpha_i \in C'$ belong to $\mathcal{K}$, and each one of the coefficients is equal to that of F^{en/d_m} with same degree of X.

We obtain an irreducible factor by finding n and C' as follows. First, we obtain a minimal set C'' of n' conjugates of α, where n' is a multiple of d_m/e as small as possible, and the coefficients of the multiplication of n' distinct $P_{lrrrX}[\alpha_i/\alpha]$'s for $\alpha_i \in C''$ are consistently expressed by the coefficients of F^{en'/d_m}. Then, the relations between elements of $\mathcal{K}$ and symmetric polynomials of conjugates of C'' are found. If the coefficients of the expression $\mathrm{lclm}_{\alpha_i \in C''} P'_{lrrr}[\alpha_i/\alpha]$, which are symmetric for $\alpha_i \in C''$, can be consistently translated into elements of $\mathcal{K}$ using the relations, then the translated expression, say P''_{lrrr}, is an irreducible factor of P over $\mathcal{K}$, and n' and C'' are to be equal to n and C', respectively. Otherwise, we attempt to find larger C'' and n' again in the same manner. We obtain n and C' by the existence of an irreducible factor before $n' > d_m$ holds.

Finally, the left factor $P/(P''_{lrrr}P'_r)$ of P is obtained.

Algorithm : Factorization algorithm 4 (*decom2*)

Input. *Nzct* polynomial P.
Output. List of three factors such that central one is irreducible.
Assumption.
There is a univariate polynomial P_X with a variable X in P.
α is a root of an irreducible factor of P_X.

1. (Factorization over $\mathcal{K}(\alpha)$)
1.1 $\overline{P} \leftarrow P[X + \alpha/X]$;
1.2 $(\overline{P_{ll}}, \overline{P_{lrl}}, \overline{P_{lrr}}, \overline{P_r}) \leftarrow decom1(\overline{P})$;
2. (Moving *zct* factor to the right)
2.1 $\overline{P'_{lrrl}} \leftarrow nzlf(\overline{P_{lrr}}\,\overline{P_r})$;
2.2 $\overline{P'_r} \leftarrow nzrf((\overline{P_{lrr}}\,\overline{P_r}) \backslash \overline{P'_{lrrl}})$;
2.3 $\overline{P'_{lrrr}} \leftarrow ((\overline{P_{lrr}}\,\overline{P_r}) \backslash \overline{P'_{lrrl}}) / \overline{P'_r}$;
3. (Inverse transformation)
3.1 $P'_{lrrr} \leftarrow \overline{P'_{lrrr}}[X - \alpha/X]$;
3.2 $P'_r \leftarrow \overline{P'_r}[X - \alpha/X]$;
4. (Translation $\mathcal{K}(\alpha) \rightarrow \mathcal{K}$)
4.1 $P''_{lrrr} \leftarrow \mathrm{lclm}_{\alpha_i \in C'}(P'_{lrrr}[\alpha_i/\alpha])$, whose coefficients are translated into $\mathcal{K}$, where C' is the minimal set of the conjugates of α such that the coefficients are translated into $\mathcal{K}$.
4.2 return $(P/(P''_{lrrr}P'_r), P''_{lrrr}, P'_r)$;

Fig. 7 Factorization algorithm *decom2* for an *nzct* polynomial.

Table 1 Examples with computing times.

No.	Factorized formula	Degree / Number of terms / Number of factors	Naïve method [sec] / Constant term method [sec]
1.	$(XY+3X+2Y)^4$	8 / 73 / 4	312.5 / 9.1
2.	$(XY+3X+2Y+5)^4$	8 / 88 / 4	325.8 / 14.6
3.	$(XY+3X+2Y)^4+7$	8 / 74 / 1	1702.8 / 33.4
4.	$XY^2X+X^2+XY+YX+1$	4 / 5 / 1	3.1 / 1.4
5.	$X^5Y^2X^5+X^{10}+X^5Y+YX^5+1$	12 / 5 / 1	236.6 / 11.4
6.	$(4YXY+XYX)X^{10}+Y$	13 / 3 / 1	248.7 / 0.8
7.	$3XYXWYX^2+2YXYXYZ$ $-3Y^2W+ZX-6Y+5$	7 / 6 / 1	49.4 / 1.5
8.	$3XYZXYX^2+4XYXZY+7YX^2Y$ $-2Y^2X-XY-5XZ+3Y^2+2X-3Z+3$	7 / 10 / 1	84.0 / 2.9
9.	$(XY-YX+1)^2$	4 / 7 / 2	2.9 / (3.2)
10.	$(XY-YX+1)^2(XY+3)$	6 / 11 / 3	10.5 / (4.9)

In **Fig. 7**, we show the algorithm '*decom2*' directly obtained from the above argument. This *decom2* requires an *nzct* polynomial P and returns a list of factors $(P/(P''_{lrrr}P_r), P''_{lrrr}, P'_r)$, where P''_{lrrr} is irreducible over $\mathcal{K}$. The labels 1., 2., 3., and 4. in Fig. 7 correspond to the numbers in square brackets of Fig. 6.

3.2.3 Irreducible factorization

An irreducible factorization over $\mathcal{K}$ is obtained by repeatedly applying the algorithms *decom1* and *decom2* mentioned in Subsections 3.2.1 and 3.2.2 to polynomials except the factors which are mapped into $\mathcal{K}-\{0\}$ by f_c. The polynomials mapped into $\mathcal{K}-\{0\}$ by f_c can be irreducibly factorized using the naïve method mentioned in Subsection 3.1.

4. Examples

In this section, we show some examples of factorizations over the rational number field $\mathbb{Q}$ with computing times. The algorithms are implemented on REDUCE3.3[7] by Staff LISP[8] on SONY NWS-821.

We have examined factorization of polynomials by two methods: (1) the naïve method mentioned in Subsection 3.1, and (2) the constant term method mentioned in Subsection 3.2. The naïve method uses the computation of Gröbner basis and the factorization of commutative polynomial over $\mathbb{Q}$ in order to solve the decomposition equations.

Examples are shown in **Table 1** with measured computing times in seconds. For the convenience of the reader and the size of expression, all listed polynomials are given in irreducibly factorized form (over $\mathbb{Q}$), but our measurement was made using expanded formulas. Computing times of the upper and lower sides correspond to the naïve and constant term methods, respectively. Degrees, the numbers of terms, and the numbers of irreducible factors of polynomials are also given in Table 1.

Polynomial No. 1 is *zct*. It can be irreducibly factorized by *decom 1*, since all irreducible factors are *zct*. Polynomial No. 2 is *nzct*. Factors of No. 2 are equal to those of No. 1 except for the addition of a constant term 5. By replacing* X by $X-5/3$, all factors of No. 2 turn out to be *zct*. Thus, an irreducible factor-

* It is also possible to factorize it by replacing Y by $Y-5/2$. This simply depends on the implementation of the algorithms.

ization of No. 2 by the constant term method is obtained using the operations only over $\mathbb{Q}$. Polynomial No. 3 is equal to No. 1 except for the addition of a constant term 7. This, however, cannot be converted to *zct* factors only by linear transformations of the variables over $\mathbb{Q}$. Therefore, when the constant term method is used, No. 3 is first factorized over $\mathbb{Q}(\alpha)$, where α is a root of a minimal polynomial* $(3X)^4+7$, which is a univariate polynomial in No. 3. Then, an irreducible right factor $(XY+2Y+3X-3\alpha)$ over $\mathbb{Q}(\alpha)$ is obtained. An irreducible factor over $\mathbb{Q}$, which is equal to No. 3, is obtained from the least common left multiple $\mathrm{lclm}_{0\le i\le 3}(XY+2Y+3X-3\alpha_i)$, where α_i's are conjugates of α. In the constant term method, No. 2 is factorized 1.6 times slower than No. 1. This difference is caused by linear transformations of the variables over $\mathbb{Q}$ of No. 2, while such transformations are not necessary for No. 1. No. 3 is factorized 3.7 times slower than No. 1. This is due to the linear transformation of a variable over $\mathbb{Q}(\alpha)$ and the operation of the algebraic numbers in No. 3. The comparisons of the constant term and naïve methods show that the computing times for Nos. 1, 2, and 3 of the former are 34.3, 22.3, and 51.0 times faster than those of the latter, respectively.

Polynomial No. 4 is P_2 in the example of Subsection 2.1. When the constant term method is used, the irreducible factor over $\mathbb{Q}$ is obtained by $\mathrm{lclm}(YX-iX+1,\ YX+iX+1)$, where both $YX-iX+1$ and $YX+iX+1$ are irreducible right factors of No. 4 over $\mathbb{Q}(i)$. Concerning computing time, the constant term method is 2.2 times faster than the naïve method. With No. 5, however, which is obtained by replacing X by X^5 in No. 4, the constant term method is 20.8 times faster than the naïve one.

Polynomial No. 6 is irreducible. The constant term method is 310.9 times faster than the naïve one. The great difference of the computing times is due to the following: (1) In the naïve method, the numbers of the constructing and solving of the decomposition equations are 12 each, which is equal to the degree minus 1. After unsuccessful solvings, it is found that it is irreducible. (2) On the other hand, in the constant term method, irreducibility is established by only a single application of *decom 1*. Moreover, the computation without linear transformations of variables and extension of the coefficient field increases the efficiency. This is a lucky case for the constant term method.

Polynomials Nos. 7 and 8 are also irreducible. They should be linearly transformed when the constant term method is used. The factorizations of Nos. 7 and 8 using the constant term method are slower than that of No. 6, but 32.9 and 29.0 times faster than those using the naïve one, respectively.

Some irreducible factors of polynomials Nos. 9 and 10 are mapped into $\mathcal{K}-\{0\}$ by f_c. They cannot be irreducibly factorized using only the constant term method. The numerical values of the constant term method in parentheses listed in Table 1 are the computing times whose factorizations use the naïve method when it is found that the factorizing polynomials are mapped into $\mathcal{K}-\{0\}$ by f_c. By examining whether it is mapped into $\mathcal{K}-\{0\}$ by f_c or not, it is found that No. 9 is mapped into $\mathcal{K}-\{0\}$ by f_c, and it is factorized using the naïve method. For No. 10, when the constant term method is applied, first the right factor $(XY+3)$ is obtained, and then the left factor, whose factorized form is $(XY-YX+1)^2$, is factorized using the naïve method. In the factorization of No. 9, the naïve method is 1.1 times faster than the constant term one. On the other hand, in that of No. 10, the constant term method is 2.1 times faster than the naïve one. This is due to the effectiveness of the first factorization using the constant term method for No. 10. The constant term method is faster than the naïve one for total factorization time of No. 10.

5. Conclusions and Comments

We have investigated the factorization for noncommutative polynomials, and developed two factorization methods: the naïve method and the constant term method. The motivation of this investigation is first to find the algorithm of the factorization for noncommutative polynomials, and next to prove mathematically the correctness of these algorithms. Therefore, in the current stage, applicability of this investigation to computer algebra is not evident, but we are convinced that, in the near future, the developed methods will be used with the advance of computer algebra.

* It is also possible that α is a root of a minimal polynomial $(2Y)^4+7$.

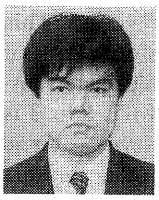
The naïve method is simple, but inefficient. On the other hand, the constant term method is efficient, but complicated, since the method factorizes noncommutative polynomials in one of two ways according to their constant term. *Nzct* polynomials are converted into *zct* ones by linear transformations of variables to factorize them. So, there exists a difference of efficiency between *zct* and *nzct* polynomials. To decrease such difference, we are now developing the factorization algorithms without linear transformations of variables for *nzct* polynomials which are not mapped into $\mathcal{K}$ by f_c. In addition, we are attempting to modify the constant term method in order that it need not use the naïve one even if some factors of a polynomial are mapped into $\mathcal{K}-\{0\}$ by f_c.

Acknowledgments We are grateful to Professor Kenichi Abe at Tohoku University and Professors Osami Saito and Taiichi Yuasa at Toyohashi University of Technology. They provided us with considerable encouragement and moral support. We would also like to thank the referees for careful and sensitive reading of the manuscript and for a great number of suggestions which helped to improve the exposition.

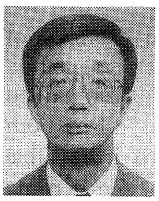
References

1) Knuth, D. E.: *The Art of Computer Programming, Seminumerical Algorithms* (2nd ed.). Addison-Wesley (1981).
2) Berlekamp, E. R.: Factoring Polynomials over Finite Fields, *Bell System Technical Journal* (*AT & T*), Vol. 46, No. 8, pp. 1853 - 1859 (1967).
3) Abbott, J. A., Bradford, R. J. and Davenport, J. H.: Factorisation of Polynomials: Old Ideas and Recent Results, In *LNCS # 296 Trends in Computer Algebra*, pp. 81-91, Springer-Verlag (1988).
4) Davenport, J. H., Siret, Y. and Tournier, E.: *Computer Algebra*, Academic Press (1988).
5) Cohn, P. M.: Rings with a Weak Algorithm, *Transactions of the American Mathematical Society*, Vol. 109, pp. 332-356 (1963).
6) Schruefer, E.: *Algebraic Number Fields*, GMD, Institut F1, Postfach 1240, 5205 St. Augustin, Germany. One of User Contributed Packages of REDUCE 3.3.
7) Hearn, A. C.: *REDUCE User's Manual Version 3.3*, The Rand Corporation, Santa Monica (1987).
8) B. U. G. Inc.: *Staff LISP User's Manual* (*Ver 3. X*) (1988) in Japanese.

(Received February 17, 1992)
(Accepted July 8, 1993)



Kazuyoshi Mori was born in 1965. He received the B.E. and M. E. degrees from Toyohashi University of Technology. He is currently a research associate of the Information and Computer Sciences, Toyohashi University of Technology. His research area includes symbolic and algebraic manipulation system.



Saburou Iida was born in 1943. He received the B.S. degree in Astronomy from Tokyo University, and the M.S. and D.S. degrees in Physics from Nagoya University. He is currently a professor of the School of Computer and Cognitive Sciences, Chukyo University. His primary interests include symbolic and algebraic manipulation system, and computer architecture. He is a member of IPSJ.