COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 72, No. 1 2024

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

On Factorization of Parametric Polynomials

by

Kazuhiro YOKOYAMA

(Received September 5, 2023)
(Revised December 5, 2023)

Abstract. We deal with the *irreducible factorization* of polynomials whose coefficients contain some parameter(s), and present a concrete algorithm for such *parametric polynomials* in the most fundamental case where parametric polynomials are bivariate polynomials in variables x, y with a single parameter a over a field K. In this case, if a polynomial $f(x, y, a)$ is absolutely irreducible over $K(a)$, the rational function field in a over K, we can compute all parameter values a such that $f(x, y, a)$ is reducible over K. This result can be considered as the *first step* for *parametric primary decomposition*, that is, classifying all parameter values for each of which the ideal generated by given parametric polynomials has a *stable primary decomposition*.

1. Introduction

Computation of Gröbner bases plays very important roles in analyzing the structure of polynomial ideals and their varieties. Lots of efforts have been devoted to improve the efficiency of such computations, and these developed efficient methods contributed to solving engineering problems. However, generators of polynomial ideals derived from engineering or pure mathematics often contain parameters in coefficients, and the structures of ideals/varieties depend on the values of these parameters. Here we call such polynomials and ideals *parametric polynomials* and *parametric ideals*, respectively. For such parametric ideals, algorithms for their Gröbner bases and several ideal operations have been studied by several authors. (For example, see [9, 11, 13, 18].)

In particular, to analyze their algebraic structures, their primary decompositions are very important. However, it is very difficult to *comprehensively classify* primary decompositions of a parametric ideal, since the primality of an ideal can not be described *in terms of algebraic conditions in general*. In more details, a problem to examine if an ideal is a prime ideal in a polynomial ring over a field K can be reduced to a problem to examine if a polynomial is irreducible over K. (See [4, 14, 16] for fundamentals on primary decomposition.) But, *the irreducibility is not an algebraic condition in general*. For example, a univariate polynomial $f(x, a) = x^2 - a$ with a parameter a over $\mathbb{Q}$ is reducible over $\mathbb{Q}$ if and only if a is a square of a rational number. In this case, "being a square" is not an algebraic condition. (But, we may say, in another style, that $f(x, a)$ is reducible if and only if a can be expressed as c^2 for some c in $\mathbb{Q}$.)

To attack this hard problem, an naive but rough approach was proposed in [18]. (Here we call it the *naive method*.) And, as its continuation, a new notion of *feasible comprehensive primary decomposition* was introduced in [5] based on *Hilbert's irreducibility theorem*, where the primality can be guaranteed for *almost every* parameter values.

In this paper, we concentrate on the irreducible factorization of *parametric polynomials* in the most fundamental case where we consider only a bivariate polynomial $f(x, y, a)$ in two variables x, y and with a single parameter a over a field K. And, by revising the *naive method* for this special setting, we have the following main theorem:

MAIN THEOREM (THEOREM 3.13 IN SECTION 3.1): If $f(x, y, a)$ is *absolutely irreducible* over the rational function field $K(a)$ in a over K, the set of parameter values for a such that $f(x, y, a)$ is reducible is finite and computed with a help of Gröbner basis of *decomposition ideals* derived from $f(x, y, a)$.

We note that the absolute irreducibility can be tested by Kaltofen's method proposed in [8], which can be efficiently computed by *ordinary* primary decomposition for non-parametric ideals. (See Section 3.1.) We also remark that such absolutely irreducible polynomials form a wider class among all irreducible polynomials. (See QUICK TEST in Remark 3.6.)

Based on the main theorem, we can extract algebraic conditions for absolutely irreducible parametric polynomials having a *specified factorization pattern* (See Section 2.1), and we also have a concrete and effectively computable algorithm for parametric irreducible factorization. (See Algorithm 1 in Section 4.) In Algorithm 1, it is enough to consider *primitive factorization patterns* (Definition 4.1), by which the efficiency and effectivity can be much improved.

Also for a parametric polynomial which is not absolutely irreducible, we also propose a new *representation* of parameter values, by which we can describe the parameter values a such that $f(x, y, a)$ is reducible. (See Section 3.2.)

REMARK 1.1. *It can be shown that the main theorem also holds for polynomials in three or more variables with a single parameter.*

The effectivity of Algorithm 1 was examined by computational experiments using Risa/Asir system [12], where it worked well for smaller degrees. (Examples in Section 2.1 were all computed by Risa/Asir system.) However, for larger degrees, it took a lots of computational time due to the heavy growth of the number of variables in decomposition ideals. Thus, improving the efficiency shall be our task in further study.

This paper is organized as follows. In Section 2, we show some preliminaries on our setting and explain the *naive method* for irreducible factorization of parametric polynomials. We also show how the naive method is applied to simple examples. In Section 3, we provide the notion of *absolute irreducibility* and Kaltofen's test modified to our case, and show our main theorem for bivariate polynomials with a single parameter. Also we discuss how to represent parameter values for non-absolutely irreducible polynomials. In Section 4, we introduce a notion of *primitive pattern* and based on it, we show a concrete and effective factorization algorithm for absolutely irreducible parametric polynomials. In Section 5, we

explain the conclusion and future works. Moreover, as we use a modification of Kaltofen's test, we give a simple proof for it in Appendix.

Finally we remark that an outline of the results in this paper was orally presented in Applications of Computer Algebra 2022 [20].

2. Preliminaries for Factorization of Parametric Polynomials and Examples

For the irreducible factorization of a parametric polynomial, decomposition ideals are proposed in [18] inspired by an idea in [15]. Here we show our *naive method* [1] in *general setting* not restricted to the bivariate and a single parameter case.

- Let $A = \{a_1, \ldots, a_m\}$ be the set of parameters and $X = \{x_1, \ldots, x_n\}$ the set of variables. Also, let K be a *field* and $\overline{K}$ its algebraic closure. (We mainly consider $K = \mathbb{Q}$, the rational number field.) Here we call a polynomial in $K[X, A]$ a *parametric polynomial*.
- For a parametric polynomial $f(X, A)$, we choose one variable z from X as the *main variable* and consider $f(X, A)$ as a univariate polynomial in z over $K[A, Y]$, where $Y = X \setminus \{z\}$. (Y can be an empty set.) For simplicity, we denote it by $f(z)$ for highlighting the main variable z.
- To simplify our arguments and methods, $f(X, A)$ is *irreducible* in $K[X, A]$ and *monic* with respect to the main variable z. Because, we can deal with non-monic cases by the same arguments. (But, in this case, we have to classify parameter values for stable degree of $f(X, A)$ with respect to z beforehand.)

REMARK 2.1 (Density of Values of A Making $f(X, A)$ Irreducible). *In our setting with $K = \mathbb{Q}$, we may expect that $f(X, \alpha)$ is irreducible over K for almost all parameter values α for A by* Hilbert's irreducible theorem. *(See [2, Theorem 4.1.2] and [10, Corollary 2.5 of Chapter 9].)*

HILBERT'S IRREDUCIBLE THEOREM: *Let $f(X, A)$ be an irreducible (non-constant) polynomial in $\mathbb{Q}[X, A]$. Then, there exist infinitely many points α in $\mathbb{Q}^m$ such that the specialized polynomial $f(X, \alpha)$ is irreducible in $\mathbb{Q}[X]$. Moreover, there exists a* Zariski dense set *$\mathcal{O}$ of $\mathbb{Q}^m$ such that $f(X, \alpha)$ is irreducible in $\mathbb{Q}[X]$ for any α in $\mathcal{O}$. We say that a subset $\mathcal{O}$ is a* Zariski dense *if the* Zariski closure *of $\mathcal{O}$ coincides with $\mathbb{Q}^m$.*

We note that a field K satisfying Hilbert's irreducible theorem is called a Hilbertian. *$\mathbb{Q}$ and its extensions are Hilbertian, but finite fields are not.*

The set of all points α in $\mathbb{Q}^m$ such that $f(X, \alpha)$ is irreducible over $\mathbb{Q}$ is called a basic Hilbert subset. The intersection of finitely many basic Hilbert subset and finitely many Zariski-open sets is called a *Hilbert subset*. Then, by [10, Corollary 2.5 of Chapter 9], it is shown that every Hilbert subset is a *dense set* for the ordinary topology on $\mathbb{Q}^m$

[1] In [18], the method were named *successive construction of parametric ideals*.

2.1. Outline of Naive Method

Let our target parametric polynomial be $f(z, Y, A) = z^d + f_{d-1}(Y, A)z^{d-1} + \cdots + f_0(Y, A)$, where z is the main variable and $Y = \{y_1, \ldots, y_r\}$. (Thus $r = n - 1$.) Here we give an outline of the naive method.

- We consider *a possible factorization* with monic factors:

$$f(z) = g_1(z) \cdots g_s(z)\,, \tag{1}$$

  where $d_1 = \deg_z(g_1) \leq \ldots \leq d_s = \deg_z(g_s)$ and $d = d_1 + \cdots + d_s$. Here we denote the degree of f with respect to x_i by $\deg_{x_i}(f)$. We call $\mathbf{d} = (d_1, \ldots, d_s)$ a *factorization pattern* or a *pattern* in short. We remark that, in order to handle the irreducible case, we call $\mathbf{d} = (d)$ the *trivial* (factorization) pattern. For our computation, patterns with $s = 2$ are essential and called *primitive patterns* (Definition 4.1 and Lemma 4.3). (See also Remark 2.3.)
- We introduce *new variables* B which represent all possible coefficients of $g_1(z)$, $\ldots$, $g_s(z)$, that is,

  $$B = \{b^{(i)}_{k,e_1,\ldots,e_r} \mid 1 \leq i \leq s, 0 \leq k \leq d_i, 0 \leq e_1 \leq D_1, \ldots, 0 \leq e_r \leq D_r\}$$

  where $D_j = \deg_{y_j}(f)$ for each y_j, and factors are expressed as follows:

$$\begin{cases} g_1(z) &= z^{d_1} + \sum_{k<d_1, e_1 \leq D_1, \ldots, e_r \leq D_r} b^{(1)}_{k,e_1,\ldots,e_r} y_1^{e_1} \cdots y_r^{e_r} z^k\,, \\ g_2(z) &= z^{d_2} + \sum_{k<d_2, e_1 \leq D_1, \ldots, e_r \leq D_r} b^{(2)}_{k,e_1,\ldots,e_r} y_1^{e_1} \cdots y_r^{e_r} z^k\,, \\ \vdots & \\ g_s(z) &= z^{d_s} + \sum_{k<d_s, e_1 \leq D_1, \ldots, e_r \leq D_r} b^{(s)}_{k,e_1,\ldots,e_r} y_1^{e_1} \cdots y_r^{e_r} z^k\,. \end{cases}$$

- For each monomial $z^k y_1^{e_1} \cdots y_r^{e_r}$, where $0 \leq k < d$, $0 \leq e_1 \leq D_1, \ldots, 0 \leq e_r \leq D_r$, by comparing the coefficient of $f(z)$ with that of $g_1(z) \cdots g_s(z)$, we have *algebraic equations*. Gathering such equations for all monomials, we have a *system of algebraic equations*, which gives an ideal $\mathcal{J}_\mathbf{d}$ of $K[A, B]$. (See Example 2.4.) We call $\mathcal{J}_\mathbf{d}$ the *decomposition ideal* with respect to the factorization pattern $\mathbf{d} = (d_1, \ldots, d_s)$. For each zero of the decomposition ideal, that is, a solution of the system of algebraic equations, we call its A-component a *feasible value* for the factorization pattern $\mathbf{d}$. Then, for each feasible value α of A in K^m, $f(z, Y, \alpha)$ has a factorization of pattern $\mathbf{d}$ over K.
- The *existence* of the factorization (1) can be reduced to the *non-triviality* of $\mathcal{J}_\mathbf{d}$, from which we can deduce the condition for feasible values of A. If $\mathcal{J}_\mathbf{d}$ is trivial, then f cannot have a factorization of pattern $\mathbf{d}$ for any value of A.

In below we assume that the decomposition ideal $\mathcal{J}_\mathbf{d}$ is *non-trivial*.

- We compute a Gröbner basis of the *elimination ideal* $K[A] \cap \mathcal{J}_\mathbf{d}$ by using an elimination order $A \prec\prec B$. (See [1, Chapter 3].) We denote the elimination ideal by $\mathcal{E}_\mathbf{d}$. We note that $\mathcal{E}_\mathbf{d}$ can be trivial, that is, $\mathcal{E}_\mathbf{d} = \{0\}$. In this case, there is no Gröbner basis for it.

- If the elimination ideal $\mathcal{E}_{\mathbf{d}}$ is non-trivial, that is, it has a non-trivial Gröbner basis, its Gröbner basis gives an *necessary* condition for feasible values of A for the factorization pattern $\mathbf{d}$. The correctness of the obtained condition can be examined by computing *prime decomposition* of the radical of ideal generated by the computed condition on A and f in $K[X, A]$.
- If the elimination ideal $\mathcal{E}_{\mathbf{d}}$ is trivial, that is, $\{0\}$, the condition for the factorization pattern $\mathbf{d}$ shall be given in a *different manner*.

REMARK 2.2. *The elimination ideal $\mathcal{E}_{\mathbf{d}} = K[A] \cap J_{\mathbf{d}}$ can be trivial even if $\mathcal{J}_{\mathbf{d}}$ is non-trivial. For example, if f is (weighted) homogeneous in x_1, x_2, f can be factorized into linear factors over $\overline{K}$ for any parameter value. For such a case, we have to describe the parameter values in another way. (See Example 2.7.) If the elimination ideal $\mathcal{E}_{\mathbf{d}}$ is non-trivial and A consists of one parameter, the decomposition ideal $\mathcal{J}_{\mathbf{d}}$ is 0-dimensional. (See Lemma 3.10.) In this case, by so-called* Extension Theorem*, for every feasible value α, there is a zero whose A-component is α. (See [1, Chapter 3] and Theorem 3.13.)*

REMARK 2.3. *For a parametric polynomial, if its non-trivial decomposition ideals always give necessary conditions for feasible values, we do not need to consider all factorization patterns. Instead, we only need to consider* primitive factorization patterns *(Definition 4.1 and Lemma 4.3), by which we can avoid certain combinatorial explosion. (See Section 4.)*

On the other hand, there is a parametric polynomial such that some non-trivial decomposition ideal cannot give any necessary condition. See Example 2.6, where we have a necessary condition for the pattern $(1, 2)$ *but not for the pattern* $(1, 1, 1)$.

2.2. Simple Examples

Here we give several examples for understanding our naive method.

EXAMPLE 2.4 (The Most Basic Case). *We consider one of the most basic case, where $K = \mathbb{Q}$, $A = \{a\}$, $X = \{z, y\}$ and $f(z, y, a) = z^2 - y^2 - ay - a$. In this case we can show that $f(z, y, a)$ is reducible over $\mathbb{Q}$ if and only if $a = 0$ or $a = 4$. As $\deg_z(f(z, y, a)) = 2$, $(1, 1)$ is the unique non-trivial factorization pattern.*

- *We consider the factorization pattern* $(1, 1)$. *Introducing new variables $b_{0,2}^{(1)}, b_{0,1}^{(1)}$, $b_{0,0}^{(1}, b_{0,2}^{(2)}, b_{0,1}^{(2)}, b_{0,0}^{(2)}$, we consider the following factorization:*

$$f(x, y) = \left(z + b_{0,2}^{(1)} y^2 + b_{0,1}^{(1)} y + b_{0,0}^{(1)}\right)\left(z + b_{0,2}^{(2)} y^2 + b_{0,1}^{(2)} y + b_{0,0}^{(2)}\right),$$

from which we obtain a system of algebraic equations in the variable a *and* $b_{0,2}^{(1)}$, $b_{0,1}^{(1)}, b_{0,0}^{(1}, b_{0,2}^{(2)}, b_{0,1}^{(2)}, b_{0,0}^{(2)}$ *as follows.*

$$\begin{cases} b_{0,2}^{(1)} + b_{0,2}^{(2)} = 0 & \text{from the coefficient of } zy^2\,, \\ b_{0,1}^{(1)} + b_{0,1}^{(2)} = 0 & \text{from the coefficient of } zy\,, \\ b_{0,0}^{(1)} + b_{0,0}^{(2)} = 0 & \text{from the coefficient of } z\,, \\ b_{0,2}^{(1)} b_{0,2}^{(2)} = 0 & \text{from the coefficient of } y^4\,, \\ b_{0,2}^{(1)} b_{0,1}^{(2)} + b_{0,1}^{(1)} b_{0,2}^{(2)} = 0 & \text{from the coefficient of } y^3\,, \\ b_{0,2}^{(1)} b_{0,0}^{(2)} + b_{0,1}^{(1)} b_{0,1}^{(2)} + b_{0,0}^{(1)} b_{0,2}^{(2)} + 1 = 0 & \text{from the coefficient of } y^2\,, \\ a + b_{0,1}^{(1)} b_{0,0}^{(2)} + b_{0,0}^{(1)} b_{0,1}^{(2)} = 0 & \text{from the coefficient of } y\,, \\ a + b_{0,0}^{(1)} b_{0,0}^{(2)} = 0 & \text{from the constant}\,. \end{cases}$$

- *Computing the elimination ideal* $\mathcal{E}_{(1,1)}$ *of the decomposition ideal* $\mathcal{J}_{(1,1)}$*, we have the following necessary condition in* a *such that* $f(z, y, a)$ *is reducible over* $\mathbb{Q}$*:*

$$a^2 - 4a = 0\,.$$

Thus, if $a \neq 0, 4$*, then* $f(z, y, a)$ *is irreducible over* $\mathbb{Q}$*. For* $a = 0, 4$*, we have* $f(z, y, 0) = (z - y)(z + y)$ *and* $f(z, y, 4) = (z - y - 2)(z + y + 2)$.

EXAMPLE 2.5 (Another Basic Case). *Consider* $K = \mathbb{Q}$, $A = \{a\}$, $X = \{z, y\}$ *and*

$$f(z, y, a) = z^4 + (-y^2 + y)z^3 + (-y^3 + 3y^2 + y + a^2 - 4)z^2 + (-y^4 + 2y^3 + (-a^2 + a + 1)y^2 - 3y - a + 1)z - y^5 + y^4 + (a^2 - a + 3)y^3 + (a - 3)y^2 - 2y + a^2 - 2a + 2.$$

As the degree $\deg_z(f)$ *of* f *in* z *is* 4*, possible non-trivial factorization patterns are* $(1, 3)$, $(2, 2)$, $(1, 1, 2)$, $(1, 1, 1, 1)$. *We remark that* $(1, 3)$ *and* $(2, 2)$ *are primitive patterns.*

- *For the factorization pattern* $(1, 3)$*, the reduced Gröbner basis of the decomposition ideal* $\mathcal{J}_{(1,3)}$ *with respect to an elimination order* $a \prec\prec B$ *is*

$$\{a, (b_{0,0}^{(1)})^2 - b_{0,0}^{(1)} - 2, b_{0,0}^{(1)} + 3b_{0,1}^{(1)} - 2, \ldots\}\,.$$

Thus, its elimination ideal $\mathcal{E}_{(1,3)}$ *is* $\langle a \rangle$ *and* $a = 0$ *is a necessary condition on* A *for* f *having the factorization pattern* $(1, 3)$.

- *For the factorization pattern* $(2, 2)$*, the reduced Gröbner basis of the decomposition ideal* $\mathcal{J}_{(1,3)}$ *with respect to a* $\prec\prec B$ *is*

$$\{a^2 - a, (b_{0,0}^{(1)} + 1)a, (b_{0,0}^{(1)})^2 + 3b_{0,0}^{(1)} + 2, \ldots\}\,.$$

Thus, its elimination ideal $\mathcal{E}_{(2,2)}$ *is* $\langle a^2 - a \rangle$ *and, for its zeros* $a = 0, 1$*,* f *can be factorized into two quadratic factors.*

- *Combining the conditions for two primitive patterns* $(1, 3)$ *and* $(2, 2)$*, we can conclude that* $a = 0$ *is the condition for the factorization pattern* $(1, 1, 2)$ *and the factorization pattern* $(1, 1, 1, 1)$ *can not occur. For all* $a \neq 0, 1$*,* f *is irreducible over* $\mathbb{Q}$ *(and over* $\overline{\mathbb{Q}}$*).*

- *We note that, by substituting a with $0, 1$, we can examine the correctness of the conditions.*

EXAMPLE 2.6 (Two Parameters Case). *We consider* two parameters case, *where* $K = \mathbb{Q}$, $A = \{a_1, a_2\}$, $X = \{z, y\}$ *and*

$$f(z, y, a_1, a_2) = z^3 + (-y^2 + a_1 y + a_2)z^2 - a_1 y^2 z + a_1 y^4 - a_1^2 y^3 - a_2 y^2 .$$

In this case, possible non-trivial factorization patterns are $(1, 2)$, $(1, 1, 1)$. *As* $(1, 1, 1)$ *is a sub case of* $(1, 2)$, *we first consider the primitive pattern* $(1, 2)$. *Then we have the following reduced Gröbner basis of the decomposition ideal* $\mathcal{J}_{(1,2)}$ *with respect to an elimination order* $\{a_1 \prec a_2\} \prec\prec B$:

$$\{a_2 a_1^2 - a_2 a_1, a_2^3 a_1 + a_2^2 a_1 - a_2^3 - a_2^2, b_{0,0}^{(1)} a_1^3 - b_{0,0}^{(1)} a_1^2, \ldots\}$$

The elimination ideal $\mathcal{E}_{(1,2)} = \mathcal{J}_{(1,2)} \cap \mathbb{Q}[a_1, a_2]$ *is* $\langle a_2 a_1^2 - a_2 a_1, a_2^3 a_1 + a_2^2 a_1 - a_2^3 - a_2^2 \rangle$ *which has three prime components;* $\langle a_1 - 1 \rangle$, $\langle a_2 \rangle$, *and* $\langle a_1, a_2 + 1 \rangle$. *Thus, for* $a_1 = 1$, $a_2 = 0$ *or* $a_1 = 0 \wedge a_2 = -1$, f *has a linear factor. In more detail, we have*

$$f(z, y, a_1, a_2) = \begin{cases} (z - y)(z + y)(z - y^2 + y + a_2) & \text{for } a_1 = 1 , \\ (z - y^2 + a_1 y)(z^2 - a_1 y^2) & \text{for } a_2 = 0 , \\ (z - 1)(z^2 - y^2 z - y^2) & \text{for } (a_1, a_2) = (0, -1) . \end{cases}$$

For further check of a possible pattern $(1, 1, 1)$, *the first case actually corresponds to the pattern* $(1, 1, 1)$ *but the last one (having no parameter) does not corresponds. For the second case, we have to examine when a homogeneous factor* $z^2 - a_1 y^2$ *splits into linear factors. For this check, see Example 2.7.*

EXAMPLE 2.7 (Homogeneous Case). *Consider the factor* $z^2 - a_1 y^2$ *in Example 2.6. For the factorization pattern* $(1, 1)$, *we have the following reduced Gröbner basis of* $\mathcal{J}_{1,1}$ *with respect to* $a_1 \prec\prec B$:

$$\{b_{0,0}^{(1)} a, (b_{0,2}^{(1)})^2, -b_{0,1}^{(1)} - b_{0,1}^{(2)}, \ldots\}$$

In this case, the elimination ideal $\mathcal{E}_{(1,1)}$ *is trivial. On the other hand, the decomposition ideal* $\mathcal{J}_{(1,1)}$ *has one isolated prime component* $\mathcal{P}$ *which has the following Gröbner basis:*

$$\{a_1 - (b_{0,1}^{(2)})^2, b_{0,0}^{(1)}, b_{0,0}^{(2)}, b_{0,1}^{(1)} + b_{0,1}^{(2)}, b_{0,2}^{(1)}, b_{0,2}^{(2)}\}$$

Thus, $\mathcal{P}$ *has* $\{b_{0,1}^{(2)}\}$ *as its maximally independent set (MIS), that is, the extension ideal* $\mathcal{P}^e$ *in* $\mathbb{Q}(b_{0,1}^{(2)})[a_1 \cup B \setminus \{b_{0,1}^{(2)}\}]$ *is* 0*-dimensional over* $\mathbb{Q}(b_{0,1}^{(2)})$, *and* a_1 *is expressed as a polynomial* $(b_{0,1}^{(2)})^2$ *in* $b_{0,1}^{(2)}$. *(See [14, Chapter 3.5] for the definition of MIS in general setting.) In other words, for the pattern* $(1, 1)$, *the set of* feasible values *over* $\mathbb{Q}$ *for* a_1 *is* $\{c^2 \mid c \in \mathbb{Q}\}$. *Actually, by substituting* a_1 *with* c^2 *in* f, *where* c *ranges over* $\mathbb{Q}$, $f(z, y, c^2)$ *has two linear factors* $z - cy, z + cy$ *over* $\mathbb{Q}$.

3. Main Theorem for Parametric Polynomials with a Single Parameter

As the *first step for obtaining a complete algorithm for parametric factorization*, we consider the most basic case with two variables z, y and one parameter a.

REMARK 3.1. *By effective Hilbert's irreducibility theorem in [7], the irreducibility of three or more variable polynomials can be reduced to that of bivariate (one main-variable and one chosen sub-variable) polynomials by substituting other variables with linear forms in the main variable and the chosen sub-variable. Thus, the bivariate case can be considered as a fundamental case.*

From now on, we consider a parametric polynomial $f(z, y, a)$, which is irreducible in $K[z, y, a]$ and monic with respect to z, and its factorization with a pattern $\mathbf{d} = (d_1, \ldots, d_s)$, where $d = \deg_z(f) = d_1 + \cdots + d_s$.

3.1. Absolute Irreducibility and Kaltofen's Test

We begin by introducing the notion of *absolute irreducibility* in order to *guarantee the non-triviality* of the elimination ideal when the decomposition ideal is non-trivial.

DEFINITION 3.2 (Absolute Irreducibility over $K(a)$). *An irreducible and monic bivariate polynomial $f(z, y, a)$ in z, y over $K(a)$ is said to be* absolutely irreducible over $K(a)$, if $f(z, y, a)$ is irreducible over the algebraic closure $\overline{K(a)}$.

REMARK 3.3. *Suppose that $f(z, y, a)$ is reducible over $\overline{K(a)}$. Then $f(z, y, a) = g(z, y) \times h(z, y)$ for non-constant $g(z, y), h(z, y)$ over $\overline{K(a)}$. Thus, by letting L be an extension field obtained by adjoining all coefficients of $g(z, y)$ and those of $h(z, y)$, $f(z, y, a)$ is also factorized to $g(z, y) \times h(z, y)$ over L. As all coefficients are algebraic over $K(a)$, L is a finite extension over $K(a)$. Thus, we may use the following as an equivalent definition: $f(z, y, a)$ is absolutely irreducible over $K(a)$, if $f(z, y, a)$ is irreducible over any finite extension of $K(a)$.*

We have the following *absolute irreducibility test* for our case by modifying a well-known test by Kaltofen in [8]. (There are other tests based on geometrical approach. For example, see [3].)

PROPOSITION 3.4 (Bivariate Absolute Irreducibility Test over $K(a)$).
Let $f(z, y, a)$ be an irreducible and monic bivariate polynomial in z, y over $K(a)$. Suppose that $f(z, \beta, a)$ is square free over $K(a)$ for some $\beta \in K$ or $K(a)$ and $h(z, a)$ is any irreducible factor of $f(z, \beta, a)$ over $K(a)$. Then, $f(z, y, a)$ is absolutely irreducible, if $f(z, y, a)$ is irreducible over the extension field $K(a)[w]/\langle h(w, a)\rangle$. The irreducibility of $f(z, y, a)$ over $K(a)[w]/\langle h(w, a)\rangle$ can be checked by testing the primality of the ideal in $K[z, y, w, a]$ or $K(a)[z, y, w]$ generated by $f(z, y, a)$ and $h(w, a)$.

REMARK 3.5 (Square Freeness). *Here we recall the definition and some properties of square freeness. For a polynomial $h(X)$ in $K[X]$, $h(X)$ is said to be square free (over K), if $h(X)$ has no multiple factors over $\overline{K}$. Thus, when K is of characteristic 0 or a finite field, if $h(X)$ is irreducible over K, then $h(X)$ is square free. However, when K is an infinite field of positive characteristic p, even though $h(X)$ is irreducible over K, $h(X)$ is not necessarily square free. In more detail, for an irreducible polynomial $h(X)$, if $h(X)$ is not square free, then $h(X) = h_1(X)^p$ for some $h_1(X)$ in $\overline{K}[X]$.*

REMARK 3.6 (Modification of Kaltofen's Test and Quick Test). *Although the original Kaltofen's test was mainly applied to $K = \mathbb{Q}$, the test is also applicable to any computable field. (See [8].) In Appendix, we give a proof of Proposition 3.4 based on Galois*

theory whose original form was once given aurally in [19]. From the proof, if an irreducible polynomial f is not absolutely irreducible, then f can be factorized into a product of conjugate factors. *(See Definition A.2 of* conjugate factor *in Appendix.) Therefore, in this case, the factorization pattern is $d_1 = d_2 = \cdots = d_s$ and s is a common divisor of* $\deg_z(f)$ *and* $\deg_y(f)$. *This gives the following test:*

QUICK TEST FOR ABSOLUTE IRREDUCIBILITY: *If* $\deg_z(f)$ *and* $\deg_y(f)$ *are prime to each other, then f is absolutely irreducible.*

REMARK 3.7 (Parameter Values for Square Freeness). *Suppose that $f(z, y, a)$ is monic with respect to z and square free over $K(a)$. Let $R(y, a)$ be the resultant of $f(z, y, a)$ and its partial derivative $\frac{\partial f}{\partial z}$ with respect to z. Then, by resultant theory (see [1, 14]), it follows that $R(y, a)$ is a bivariate polynomial in y, a over K and $R(y, a) \neq 0$. For an element β in $K(a)$, $f(z, \beta, a)$ is square free over $K(a)$ if and only if $R(\beta, a) \neq 0$. Hence, we can prove that the number of elements β in K such that $f(z, \beta, a)$ is not square free over $K(a)$ is finite, since those are common zeros of polynomials $r_k(y), \ldots, r_0(y)$, where $R(y, a) = r_k(y)a^k + \cdots + r_0(y)$. Thus, if K is an infinite field or has enough large order, we can say that almost every β in K makes $f(z, \beta, a)$ square free.*

EXAMPLE 3.8. *The polynomial $f(z, y, a)$ given in Example 2.5 is absolutely irreducible over $\mathbb{Q}(a)$. But, the polynomial $g(z, y, a_1) = z^2 - a_1 y^2$ in Example 2.7 is not absolutely irreducible over $\mathbb{Q}(a_1)$. In fact, $h(w, a_1) = g(w, 1, a_1) = w^2 - a_1$ is irreducible over $\mathbb{Q}(a_1)$ and, from the prime decomposition of $\langle z^2 - a_1 y^2, h(w, a_1)\rangle$, we have*

$$z^2 - a_1 y^2 \equiv (z - wy)(z + wy) \pmod{w^2 - a_1}.$$

EXAMPLE 3.9. *Consider $f(z, y, a) = (z - y + 1)^3 + a(z - y + a)$. Unfortunately, $f(z, y, a)$ is not absolutely irreducible over $\mathbb{Q}(a)$. Because, $h(z, a) = f(z, 0, a) = z^3 + 3z^2 + (a + 3)z + a^2 + 1$ is irreducible (and square free) over $\mathbb{Q}$ and so over $\mathbb{Q}(a)$, but $f(z, y, a)$ is reducible over $L = K(a)[w]/\langle h(w, a)\rangle$. Actually, $\langle f(x, y, a), h(w, a)\rangle$ has the following primary components in $\mathbb{Q}[a, z, y, w]$:*

$$\langle z - y - w, h(w, a)\rangle,$$
$$\langle z^2 + (-2y + w + 3)z + y^2 + (-w - 3)y + w^2 + 3w + a + 3, h(w, a)\rangle.$$

Thus, we have the following factorization over L:

$$f(z, y, a) \equiv (z - y - w)(z^2 + (-2y + w + 3)z + y^2 + (-w - 3)y + w^2 + 3w + a + 3) \pmod{h(w, a)}.$$

3.2. Properties of Decomposition Ideal and Elimination Ideal

Before giving our main theorem, we provide necessary lemmas. From our setting, $f(z, y, a)$ is monic with respect to z and irreducible over K. Moreover, suppose that the decomposition ideal $\mathcal{J}_{\mathbf{d}}$ is non-trivial for a factorization pattern $\mathbf{d}$. Also, for simplicity, we set $B = \{b_1, \ldots, b_N\}$, where $N = \#B$. Then, for each zero $(\alpha, \beta_1, \ldots, \beta_N)$ in $V_{\overline{K}}(\mathcal{J}_{\mathbf{d}})$, where α is the value of the a-component and β_i is that of the b_i-component, we set V_A and $V(\alpha)$ as follows:

$$V_A = \{\alpha \mid (\alpha, \beta_1, \ldots, \beta_N) \in V_{\overline{K}}(\mathcal{J}_{\mathbf{d}})\},$$

$$V(\alpha) = \{(\beta_1, \ldots, \beta_N) \mid (\alpha, \beta_1, \ldots, \beta_N) \in V_{\overline{K}}(\mathcal{J}_{\mathbf{d}})\}.$$

LEMMA 3.10. *For each α in V_A, $V(\alpha)$ is a finite set. Thus, if V_A is a finite set, then $V_{\overline{K}}(\mathcal{J}_{\mathbf{d}})$ is a finite set. This implies that $\mathcal{J}_{\mathbf{d}}$ is 0-dimensional.*

Proof. For α in V_A, each element in $V(\alpha)$ corresponds to coefficients of factors $(g_1(z), \ldots, g_s(z))$ in (1). On the other hand, such factors $g_1(z), \ldots, g_s(z)$ can be given by some products of absolutely irreducible factors of $f(z, y, \alpha)$ over $\overline{K}$. As absolutely irreducible factors with multiplicity counted are determined uniquely, the number of factor sequences $(g_1(z), \ldots, g_s(z))$ is finite and so is the number of possible values for coefficients. This implies that $V(\alpha)$ is a finite set. □

LEMMA 3.11. *If V_A is not a finite set, then the elimination ideal $\mathcal{E}_{\mathbf{d}}$ is trivial and the decomposition ideal $\mathcal{J}_{\mathbf{d}}$ has the variable a as its maximally independent set and $\mathcal{J}_{\mathbf{d}}$ is 1-dimensional.*

Proof. Suppose that V_A is not a finite set. Then, as $K[a]$ is a principal ideal domain, its ideal $\mathcal{E}_{\mathbf{d}}$ should be $\{0\}$ and a is an independent set for $\mathcal{J}_{\mathbf{d}}$. Then, the extension ideal $\mathcal{J}_{\mathbf{d}}^e$ in $K(a)[B]$ is non-trivial. In this case, each zero β in $V_{\overline{K(a)}}(\mathcal{J}_{\mathbf{d}}^e)$ corresponds to coefficients of factors in (1). By similar manner as the proof of Lemma 3.10, $V_{\overline{K(a)}}(\mathcal{J}_{\mathbf{d}}^e)$ is a finite set and thus, the extension ideal $\mathcal{J}_{\mathbf{d}}^e$ is 0-dimensional in $K(a)[B]$. This implies that the variable a is a maximally independent set of $\mathcal{J}_{\mathbf{d}}$ and $\mathcal{J}_{\mathbf{d}}$ is 1-dimensional. □

REMARK 3.12. *Let $\mathcal{J}_{\mathbf{d}} = \cap_{i=1}^{M} \mathcal{Q}_i$ be an irredundant primary decomposition of $\mathcal{J}_{\mathbf{d}}$ in $K[a, b_1, \ldots, b_N]$. Then, by considering $V_{\overline{K}}(\mathcal{Q}_i)$ and $V_{\overline{K(a)}}(\mathcal{Q}_i^e)$, where $\mathcal{Q}_i^e$ is the extension of $\mathcal{Q}_i$ in $K(a)[B]$, we can use Lemma 3.10 and Lemma 3.11 for each $\mathcal{Q}_i$. Thus, if $\mathcal{Q}_i \cap K[a]$ is not trivial, then $\mathcal{Q}_i$ is 0-dimensional. If $\mathcal{Q}_i \cap K[a]$ is trivial, then the extension $\mathcal{Q}_i^e$ of $\mathcal{Q}_i$ in $K(a)[B]$ is 0-dimensional. Therefore, in this case, $\mathcal{Q}_i$ is 1-dimensional. (Thus, $\mathcal{J}_{\mathbf{d}}$ is 1-dimensional.)*

3.3. Main Theorem for Absolutely Irreducible Polynomials

In this subsection, we suppose that $f(z, y, a)$ is absolutely irreducible over $K(a)$. We will show that, if the decomposition ideal $\mathcal{J}_{\mathbf{d}}$ is non-trivial for a possible non-trivial factorization pattern $\mathbf{d}$, then its elimination ideal $\mathcal{E}_{\mathbf{d}}$ is also non-trivial, by which we can extract algebraic conditions on a.

THEOREM 3.13 (Parametric Factorization for Absolutely Irreducible Polynomial). *Suppose that a monic polynomial $f(z, y, a)$ is absolutely irreducible over $K(a)$ and the decomposition ideal $\mathcal{J}_{\mathbf{d}}$ is non-trivial for a non-trivial factorization pattern $\mathbf{d} = (d_1, \ldots, d_s)$. Then all of the following hold:*

1. *The elimination ideal $\mathcal{E}_{\mathbf{d}} = K[a] \cap \mathcal{J}_{\mathbf{d}}$ is non-trivial.*
2. *$\mathcal{J}_{\mathbf{d}}$ is 0-dimensional in $K[a, B]$ and $V_{\overline{K}}(J_{\mathbf{d}})$ is finite.*
3. *Each zero of $V_{\overline{K}}(\mathcal{J}_{\mathbf{d}})$ gives a factorization of f with the non-trivial factorization pattern $\mathbf{d}$, where zeros of V_A are values for a. In particular, by picking up parameter values for a from $V_A \cap K$ (if exists), we have a factorization of f over K with the factorization pattern $\mathbf{d}$.*
4. *V_A coincides with $V_{\overline{K}}(\mathcal{E}_{\mathbf{d}})$. This implies $\mathcal{E}_{\mathbf{d}}$ gives an equivalent condition for f such that f has a factorization of the pattern $\mathbf{d}$.*

Proof. (1) We assume, to the contrary, that $\mathcal{E}_{\mathbf{d}}$ is trivial. Then, by Lemma 3.11, $\{a\}$ is a maximally independent set of $\mathcal{J}_{\mathbf{d}}$ and the extension $\mathcal{J}_{\mathbf{d}}^e$ in $K(a)[B]$ is 0-dimensional. This implies that $V_{\overline{K(a)}}(\mathcal{J}_{\mathbf{d}}^e)$ is not-empty and each zero $(\bar{\beta}_1, \ldots, \bar{\beta}_N)$ corresponds to coefficients of factors $g_1(z), \ldots, g_s(z)$ in (1) over $\overline{K(a)}$. Thus, $f(z, y, a)$ is factorized into $g_1(z) \cdots g_s(z)$ over $\overline{K(a)}$ and it is not absolutely irreducible over $K(a)$. This contradicts the assumption.

(2) By Lemma 3.10, since $\mathcal{E}_{\mathbf{d}}$ is not trivial, $\mathcal{J}_{\mathbf{d}}$ is 0-dimensional in $K[a, B]$ and $V_{\overline{K}}(\mathcal{J}_{\mathbf{d}})$ is a finite set.

(3) Each zero in $V_{\overline{K}}(\mathcal{J}_{\mathbf{d}})$ corresponds to factors $g_1(z), \ldots, g_s(z)$ in (1). Zeros in V_A correspond to the values for a for the factorization pattern $\mathbf{d}$.

(4) As $\mathcal{J}_{\mathbf{d}}$ is 0-dimensional, by so-called *Extension Theorem* (see [1, Chater 3]), each zero of the elimination ideal $\mathcal{E}_{\mathbf{d}}$ can be extended to some zero of the original ideal $\mathcal{J}_{\mathbf{d}}$. □

By Theorem 3.13, for an absolutely irreducible and monic polynomial $f(z, y, a)$, we can classify parameter values for possible non-trivial factorization patterns completely. For each non-trivial factorization patterns, the number of feasible values for a is finite. Thus, all but finitely many values for a make $f(z, y, a)$ irreducible. This is our main theorem in Section 1.

COROLARY 3.14. *Lemma 3.10, Lemma 3.11 and Theorem 3.13 hold for the* more than three variables case *with a single parameter a.*

3.4. Non Absolutely Irreducible Case

Finally in this section, we consider the non absolutely irreducible case. Suppose that $f(z, y, a)$ is not absolutely irreducible over $K(a)$ and the decomposition ideal $\mathcal{J}_{\mathbf{d}}$ is non-trivial for a non-trivial factorization pattern $\mathbf{d} = (d_1, \ldots, d_s)$. We outline our approach for dealing with such a polynomial as follows:

- The elimination ideal $\mathcal{E}_{\mathbf{d}}$ is trivial, and the Zariski-closure of the set of all *non-feasible* parameter values for the pattern $\mathbf{d}$ is $\overline{K}$ if K is Hilbertian. (See Remark 2.1.) Thus, we cannot derive any algebraic condition expressed only in a from $\mathcal{E}_{\mathbf{d}}$.
- Instead, we compute associated prime ideals $\mathcal{P}_1, \ldots, \mathcal{P}_k$ of $\mathcal{J}_{\mathbf{d}}$. That is, $Ass(\mathcal{J}_{\mathbf{d}}) = \{\mathcal{P}_1, \ldots, \mathcal{P}_k\}$.
- For each prime ideal $\mathcal{P}_i$, we compute the reduced Gröbner basis of its elimination ideal $\mathcal{P}_i \cap K[a]$.
  - If $\mathcal{P}_i \cap K[a]$ is non-trivial, its Gröbner basis give an algebraic condition in a that $f(z, y, a)$ has the factorization of pattern $\mathbf{d}$. (See Lemma 3.10.)
  - If $\mathcal{P}_i \cap K[a]$ is trivial, $\mathcal{P}_i$ is 1-dimensional by Lemma 3.11. Using its maximally independent set $\{b_j\}$ for some $b_j \in B$, the extended ideal $\mathcal{P}_i^e$ in $K(b_j)[\{a\} \cup B \setminus \{b_j\}]$ is 0-dimensional. Then, a is algebraic over $K(b_j)$ and, a can be expressed as an *algebraic function* in b_j. (See Example 3.15.) In a *lucky case*, a can be expressed as a polynomial or a rational function in b_j. (See Example 2.7.) Thus, we may use such a function as a representation of parameter values for a.

EXAMPLE 3.15 (Continuation of Example 3.9). *Consider* $f(z, y, a) = (z-y+1)^3 + a(z - y + a)$. *Although the decomposition ideal* $J_{(1,2)}$ *is non-trivial, the elimination ideal* $\mathbb{Q}[a] \cap \mathcal{J}_{(1,2)}$ *is trivial. Because, the following is the Gröbner basis for the decomposition ideal* $\mathcal{J}_{(1,2)}$*:*

$$\{a^2 - b_{0,0}^{(1)}a - (b_{0,0}^{(1)})^3 + 3(b_{0,0}^{(1)})^2 - 3b_{0,0}^{(1)} + 1, -a - (b_{0,0}^{(1)})^2 + 3b_{0,0}^{(1)} + b_{0,0}^{(2)} - 3, \ldots\}$$

The decomposition ideal has one isolated component $\mathcal{P}_1$ *of dimension* 1 *and two embedding components of dimension* 0*. Then,* $b_{0,0}^{(1)}$ *is a maximally independent set of* $\mathcal{P}_1$ *and* a *can be expressed in an algebraic function in* $b_{0,0}^{(1)}$*. Letting* $c = b_{0,0}^{(1)}$*, we have*

$$a = \frac{c \pm \sqrt{4c^3 - 11c^2 + 12c - 4}}{2}.$$

In this case, $f(z, y, a)$ *can be factorized as follows:*

$$f(z, y, a) = (z - y + c)(z^2 - (2y + c - 3)z + y^2 - (-c + 3)y + a + c^2 - 3c + 3$$

From the embedded components, we have $a = 0$ *or* $27a^2 - 50a + 27 = 0$*. For* $a = 0$*,* $f(z, y, a) = (z-y+1)^3$ *and for* $27a^2-50a+27 = 0$*, that is,* $a = \frac{25\pm2\sqrt{-26}}{27}$*,* $f(z, y, a) = (z - y - 3a + 4)(z - y + \frac{3}{2}a - \frac{1}{2})^2$*. (In this case,* a *cannot be a rational number.)*

EXAMPLE 3.16 (Homogeneous Case (=Univariate Case)). *Factorization of a homogeneous bivariate polynomial is reduced to that of its dehomogenized univariate polynomial. Let* $f(z, y, a) = z^3 - az^2y + (a - 3)zy^2 + y^3$*. Then, factorization of* $f(z, y, a)$ *is exactly the same as that of its dehomogenization* $f(z, 1, a) = z^3 - az^2 + (a-3)z+1$*. Here* $f(z, 1, a)$ *is known as a* generic polynomial of cyclic Galois group of order 3. *(See [6, Section 2.1].) For the pattern* $(1, 2)$*, the decomposition ideal* $\mathcal{J}_{1,2}$ *has a unique isolated prime component* $\mathcal{P}$ *and* $\{b_{0,1}^{(1)}\}$ *is a maximally independent set for* $\mathcal{P}$*. Then, the extension ideal* $\mathcal{P}^e$ *over* $\mathbb{Q}(b_{0,1}^{(1)})$ *has the following Gröbner basis, where we omit unnecessary coefficient variables:*

$$\{((b_{0,1}^{(1)})^2 + b_{0,1}^{(1)})a + (b_{0,1}^{(1)})^3 - 3b_{0,1}^{(1)} - 1, (b_{1,1}^{(2)} + 1)(b_{0,1}^{(1)})^2 + (b_{1,1}^{(2)} + 3)b_{0,1}^{(1)} + 1, b_{0,1}^{(1)}b_{0,2}^{(2)} - 1\}$$

Thus, by letting $c = b_{0,1}^{(1)}$*, the parameter value* a *can be expressed as a rational function*

$$\frac{-c^3 + 3c + 1}{c^2 + c}$$

in c *except for* $c = 0, -1$*. (We note that* $c = 0, -1$ *cannot occur, that is, those cannot be the* $b_{0,1}^{(1)}$*-component of any zero of* $J_{1,2}$*.)*

Actually, for $f(z, 1, a)$ *substituted* a *with* $\frac{-c^3+3c+1}{c^2+c}$*, where* c *ranges* $\mathbb{Q} \setminus \{0, -1\}$*,* $f(z, 1, a)$ *has three linear factors* $x + c$*,* $x - \frac{c+1}{c}$*,* $x - \frac{1}{c+1}$ *over* $\mathbb{Q}$*.*

4. Effective Algorithm for Factoring Parametric Polynomials

Here we consider absolutely irreducible polynomials and present an effective factorization algorithm based on Theorem 3.13 which gives *feasible values* for each factorization pattern. For effective realization of our parametric factorization, we utilize a *stair structure* of factorization patterns.

DEFINITION 4.1 (Primitive Pattern). *For a non-trivial factorization pattern* $\mathbf{d} = (d_1, \ldots, d_s)$*, where* $d = d_1 + \cdots + d_s$*,* $\mathbf{d}$ *is said to be primitive, if* $\mathbf{d}$ *cannot be a refinement for any other pattern except the trivial pattern* (d)

EXAMPLE 4.2. *For* $d = 3$*, possible factorization patterns are* $(3), (1, 2), (1, 1, 1)$*. Then,* $(1, 2)$ *is a primitive pattern but* $(1, 1, 1)$ *is not, as* $(1, 1, 1)$ *is a refinement of* $(1, 2)$*.*

For $d = 4$*, possible factorization patterns are* $(4), (1, 3), (1, 1, 2), (1, 1, 1, 1), (2, 2)$*. Then,* $(1, 3)$ *and* $(2, 2)$ *are primitive patterns but neither* $(1, 1, 2)$ *nor* $(1, 1, 1, 1)$*, as* $(1, 1, 2)$ *and* $(1, 1, 1, 1)$ *are refinements of* $(1, 3)$*.*

For a non-trivial factorization pattern $\mathbf{d} = (d_1, \ldots, d_s)$, if $s > 2$, then $\mathbf{d}$ is a refinement of a non-trivial factorization pattern $\mathbf{d}' = (d_1 + d_2, d_3, \ldots, d_s)$. Thus, we have the following lemma. (We omit its easy proof.)

LEMMA 4.3. *For a fixed degree* d*, primitive patterns are as follows:*

$$(1, d-1), (2, d-2), \ldots, \left(\frac{d-1}{2}, \frac{d+1}{2}\right) \text{ for odd } d\,,$$

$$(1, d-1), (2, d-2), \ldots, \left(\frac{d}{2}, \frac{d}{2}\right) \text{ for even } d\,.$$

As we can pick all (finitely many) parameter values in K (or $\overline{K}$) for *possible non-trivial factorization* of pattern $\mathbf{d}$, it is sufficient to compute feasible values for primitive patterns, like in Example 2.5. We explain more details here.

For each non-primitive pattern $\mathbf{d}$, there is a primitive pattern $\mathbf{d}_0$ such that $\mathbf{d}$ is a refinement of $\mathbf{d}_0$. If $\mathcal{E}_{\mathbf{d}}$ is non-trivial, then $\mathcal{E}_{\mathbf{d}_0}$ is also non-trivial. This implies that for finding feasible values for $\mathbf{d}$, we pick up them from feasible values α for $\mathbf{d}_0$ by testing if $f(z, y, \alpha)$ admits the factorization pattern $\mathbf{d}$. Thus, by factorizing $f(z, y, \alpha)$ for all feasible values for primitive patterns, we can classify parameter values for possible *non-trivial* irreducible factorization.

ALGORITHM 1 (Parametric Factorization for Absolutely Irreducible Bivariate Polynomials).

INPUT*: an absolutely irreducible bivariate monic polynomial* $f(z, y, a)$*.*

OUTPUT*: a set* S *of pairs* $(\alpha, \{g_1(z, y), \ldots, g_s(z, y)\})$*, where* $\alpha \in K$*,* $f(\alpha, z, y)$ *is not irreducible and factorized into its irreducible factors* $g_1(z, y), \ldots, g_s(z, y)$*.*

(1) *Generate all primitive patterns for* d*.*

(2) *For each pattern* $\mathbf{d}$*, compute a Gröbner basis of the decomposition ideal* $J_{\mathbf{d}}$*.*

   (i) *If* $J_{\mathbf{d}}$ *is non-trivial, compute the reduced Gröbner basis* G *of* $\mathcal{J}_{\mathbf{d}}$ *with respect to an elimination order* $a \prec\prec B$*. Let* $g(a)$ *be the unique polynomial in* $K[a] \cap G$ *which generates* $\mathcal{E}_{\mathbf{d}}$*.*

Compute all roots of $g(a)$ over K by finding linear factors of $g(a)$ over K.
For each root α of $g(a)$ over K, compute the irreducible factorization of $f(z, y, \alpha) = g_1(z, y) \cdots g_s(z, y)$ for some $s \geq 2$.
Append $(\alpha, \{g_1(z, y), \ldots, g_s(z, y)\})$ to S.

(ii) *If $J_{\mathbf{d}}$ is trivial, factorization with pattern $\mathbf{d}$ does not occur for any value of a.*

5. Concluding Remarks and Future Work

As a continuation of [18], we reported our current status of realization of parametric factorization based on the naive method, and gave some practical improvement. Here we summarize our contributions and give some prospects for generalization of our main theorem and for more efficient algorithms, which will be done in our future works.

Theoretical Details on the Naive Method: For a single parameter case, it is clarified that, if the target polynomial is absolutely irreducible, we can compute all values of the parameter for each specified factorization pattern. However, the main theorem is only applicable for monic polynomials with a single parameter. In our future work, we will generalize it to be applicable to non-monic polynomials and to polynomials with two or more parameters.

For non absolutely irreducible polynomials, we propose to represent parameter values in an algebraic function. However, it is not clear what is the best way for describing the parameter values. This shall be our further study.

Practicality of the Naive Method: First we remark that it is difficult to provide *appropriate test suits (sample polynomials)* for testing the efficiency of factoring methods. By our current experiment, for polynomials of smaller degree, our naive method works well and succeeded in showing examples in Section 2.2 and Section 3.2.

Since the efficiency of Algorithm 1 heavily depends on that of the Gröbner bases computation of decomposition ideals of a given parametric polynomial $f(z, y, a)$, it is very important to apply several practical improvements to the Gröbner bases computation with an efficient monomial ordering. Also, as the size of additional variables B is $O(\deg_z(f) \deg_y(f))$, it is highly required to prune away unnecessary additional variables and make good use of the structure of the derived system of equations. In particular, if the input polynomial is a sparse polynomial, making good use of its sparsity is very important.

Acknowledgment. The author thanks the anonymous reviewer for her/his comments to improve the presentation of the work.

References

[1] Cox D., Little J., and O'Shea D. (2015). Ideals, Varieties, and Algorithms, 4-th edition, UTM, Springer-Verlag.

[2] Corvaja, P. (2016). Integral Points on Algebraic Varieties. An Introduction to Diophantine Geometry. Springer-Verlag.

[3] Gao S., (2001). Absolutely irreducibility of polynomials via Newton polytopes. J. Algebra **237**, 501–520.

[4] Gianni P., Trager B., and Zacharias G. (1988). Gröbner base and primary decomposition of polynomial ideals. J. Symb. Comp. **6**, 149–167.
[5] Ishihara Y., and Yokoyama, K. (2024). Parametric primary decomposition via comprehensive Gröbner systems. Preprint.
[6] Jensen C.U., Ledet A., and Yui N. (2002). Generic Polynomials. Mathematical Science Research Institute Publications.
[7] Kaltofen, E. (1985). Effective Hilbert irreducibility. Inf. Control. **66**, 123–137.
[8] Kaltofen, E. (1985). Fast parallel absolute irreducibility testing. J. Symb. Comp. **1**, 57–67.
[9] Kapur, D., Sun, Y., and Wang, D. (2013). An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial system. J. Symb. Comp. **49**, 27–44.
[10] Lang, S. (1983). Fundamentals of Diophantine Geometry. Springer-Verlag.
[11] Montes, A., and Wibmer, M. (2010). Gröbner bases for polynomial systems with parameters. J. Symb. Comp. **45**, 1391–1425.
[12] Noro, M., and Takeshima, T. (1992). Risa/Asir – a computer algebra system. In Proceedings of ISSAC 1992, ACM Press, New York, pp.387–396.
[13] Nabeshima, K., and Tajima, S. (2021). Testing zero-dimensionality of varieties at a point. Math. Comput. Sci. **15**, 317–331.
[14] Greuel, G.-M., and Pfister, G. (2002). A Singular Introduction to Commutative Algebra. Springer-Verlag.
[15] Sen, H., Wang, D. (1986). Fast factorization of polynomials over rational number field or its extension fields. Kexue Tongbao **31**, 150–156.
[16] Shimoyama T., Yokoyama K. (1996). Localization and primary decomposition of polynomial ideals. J. Symb. Comp. **22**, 247–277.
[17] Suzuki, A., and Sato, Y. (2006). A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases. In Proceedings of ISSAC 2006, ACM Press, New York, pp.326-331.
[18] Yokoyama, K. (2006). Stability of parametric decomposition. In Mathematical Software – ICMS 2006, Lecture Notes in Computer Science **4151**, Springer-Verlag, pp. 391–402,
[19] Yokoyama, K., Noro, M., and Takeshima, T. (1990). On factoring multi-variate polynomials over algebraically closed field (extended abstract). In Proceedings of ISSAC 1990, ACM Press, pp.297.
[20] Yokoyama, K.: Implementation report on parametric absolute factorization of multi-variate polynomials. presented orally in Applications of Computer Algebra 2022 held at Gebze Technical University in Turkey from 15 August to 19 August in 2022.

A. Bivariate Absolute Irreducibility Test

Let K be a field. For bivariate polynomials which are irreducible over K, we give a brief proof for *absolute irreducibility criterion* in algebraic way.

Kaltofen's Theorem. Let $f(x, y)$ be a square free polynomial over K and monic with respect to x. For an element α in K, if $f(x, \alpha)$ is square free over K, then absolutely irreducible factorization of $f(x, y)$ can be obtained over an algebraic extension field $K(\beta)$ for any root β of $f(x, \alpha)$.

As its corollary, we have the following criterion corresponding to Proposition 3.4, where the rational function field $K(a)$ is considered as the coefficient field.

Absolute irreducibility Criterion: Let $f(x, y)$ be an irreducible polynomial over K and monic with respect to x. For an element α in K, if $f(x, \alpha)$ is square free and $f(x, y)$ is irreducible over $K(\beta)$ for a root β of $f(x, \alpha)$, then $f(x, y)$ is absolutely irreducible over K.

REMARK A.1. *Let $f(x, y)$ be a polynomial over K monic with respect to x. If $f(x, \alpha)$ is square free for some α in K, then $f(x, y)$ is square free.*

Proof for Criterion: We show the criterion by using *Galois theoretical arguments*. We assume that $f(x, y)$ is an irreducible polynomial over K and monic with respect to x. Moreover, we assume that for an element α in K, $f(x, \alpha)$ is square free over K. (This implies that $f(x, y)$ is also square free.) Now, let $g(x, y)$ be a monic irreducible factor of $f(x, y)$ over $\overline{K}$, that is, an absolutely irreducible factor of $f(x, y)$. Let $n = \deg_x(f)$, $m = \deg_y(f)$, $n' = \deg_x(g)$ and $m' = \deg_y(g)$. We write these polynomials as

$$f(x, y) = x^n + \sum_{i=0}^{n-1} \sum_{j=0}^{m} f_{i,j} x^i y^j, \quad g(x, y) = x^{n'} + \sum_{i=0}^{n'-1} \sum_{j=0}^{m'} g_{i,j} x^i y^j.$$

Let L_g be the extension field over K obtained by adjoining all coefficients $g_{i,j}$ over K, and $\mathcal{E}$ the set of all embeddings of L_g into $\overline{K}$. (We call L_g a *feasible field* for g.) We define *conjugates* of g over K in a natural way as follows:

DEFINITION A.2 (Conjugate of Factor). *For each embedding σ in $\mathcal{E}$, a* conjugate *$\sigma(g)$ of g is defined by*

$$\sigma(g) = \sum_{i=0}^{n'} \sum_{j=0}^{m'} \sigma(g_{i,j}) x^i y^j = x^{n'} + \sum_{i=0}^{n'-1} \sum_{j=0}^{m'} \sigma(g_{i,j}) x^i y^j.$$

Since L_g is the field obtained by adjoining all $g_{i,j}$, for distinct embeddings σ and σ', the conjugates $\sigma(g)$ and $\sigma'(g)$ are distinct. Therefore, the number N of distinct conjugates equals to that of distinct embeddings, which equals to the separable extension degree of L_g over K. (If K is of characteristic 0 or a finite field, N equals to the extension degree $|L_g : K|$.)

LEMMA A.3. *Let $h_1(= g), ..., h_N$ be all conjugates of g. Then $f = h_1 \cdot h_2 \cdots h_N$ and $h_1, ..., h_N$ are all irreducible factors of f over $\overline{K}$.*

Proof. Let $\tilde{f} = h_1 \cdots h_N$. Then for any embedding σ in $\mathcal{E}$, $\sigma(\tilde{f}) = \tilde{f}$. Therefore, $\tilde{f}$ is a polynomial over K if K is of characteristic 0 or a finite field. And, for an infinite field of positive characteristic p, $\tilde{f}^q$ for some $q = p^e$ is a polynomial over K. On the other hand, since f is divisible by h_1, f should also be divisible by any h_i. So, f should have every h_i as its factor. Thus, f has $\tilde{f}$ as its factor, and by the irreducibility and the square freeness of f, f should coincide with $\tilde{f}$. Moreover, the fact that $h_1 = g$ is irreducible over $\overline{K}$ implies that every conjugate h_i is also irreducible over $\overline{K}$. □

COROLARY A.4. *$n = n' \cdot N$ and $m = m' \cdot N$. Therefore, N is a common divisor of n and m. In particular, if n and m are prime to each other, then $N = 1$ and f is irreducible over $\overline{K}$, that is, f is absolutely irreducible over K.*

Next we define a *square free element*.

DEFINITION A.5 (Square Free Element). *We call an element α in K such that $f(x, \alpha)$ is square free a* square free element *for f.*

REMARK A.6. *The resultant $R(y)$ of $f(x, y)$ and its partial derivative $\frac{\partial f(x,y)}{\partial x}$ with respect to x is a univariate polynomial in y of degree at most $2nm$. Then, since $f(x, y)$ is monic with respect to x and square free, it can be shown that an element α in K is a square free element if and only if $R(\alpha) \neq 0$. Thus, if there is a square free element in K, $R(y)$ is non-trivial and the number of non-square free elements is less than $2nm$.*

Since $g(x, y)$ is a factor of $f(x, y)$, for an element α in K, the univariate polynomial $f(x, \alpha)$ has $g(x, \alpha)$ as a factor over $\overline{K}$. For each i, $0 \leq i \leq n'$, the coefficient $g_i(\alpha)$ of x^i in $g(x, \alpha)$ can be expressed as

$$g_i(\alpha) = \sum_{j=0}^{m'} g_{i,j}\alpha^j. \tag{2}$$

Thus, $g_i(\alpha) \in L_g$ for every i and

$$K(g_0(\alpha), ..., g_{n'}(\alpha)) \subset K(g_{0,0}, ..., g_{n',m'}) = L_g.$$

We note $g_{n'}(\alpha) = 1$, $g_{n',0} = 1$, and $g_{n',1} = \cdots = g_{n',m'} = 0$.

REMARK A.7. *If $f(x, \alpha)$ is square free, then the splitting field $S_{f(x,\alpha)}$ of $f(x, \alpha)$ is a separable extension over K. Since each $g_i(\alpha)$ is the i-th symmetric function on the roots of $g(x, \alpha)$ which belong to $S_{f(x,\alpha)}$, $K(g_0(\alpha), \ldots, g_{n'}(\alpha))$ is a subfield of $S_{f(x,\alpha)}$ and is a separable extension field of K.*

LEMMA A.8. *If α is a square free element for $f(x, y)$, that is, $f(x, \alpha)$ is square free, then $K(g_0(\alpha), ..., g_{n'}(\alpha)) = L_g$ holds.*

Proof. Suppose that $K(g_0(\alpha), ..., g_{n'}(\alpha)) \neq L_g$. If K is of characteristic 0 or a finite field, then the extension L_g/K is separable and there is a non-identical embedding σ in $\mathcal{E}$ such that σ fixes every element in $K(g_0(\alpha), ..., g_{n'}(\alpha))$. Therefore, $\sigma(g_i(\alpha)) = g_i(\alpha)$ for all i, $0 \leq i \leq n'$. This implies that $g(x, \alpha) = \sigma(g(x, \alpha))$. On the other hand, since σ is a non-identical embedding, there is an integer $j \neq 1$ such that $\sigma(h_1(x, y)) = h_j(x, y)$. From this, we have $h_1(x, \alpha) = g(x, \alpha) = \sigma(g(x, \alpha)) = h_j(x, \alpha)$, and $f(x, \alpha)$ has a multiple factor $g(x, \alpha)$. This contradicts the square freeness of $f(x, \alpha)$.

Next consider the case where K is an infinite field of positive characteristic. In this case, for distinct $m' + 1$ square free elements $\alpha_1, \ldots, \alpha_{m'+1}$ in K, it can be shown that coefficients $g_{i,0}, \ldots, g_{i,m'}$ belong to $K(g_i(\alpha_1), \ldots, g_i(\alpha_{m'+1}))$, by considering the following system of linear equations derived from Equation (2):

$$(g_{i,0}, g_{i,1}, \ldots, g_{i,m'}) = (g_i(\alpha_1), g_i(\alpha_2), \ldots, g_i(\alpha_{m'+1})) \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{m'+1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{m'} & \alpha_2^{m'} & \cdots & \alpha_{m'+1}^{m'} \end{pmatrix}^{-1}$$

(We note that there are infinitely many square free elements by Remark A.6 and the matrix is invertible, since it is a Vandermonde matrix.) Then, L_g is a subfield of the composite field of $m' + 1$ separable extension fields
$K(g_0(\alpha_1) \ldots, g_{n'}(\alpha_1)), \ldots, K(g_0(\alpha_{m'+1}), \ldots, g_{n'}(\alpha_{m'+1}))$. Hence, L_g is also a separable extension and we can apply the same arguments. □

Now we take a square free element α and fix it. Let $\Omega(f)$ be the set of all roots of $f(x,\alpha)$, and $\Omega(h_i)$ the set of all roots of $h_i(x,\alpha)$ for each i. Since α is a square free element, roots of $f(x,\alpha)$ are all distinct and thus, $\Omega(f)$ is the disjoint union of $\Omega(h_1),\ldots,\Omega(h_N)$. For simplicity, we set $\Omega(f)=\{\beta_1,\ldots,\beta_n\}$ and $\Omega(h_1)=\{\beta_1,\ldots,\beta_{n'}\}$. Moreover, let $\mathcal{G}$ be the Galois group of the splitting field $S_{f(x,\alpha)}$ of $f(x,\alpha)$, and let $\mathcal{H}$ be the stabilizer of L_g in $\mathcal{G}$, that is, $\mathcal{H}$ fixes all elements of L_g.

LEMMA A.9. *$\Omega(h_1),\ldots,\Omega(h_N)$ form a* system of imprimitive block *of the action of $\mathcal{G}$ on $\Omega(f)$. That is, they satisfy the following:*

(1) *$\Omega(f)$ is the disjoint union of $\Omega(h_i)$'s.*
(2) *For each element σ in $\mathcal{G}$ and each $\Omega(h_i)$, $\sigma(\Omega(h_i))=\Omega(h_j)$ for some h_j.*
(3) *For every distinct pair $(\Omega(h_i),\Omega(h_j))$, there is an element σ in $\mathcal{G}$ such that $\sigma(\Omega(h_i))=\Omega(h_j)$.*

Proof. (1) is already shown. As for the conditions (2) and (3), we consider the action of $\mathcal{G}$ on L_g. Since the splitting field $S_{f(x,\alpha)}$ includes L_g, $S_{f(x,\alpha)}$ also includes the image of L_g by an element of $\mathcal{G}$. Thus, each element of $\mathcal{G}$ can be treated as an embedding of L_g into $\overline{K}$. In more detail, we can identify the set of embeddings $\mathcal{E}$ with the coset $\mathcal{G}/\mathcal{H}$. Then, for each element σ there is an integer j such that $\sigma(h_1(x,\alpha))=h_j(x,\alpha)$. This implies that $\sigma(S_i(\beta_1,...,\beta_{n'})=S_i(\beta'_1,...,\beta'_{n'})$ for $1\le i\le n'$, where $\beta'_1,...,\beta'_{n'}$ are all roots of $h_j(x,\alpha)$ and S_i denotes the i-th *fundamental symmetric function*. Hence, $\sigma(\{\beta_1,...,\beta_{n'}\})=\{\beta'_1,...,\beta'_{n'}\}$. This implies that $\Omega(h_1),...,\Omega(g_N)$ satisfies the condition (2). Moreover, $h_1(x,y),...,h_N(x,y)$ are $\mathcal{E}$-conjugates by Lemma A.3, we can verify the statement (3). □

THEOREM A.10 (Kaltofen's Theorem). *For each root β of $f(x,\alpha)$, $K(\beta)$ includes L_g.*

Proof. Without loss of generality, we may assume that $\beta=\beta_1$, a root of $h_1(x,a)$, and consider the stabilizer $\mathcal{H}_1$ of β_1 in $\mathcal{G}$. Then, the subfield of $S_{f(x,\alpha)}$ consisting of all elements fixed by $\mathcal{H}_1$ coincides with $K(\beta_1)$ by the fundamental theorem of Galois theory. For every element σ in $\mathcal{H}_1$, we have $\sigma(\Omega(h_1))=\Omega(h_1)$ since $\sigma(\beta_1)=\beta_1$ and $\sigma(\Omega(h_1))\cap\Omega(h_1)\neq\emptyset$. This implies that each $S_i(\beta_1,...,\beta_{n'})$ is fixed by every element in $\mathcal{H}_1$. Therefore, $\mathcal{H}_1$ fixes every $g_i(\alpha)$, and $K(\beta_1)$ includes every $g_i(\alpha)$. Hence $K(\beta_1)$ includes $L_g=K(g_0(\alpha),\ldots,g_{n'}(\alpha))$. □

Kazuhiro YOKOYAMA
Department of Mathematics,
Rikkyo University
3–34–1 Nishi-Ikebukuro, Toshima-ku,
Tokyo, 171–8501, Japan
e-mail: kazuhiro@rikkyo.ac.jp