九州大学学術情報リポジトリ
Kyushu University Institutional Repository

On systems of algebraic equations with parametric exponents

Yokoyama, Kazuhiro
Faculty of Mathematics, Kyushu University

https://hdl.handle.net/2324/11822

出版情報：Proceedings of the 2004 international symposium on Symbolic and algebraic computation, pp.312-319, 2004-07-04. Association for Computing Machinery
バージョン：
権利関係：

KYUSHU UNIVERSITY

MHF Preprint Series

Kyushu University
21st Century COE Program
Development of Dynamic Mathematics with High Functionality

On systems of algebraic equations with parametric exponents

K. Yokoyama

MHF 2003-4

(Received December 30, 2003)

Faculty of Mathematics
Kyushu University
Fukuoka, JAPAN

On systems of algebraic equations with parametric exponents

Kazuhiro Yokoyama
Faculty of Mathematics, Kyushu University
6-10-1 Higashiku, Fukuoka, 812-8581, Japan
yokoyama@math.kyushu-u.ac.jp

ABSTRACT

We deal with systems of algebraic equations with parametric exponents. As the first step for solving such systems, we introduce a simple formulation and basic notions in ideal theory. Then we give a concrete method for most simple cases, univariate case and 0-dimensional case.

1. INTRODUCTION

In mathematical problem, there arise systems of algebraic equations with parameters. For solving systems with parametric coefficients, many works were done by several authors, where complete methods are proposed. (See [10, 5, 11].) Systems with parametric exponents are also important and very interesting. However, as few works were done for those systems, many questions/problems seem untouched. Here we consider certain *stability* of systems with parametric exponents and *computability* of their solutions. These problems can be translated to problems on the structure of ideals generated by polynomials with parametric exponents.

The problems dealt with here are originally raised by Prof. Tadashi Takahashi of Kobe University in order to give a computational proof of non-degeneracy conditions of singularities of algebraic surfaces [9]. We show one typical type of his problem.

Example 1. *What is the singularity of $S_{k,0}$ [1, 9]*

$$f = x^2z + yz^2 + y^{4k+1} + axy^{3k+1} + bzy^{2k+1},$$

where k is a positive integer and a, b are complex numbers. Then we have to solve the following system

$$f = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = \frac{\partial f}{\partial z} = 0.$$

The "parameter" k appears in coefficients, which makes the problem more difficult.

Here we set our problem and our goal as follows:

Goal: For ideals which are generated by finitely many polynomials with parametric exponents, we want to examine the following two problems. When one fixes a value (a positive integer) for each parameter, the Gröbner basis ([2, 3]) can be determined with respect to a fixed ordering. Then,

(1) **Structural Stability:**
When the values of parameters are large enough, does the structure of the ideal become "stable"? Or the structure can be determined uniformly by parameters?

(2) **Computability:**
If the structure of the ideal is "stable" for sufficiently large values for parameters, are there algorithms for computing its Gröbner basis? That is, do algorithms stop in finitely many (independent to the values of parameters) steps ?

The problems are also heavily related to the following:

(3) **Effects of "sparsity" of generating sets on the computational complexity:** When the values of parameters are sufficiently large, the inputs are sparse polynomials. Especially, in 0-dimensional case, the computational complexity is estimated using the Bezout bound, when one use a revlex ordering. Since the Bezout bound will be given as a polynomial function in parameters in our problem, the study on ideals with parametric exponents might give some insights on the problem.

Here, as the first attempt to attack the problems, we will introduce a "simple formalization" and important basic notions to make our goal clear, which are derived from studies on the most simple cases, univariate case and 0 dimensional case with one parameter. And we will give a concrete answer for those cases.

2. FORMULATION

Here we give a precise settings on the problems and necessary notions in order to solve them.

Settings: We consider a polynomial ring $\mathbf{Q}[X]$ where $X = \{x_1, \ldots, x_n\}$. So, polynomials with parametric exponents

are treated as "ordinary" polynomials with fixed (but unknown) integer values substituted in parameters. (So, parameters are not treated as variables.) As every exponent is non-negative, there might be certain restriction on the values of parameters. But, by shifting values, without loss of generality, we can assume that parameters can range all positive integers.

Definition 1 (Ep-term and Ep-Ideal). *We call a term with parametric exponent an* ep-term *and a polynomial with ep-term an* ep-polynomial. *When an ideal has an ep-polynomial in its generator, we call the ideal an* ep-ideal. *In distinction to ep-polynomials and ep-ideals, we call a polynomial without ep-term an* ordinary *polynomial, and an ideal generated by ordinary polynomials an* ordinary *ideal.*

Example 2. *The polynomial in Example 1*

$$f = x^2z + yz^2 + y^{4k+1} + axy^{3k+1} + bzy^{2k+1}$$

is an ep-polynomial in $\mathbf{Q}[x, y, z]$, *where* y^{4k+1}, xy^{3k+1}, y^{2k+1} *are ep-terms with parameter* $k \geq 1$.

In Example 2, y^k plays an essential role. Because, by replacing y^k with a new variable w, we have an ordinary polynomial

$$g = x^2z + yz^2 + w^4y + axw^3y + bzw^2y.$$

Definition 2 (Essential Ep-Term). *For an ep-polynomial* f, *there are ep-terms* $t_1, \ldots, t_s$ *such that one can obtain an ordinary polynomial by replacing each* t_i *with a new variable* y_i. *We call these* $t_1, \ldots, t_s$ essential ep-terms *for* f. *Moreover, for a generating set* G *of an ideal* $\mathcal{I}$, *if ep-terms* $t_1, \ldots, t_s$ *are essential ep-terms for every element in* G, *we call these* $t_1, \ldots, t_s$ essential ep-terms *for* $\mathcal{I}$.

Here we use forms of Gröbner bases in order to give certain "stability" of ep-ideals. From now on, we fix a term order $<$.

Definition 3 (Stability and Form of Gröbner Basis). *Let* G *be the reduced Gröbner basis of an ep-ideal* $\mathcal{I}$. *Then* G, *or equivalently* $\mathcal{I}$, *is said to be* stable *if* G *has one of the following forms:*

(1) **General Form:** *The number of elements of* G *does not depend on the values of parameters. And each element has finitely many (independent to the values of parameters) terms and is expressed by fixed ep-terms and ordinary terms. So, for fixed values of parameters, we have the reduced Gröbner base by simply substituting those values. In this case,* G *is called of* General form.

(2) **Finite Form:** *Each element of* G *does not have any ep-term, and moreover,* G *satisfies one of the followings. In this case,* G *is said to be of* finite form. *Let* $p_1, \ldots, p_s$ *be parameters.*

Periodic: *There exists a vector* $N = (n_1, \ldots, n_s)$ *with positive integral components such that* G *is determined uniquely by the values* $(p_1 \bmod N_1, \ldots, p_s \bmod N_s)$. *In this case,* G *is said to be* periodic. *And* N *is called a* period. *As its special case, there is a case where* G *does not depend on any values of parameters. In this case,* G *is said to be* completely stable.

Bounded: *There exists a vector* $N = (n_1, \ldots, n_s)$ *with positive integral components such that* G *is trivial* ($G = \{1\}$) *if* $p_i > n_i$ *for every* p_i. *In this case,* G *is said to be* bounded. *And* N *is called a* bound.

Example 3. *The following is a Gröbner basis of the ideal generated by itself with respect to lex ordering* $x_1 < x_2 < x_3$. *It is of general form.*

$$\begin{aligned} f_1 &= x_1^n + 1 \\ f_2 &= x_2 - x_1^{n-1} - x_1 + 1 \\ f_3 &= x_3 - x_1^{n-2} - 1 \end{aligned}$$

The radical of the ideal for $S_{k,0}$ *is* $< x, y, z >$ *for almost every complex values for* a *and* b, *which gives an example of finite form (completely stable). (See Example 5.)*

Example 4. *(1) The ideal* $< x^k - 1, x^2 + x + 1 >$ *becomes* $< x^2 + x + 1 >$ *if* $k \equiv 0 \pmod 3$ *and* $< 1 >$ *for otherwise. This is a periodic case.*

(2) For the ideal $< x^k - 5x + 2, x^2 + x - 6 >$, *it becomes* $< x - 2 >$ *if* $k = 3$, *and* $< 1 >$ *otherwise. This is a bounded case.*

(3) For the ideal $< x^{k+1} - x^k + x^2 - 1, x^2 + x - 2 >$, *it becomes* $< x - 1 >$ *for every* $k \geq 1$. *This is a completely stable case.*

Remark 1. *With respect to the lex ordering* $x < y$, *the ideal* $< x^k - 1, (x - 1)y - 1 >$ *does not have its Gröbner basis* G *of general form, but* G *can be expressed by a certain "finite form" as follows:*

$$\frac{(x^k - 1)}{(x - 1)},\ y + \frac{(x^k - ky + k - 1)}{(x - 1)^2}.$$

But, as mentioned in Example 7, it has certain difficulty in computation. So, it seems difficult to handle such a case as a general form case.

2.1 Applicable Techniques

Here we mention two important techniques which seem very useful to solve a system of algebraic equations with parametric exponents and to compute its Gröbner basis. From now on, we assume that $\mathcal{I}$ is an ep-ideal generated by $F = \{f_1, \ldots, f_r\}$, and $T = \{t_1, \ldots, t_s\}$ is the set of essential ep-terms. See [4, 3] for elimination ideal and [10, 11] for comprehensive Gröbner bases.

Slack Variables and Elimination:
If $\mathcal{I}$ has a Gröbner basis of finite form, it might be effective to eliminate all ep-terms.

From F, by replacing essential ep-terms $t_1, \ldots, t_s$ with new slack variables $y_1, \ldots, y_s$, we have a set F_0 of ordinary polynomials in $\mathbf{Q}[X, Y]$. That is, from each f_i, we have a new polynomial $f_{i,0}(X, Y)$ such that $f_{i,0}(X, T) = f_i(X)$.

Let $\mathcal{I}_0$ be the ideal in $\mathbf{Q}[X, Y]$ generated by F_0. By computing the elimination ideal $\mathcal{J} = \mathcal{I}_0 \cap \mathbf{Q}[X]$ with some fixed elimination order $X << Y$, we find ordinary polynomials belonging to the ep- ideal $\mathcal{I}$. Let H be a Gröbner basis of $\mathcal{J}$. Then,

LEMMA 1. *H is contained in $\mathcal{I}$, that is, $\mathcal{J}$ is contained in $\mathcal{I}$.*

PROOF. For each polynomial $h(X)$ in H, we show that $h(X)$ belongs to $\mathcal{I}$. As $h(X) \in \mathcal{J} = \mathcal{I}_0 \cap \mathbf{Q}[X]$, there are polynomials $a_i(X, Y)$ such that

$$h(X) = \sum_{i=1}^{r} a_i(X, Y) f_{i,0}(X, Y).$$

Then, substituting t_i for each y_i, we have

$$h(X) = \sum_{i=1}^{r} a_i(X, T) f_i(X).$$

This implies that $h(X)$ belongs to $\mathcal{I}$. $\square$

DEFINITION 4. *We call the above elimination ideal $\mathcal{J}$ the* finite sub *ideal of $\mathcal{I}$. We call an ordinary polynomial in the finite sub ideal $\mathcal{J}$ a* finite polynomial *of $\mathcal{I}$.*

As $\mathcal{J} \subset \mathcal{I}$, the set of zeros $V(\mathcal{J})$ contains $V(\mathcal{I})$. Thus, all zeros of $\mathcal{I}$ can be obtained by checking if each zero of $\mathcal{J}$ satisfies the original generating set F. This method is very efficient when $V(\mathcal{J})$ is a finite set, that is, $\mathcal{J}$ is 0-dimensional.

Moreover, it might be much efficient to use prime decomposition of the finite sub ideal $\mathcal{J}$. (See [3, 8] for detailed algorithms.) For each component $\mathcal{P}$, we compute $\mathcal{I} + \mathcal{P}$. Then, gathering the computational results of $\mathcal{I} + \mathcal{P}$ for all components $\mathcal{P}$, we have the final result.

EXAMPLE 5. *For the ep-polynomial $S_{k,0}$*

$$f = x^2 z + y z^2 + y^{4k+1} + a x y^{3k+1} + b z y^{2k+1},$$

y^k is the unique essential term. So, by replacing y^k with w, we have an ordinary polynomial in 4 variables

$$f_0 = x^2 z + y z^2 + w^4 y + a x w^3 y + b z w^2 y.$$

In Takahashi's Problem $S_{k,0}$, we have the following 3 additional polynomials obtained by partial differentiation:

$$\begin{aligned} f_1 &= 2xz + a w^3 y \\ f_2 &= z^2 + (4k+1) w^4 + (3k+1) a x w^3 + (2k+1) b z w^2 \\ f_3 &= x^2 + 2yz + b w^2 y. \end{aligned}$$

Then, by considering a, b, k as other variables, we can compute an elimination ideal $\mathcal{J}$ of $< f_0, f_1, f_2, f_3 >$ eliminating w in the polynomial ring $\mathbf{Q}(a, b, k)[x, y, z, w]$.

With lex ordering $w > z > y > x$, we computed $\mathcal{J}$ and also computed all its prime divisors. Then $\mathcal{J}$ has two prime divisors

$$< x, y >, < x, z > .$$

We divide the problem into two cases, the case $x = y = 0$ and the case $x = z = 0$. Then, we have

$$\begin{aligned} x = y = 0 \quad &\rightarrow \quad z = 0 \\ x = z = 0 \quad &\rightarrow \quad y = 0, \end{aligned}$$

which shows that $< x, y, z >$ is the radical of the ep-ideal $\mathcal{I}$.

REMARK 2. *In Example 5, the parameter k also appears in coefficients. So, the above computation corresponds to "general case", that is, a, b, k does not satisfy certain algebraic constraints. For solving such parametric systems precisely, see Chapter 6 Section 3 in [4] or comprehensive Gröbner basis computation [10, 5, 11].*

If one wants to classify all possible forms of the Gröbner basis, one needs the technique derived from COMPREHENSIVE GRÖBNER BASIS[10, 5, 11].

Comprehensive Gröbner basis:
We execute Buchberger algorithm [2, 4, 3] stepwise, where we decide which term should be the leading term. So, there might appear some branches depending on the values of parameters.

EXAMPLE 6. *If two ep-terms y^{3k+2} and y^{2k+20} appear, their order will depend on the value of k as follows:*

$$\begin{aligned} k > 6 \quad &\rightarrow \quad y^{3k+2} > y^{2k+8} \\ k < 6 \quad &\rightarrow \quad y^{3k+2} < y^{2k+8} \\ k = 6 \quad &\rightarrow \quad \textit{we must merge } y^{3k+2} \textit{ and } y^{2k+8}. \end{aligned}$$

The most crucial problem is the termination of Buchberger algorithm in finitely many steps independent to the values of parameters. There is a case where the computational complexity of Buchberger algorithm depends on the value of parameters. The following example requires $O(k)$ steps.

EXAMPLE 7.

$$\begin{aligned} f(x, y) &= x^k - 1 \\ g(x, y) &= xy - y - 1 \end{aligned}$$

With respect to lex ordering $y > x$, the Gröbner basis will be

$$\{x^{k-1} + x^{k-2} + \cdots + 1, x^{k-2} + 2x^{k-3} + \cdots + (k-2)x + (k-1) + ky\}.$$

This implies that the Buchberger algorithm requires at least k monomial reductions.

From now on, for simplicity, we will consider the case where the number of essential terms is 1, and the essential term has only one variable.

3. UNIVARIATE CASE

Here we consider an ep-ideal in $\mathbf{Q}[x]$. And suppose that the term x^k is the unique essential ep-term for the given ep-ideal $\mathcal{I}$. In general, it is not true that the structure of the ideal becomes stable. But, in this case, there is a certain stability.

REMARK 3. *In many systems appearing in Mathematics, k is supposed to be sufficiently large, or terms with different expressions are supposed different to each other for any values of parameters. From these assumptions, there are certain restrictions on values of parameters. For example, for the expression $f(x) = x^{2k} + x^{k+5} + x^{12}$ the condition $k > 7$ might be given to assert that $2k > k + 5 > 12$.*

Settings: For ep-polynomials $f(x), g(x)$ over $\mathbf{Q}$ with essential ep-term x^k, we compute $\gcd(f(x), g(x))$, which is a generator of the ideal $< f(x), g(x) >$. (We assume that k does not appear in coefficients.) Moreover, for simplicity, $f(x)$ and $g(x)$ have non zero constant terms. (We remove the factor x from $f(x)$ and $g(x)$ in advance.)

Then we have the following result.

THEOREM 1. *There are positive integers N, B such that for each value $a \geq B$ of the parameter k, $\gcd(f(x), g(x))$ is determined uniquely by the value $a \bmod N$. Moreover, N and B can be computed from $f(x), g(x)$.*

In the below, we will give a concrete procedure for computing $\gcd(f(x), g(x))$, which gives a proof of Theorem 1.

First, replacing x^k with a new variable y, we compute bivariate polynomials f_0, g_0 from f, g. So, $f(x) = f_0(x, x^k)$ and $g(x) = g_0(x, x^k)$. Then, as bivariate polynomials, we compute $\gcd(f_0(x, y), g_0(x, y))$ which we denote by $h_0(x, y)$. Then, $h(x) = h_0(x, x^k)$ is a common factor of $f(x), g(x)$. We call $h(x)$ *the general form factor.*

Next we consider $f'(x) = f(x)/h(x)$ and $g'(x) = g(x)/h(x)$ and try to compute $\gcd(f'(x), g'(x))$. Replacing x^k with a new variable y in f', g', we have bivariate polynomials f_1, g_1 from f', g', that is, $f'(x) = f_1(x, x^k)$ and $g'(x) = g_1(x, x^k)$.

As $f_0 = f_1 h_0$ and $g_0 = g_1 h_0$, f_1 and g_1 have no common factor as bivariate polynomials. So, the resultant $\mathrm{res}_y(f_1, g_1)$ does not vanish, and it is a finite polynomial of $< f'(x), g'(x) >$.

Consider the sub finite ideal $< f_1(x, y), g_1(x, y) > \cap \mathbf{Q}[x]$ which is not $\{0\}$, and let $m(x)$ be its generator. Then $m(x)$ belongs $< f'(x), g'(x) >$ by Lemma 1.

If $m(x)$ is a constant (non zero), then $< f'(x), g'(x) >= 1$ and so there is no common factor of $f'(x), g'(x)$.

If $m(x)$ is not a constant, we factorize $m(x)$ into its irreducible factors $m_i(x)$ over $\mathbf{Q}$:

$$m(x) = \prod_{i=1}^{r} m_i(x)^{e_i}.$$

Since $m(x)$ belongs to the ideal $< f'(x), g'(x) >$ and $m_i(x)^{e_i}$'s are pairwise prime, we have

$$\gcd(f', g') = \gcd(f', g', m) = \prod_{i=1}^{r} \gcd(f', g', m_i(x)^{e_i}).$$

Thus, the gcd computation is reduced to the computation of $\gcd(f', g', m_i(x)^{e_i})$. (We exclude x from factors.)

Now we divide factors m_i into two cases:

DEFINITION 5. *If $m_i(x)$ is a factor of some* cyclotomic polynomial $x^n - 1$ *with a positive integer n, we call $m_i(x)$ a* cyclotomic factor. *And we call the smallest positive integer n such that $m_i(x)$ divides $x^n - 1$ the* period *of $m_i(x)$. Otherwise, we call $m_i(x)(\neq x)$ a* non cyclotomic factor.

Cyclotomic Case:
Suppose that $m_i(x)$ is a cyclotomic factor $m_i(x)$ of the period N_i. In this case, we have the following.

PROPOSITION 1. *$\gcd(f'(x), g'(x), m_i(x))$ is determined uniquely by the value $k \bmod N_i$.*

PROOF. For each value k, we denote $k \bmod N_i$ simply by a, where $a \in \{0, 1, \ldots, N_i - 1\}$. As $m_i(x)$ is irreducible, $\gcd(f'(x), g'(x), m_i(x))$ is non-trivial if and only if $f'(x), g'(x)$ are divided by $m_i(x)$. As $m_i(x)$ divides $x^{N_i} - 1$, x^k and x^a are congruent modulo $m_i(x)$, that is, both belong to the same residue class in the residue class ring $\mathbf{Q}[x]/m_i(x)$. By substituting a for k, we have an ordinary polynomial $f'_a(x)$ congruent to $f'(x)$ modulo $m_i(x)$. Then, as $m_i(x)$ divides $f'(x) - f'_a(x)$, $m_i(x)$ divides $f'_a(x)$ if and only if $m_i(x)$ divides $f'(x)$. Samely, we also have an ordinary polynomial $g'_a(x)$ congruent to $g'(x)$. This arguments shows that $\gcd(f'(x), g'(x), m_i(x))$ is determined by $\gcd(f'_a(x), g'_a(x), m_i(x))$ and hence, it is determined uniquely by the value $a = k \bmod N_i$. $\square$

Thus, we can determine whether $\gcd(f(x), g(x))$ has $m_i(x)$ as its factor simply by dividing $f'_a(x)$ and $g'_a(x)$ by $m_i(x)$ for each $a \in \{0, 1, \ldots, N_i - 1\}$. ($f'_a(x)$ and $g'_a(x)$ are obtained from $f'(x)$ and $g'(x)$ by substituting a for k.) If $e_i = 1$, we have done.

For the case $e_i > 1$, we need "differential" to know the power e such that $\gcd(f'(x), g'(x)) = m_i(x)^e$. Suppose that we already know $m_i(x)$ divides $\gcd(f(x), g(x))$. Then, $m_i(x)^2$ divides $\gcd(f(x), g(x))$ if and only if $m_i(x)$ also divides both of $\frac{df'(x)}{dx}$ and $\frac{dg'(x)}{dx}$. We note that there appear parametric coefficients (linear in k) in $\frac{df'(x)}{dx}$ and $\frac{dg'(x)}{dx}$.

For each $a \in \{0, 1, \ldots, N_i - 1\}$, we replace the parameter k in exponents with a. (For $a = 0$, some exponent may be negative. In this case, we replace k with N_i instead of 0.) But, for parametric coefficient linear in k, we introduce another parameter s and replace the parameter k in coefficients with $sN_i + a$. We denote new ordinary polynomials obtained from $\frac{df'(x)}{dx}$ and $\frac{dg'(x)}{dx}$ by $f''_a(x)$ and $g''_a(x)$, respectively.

Then we compute resultants $R_{a,f} = \mathrm{res}_x(m_i(x), f''_a(x))$ and $R_{a,g} = \mathrm{res}_x(m_i(x), f''_a(x))$, where s is considered as a variable and polynomials are considered in $\mathbf{Q}[x, s]$. Then $R_{a,f}$ and $R_{a,g}$ are univariate polynomials in s.

LEMMA 2. *For each $a = k \bmod N_i$ and $sN_i + a$, the followings hold:*

(1) If both of $R_{a,f}$ and $R_{a,g}$ are zero polynomials, then $m_i(x)^2$ divides $\gcd(f'(x), g'(x))$ for any $k = sN_i + a$.

(2) If at least one of $R_{a,f}$ or $R_{a,g}$ is non zero constant, then $m_i(x)^2$ does not divides $\gcd(f'(x), g'(x))$ for any $k = sN_i + a$.

(3) If at least one of $R_{a,f}$ and $R_{a,g}$ is a non constant polynomial and the other is not a non zero constant, then $m_i(x)^2$ divides $\gcd(f'(x), g'(x))$ only for special values $k = sN_i + a$, where s are positive integral common roots of $R_{a,f}(s)$ and $R_{a,g}(s)$. (Where we consider all integer as roots of zero polynomial.) Conversely, in this case, let M be the maximal value of $k = sN_i + a$, where s ranges all positive integral common roots. (If there is no such common root, we set $M = 0$.) Then, for any $k = sN_i + a > M$, $m_i^2(x)$ does not divide $\gcd(f'(x), g'(x))$.

PROOF. For each $a = k \bmod N_i$ and $sN_i + a$, $m_i(x)^2$ divides $\gcd(f'(x), g'(x))$ if and only if $m_i(x)$ divides both of $f''_a(x)$ and $g''_a(x)$. By using this fact, we have only to consider wether $m_i(x)$ divides both of $f''_a(x)$ and $g''_a(x)$. Then, by using resultant theory, we have (1),(2) and (3). Here, as $m_i(x)$ has no parametric coefficient, we do not need to check if the leading coefficients of $f''_a(x)$ and $g''_a(x)$ vanish or not. (See [4] Chapter 6 Section 3.) $\square$

By Lemma 2, we can decide if $m_i(x)^2$ divides $\gcd(f'(x), g'(x))$ for any $k = sN_i + a$. And, if not, we also have a bound, say $M_a^{(2)}$ such that for any $k = sN_i + a > M_a^{(0)}$, $m_i^2(x)$ does not divide $\gcd(f'(x), g''(x))$. In this case, we only need to compute $\gcd(f'(x), g'(x), m_i(x)^{e_i})$ only for the special values $k = sN_i + a$,

Repeating the same procedure for higher differential $\frac{d^e f'_a}{dx^e}$ and $\frac{d^e g'_a}{dx^e}$ while $e \le e_i$ and $m_i(x)^{e-1}$ divides $\gcd(f'(x), g'(x))$, we can decide wether $m_i(x)^e$ divides $f'_a(x)$ for every k with $k \equiv a \pmod{N_i}$. Moreover, if not, we have a bound $M_a^{(e)}$ such that $m_i(x)^e$ does not divide $f'(x)$ for any $k > M_a^{(e)}$ with $k \equiv a \pmod{N_i}$.

Thus, gathering these informations on the divisibility, we have Proposition 2 and Procedure [CYCLOTOMIC CASE].

REMARK 4. *For the differentials $\frac{d^e f'_a}{dx^e}$ and $\frac{d^e g'_a}{dx^e}$, every exponents must be non-negative. Therefore, we need the condition $k \ge e_i$ and we use $a + dN_i$ for some positive integer d for substitution instead of a. From this modification, for smaller value $k < e_i$, we have to compute $\gcd(f'(x), g'(x), m_i(x)^{e_i})$ individually.*

PROPOSITION 2. *There exists a positive integer M_i such that if $k > M_i$, then $\gcd(f'(x), g'(x), m_i(x)^{e_i})$ is determined uniquely by the value $k \bmod N_i$. Moreover, M_i can be computed by $f(x), g(x)$ and $m_i(x)$.*

PROCEDURE [CYCLOTOMIC CASE]
For each value $a \in \{0, 1, \ldots, N_i - 1\}$, execute the following:

1. Compute ordinary polynomials $f'_a(x), g'_a(x)$ by substituting a for k.
2. Compute $\gcd(f'_a(x), g'_a(x), m_i(x))$.
3. If $\gcd(f'_a(x), g'_a(x), m_i(x)) = 1$, return 1.
4. If $\gcd(f'_a(x), g'_a(x), m_i(x)) = m_i(x)$ then set $E = e_i$, $F = f'(x)$, $G = g'(x)$ and $A = m_i(x)$.
5. If $E = 1$, then return A. Otherwise set $E = E - 1$.
6. while($E > 0$)
   - 6.1. Compute $\frac{dF}{dx}$ and $\frac{dF}{dx}$. Set $F = \frac{dF}{dx}$ and $G = \frac{dF}{dx}$.
   - 6.2. Compute F_a and G_a by substituting a for k in ep-terms and replacing k with $sN_i + a$ in coefficients. (See Remark 4 for a modification.)
   - 6.3. Compute $\mathrm{res}_x(F_a, m_i)$ and $\mathrm{res}_x(G_a, m_i)$.
   - 6.4. If both resultants vanishes, then $A = A \times m_i(x)$ and return to the top of 6.
   - 6.5. Otherwise, compute the set R of all common positive integer roots of $\mathrm{res}(F_a, m_i)$ and $\mathrm{res}(G_a, m_i)$.
   - 6.6. If $R = \emptyset$, return A.
   - 6.7. Let $B = [A]$. For each root s in R,
     compute F_k and G_k from $f'(x)$ and $g'(x)$ by replacing k with $sN_i + a$, and
     compute $\gcd(F_k(x), G_k(x), m_i(x)^{e_i})$ and append $(sN_i + a, \gcd(F_k(x), G_k(x), m_i(x)^{e_i}))$ to B.
   - 6.8. return B.
7. return A.

EXAMPLE 8. *Consider the following polynomials.*

$$\begin{aligned} f(x) &= x^{3k} - 2x^{k+6} + 1, \\ g(x) &= (x^k - 1)^2 + (x^2 + x + 1)^2 \end{aligned}$$

The elimination ideal is generated by $m(x) = (x^2 + x + 1)^2 m'(x)$, where $m'(x)$ is a non cyclotomic factor. For $k \equiv 0 \pmod 3$, $f(x), g(x)$ are divided by $x^2 + x + 1$. Then their differentials are as follows.

$$\begin{aligned} \frac{f(x)}{dx} &= 3kx^{3k-1} - 2(k+6)x^{k+5}, \\ \frac{g(x)}{dx} &= 2kx^{k-1}(x^k - 1) + 2(x^2 + x + 1)(2x + 1) \end{aligned}$$

Letting $k = 3s$, where $s \ge 1$, and replacing k in the exponents with 3, we have

$$\begin{aligned} \frac{f(x)}{dx} &\to (3s - 12)x^8 \\ \frac{g(x)}{dx} &\to 2sx^2(x^3 - 1) + 2(x^2 + x + 1)(2x + 1). \end{aligned}$$

By resultant computation, we can show that $f(x), g(x)$ are divided by $(x^2 + x + 1)^2$ only for $k = 12$, where $s = 4$.

Non Cyclotomic Case:
For each non cyclotomic factor $m_i(x)(\neq x)$, we have

PROPOSITION 3. *There is a positive integer B_i such that $\gcd(f'(x), g'(x), m_i(x)^{e_i})$ is trivial for every $k > B_i$. Moreover, B_i can be computed by $f(x), g(x)$ and $m_i(x)$.*

PROOF. Suppose that $m_i(x)(\neq x)$ is a non cyclotomic factor. For bivariate polynomials $f_1(x,y), g_1(x,y)$ obtained by replacing x^k with y. we set

$$\begin{aligned} F(y) &= \mathrm{res}_x(f_1(x,y), m_i(x)) \\ G(y) &= \mathrm{res}_x(g_1(x,y), m_i(x)). \end{aligned}$$

Then, at least $F(y) \neq 0$ or $G(y) \neq 0$ holds. Because, if $F(y) = G(y) = 0$, then $m_i(x)$ must divide both of $f_1'(x,y)$ and $g_1'(x,y)$. But, as assumption, $f_1'(x,y)$ and $g_1'(x,y)$ have no common factor, this is a contradiction. So, without loss of generality, we can assume that $F(y) \neq 0$.

Suppose that $m_i(x)$ divides $f'(x)$ for some value k. Then, by the property of resultant, we can show that for any root α of $m_i(x)$, α^k must be a root of $F(y)$. Now we fix a root α of $m_i(x)$.

On the other hand, as $F(y)$ is an ordinary univariate polynomial in y over $\mathbf{Q}$, we can set U and L as the maximal absolute value of roots of $F(y)$ and the minimum absolute value of non zero roots of $F(y)$. Then, if $|\alpha| > 1$, it follows $|\alpha^k| = |\alpha|^k \leq U$ and we obtain $k \leq log_{|\alpha|}(U)$. If $|\alpha| < 1$, it follows $|\alpha^k| = |\alpha|^k \geq L$ and we obtain $k \leq log_{|\alpha|}(L)$. Therefore, letting B be $log_{|\alpha|}(U)$ or $log_{|\alpha|}(L)$, $m_i(x)$ does not divide $f'(x)$ for any $k > B$. In this case, $\gcd(f'(x), g'(x), m_i(x))$ becomes trivial. Moreover, the above B can be computed exactly by numerical computation of approximate value of roots of $m_i(x)$ with rigorous error analysis. See [6, 7] for exact methods and rigorous error analysis. □

Now we give a concrete procedure.

PROCEDURE [NON CYCLOTOMIC CASE]

1. Compute a root α of $m_i(x)$ with rigorous error analysis and compute a correct bound A on $|\alpha|$ so that
   - $|\alpha| > A > 1$ if $|\alpha| > 1$, and
   - $|\alpha| < A < 1$ if $|\alpha| < 1$.
2. Compute $F(y), G(y)$ by
$$\begin{aligned} F(y) &= \mathrm{res}_x(f_0'(x,y), m_i(x)) \\ G(y) &= \mathrm{res}_x(g_0'(x,y), m_i(x)). \end{aligned}$$
3. If $F(y) \neq 0$, then compute a bound B on the absolute value of roots of $F(y)$ so that
   - $B > |\beta|$ for any root β of $F(y)$ if $|\alpha| > 1$, and
   - $0 < B < |\beta|$ for any non-zero root β of $F(y)$ if $|\alpha| < 1$.

   If $F(y) = 0$, then compute a bound B on the absolute value of roots of $G(y)$ so that
   - $B > |\beta|$ for any root β of $G(y)$ if $|\alpha| > 1$, and
   - $0 < B < |\beta|$ for any non-zero root β of $G(y)$ if $|\alpha| < 1$.
4. Compute the smallest positive integer N_i such that
   - if $|\alpha| > 1$, $A^{N_i} > B$, and
   - if $|\alpha| < 1$, $A^{N_i} < B$.

   Then, $\gcd(f(x), g(x), m_i(x))$ is trivial if $k > N_i$.
5. Substituting $1, ..., N_i$ for k, compute
$$\gcd(f(x), g(x), m_i(x))$$
   and return them.

REMARK 5. *For the bound on $|\alpha|^k$, we use $F(y)$. But, $F(y)$ tends to be very large, as the degree of $F(y)$ increases to the product of the y-degree of $f_0'(x,y)$ and the x-degree of $m_i(x)$. Instead of $F(y)$ we can use another polynomial obtained from $f_1(x,y)$ by substituting for x an approximate value $\bar{\alpha}$ of the root α of $m_i(x)$ with rigorous error analysis. By Rouché's theorem, roots of a polynomial are continuous function in coefficients. From this theorem and precise approximation, we can estimate the absolute value of roots of $f_1(\alpha, y)$.*

EXAMPLE 9. *Consider the following polynomials:*

$$\begin{aligned} f(x) &= x^{2k} + x^{2+k} + 2x^k + 2, \\ g(x) &= x^2 + 2 \end{aligned}$$

Then, $m(x) = x^2 + 2$ is a generator of the elimination ideal and it is irreducible. The absolute value of roots of $m(x)$ is $\sqrt{2}$, and the absolute value of roots of $F(y) = (y^2+2)^2$ is also $\sqrt{2}$. Therefore, we have $A = \sqrt{2}$ and $U = \sqrt{2}$, by which we obtain $B = 1$. Thus, for any $k > 2$, $\gcd(f(x), g(x)) = 1$. For $k = 1$, as $f(x) = x^3 + x^2 + 2x + 2$, $g(x) = x^2 + 2$, we have $\gcd(f(x), g(x)) = x^2 + 2$.

By combining two cases, cyclotomic case and non-cyclotomic case, we gather bounds M_i, B_j and periods N_i. Then, by letting

$$\begin{aligned} N &= \mathrm{LCM}(N_i \mid m_i \text{ is a cyclotomic factor } \} \\ B &= \max\{M_i, B_j \mid m_i \text{ is a cyclotomic factor and} \\ &\quad\ m_j \text{ is a non-cyclotomic factor } \}, \end{aligned}$$

we obtain Theorem 1.

GENERAL PROCEDURE (Assume that $f(0) \neq 0$ and $g(0) \neq 0$.)

1. Replacing x^k with a new variable y, compute bivariate polynomials f_0, g_0 from f, g.
2. In the polynomial ring $\mathbf{Q}[x,y]$, compute the elimination ideal $\mathcal{J} =< f_0(x,y), g_0(x,y) > \cap \mathbf{Q}[x]$.
3. *(General Form Factor)* If $\mathcal{J} = \{0\}$, we compute
$$h_0 = \gcd(f_0(x,y), g_0(x,y))$$
   and $h(x) = h_0(x, x^k)$, which is a common divisor of $f(x), g(x)$. To check if other common divisor exists or not, we return the top and apply f/h and g/h.
4. *(Finite From Factor)* If $\mathcal{J} \neq \{0\}$, we compute its generator $m(x)$ by eliminating the variable y. (Then $m(x)$ is an ordinary polynomial.)

5. Factorize $m(x) = \prod_{i=1}^{r} m_i(x)^{e_i}$. Then divide irreducible factors $m_i(x)$ into factors of cyclotomic polynomials and others. (We exclude x from factors.)

6. For each factor $m_i(x)$, execute the following:

   6.1. For each cyclotomic factor $m_i(x)$, compute $\gcd(f(x), g(x), m_i(x)^{e_i})$ by Procedure Cyclotomic Case.

   6.2. For each non-cyclotomic factor $m_i(x)$, compute $\gcd(f(x), g(x), m_i(x)^{e_i})$ by Procedure Non Cyclotomic Case.

7. Unify all obtained informations and return the final result.

4. 0-DIMENSIONAL CASE

Here we consider another simple and easy case, where arguments used for univariate case can be applied directly.

Suppose that an ep-ideal $\mathcal{I}$ generated by $F = \{f_1, \ldots, f_r\}$ in $\mathbf{Q}[x_1, \ldots, x_n]$ satisfies the following:

1. There is a unique essential ep-term x_1^k with single parameter k.

2. The finite sub ideal $\mathcal{J}$ of $\mathcal{I}$ obtained by Slack variable and Elimination is 0-dimensional.

In this case, we have the similar procedure for computing the Gröbner basis of $\mathcal{I}$ as procedures in the previous section. Here we give an outline of a concrete procedure for computing the radical $\sqrt{\mathcal{I}}$. For simplicity, we assume that each $f_i(X, y)$ is primitive as a univariate polynomial in y over $\mathbf{Q}[X]$.

From F, we have a set $F_0 = \{f_{1,0}(X, y), \ldots, f_{r,0}\}$ such that $f_{i,0}(X, x_1^k) = f_i(X)$ for $1 \le i \le r$, and the ideal $\mathcal{I}_0$ generated by F_0 in $\mathbf{Q}[X, y]$. Then we can compute the finite sub ideal $\mathcal{J} = \mathcal{I}_0 \cap \mathbf{Q}[X]$ with some fixed elimination order $X << y$. As $\mathcal{J}$ is 0-dimensional, $\mathcal{I}$ is 0-dimensional (or trivial) for any k.

First we compute the minimal polynomial $m(x_1)$ of x_1 with respect to $\mathcal{J}$. ($m(x_1)$ is an ordinary polynomial in x_1 over $\mathbf{Q}$.) And then, we factorize $m(x_1)$ as

$$m(x_1) = \prod_{i=1}^{s} m_i(x_1)^{e_i}.$$

As $\mathcal{I}$ and $\mathcal{J}$ are 0-dimensional for each fixed value k, we have

$$\begin{aligned}
\mathcal{J} &= \cap_{i=1}^{s}(\mathcal{J} + < m_i^{e_i}(x_1) >) \\
\sqrt{\mathcal{J}} &= \cap_{i=1}^{s}(\sqrt{\mathcal{J}} + < m_i(x_1) >) \\
\mathcal{I} &= \cap_{i=1}^{s}(\mathcal{I} + < m_i^{e_i}(x_1) >) \\
\sqrt{\mathcal{I}} &= \cap_{i=1}^{s}(\sqrt{\mathcal{I}} + < m_i(x_1) >),
\end{aligned}$$

as ordinary polynomial ideals. (See [3, 8].) Then, samely as univariate case, we divide factors of $m(x_1)$ into cyclotomic factors and non-cyclotomic factors. Here, we exclude x from factors. If x is a factor $m(x)$, we compute the Gröbner basis of the ideal $< f_1(0, x_2, \ldots, x_n), \ldots, f_r(0, x_2, \ldots, x_n) >$ in $\mathbf{Q}[x_2, \ldots, x_n]$.

Cyclotomic Case: If m_i is a cyclotomic factor of period N_i, then $x_1^k \equiv x_1^a \pmod{\sqrt{I} + < m_i >}$ if $k \equiv a \pmod{N_i}$,

Then, the Gröbner basis of $\sqrt{\mathcal{I}} + < m_i(x) >$ is determined uniquely by the value $k \bmod N_i$. By replacing k with each value a in $\{0, 1, 2, \ldots, N_i - 1\}$, $\mathcal{I}$ becomes an ordinary ideal and we can compute the Gröbner basis of $\sqrt{\mathcal{I}} + < m_i(x_1) >$.

Non-Cyclotomic Case: If $m_i(x)(\neq x)$ is a non cyclotomic factor, by using *minimal polynomial computation* instead of *resultant computation* in univariate case, we can compute the Gröbner basis of $\sqrt{\mathcal{I}} + < m_i(x_1) >$.

1. Compute $\mathcal{J}_i = \sqrt{J} + < m_i(x_1) >$. Let G_i be the Gröbner basis of $\mathcal{J}_i$.

2. Compute a root α of $m_i(x_1)$ with rigorous error analysis and compute a correct bound A on $|\alpha|$ such that
   - $|\alpha| > A > 1$ if $|\alpha| > 1$, and
   - $|\alpha| < A < 1$ if $|\alpha| < 1$.

3. For each $f_{j,0} \in F_0$, execute the following:

   3.1. Consider the ideal $\mathcal{H}_j$ in $\mathbf{Q}[X, y]$ generated by $\mathcal{J}_i$ and $f_{j,0}$. Then either $f_{j,0}$ is divided by $m_i(x_1)$ or $\mathcal{H}_j$ become a 0-dimensional ideal in $\mathbf{Q}[X, y]$. If $f_{j,0}$ is divided by $m_i(x_1)$, then return to the top of 3.
   Otherwise compute the minimal polynomial $F_j(y)$ of y with respect to $\mathcal{H}_j$.

   3.2. Compute a bound B_j on the absolute value of roots of $F_j(y)$ so that
   - $B > |\beta|$ for any root β of $F(y)$ if $|\alpha| > 1$, and
   - $0 < B < |\beta|$ for any non-zero root β of $F(y)$ if $|\alpha| < 1$.

4. Compute the smallest positive integer N_i such that
   - if $|\alpha| > 1$, $A^{N_i} > min\{B_1, \ldots, B_s\}$
   - if $|\alpha| < 1$, $A^{N_i} < max\{B_1, \ldots, B_s\}$,

   where we omit undefined B_j's. Then, the ideal $\sqrt{\mathcal{I}} + < m_i(x) >$ is trivial if $k > N_i$.

5. Substituting $1, ..., N_i$ for k, compute the Gröbner basis of $\sqrt{I} + < m_i(x) > = \sqrt{< F, m_i(x) >}$ and return them.

5. CONCLUDING REMARKS

In this paper we give basic notions on stability of ideals with parametric exponents, and give a concrete procedure for computing the Gröbner bases in the most simple cases, univariate case and 0-dimensional case with unique essential ep-term. However, for the proposed procedures, neither analysis on the efficiency nor actual implementation is not examined, Thus, in the next step, we will give more precise procedure and examine its efficiency/ability by complexity analysis and experiments on real computer. As the problem seems very hard in general settings, it is very important to go further *stepwise*. In the below, we list our next steps for further development.

1. Find efficient/effective criteria for stability and computability of Gröbner bases.

2. Find classes of polynomial ideals where the stability or the computability of Gröbner basis is guaranteed.

3. For special cases like as ideals in fewer variables (bivariate, tri-variate), find efficient/effective criteria for stability and computability of Gröbner basis. Also it is very interesting to examine the effectivity of SLACK VARIABLES AND ELIMINATION for special cases where the number of generating polynomials exceeds the sum of the number of essential ep-terms and the number of variables.

4. Apply developed methods to actual problems arising from Mathematics and engineering. As those problems tend to have parametric coefficients like as Takahashi's problem, we have to deal with systems with parametric coefficients and parametric exponents. To solve such complicated problems, extending/improving the technique of comprehensive Gröbner basis is indispensable.

6. REFERENCES

[1] Arnol'd, V.I. (1975). Critical points of smooth functions and their normal forms. *Russian Math. Surveys* **30:5**, 1-75.

[2] Buchberger, B. (1965). An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal (German). PhD Thesis, University of Innsbruck, Institute for Mathematics.

[3] Becker, T., Weispfenning, V. (1993). *Gröbner Bases.* GTM 141 Springer-Verlag, New York.

[4] Cox, D., Little, J., O'Shea, D. (1992). *Ideals, Varieties, and Algorithms.* UTM Springer-Verlag, 1992.

[5] Montes, A. (2002). A new algorithm for discussing Gröbner bases with parameters. *J. Symb. Comput.*, **33**, 183-208.

[6] Neumaier, A. (2001). Introduction to Numerical Analysis. Cambridge University Press.

[7] Rump, S.M. (1983). Solving algebraic problems with high accuracy. In: A New Approach to Scientific Computation, Notes and Reports in Computer Science and Applied Mathematics 7, ACADEMIC Press, pp.51-120.

[8] Shimoyama, T., Yokoyama, K. (1996). Localization and primary decomposition of polynomial ideals. *J. Symb. Comp.* **22**, 247-277.

[9] Takahashi, T. (2003) An application of Gröbner bases for a hierarchical defining equation of singularity. preprint.

[10] Weispfenning, V. (1992). Comprehensive Gröbner bases. *J. Symb. Comput.*, **14**, 1-29.

[11] Weispfenning, V. (2002). Canonical comprehensive Gröbner bases. In: *ISSAC 2002*, ACM Press, pp.270-276.

List of MHF Preprint Series, Kyushu University

21st Century COE Program
Development of Dynamic Mathematics with High Functionality

MHF

2003-1 Mitsuhiro T. NAKAO, Kouji HASHIMOTO & Yoshitaka WATANABE
A numerical method to verify the invertibility of linear elliptic operators with applications to nonlinear problems

2003-2 Masahisa TABATA & Daisuke TAGAMI
Error estimates of finite element methods for nonstationary thermal convection problems with temperature-dependent coefficients

2003-3 Tomohiro ANDO, Sadanori KONISHI & Seiya IMOTO
Adaptive learning machines for nonlinear classification and Bayesian information criteria

2003-4 Kazuhiro YOKOYAMA
On systems of algebraic equations with parametric exponents