On the radical of a polynomial ideal with parameters

Ryosuke Kuramochi[1], Kazuki Tanaka[2], and Katsusuke Nabeshima[3]

[1] Graduate School of Science, Tokyo University of Science,
1-3, Kagurazaka, Shinjuku, Tokyo, Japan
1422513@ed.tus.ac.jp
[2] Graduate School of Science, Tokyo Metropolitan University,
1-1, Minamiosawa, Hachioji, Tokyo, Japan
tanaka-kazuki@ed.tmu.ac.jp
[3] Department of Applied Mathematics, Tokyo University of Science,
1-3, Kagurazaka, Shinjuku, Tokyo, Japan
nabeshima@rs.tus.ac.jp

Abstract. A parametric radical system is introduced as a new concept within parametric ideals. It is demonstrated that an algorithm for computing the radical of a non-parametric ideal can be generalized to its parametric version by utilizing several tools related to parametric ideals. The keys to this generalization are two types of comprehensive Gröbner systems.

Keywords: radical · comprehensive Gröbner system · parametric radical system.

1 Introduction

One of the major advantages of symbolic computation is its capability to precisely handle ideals with parameters, known as parametric ideals. For instance, a comprehensive Gröbner system (CGS) and quantifier elimination method (QE) are highly effective tools for analyzing parametric ideals. However, there is a scarcity of convenient tools and implementations specifically tailored for parametric ideals. There is a pressing need to develop numerous algorithms for analyzing parametric ideals.

In this paper, we investigate the computation of radicals for a parametric ideal, introducing a *parametric radical system* as a novel concept within parametric ideals in the realm of symbolic computation. The primary contribution of this study is the provision of an algorithm for computing a radical system of a parametric ideal.

In 1988, Gianni-Trager-Zacharias introduced an algorithm for computing the radical of an ideal, along with an algorithm for computing primary decomposition [4]. Currently, these algorithms are implemented in many computer algebra systems. However, there is a lack of algorithms and implementations for parametric ideals. The purpose of this paper is to generalize the algorithm presented by Gianni-Trager-Zacharias to parametric cases. We demonstrate that two types of comprehensive Gröbner systems are necessary for this generalization.

This paper is organized as follows: In Section 2, we review comprehensive Gröbner systems. In Section 3, we present several tools for parametric ideals. In Section 4, we introduce a parametric radical system as a new concept within parametric ideals. In Section 5, we describe an algorithm for computing a parametric radical system of a zero-dimensional ideal. In Section 6, we present the key result of this paper, which is a special type of comprehensive Gröbner system. Finally, in Section 7, we provide an algorithm for computing a parametric radical system of a non-zero-dimensional ideal.

2 Comprehensive Gröbner systems

Here we briefly recall comprehensive Gröbner systems that will be frequently used in this paper. We refer the reader to [5,6,7,8,10,12,13].

2.1 Preliminaries

Let $x = \{x_1, \ldots, x_n\}$, $t = \{t_1, \ldots, t_m\}$ and $u = \{u_1, \ldots, u_\rho\}$ be sets of variables, K a field with characteristic 0 and $\overline{K}$ an algebraic closed extension of K. (We often regard t as parameters.) Moreover, let $K(u)$ be a field of rational functions with u and $\overline{K(u)}$ an algebraic closed extension of $K(u)$. Symbols $\mathit{Term}(t)$, $\mathit{Term}(x)$ and $\mathit{Term}(t,x)$ mean the set of terms of t, the set of terms of x and the set of terms of $t \cup x$, respectively.

In what follow, we fix $L = K$ or $K(u)$.

Fix a term order $\prec$ on $\mathit{Term}(x)$ and let $f \in L[t][x]$. Then $\mathrm{lt}(f), \mathrm{lm}(f)$ and $\mathrm{lc}(f)$ denote the leading term, leading monomial and leading coefficient of f i.e. $\mathrm{lm}(f) = \mathrm{lc}(f)\,\mathrm{lt}(f)$. For $F \subset L[t][x]$ and $f_1, \ldots, f_\nu \in L[t][x]$, $\mathrm{lt}(F) = \{\mathrm{lt}(f) | f \in F\}$ and $\langle f_1, \ldots, f_\nu \rangle = \{\sum_{i=1}^{\nu} h_i f_i | h_1, \ldots, h_\nu \in L[t][x]\}$. The set of natural numbers $\mathbb{N}$ includes zero, $\mathbb{Q}$ is the field of rational numbers and $\mathbb{C}$ is the field of complex numbers.

For $g_1, \ldots, g_\ell \in L[t]$, $\mathbf{V}_{\overline{L}}(g_1, \ldots, g_\ell) \subset \overline{L}^m$ denotes the affine variety of $g_1, \ldots, g_\ell$, i.e. $\mathbf{V}_{\overline{L}}(g_1, \ldots, g_\ell) = \{\bar{t} \in \overline{L}^m | g_1(\bar{t}) = \cdots = g_\ell(\bar{t}) = 0\}$, and $\mathbf{V}_{\overline{L}}(0) = \overline{L}^m$. We call an algebraically constructible set of the form $\mathbf{V}_{\overline{L}}(f_1, \ldots, f_\ell) \backslash \mathbf{V}_{\overline{L}}(f'_1, \ldots, f'_{\ell'}) \subset \overline{L}^m$, a stratum where $f_1, \ldots, f_\ell, f'_1, \ldots, f'_{\ell'} \in L[t]$. As it is clear that $\mathbf{V}_{\overline{L}}(1) = \emptyset$, thus $\mathbf{V}_{\overline{L}}(f_1, \ldots, f_\ell) \backslash \mathbf{V}_{\overline{L}}(1) = \mathbf{V}_{\overline{L}}(f_1, \ldots, f_\ell)$. For $\bar{t} \in \overline{L}^m$, the canonical specialization homomorphism $\sigma_{\bar{t}} : L[t][x] \to \overline{L}[x]$ (or $L[t] \to \overline{L}$) is defined as the map that substitutes t by $\bar{t}$ in $f(t,x) \in L[t][x]$. The image $\sigma_{\bar{t}}$ of a set $F \subset L[t][x]$ is denoted by $\sigma_{\bar{t}}(F) = \{\sigma_{\bar{t}}(f) | f \in F\} \subset \overline{L}[x]$.

2.2 Comprehensive Gröbner systems

We adopt the following as a definition of comprehensive Gröbner system.

Definition 1. *Fix a term ordering $\prec$ on $\mathit{Term}(x)$. Let $F \subset L[t][x]$, $E_1, \ldots, E_s$, $N_1, \ldots, N_s \subset L[t]$, $G_1, \ldots, G_s \subset L[t][x]$. If a finite set $\mathcal{G} = \{(E_1, N_1, G_1), \ldots, (E_s, N_s, G_s)\}$ of triples satisfies the properties such that*

(i) for each i, $\mathbf{V}_{\overline{L}}(E_i) \backslash \mathbf{V}_{\overline{L}}(N_i) \neq \emptyset$,

(ii) for $i \neq j$, $\left(\mathbf{V}_{\overline{L}}(E_i)\backslash\mathbf{V}_{\overline{L}}(N_i)\right) \cap \left(\mathbf{V}_{\overline{L}}(E_j)\backslash\mathbf{V}_{\overline{L}}(N_j)\right) = \emptyset$, *and*

(iii) for all $\bar{t} \in \mathbf{V}_{\overline{L}}(E_i)\backslash\mathbf{V}_{\overline{L}}(N_i)$ *and* $g \in G_i$, $\mathrm{lt}(g) = \mathrm{lt}(\sigma_{\bar{t}}(g))$ *and* $\{\sigma_{\bar{t}}(g)/\sigma_{\bar{t}}(\mathrm{lc}(g)) | g \in G_i\}$ *is a minimal Gröbner basis of* $\langle \sigma_{\bar{t}}(F)\rangle$ *in* $\overline{L}^m[x]$,

then $\mathcal{G}$ *is called a comprehensive Gröbner system (CGS) of* $\langle F\rangle$ *over* $\overline{L}$ *w.r.t.* $\prec$ *on* $\bigcup_{i=1}^{s}\left(\mathbf{V}_{\overline{L}}(E_i)\backslash\mathbf{V}_{\overline{L}}(N_i)\right)$. *We call a triple* (E_i, N_i, G_i) *segment of* $\mathcal{G}$. *We simply say that* $\mathcal{G}$ *is a comprehensive Gröbner system (CGS) of* $\langle F\rangle$ *over* $\overline{L}$ *w.r.t.* $\prec$ *if* $\bigcup_{i=1}^{s}\left(\mathbf{V}_{\overline{L}}(E_i)\backslash\mathbf{V}_{\overline{L}}(N_i)\right) = \overline{L}^m$.

There exist several algorithms and implementations for computing the CGS for $L = \mathbb{Q}$ ($\mathbb{R}$ or $\mathbb{C}$) [5,6,7,8,10].

Remark 1. There always exists a CGS $\mathcal{G}$ of $\langle F\rangle \subset L[t][x]$ over $\overline{L}$ such that $\mathcal{G}$ forms $\mathcal{G} = \bigcup_{i=1}^{s}\{(E_i, \{p_i\}, G_i)\}$ where $p_1, \ldots, p_s \in L[t]$, $E_1, \ldots, E_s \subset L[t]$, and $G_1, \ldots, G_s \subset L[t][x]$ i.e. N_i has one polynomial p_i. See [5,6]. Since this form makes the discussion easier, we adopt the form for all CGSs of this paper.

Example 1. Let $F = \{ax^3y^2 + y^2 + x^2y, x^4y + bxy\} \subset \mathbb{C}[a,b][x,y]$ where a, b are parameters. Let $\prec$ be the lexicographic term order with $y \prec x$. Then, a CGS $\mathcal{G}$ of $\langle F\rangle$ over $\mathbb{C}$ w.r.t. $\prec$ is $\mathcal{G} = \{(\{b\}, \{1\}, \{y^3, x^2y + y^2\}), (\{ab - 1\}, \{1\}, \{y^2, xy\}), (\{0\}, \{ab^2 - b\}, G_3)\}$ where $G_3 = \{(a^3b^3 - 3a^2b^2 + 3ab - 1)y^5 - b^2y^2, bxy + (a^2b^2 - 2ab + 1)y^3\}$. The set $\mathcal{G}$ means the following:

- if (a, b) belongs to $\mathbf{V}_{\mathbb{C}}(b)$ (i.e. $b = 0$), then $\{y^3, x^2y + y^2\}$ is a minimal Gröbner basis of $\langle F\rangle$ w.r.t. $\prec$,
- if (a, b) belongs to $\mathbf{V}_{\mathbb{C}}(ab - 1)$ (i.e. $ab - 1 = 0$), then $\{y^2, xy\}$ is a minimal Gröbner basis of $\langle F\rangle$ w.r.t. $\prec$, and
- if (a, b) belongs to $\mathbb{C}^2\backslash\mathbf{V}_{\mathbb{C}}(ab^2 - b)$, then G_3 is a minimal Gröbner basis of $\langle F\rangle$ w.r.t. $\prec$.

Next, let us consider the case $L = K(u)$. It is possible to compute a CGS on $\overline{K(u)}^m$ by utilizing the algorithms that are introduced in [5,6,7,10]. The algorithm has been implemented in the computer algebra system Risa/Asir [11].

Example 2. Let $F = \{3u_1x^2 + 2axy, ax^2 + 3u_2y^2\} \subset \mathbb{C}(u_1, u_2)[a][x, y]$ where a is a parameter and x, y are variables. Let $\prec$ be the graded lexicographic term order with $y \prec x$. Then, a comprehensive Gröbner system $\mathcal{G}$ of $\langle F\rangle$ w.r.t. $\prec$ is the following:

$$\begin{aligned}\mathcal{G} = \{&(\{0\}\{(4u_1a^3 + 27u_1^3u_2)a\}, \{y^3, 3u_1x^2 + 2axy, 2a^2xy - 9u_1u_2y^2\}),\\ &(\{a\}, \{1\}, \{x^2, y^2\}), (\{4u_1a^3 + 27u_1^3u_2\}, \{1\}, \{3u_1xy + 2ay^2, 9u_1^2x^2 - 4a^2y^2\})\}.\end{aligned}$$

This output means the following:

- if the parameter a belongs to $\overline{L}^2\backslash\mathbf{V}_{\overline{L}}((4u_1a^3 + 27u_1^3u_2)a)$ (i.e. $(4u_1a^3 + 27u_1^3u_2)a \neq 0$), then $\{y^3, 3u_1x^2 + 2axy, 2a^2xy - 9u_1u_2y^2\}$ is a minimal Gröbner basis of $\langle F\rangle$ w.r.t. $\prec$,
- if the parameter a belongs to $\mathbf{V}_{\overline{L}}(a)$ (i.e. $a = 0$), then $\{x^2, y^2\}$ is a minimal Gröbner basis of $\langle F\rangle$ w.r.t. $\prec$, and
- if the parameter a belongs to $\mathbf{V}_{\overline{L}}(4u_1a^3 + 27u_1^3u_2)$, then $\{3u_1xy + 2ay^2, 9u_1^2x^2 - 4a^2y^2\}$ is a minimal Gröbner basis of $\langle F\rangle$ w.r.t. $\prec$,

where $L = \mathbb{C}(u_1, u_2)$.

3 Tools for parametric ideals

In order to compute a radical of a parametric ideal, we need to compute the followings:

(1) Dimensions of a parametric ideal,
(2) Squarefree-part of a univariate polynomial with parameters,
(3) Intersection of parametric ideals,
(4) Least common multiples of parametric polynomials, and
(5) Saturation for a parametric ideal.

Here, we introduce these computational methods.

3.1 Dimensions of a parametric ideal

For a finite subset u, the cardinality of u is written by $|u|$.

Definition 2. *Let I be a proper ideal in $K[x]$ and $u = \{u_1, \ldots, u_r\}$ a subset of x. Then, u is called an independent set modulo I if $I \cap K[u] = \{0\}$. The dimension* $\dim(I)$ *is defined as*

$$\dim(I) = \max\{|u| | u \subseteq x \textit{ is an independet set modulo } I\}.$$

Moreover, $u \subset x$ is called a maximal independent set (MIS) modulo I if it is an independent set modulo I and the cardinality of u is equal to $\dim(I)$.

Algorithms, introduced in [2,3], for computing a MIS modulo I are based on the following theorem.

Theorem 1 ([2, p.448]). *Let I be a proper ideal in $K[x]$ and G a Gröbner basis of I w.r.t. a graded degree term order. Then,* $\dim(I) = \dim(\langle \mathrm{lt}(G) \rangle)$.

By utilizing a CGS of a parametric ideal, the parameter dependence of the dimensions can be obtained as follows.

Algorithm 1 (Dimensions of parametric ideal)

Specification: PARA_DIM(F)
Computation of dimensions of parametric ideal $\langle F \rangle$.
Input: $F \subset K[t][x]$ finite set.
Output: $(\mathcal{Z}, \mathcal{N}, \mathcal{W})$: $\mathcal{Z} = \{(E_1, \{p_1\}, G_1), \ldots, (E_\ell, \{p_\ell\}, G_\ell)\}$, $\mathcal{N} = \{(E'_1, \{p'_1\}, G'_1), \ldots, (E'_{\ell'}, \{p'_{\ell'}\}, G'_{\ell'})\}$, $\mathcal{W} = \{(D_1, \{h_1\}, H_1), \ldots, (D_s, \{h_s\}, H_s)\}$. For each $1 \le i \le \ell$, $\forall \bar{a} \in \mathbf{V}_{\overline{K}}(E_i) \backslash \mathbf{V}_{\overline{K}}(p_i)$, $\dim(\langle \sigma_{\bar{a}}(G_i) \rangle) = 0$. For each $1 \le j \le \ell'$, $\forall \bar{b} \in \mathbf{V}_{\overline{K}}(E'_j) \backslash \mathbf{V}_{\overline{K}}(p'_j)$, $\dim(\langle \sigma_{\bar{b}}(G'_j) \rangle) \neq 0$. For each $1 \le k \le s$, $\forall \bar{c} \in \mathbf{V}_{\overline{K}}(D_k) \backslash \mathbf{V}_{\overline{K}}(h_k)$, $\langle \sigma_{\bar{c}}(H_k) \rangle$ is not proper where $\overline{K}^m = \big(\bigcup_{i=1}^{\ell} \mathbf{V}_{\overline{K}}(E_i) \backslash \mathbf{V}_{\overline{K}}(p_i)\big) \cup \big(\bigcup_{j=1}^{\ell'} \mathbf{V}_{\overline{K}}(E'_j) \backslash \mathbf{V}_{\overline{K}}(p'_j)\big) \cup \big(\bigcup_{k=1}^{s} \mathbf{V}_{\overline{K}}(D_k) \backslash \mathbf{V}_{\overline{K}}(h_k)\big)$.
BEGIN
$\mathcal{Z} \leftarrow \emptyset$; $\mathcal{N} \leftarrow \emptyset$; $\mathcal{W} \leftarrow \emptyset$; $\prec \leftarrow$ A graded degree term order;
$\mathcal{G} \leftarrow$ Compute a CGS of $\langle F \rangle$ over $\overline{K}$ w.r.t. $\prec$;
for each $(E, \{p\}, G) \in \mathcal{G}$ **do**

if $G = \{1\}$ or $G = \{0\}$ **then**
 $\mathcal{W} \leftarrow \mathcal{W} \cup \{(E, \{p\}, G)\}$; /*$\langle G \rangle$ is not proper */
else if a MIS modulo $\langle \mathrm{lt}(G) \rangle$ is $\emptyset$ **then**
 $\mathcal{Z} \leftarrow \mathcal{Z} \cup \{(E, \{p\}, G)\}$; /*$\dim(\langle G \rangle) = 0$ */
else
 $\mathcal{N} \leftarrow \mathcal{N} \cup \{(E, \{p\}, G)\}$; /*$\dim(\langle G \rangle) \neq 0$ */
end-if
end-for
return $(\mathcal{Z}, \mathcal{N}, \mathcal{W})$;
END

According to the definition of CGS and Theorem 1, Algorithm 1 is guaranteed to work correctly.

3.2 Squarefree part of a univariate polynomial with parameters

Here, we present an algorithm for computing the squarefree parts of a univariate polynomial with parameters.

Let x_i be a variable in x. Let $f = \prod_{1 \leq j \leq \ell} f_j^{e_j}$ be the irreducible factorization of the monic polynomial $f \in K[x_i]$, with distinct monic irreducible $f_1, \ldots, f_\ell$ and positive $e_1, \ldots, e_r \in \mathbb{N}$. We define the squarefree part $\sqrt{f}$ of f to be $\prod_{1 \leq j \leq \ell} f_j$. It is well-known that $\sqrt{f} = f/\gcd(f, \frac{\partial f}{\partial x_i})$ for the field K of characteristic zero where $\gcd(f, \frac{\partial f}{\partial x_i})$ is the greatest common divisor of f and $\frac{\partial f}{\partial x_i}$ in $K[x_i]$.

For parametric polynomials in $K[t][x_i]$, it is convenient to replace the usual division with remainder by using a well-known pseudo-division method, which computes $q, r \in K[t][x_i]$ from $f, g \in K[t][x_i]$ $(g \neq 0)$ such that

$$\mathrm{lc}(g)^{1+\deg(f)-\deg(g)} f = qg + r, \text{ where } \deg(r) < \deg(g).$$

Note that for $f \in K[t][x_i]$, we can obtain the (parametric) greatest common divisors of f and $\frac{\partial f}{\partial x_i}$ by computing a comprehensive Gröbner system of $\langle f, \frac{\partial f}{\partial x_i} \rangle$. Therefore, by combining pseudo-division with the comprehensive Gröbner system, we present the following algorithm for computing the squarefree parts of a univariate polynomial with parameters.

Algorithm 2 (Squarefree parts of a univariate polynomial)

Specification: SQUARE_FREE(E, p, f, x_i)
Computation of squarefree parts of a univariate polynomial with parameters.
Input: $E \subset K[t]$: finite set, $p \in K[t]$, $f \in K[t][x_i]$, $x_i \in x$.
For all $\bar{t} \in \mathbf{V}_{\overline{K}}(E) \backslash \mathbf{V}_{\overline{K}}(p)$, $\sigma_{\bar{t}}(f) \neq 0$. $(\mathrm{char}(K) = 0)$
Output: $\mathcal{P} = \{(E_1, \{p_1\}, h_1), \ldots, (E_\ell, \{p_\ell\}, h_\ell)\}$: For all $\bar{t} \in \mathbf{V}_{\overline{K}}(E_i) \backslash \mathbf{V}_{\overline{K}}(p_i)$ $(1 \leq i \leq \ell)$, $\sigma_{\bar{t}}(h_i)/\sigma_{\bar{t}}(\mathrm{lc}(h_i))$ is the squarefree part of $\sigma_{\bar{t}}(f)/\mathrm{lc}(\sigma_{\bar{t}}(f))$ where $\mathbf{V}_{\overline{K}}(E) \backslash \mathbf{V}_{\overline{K}}(p) = \bigcup_{i=1}^{\ell} \big(\mathbf{V}_{\overline{K}}(E_i) \backslash \mathbf{V}_{\overline{K}}(p_i)\big)$.
BEGIN
$\mathcal{P} \leftarrow \emptyset$; $\mathcal{G} \leftarrow$ Compute a CGS of $\langle f, \frac{\partial f}{\partial x_i} \rangle$ over $\overline{K}$ on $\mathbf{V}_{\overline{K}}(E) \backslash \mathbf{V}_{\overline{K}}(p)$;

for each $(E', \{p'\}, \{g\}) \in \mathcal{G}$ **do**
  $q \leftarrow$ Compute q s.t. $\mathrm{lc}(g)^{1+\deg(f)-\deg(g)} f = qg + r \quad (\deg(r) < \deg(g))$;
  (by pseudo-division)
  $\mathcal{P} \leftarrow \mathcal{P} \cup \{(E', \{p'\}, q)\}$
end-for
return $\mathcal{P}$;
END

Theorem 2. *Algorithm 2 works correctly.*

Proof. Let us consider $(E', \{p'\}, \{g\})$ in the **while-loop**. Since, for all $\bar{t} \in \mathbf{V}_{\overline{K}}(E') \setminus \mathbf{V}_{\overline{K}}(p')$, $\{\sigma_{\bar{t}}(g)/\mathrm{lc}(\sigma_{\bar{t}}(g))\}$ is the minimal Gröbner basis of $\langle \sigma_{\bar{t}}(f), \sigma_{\bar{t}}(\frac{\partial f}{\partial x_i})\rangle$ in $\overline{K}[x_i]$, hence $\sigma_{\bar{t}}(g)/\ \mathrm{lc}(\sigma_{\bar{t}}(g))$ is the greatest common divisor of $\sigma_{\bar{t}}(f)$ and $\sigma_{\bar{t}}(\frac{\partial f}{\partial x_i})$. As $\overline{K}$ is a filed, we have $\sigma_t(g)|\sigma_{\bar{t}}(f)$. By the pseudo-division, there exists $q, r \in K[t][x_i]$ such that

$$\mathrm{lc}(g)^{1+\deg(f)-\deg(g)} f = qg + r \quad (\deg(r) < \deg(g)).$$

Hence the fact $\sigma_t(g)|\sigma_{\bar{t}}(f)$ implies $\sigma_{\bar{t}}(r) = 0$, namely,

$$\sigma_{\bar{t}}(\mathrm{lc}(g)^{1+\deg(f)-\deg(g)})\sigma_{\bar{t}}(f) = \sigma_{\bar{t}}(q)\sigma_{\bar{t}}(g) + \sigma_{\bar{t}}(r) = \sigma_{\bar{t}}(q)\sigma_{\bar{t}}(g).$$

Therefore, $\sigma_{\bar{t}}(q)/\sigma_{\bar{t}}(\mathrm{lc}(q))$ is the squarefree part of $\sigma_{\bar{t}}(f)/\ \mathrm{lc}(\sigma_{\bar{t}}(f))$. □

3.3 Intersection of parametric ideals

Here we present an algorithm for computing an intersection of parametric ideals in $K[x]$.

Theorem 3 ([3, Theorem 11]). *Let $I = \langle f_1, \ldots, f_r\rangle$ and $J = \langle g_1, \ldots, g_\ell\rangle$ be ideals in $K[x]$, and G a Gröbner basis of $\langle wf_1, \ldots, wf_r, (1-w)g_1, \ldots, (1-w)g_\ell\rangle$ in $K[x, w]$ w.r.t. a block term order $x \ll w$ on Term$(x \cup \{w\})$ where w is an auxiliary variable. Then, $I \cap J = \langle G \cap K[x]\rangle$.*

Essentially, by substituting the Gröbner basis with the CGS in the theorem mentioned above, we can compute the intersection of parametric ideals as follows.

Algorithm 3 (Intersection of parametric ideals)

Specification:PARA_INTERSECTION(E, p, F, G)
  Computation of intersections of two parametric ideals.
Input: $E \subset K[t]$: finite set, $p \in K[t]$, $F, G \subset K[t][x]$: finite sets.
Output: $\mathcal{P} = \{(E_1, \{p_1\}, G_1), (E_2, \{p_2\}, G_2), \ldots, (E_\ell, \{p_\ell\}, G_\ell)\}$: For all $\bar{t} \in \mathbf{V}_{\overline{K}}(E_i) \setminus \mathbf{V}_{\overline{K}}(p_i) \subset \overline{K}^m$ $(1 \leq i \leq \ell)$, $\langle \sigma_{\bar{t}}(F)\rangle \cap \langle \sigma_{\bar{t}}(G)\rangle = \langle \sigma_{\bar{t}}(G_i)\rangle$ where $\mathbf{V}_{\overline{K}}(E) \setminus \mathbf{V}_{\overline{K}}(p) = \bigcup_{i=1}^{\ell} \left(\mathbf{V}_{\overline{K}}(E_i) \setminus \mathbf{V}_{\overline{K}}(p_i)\right)$.
BEGIN
$I \leftarrow \langle \{wf | f \in F\} \cup \{(1-w)g | g \in G\}\rangle$ where w is an auxiliary variable;
$\prec \leftarrow$ A block term order with $x \ll w$ on Term$(x \cup \{w\})$;
$\mathcal{G} \leftarrow$ Compute a CGS of I over $\overline{K}$ on $\mathbf{V}_{\overline{K}}(E) \setminus \mathbf{V}_{\overline{K}}(p)$ w.r.t. $\prec$ in $K[t][x \cup \{w\}]$;

$\mathcal{P} \leftarrow \{(E', \{p'\}, G' \cap K[t][x]) \mid (E', \{p'\}, G') \in \mathcal{G}\}$;
return $\mathcal{P}$;
END

According to the definition of CGS and Theorem 3, Algorithm 3 is guaranteed to work correctly.

3.4 Least common multiples of parametric polynomials

An algorithm for computing the least common multiple of polynomials in $K[x]$ is provided in [3], based on the following proposition.

Proposition 1 ([3, Proposition 13]).

(i) The intersection $I \cap J$ of two principal ideals, $I, J \subset K[x]$ is a principal ideal.
(ii) If $I = \langle f \rangle$, $J = \langle g \rangle$ and $I \cap J = \langle h \rangle$ in $K[x]$, then h is the least common multiple of f and g i.e. $h = \mathrm{lcm}\{f, g\}$.

Combining this proposition with Algorithm 3 yields an algorithm for computing the least common multiples of parametric polynomials, as follows.

Algorithm 4 (Least common multiples of parametric polynomials)

Specification:PARA_LCM(E, p, F**)**
Least common multiples of parametric polynomials.
Input: $E \subset K[t]$: finite set, $p \in K[t]$, $F \subset K[t][x]$: finite set.
Output: $\{(E_1, \{p_1\}, \{g_1\}), \ldots, (E_\ell, \{p_\ell\}, \{g_\ell\})\}$: For all $\bar{t} \in \mathbf{V}_{\overline{K}}(E_i) \backslash \mathbf{V}_{\overline{K}}(p_i)$ $(1 \leq i \leq \ell), \mathrm{lcm}\{\sigma_{\bar{t}}(F)\} = \sigma_{\bar{t}}(g_i)$ where $\mathbf{V}_{\overline{K}}(E) \backslash \mathbf{V}_{\overline{K}}(p) = \bigcup_{i=1}^{\ell} \left(\mathbf{V}_{\overline{K}}(E_i) \backslash \mathbf{V}_{\overline{K}}(p_i)\right)$.
BEGIN
$\mathcal{G} \leftarrow \emptyset$; $f \leftarrow$ Select one polynomial f from F; $F \leftarrow F \setminus \{f\}$;
$\mathcal{H} \leftarrow \{(E, \{p\}, \{f\})\}$;
for each $h \in F$ **do**
  for each $(E', \{p'\}, \{f'\}) \in \mathcal{H}$ **do**
    $\mathcal{L} \leftarrow$**PARA_INTERSECTION**$(E', p', \{f'\}, \{h\})$; $\mathcal{G} \leftarrow \mathcal{G} \cup \mathcal{L}$;
  end-for
  $\mathcal{H} \leftarrow \mathcal{G}$;
end-for
return $\mathcal{H}$;
END

3.5 Saturation for a parametric ideal

Here, we introduce how to compute saturation for a parametric ideal .

Definition 3. *Let I be an ideal in $K[x]$ and $f \in K[x]$.*

(1) $I : f = \{g \in K[x] | gf \in I\}$.

(2) For the ideal I, the saturation w.r.t. f is defined by the ideal $I : f^\infty = \bigcup_{k\geq 1}(I : f^k)$.

Proposition 2 ([2, Proposition 6.37]). *Let $I = \langle f_1, \ldots, f_r\rangle$ and $f \in K[x]$. Set $J = \langle f_1, \ldots, f_r, 1 - wf\rangle$ where w is an auxiliary variable. Then, $I : f^\infty = J \cap K[x]$.*

Let G be a Gröbner basis of J w.r.t. a block term order with $x \ll w$. Then, by the proposition above, $G \cap K[x]$ becomes a basis of the ideal $I : f^\infty$.

For parametric ideals, we can extend the method described above to $K[t][x]$ by substituting the Gröbner basis with the CGS, as follows.

Algorithm 5 (Saturation for a parametric ideal)

Specification:PARA_SAT($E, p, F, f, \prec$)
Computation of the saturation $\langle F\rangle : f^\infty$.
Input: $E \subset K[t]$: finite set, $p \in K[t]$, $F \subset K[t][x]$: finite set, $f \in K[t][x]$,
$\prec$: term order on $Term(x)$.
Output: $\{(E_1, \{p_1\}, G_1), (E_2, \{p_2\}, G_2), \ldots, (E_\ell, \{p_\ell\}, G_\ell)\}$: For all $\bar{t} \in \mathbf{V}_{\overline{K}}(E_i) \backslash\mathbf{V}_{\overline{K}}(p_i)$ $(1 \leq i \leq \ell)$, $\sigma_{\bar{t}}(G_i)$ is a basis of $\langle\sigma_{\bar{t}}(F)\rangle : \sigma_{\bar{t}}(f)^\infty$ where $\mathbf{V}_{\overline{K}}(E)\backslash\mathbf{V}_{\overline{K}}(p) = \bigcup_{i=1}^{\ell} \left(\mathbf{V}_{\overline{K}}(E_i)\backslash\mathbf{V}_{\overline{K}}(p_i)\right)$.
BEGIN
$I \leftarrow \langle F \cup \{1 - wf\}\rangle \subset K[t][x, w]$ where w is an auxiliary variable;
$\prec' \leftarrow$ A block term order, with $x \ll w$ and $\prec$, on $Term(x \cup \{w\})$;
$\mathcal{G} \leftarrow$ Compute a CGS of I over $\overline{K}$ w.r.t. $\prec'$ on $\mathbf{V}_{\overline{K}}(E)\backslash\mathbf{V}_{\overline{K}}(p)$;
$\mathcal{P} \leftarrow \{(E', \{p'\}, G' \cap K[t][x]) \mid (E', \{p'\}, G') \in \mathcal{G}\}$;
return $\mathcal{P}$;
END

---

4 Parametric radical system

The aim of this paper is to develop an algorithm for computing the radical system of a parametric ideal.

Definition 4. *Let $I \subset L[x]$ be an ideal (where $L = K$ or $K(u)$). The radical of I, denoted $rad_{L[x]}(I)$, is the set $\{f | f^r \in I$ for some integer $r \geq 1\}$. I is called a radical ideal if $I = rad_{L[x]}(I)$.*

In this paper, we extend the algorithm introduced by Gianni-Trager-Zacharias in [4] for computing the radical of an ideal to its parametric version. We achieve this by utilizing two types of comprehensive Gröbner systems.

We define the radical of a parametric ideal as follows.

Definition 5. *Fix a term order $\prec$ on $Term(x)$. Let $E_1, E_2, \ldots, E_s \subset K[t]$, $N_1, N_2, \ldots, N_s \in K[t]$ and $F, G_1, G_2, \ldots, G_s \subset K[t][x]$. If a finite set*

$$\mathcal{G} = \{(E_1, N_1, G_1), (E_2, N_2, G_2), \ldots, (E_s, N_s, G_s)\}$$

of triples satisfies the properties such that

- *for each* i, $\mathbf{V}_{\overline{K}}(E_i)\backslash\mathbf{V}_{\overline{K}}(N_i) \neq \emptyset$,
- *for* $i \neq j$, $\left(\mathbf{V}_{\overline{K}}(E_i)\backslash\mathbf{V}_{\overline{K}}(N_i)\right) \cap \left(\mathbf{V}_{\overline{K}}(E_j)\backslash\mathbf{V}_{\overline{K}}(N_j)\right) = \emptyset$, *and*
- *for all* $\bar{t} \in \mathbf{V}_{\overline{K}}(E_i)\backslash\mathbf{V}_{\overline{K}}(N_i)$, $\sigma_{\bar{t}}(G_i)$ *is a basis of* $rad_{\overline{K}[x]}(\langle\sigma_{\bar{t}}(F)\rangle)$ *in* $\overline{K}[x]$,

then, $\mathcal{G}$ *is called a parametric radical system (PRS) of* $\langle F\rangle$ *on* $\bigcup_{i=1}^{s}\left(\mathbf{V}_{\overline{K}}(E_i)\backslash\mathbf{V}_{\overline{K}}(N_i)\right)$. *We call a triple* (E_i, N_i, G_i) *segment of* $\mathcal{G}$. *We simply say* $\mathcal{G}$ *is a parametric radical system of* $\langle F\rangle$ *if* $\bigcup_{i=1}^{s}\left(\mathbf{V}_{\overline{K}}(E_i)\backslash\mathbf{V}_{\overline{K}}(N_i)\right) = \overline{K}^m$

In Section 5, we explore the computation of a parametric radical system for a zero-dimensional ideal. In Section 6 we introduce a specialized type of comprehensive Gröbner system commonly employed for computing a parametric radical system for non-zero dimensional ideals. Finally, in Section 7, we present an algorithm for computing a parametric radical system for non-zero dimensional ideals.

5 Zero dimensional case

Here, we present an algorithm for computing a parametric radical system of a zero dimensional ideal with parameters. This algorithm is essentially based on the following lemma.

Lemma 1 ([2, Lemma 8.19]). *Let* $I = \langle f_1, \ldots, f_r\rangle$ *be a zero dimensional ideal in* $K[x]$. *For* $1 \leq i \leq n$, *let* g_i *be the unique monic polynomial of minimal degree in* $I \cap K[x_i]$. *Then,* $rad_{K[x]}(\langle F\rangle) = \langle f_1, \ldots, f_r, \sqrt{g_1}, \ldots, \sqrt{g_n}\rangle$ *where* $\sqrt{g_i}$ *is the squarefree part of* g_i.

If I is a zero dimensional ideal on $\mathbf{V}_{\overline{K}}(E)\backslash\mathbf{V}_{\overline{K}}(p)$ where $E \subset K[t]$ and $p \in K[t]$, then, for each $x_i \in x$, the parametric univariate polynomial g_i can be obtained by computing a CGS w.r.t. a elimination term order. After obtaining g_i, **SQUARE_FREE**(E, p, g_i, x_i) outputs squarefree parts of the parametric univariate polynomial g_i on $\mathbf{V}_{\overline{K}}(E)\backslash\mathbf{V}_{\overline{K}}(p)$.

Algorithm 6 (Parametric radical system of a zero dim. ideal)

Specification: PRS_ZERO(E, p, F**)**
  Computation of a parametric radical system of a zero dim. ideal $\langle F\rangle$.
Input: $E \subset K[t]$: finite set, $p \in K[t]$, $F \subset K[t][x]$ finite set.
  (For all $\bar{t} \in \mathbf{V}_{\overline{K}}(E)\backslash\mathbf{V}_{\overline{K}}(p)$, $\dim(\langle\sigma_{\bar{t}}(F)\rangle) = 0$.)
Output: $\mathcal{P}$: parametric radical system of $\langle F\rangle$ on $\mathbf{V}_{\overline{K}}(E)\backslash\mathbf{V}_{\overline{K}}(p)$.
BEGIN
$\mathcal{P} \leftarrow \{(E, \{p\}, F)\}$;
for each $i = 1$ to n **do** /*n variables */
  $\mathcal{H} \leftarrow \emptyset$; $\prec\leftarrow$ Set a block term order with $x_i \ll x\backslash\{x_i\}$;
  $\mathcal{G} \leftarrow$ Compute a CGS of $\langle F\rangle$ over $\overline{K}$ w.r.t $\prec$ on $\mathbf{V}_{\overline{K}}(E)\backslash\mathbf{V}_{\overline{K}}(p)$;
  for each $(E', \{p'\}, G') \in \mathcal{G}$ **do**
    $g \leftarrow$ Select the polynomial g of minimal degree in $G' \cap K[t][x_i]$
    $\mathcal{B} \leftarrow$**SQUARE_FREE**(E', p', g, x_i);
    for each $(E'', \{h\}, b) \in \mathcal{B}$ **do**

for each $(D,\{d\},H)\in\mathcal{W}$ **do**
  if $(\mathbf{V}_{\overline{K}}(E'')\backslash\mathbf{V}_{\overline{K}}(h))\cap(\mathbf{V}_{\overline{K}}(D)\backslash\mathbf{V}_{\overline{K}}(d))\neq\emptyset$ **then**
    $\mathcal{H}\leftarrow\mathcal{H}\cup\{(E''\cup D,\{\sqrt{hd}\},H\cup\{b\})\}$;
  end-if
end-for
end-for
end-for
$\mathcal{P}\leftarrow\mathcal{H}$;
end-for
return $\mathcal{P}$;
END

Remark 2. Let us consider $(\mathbf{V}_{\overline{K}}(E'')\backslash\mathbf{V}_{\overline{K}}(h))\cap(\mathbf{V}_{\overline{K}}(D)\backslash\mathbf{V}_{\overline{K}}(d))$. Then,

$$\begin{aligned}(\mathbf{V}_{\overline{K}}(E'')\backslash\mathbf{V}_{\overline{K}}(h))\cap(\mathbf{V}_{\overline{K}}(D)\backslash\mathbf{V}_{\overline{K}}(d)) &= (\mathbf{V}_{\overline{K}}(E'')\cap\mathbf{V}_{\overline{K}}(D))\setminus(\mathbf{V}_{\overline{K}}(h)\cup\mathbf{V}_{\overline{K}}(d))\\ &= \mathbf{V}_{\overline{K}}(E''\cup D)\backslash\mathbf{V}_{\overline{K}}(hd).\end{aligned}$$

Thus, if $rad_{K[x]}(\langle E''\cup D\rangle)\ni hd$, we have $(\mathbf{V}_{\overline{K}}(E'')\backslash\mathbf{V}_{\overline{K}}(h))\cap(\mathbf{V}_{\overline{K}}(D)\backslash\mathbf{V}_{\overline{K}}(d))=\emptyset$, otherwise, $(\mathbf{V}_{\overline{K}}(E'')\backslash\mathbf{V}_{\overline{K}}(h))\cap(\mathbf{V}_{\overline{K}}(D)\backslash\mathbf{V}_{\overline{K}}(d))\neq\emptyset$.

Notice that $\mathbf{V}_{\overline{K}}(hd)=\mathbf{V}_{\overline{K}}(\sqrt{hd})$, and we can replace $E''\cup D$ a Gröbner basis of $\langle E''\cup D\rangle$ or a basis of $rad_{K[t]}(E''\cup D)$.

Remark 3. To compute the univariate polynomials with parameters, we have developed an algorithm for computing the minimal polynomial modulo $\langle F\rangle$ with respect to x_i $(1\le i\le n)$. (For details on the minimal polynomials, please refer to [1].) However, our implementation of the (parametric) minimal polynomial is slower than our implementation of the CGS. As a result, we have utilized CGS computation to obtain the univariate polynomials.

Since Algorithm 6 is a natural generalization of Lemma 1 to parametric ideals, its correctness and termination are guaranteed by Lemma 1, **SQUARE_FREE**, and Remark 2.

Example 3. Let $F=\{x^2+axy,xy^2-bx+y\}\subset\mathbb{Q}[a,b][x,y]$ where a,b are parameters and x,y are variables. Then, **PARAZERO**(F) outputs $(\mathcal{Z},\emptyset,\emptyset)$ where $\mathcal{Z}=\{(\{0\},\{a\},\{bx+ay^3-y,x^2-a^2y^2,yx+ay^2\}),(\{a\},\{b\},\{y^2,bx-y\}),(\{a,b\},\{1\},\{x^2,y\})\}$.

This implies that for all $(a,b)\in\mathbb{C}^2$, $\langle F\rangle$ is zero dimensional. We execute Algorithm 6 for each segment.

(1): First we consider the case $(\mathbb{C}^2\setminus\mathbf{V}_{\mathbb{C}}(a),\{bx+ay^3-y,x^2-a^2y^2,yx+ay^2\})$ and set $F_1=\{bx+ay^3-y,x^2-a^2y^2,yx+ay^2\}$.

(1-1): A CGS of $\langle F_1\rangle$ over $\mathbb{C}$ w.r.t. the lexicographic term order $x\prec y$ on $\mathbb{C}^2\setminus\mathbf{V}_{\mathbb{C}}(a)$ is $\{\{0\},\{a\},\{x^4+(-a^2b-a)x^2,x^3-ba^2x+a^2y\}\}$. Take the univariate polynomial $x^4+(-a^2b-a)x^2$. Then,

$$\mathbf{SQUARE\_FREE}(\{0\},a,x^4+(-ba^2-a)x^2,x)$$

outputs

$\{(\{0\},\{a(ab+1)\},\{x^3+(-a^2b-a)x\}),(\{ab+1\},\{1\},\{x\})\}$.

Thus, we have $\mathcal{H}=\{(\{0\},\{a(ab+1)\},F_1\cup\{x^3+(-ba^2-a)x\}),(\{ab+1\},\{1\},F_1\cup\{x\})\}$.

(1-2): A CGS of $\langle F_1\rangle$ over $\mathbb{C}$ w.r.t. the lexicographic term order $y\prec x$ on $\mathbb{C}^2\setminus\mathbf{V}_{\mathbb{C}}(a)$ is $\mathcal{G}_y=\{(\{0\},\{ab\},\{ay^4+(-ab-1)y^2,-bx-ay^3+y\}),(\{b\},\{a\},\{ay^3-y,xy+ay^2,x^2-a^2y^2\})\}$. Take the univariate polynomial $ay^4+(-ab-1)y^2$ from the first segment of $\mathcal{G}_y$, and execute

SQUARE_FREE$(\{0\},ab,ay^4+(-ab-1)y^2,y)$.

Then, **SQUARE_FREE** outputs

$\{(\{0\},\{ab(ab+1)\},ay^3+(-ab-1)y),(\{ab+1\},\{1\},\{y\})\}$.

Thus, $\mathcal{H}$ is renewed as

$$\mathcal{H}=\{(\{0\},\{ab(ab+1)\},F_1\cup\{x^3+(-ba^2-a)x,ay^3+(-ab-1)y\}),\\ (\{ab+1\},\{1\},F_1\cup\{x,y\})\}.$$

Next, let us consider the second segment of $\mathcal{G}_y$. We take the univariate polynomial ay^3-y and apply the **SQUARE_FREE** algorithm with the inputs (b,a,ay^3-y,y). The output of **SQUARE_FREE** is (b,a,ay^3-y). Therefore, $\mathcal{H}$ is updated to

$$\mathcal{H}=\{(\{0\},\{ab(ab+1)\},F_1\cup\{x^3+(-a^2b-a)x,ay^3+(-ab-1)y\}),\\ (\{ab+1\},\{1\},F_1\cup\{x,y\}),(\{b\},\{a\},F_1\cup\{x^3+(-a^2b-a)x,ay^3-y\})\}.$$

(2) Second we consider the case $(\mathbf{V}_{\mathbb{C}}(a)\setminus\mathbf{V}_{\mathbb{C}}(b),\{y^2,bx-y\})$. As $b\neq 0$, clearly we obtain $\{(\{a\},\{b\},\{x,y\})\}$.

(3) Last we consider the case $(\mathbf{V}_{\mathbb{C}}(a,b),\{x^2,y\})$. Clearly, we obtain $\{(\{a,b\},\{1\},\{x,y\})\}$.

Therefore, the following is a parametric radical system of $\langle F\rangle$

$$\{(\{0\},\{ab(ab+1)\},F_1\cup\{x^3+(-a^2b-a)x,ay^3+(-ab-1)y\}),\\ (\{ab+1\},\{1\},F_1\cup\{x,y\}),(\{b\},\{a\},F_1\cup\{x^3+(-a^2b-a)x,ay^3-y\}),\\ (\{a\},\{b\},\{x,y\}),(\{a,b\},\{1\},\{x,y\})\}.$$

Note that each segment $(E,\{p\},G)$ of the parametric radical system above can be replaced a CGS of $\langle G\rangle$ on $\mathbf{V}_{\mathbb{C}}(E)\backslash\mathbf{V}_{\mathbb{C}}(p)$. This optimization technique is implemented in our implementation. Actually, our implementation outputs the following as a parametric radical system of $\langle F\rangle$

$$\{(\{0\},\{ab(ab+1)\},\{x^3+(-a^2b-a)x,ay^3+(-ab-1)y,x+ay\}),\\ (\{ab+1\},\{1\},\{x,y\}),(\{b\},\{a\},\{x^3-ax,ay^3-y,x+ay\}),\\ (\{a\},\{b\},\{x,y\}),(\{a,b\},\{1\},\{x,y\})\}.$$

This output means the following:

- if (a,b) belongs to $\mathbb{C}^2\backslash\mathbf{V}_{\mathbb{C}}(ab(ab+1))$, then $\{x^3+(-a^2b-a)x,ay^3+(-ab-1)y,x+ay\}$ is a basis of $rad_{\mathbb{C}[x,y]}(\langle F\rangle)$,
- if (a,b) belongs to $\mathbf{V}_{\mathbb{C}}(ab+1)$, then $\{x,y\}$ is a basis of $rad_{\mathbb{C}[x,y]}(\langle F\rangle)$,
- if (a,b) belongs to $\mathbf{V}_{\mathbb{C}}(b)\backslash\mathbf{V}_{\mathbb{C}}(a)$, then $\{x,y\}$ is a basis of $rad_{\mathbb{C}[x,y]}(\langle F\rangle)$,
- if (a,b) belongs to $\mathbf{V}_{\mathbb{C}}(a)\backslash\mathbf{V}_{\mathbb{C}}(b)$, then $\{x,y\}$ is a basis of $rad_{\mathbb{C}[x,y]}(\langle F\rangle)$, and
- if (a,b) belongs to $\mathbf{V}_{\mathbb{C}}(a,b)$, then $\{x,y\}$ is a basis of $rad_{\mathbb{C}[x,y]}(\langle F\rangle)$.

6 Key result

Here, we extend certain mathematical fundamentals to parametric scenarios. The cornerstone of this generalization is a comprehensive Gröbner system (CGS) over $\overline{K(u)}$ on $\mathbb{A} \cap \overline{K}^m$, where $\mathbb{A} \subset \overline{K(u)}^m$.

Before delving into the generalization, let's quickly review some fundamental concepts regarding the extension and contraction of ideals in mathematics.

Definition 6. *Let I be an ideal in $K[x]$. Then, the extension I^e of I to $K(u)[x\backslash u]$ is the ideal generated by the set I in the ring $K[u][x\backslash u]$ where $u \subset x$.*

Definition 7. *Let I be an ideal in $K[x]$ and $u \subset x$. Then, the extension I^e of I to $K(u)[x\backslash u]$ is the ideal generated by the set I in the ring $K(u)[x\backslash u]$. If J is an ideal in $K(u)[x\backslash u]$, then the contraction J^c of J to $K[x]$ is defined as $J \cap K[x]$.*

Lemma 2 ([2, Lemma 8.91]). *Let u be a subset of x, $F \subset K[x]$, $\prec$ a term order on $\mathrm{Term}(x\backslash u)$. Suppose J is an ideal generated by F in $K(u)[x\backslash u]$, and G is a Gröbner basis of $J \subset K(u)[x\backslash u]$ w.r.t. $\prec$ such that $G \subset K[u][x\backslash u]$. Let I be the ideal generated by F in $K[x]$, and set f as a least common multiple of $\{\mathrm{lc}(g) | g \in G\}$ (i.e. $f = \mathrm{lcm}\{\mathrm{lc}(g) | g \in G\}$), where $\mathrm{lc}(g) \in K[u]$ is taken of g as an element of $K(u)[x\backslash u]$. Then, $J^c = I : f^\infty$.*

Lemma 2 provides instructions on computing the contraction J^c as follows.

Step 1: Compute a Gröbner basis G of $J = \langle F \rangle$ in $K(u)[x\backslash u]$.
Step 2: Compute $f = \mathrm{lcm}\{\mathrm{lc}(g) | g \in G\}$.
Step 3: Compute a basis G' of $I : f^\infty$ in $K[x]$ where $I = \langle F \rangle$ in $K[x]$.
As $J^c = \langle G' \rangle$, output G'.

Let us extend the computational method above to parametric cases. Specifically, we consider the scenario where the ideal J is in $K(u)[t][x\backslash u]$.

The parametric case cannot be solved by simply replacing the Gröbner basis with a CGS of J because we have three types of symbols

$$x\backslash u\text{: main variables,}\quad t\text{: parameters,}\quad u\text{: variables of } K(u).$$

The aim of this paper is to develop an algorithm for computing a parametric radical system of a parametric ideal. A parametric ideal contains genuine parameters that do not belong to $\overline{K(u)}$. Since $\overline{K}^m$ is a subset of $\overline{K(u)}$, in order to apply a CGS over $\overline{K(u)}$ to the parametric ideal, we need to restrict a stratum of the CGS over $\overline{K(u)}$ to $\overline{K}^m$. Specifically, for $\mathbb{A} \subset \overline{K(u)}^m$, it is necessary to verify whether $\mathbb{A} \cap \overline{K}^m$ is empty or not.

In a previous study by the third author [9], generic standard bases of parametric ideals were discussed in a local ring. One can employ the ideas from that study to address this problem. The following proposition is adapted from [9].

Proposition 3. *Let ρ be the cardinality of u in $\mathbb{N}$ and $u = \{u_1, u_2, \ldots, u_\rho\}$. Let $\mathbf{V}_{\overline{K(u)}}(E)$ be a non-empty stratum in $\overline{K(u)}^m$ where $E \subset K[u][t]$. Set*

$$T = \bigcup_{g\in E} \left\{ c_{\alpha_i} \in K[t] \,\middle|\, g = \sum_{i=1}^{r} c_{\alpha_i} u^{\alpha_i}, \alpha_i \in \mathbb{N}^{\ell}, \alpha_j \neq \alpha_k \ (1 \leq j < k \leq r) \right\}$$

where $u^{\alpha} = u_1^{a_1} u_2^{a_2} \cdots u_{\rho}^{a_{\rho}}$ *for* $\alpha = (a_1, a_2, \dots, a_{\rho}) \in \mathbb{N}^{\rho}$.

Then, $\left(\mathbf{V}_{\overline{K(u)}}(E) \cap \overline{K}^m\right) = \mathbf{V}_{\overline{K}}(T)$ *holds.*

Proof. As $\overline{K}^m \supset \mathbf{V}_{\overline{K}}(T)$ and $\mathbf{V}_{\overline{K(u)}}(E) \supset \mathbf{V}_{\overline{K}}(T)$, thus we have $\left(\mathbf{V}_{\overline{K(u)}}(E) \cap \overline{K}^m\right) \supset \mathbf{V}_{\overline{K}}(T)$. Assume that $\left(\mathbf{V}_{\overline{K(u)}}(E) \cap \overline{K}^m\right) \supsetneq \mathbf{V}_{\overline{K}}(T)$, then exists $b \in \left(\mathbf{V}_{\overline{K(u)}}(E) \cap \overline{K}^m\right)$ such that $b \notin \mathbf{V}_{\overline{K}}(T)$. Moreover, there exist $p_1(t), \dots, p_{\nu}(t) \in T \subset K[t]$ and $g \in E$ such that $p_1(b) \neq 0, \dots, p_{\nu}(b) \neq 0$ and $g = \sum_{\alpha} c_{\alpha} u^{\alpha} + \sum_{i=1}^{\nu} p_i(t) u^{\alpha_i}$ where $c_{\alpha} \in K[t]$ and $u^{\alpha_1}, \dots, u^{\alpha_{\nu}} \in \mathbb{N}^{\rho}$. Since u^{α}s and $u^{\alpha_1}, \dots, u^{\alpha_{\nu}}$ are linearly independent over $\overline{K}$ and $p_i(b)u^{\alpha_i} \neq 0$, hence $g(b) \neq 0$. However, as $b \in \left(\mathbf{V}_{\overline{K(u)}}(E) \cap \overline{K}^m\right)$, we have $g(b) = 0$. This is a contradiction. Therefore, $\left(\mathbf{V}_{\overline{K(u)}}(E) \cap \overline{K}^m\right) = \mathbf{V}_{\overline{K}}(T)$. □

Definition 8. *Using the same notation as in Proposition 3, the set T is denoted as* $\mathrm{Coef}(E)$.

Example 4. Let $E = \{t_1^2 u_1^2 u_2 + (t_2+1)u_2 + t_1\}$ in $\mathbb{C}[u_1, u_2][t_1, t_2]$. Then, $\mathrm{Coef}(E) = \{t_1^2, t_2 + 1, t_1\}$ and $\mathbf{V}_{\overline{\mathbb{C}(u_1,u_2)}}(E) \cap \mathbb{C}^n = \mathbf{V}_{\mathbb{C}}(\mathrm{Coef}(E)) = \mathbf{V}_{\mathbb{C}}(t_1, t_2 + 1)$.

Note that it is clear that $\left(\mathbf{V}_{\overline{K(u)}}(E) \cap \overline{K}^m\right) = \mathbf{V}_{\overline{K}}(\mathrm{Coef}(E))$, and, for $E, N \subset K[u][x]$,

$$\begin{aligned}\left(\mathbf{V}_{\overline{K(u)}}(E) \backslash \mathbf{V}_{\overline{K(u)}}(N)\right) \cap \overline{K}^m &= \left(\mathbf{V}_{\overline{K(u)}}(E) \cap \overline{K}^m\right) \backslash \left(\mathbf{V}_{\overline{K(u)}}(N) \cap \overline{K}^m\right) \\ &= \mathbf{V}_{\overline{K}}(\mathrm{Coef}(E)) \backslash \mathbf{V}_{\overline{K}}(\mathrm{Coef}(N)).\end{aligned}$$

Hence, if $rad_{K[t]}(\mathrm{Coef}(E)) = rad_{K[t]}(\mathrm{Coef}(N))$, then $\left(\mathbf{V}_{\overline{K(u)}}(E) \backslash \mathbf{V}_{\overline{K(u)}}(N)\right) \cap \overline{K}^m = \emptyset$, otherwise $\left(\mathbf{V}_{\overline{K(u)}}(E) \backslash \mathbf{V}_{\overline{K(u)}}(N)\right) \cap \overline{K}^m \neq \emptyset$.

Corollary 1. *Let $E \subset K[u][t]$ and $f \in K[u][t]$. Then, if the radical of $\langle \mathrm{Coef}(E) \rangle$ includes f in $K(u)[t]$, then $\left(\mathbf{V}_{\overline{K(u)}}(E) \backslash \mathbf{V}_{\overline{K(u)}}(f)\right) \cap \overline{K}^m = \emptyset$, otherwise $\left(\mathbf{V}_{\overline{K(u)}}(E) \backslash \mathbf{V}_{\overline{K(u)}}(f)\right) \cap \overline{K}^m \neq \emptyset$.*

Proof. Since $\left(\mathbf{V}_{\bar{K(u)}}(f) \cap \overline{K}^m\right) = \mathbf{V}_{\overline{K}}(\mathrm{Coef}(\{f\})$, if the radical of $\langle \mathrm{Coef}(E) \rangle$ includes f, then $\mathbf{V}_{\bar{K}}(\mathrm{Coef}(\{f\}) \supset \mathbf{V}_{\overline{K}}(\mathrm{Coef}(E))$. Therefore, $\left(\mathbf{V}_{\overline{K(u)}}(E) \backslash \mathbf{V}_{\overline{K(u)}}(f)\right) \cap \overline{L}^m = \mathbf{V}_{\overline{K}}(\mathrm{Coef}(E)) \backslash \mathbf{V}_{\bar{K}}(\mathrm{Coef}(\{f\}) = \emptyset$. If the radical of $\langle \mathrm{Coef}(E) \rangle$ does not include f in $K(u)[t]$, then $\mathbf{V}_{\bar{K}}(\mathrm{Coef}(\{f\}) \not\supset \mathbf{V}_{\overline{K}}(\mathrm{Coef}(E))$. Therefore, $\left(\mathbf{V}_{\overline{K(u)}}(E) \backslash \mathbf{V}_{\overline{K(u)}}(f)\right) \cap \overline{K}^m \neq \emptyset$. □

In what follows, we assume that any segment $(E, \{p\}, G)$ of a CGS over $\overline{K(u)}$ in $K(u)[t][x \backslash u]$ satisfies "$E \subset K[u][t]$, $p \in K[u][t]$ and $G \subset K[u][t][x \backslash u]$," namely, all coefficients are in $K[u]$.

The CGS over $\overline{K(u)}$ is modified as follows by Proposition 3 and Corollary 1.

Algorithm 7 (CGS over $\overline{K(u)}$ on $\mathbb{A} \subset \overline{K}^m$)

Specification: CGS_RATIONAL($E, p, F, u, \prec$)
Computation of a CGS over $\overline{K(u)}$ on $\left(\mathbf{V}_{\overline{K(u)}}(E)\backslash\mathbf{V}_{\overline{K(u)}}(p)\right) \cap \overline{K}^m$.
Input: $E \subset K[t]$: finite set, $p \in K[u][t]$, $F \subset K(u)[t][x \setminus u]$ finite set, $u \subset x$,
$\prec$: term order on $Term(x \setminus u)$
Output: $\mathcal{Q}$: a CGS of $\langle F\rangle \subset K(u)[t][x \setminus u]$ over $\overline{K(u)}$ on $\mathbb{A} \cap \overline{K}^m$ where $\mathbb{A} = \mathbf{V}_{\overline{K(u)}}(E)\backslash\mathbf{V}_{\overline{K(u)}}(p)$.
BEGIN
$\mathcal{Q} \leftarrow \emptyset$;
$\mathcal{G} \leftarrow$ Compute a CGS of $\langle F\rangle$ over $\overline{K(u)}$ on $\left(\mathbf{V}_{\overline{K(u)}}(E)\backslash\mathbf{V}_{\overline{K(u)}}(p)\right)$ w.t.r. $\prec$;
for each $(E', \{p'\}, G') \in \mathcal{G}$ **do**
  $T \leftarrow \mathrm{Coef}(E')$;
    if $p' \notin rad_{K(u)}(\langle T\rangle)$ **then**
      $\mathcal{Q} \leftarrow \mathcal{Q} \cup \{(T, \{p'\}, G')\}$;
    end-if
end-for
return $\mathcal{Q}$;
END

Algorithm 7 is a crucial tool in this paper.

Remark 4. A segment of $\mathcal{Q}$ is formed by $(E, \{p'\}, G')$ where $E \subset K[t]$, $p' \in K[u][t]$, and $G' \subset K[u][t][x\backslash u]$. It is important to note that p' may still contain the symbol u. However, p' behaves like $\mathrm{Coef}(q) \subset K[t]$, as indicated by the fact that $\mathbf{V}_{\overline{K(u)}}(p') \cap \overline{K}^m = \mathbf{V}_{\overline{K}}(\mathrm{Coef}(p'))$ and Corollary 1. In other words, the symbol u in p' is not affected by any other computations in this paper. Conversely, by keeping $p' \in K[u][t]$, we maintain simplicity in the style of our algorithms. This serves as one of our optimization techniques.

Thanks to **CGS_RATIONAL**, we can generalize the computational method for contracting an ideal to parametric cases.

Algorithm 8 (Contraction of parametric ideals)

Specification:PARA_CONT($E, p, F, u, \prec$)
Computation of the contraction for parametric ideals.
Input: $E \subset K[t]$: finite set, $p \in K[u][t]$, $F \subset K(u)[t][x \setminus u]$: finite set, $u \subset x$,
$\prec$: a term order on $Term(x)$.
Output: $\mathcal{C} = \{(E_1, \{p_1\}, G_1), \ldots, (E_r, \{p_r\}, G_r)\}$: For all $\bar{t} \in \mathbf{V}_{\overline{K}}(E_i)\backslash\mathbf{V}_{\overline{K}}(\mathrm{Coef}(p_i))$ $(1 \le i \le r)$, $\sigma_{\bar{t}}(G_i)$ is a Gröbner basis of $\langle\sigma_{\bar{t}}(F)\rangle^c$ w.r.t. $\prec$ in $\overline{K}[x]$ where $\mathbf{V}_{\overline{K}}(E)\backslash\mathbf{V}_{\overline{K}}(p) = \bigcup_{i=1}^{r}\left(\mathbf{V}_{\overline{K}}(E)\backslash\mathbf{V}_{\overline{K}}(p)\right)$.
BEGIN
$\mathcal{C} \leftarrow \emptyset$; $\prec_1 \leftarrow$ A term order on $Tern(x\backslash u)$;
$\mathcal{G} \leftarrow$ **CGS_RATIONAL**$(E, p, F, u, \prec_1)$;
for each $(E', \{p'\}, G') \in \mathcal{G}$ **do**

$LC \leftarrow \{\mathrm{lc}(g)|g \in G'\}$; $\mathcal{H} \leftarrow$**PARA_LCM**(E', p', LC);
for each $(D, \{d\}, f) \in \mathcal{H}$ **do**
$\mathcal{Z} \leftarrow$ **PARA_SAT**$(D, d, G', f, \prec)$; $\mathcal{C} \leftarrow \mathcal{Z} \cup \mathcal{C}$;
end-for
end-for
return $\mathcal{C}$;
END

Next, we discuss the contraction of J^e, where $J \subset K[t][x]$.

The following proposition and lemma provide us with the relation between I and I^{ec}, where I is an ideal in $K[x]$.

Proposition 4 ([2, Proposition 8.94]). *Let $\prec$ be a term order on $\mathrm{Term}(x\backslash u)$, and suppose I is an ideal of $K[x]$ and G is a Gröbner basis of I w.r.t. $\prec$ in $K(u)[x\backslash u]$. Set q as a least common multiple of $\{\mathrm{lc}(g)|g \in G\}$ (i.e. $q = \mathrm{lcm}\{\mathrm{lc}(g)|g \in G\}$), where $\mathrm{lc}(g) \in K[u]$ is taken of g as an element of $K(u)[x\backslash u]$. Then, $I^{ec} = I : q^{\infty}$.*

Lemma 3 ([2, Lemma 8.95]). *Let $I = \langle f_1, \dots, f_r\rangle \subset K[x]$. Suppose $q \in K[x]$ and $s \in \mathbb{N}\backslash\{0\}$ are such that $I : q^s = I : q^{\infty}$. Then, $I = \langle f_1, \dots, f_r, q^s\rangle \cap (I : q^s)$.*

Notice that

$$\begin{aligned} rad_{K[x]}(I) &= rad_{K[x]}\left(\langle\{f_1, \dots, f_r\} \cup \{q^s\}\rangle\right) \cap rad_{K[x]}\left(I : q^{\infty}\right)\right) \\ &= rad_{K[x]}\left(\langle\{f_1, \dots, f_r\} \cup \{q\}\rangle\right) \cap rad_{K[x]}\left(I : q^{\infty}\right)\right). \end{aligned}$$

Therefore, the integer s is not necessary for computing the basis of $rad_{K[x]}(I)$; only the polynomial $q \in K[u]$ is required. Since, in Proposition 4, the Gröbner basis G of $I \subset K(u)[x\backslash u]$ is computed to obtain the polynomial q, the algorithm **CGS_RATIONAL** is again necessary to generalize Proposition 4 and Lemma 3 to parametric cases.

Algorithm 9 (Cut $\langle F\rangle^{ec}$ down to $\langle F\rangle$)

Specification: PARA_EXTCONT(E, p, F, u)
Cut $\langle F\rangle^{ec}$ down to $\langle F\rangle$ on $\mathbf{V}_{\overline{K}}(E)\backslash\mathbf{V}_{\overline{K}}(p)$.
Input: $E \subset K[t]$: finite set, $p \in K[u][t]$, $F \subset K[t][x]$: finite set, $u \subset x$,
$\prec$: a term order on $Term(x)$.
Output: $\mathcal{L} = \{(E_1, \{p_1\}, q_1), \dots, (E_r, \{p_r\}, q_r)\}$: For all $\bar{t} \in \mathbf{V}_{\overline{K}}(E_i)\backslash\mathbf{V}_{\overline{K}}(p_i)$ $(1 \le i \le r)$,

$$rad_{\overline{K}[x]}(\langle\sigma_{\bar{t}}(F)\rangle) = rad_{\overline{K}[x]}(\langle\sigma_{\bar{t}}(F \cup \{q_i\})\rangle) \cap rad_{\overline{K}[x]}(\langle\sigma_{\bar{t}}(F)\rangle^{ec})$$

where $q_1, \dots, q_r \in K[t][u]$ and $\mathbf{V}_{\overline{K}}(E)\backslash\mathbf{V}_{\overline{K}}(p) = \bigcup_{i=1}^{r} \mathbf{V}_{\overline{K}}(E_i)\backslash\mathbf{V}_{\overline{K}}(p_i)$.
BEGIN
$\mathcal{L} \leftarrow \emptyset$;
$\mathcal{G} \leftarrow$ **CGS_RATIONAL**$(E, p, F, u, \prec)$;
for each $(E', \{p'\}, G') \in \mathcal{G}$ **do**
$LC \leftarrow \{\mathrm{lc}(g)|g \in G\}$;

$\mathcal{H} \leftarrow$**PARA_LCM**$(E', \{p'\}, LC)$; $\mathcal{L} \leftarrow \mathcal{L} \cup \mathcal{H}$;
end-for
return $\mathcal{L}$;
END

7 Non-zero dimensional case

Here, we describe an algorithm for computing a parametric radical system of a non-zero dimensional ideal with parameters. The following lemma is a well-known fact and is utilized to reduce the problem to the zero dimensional case by means of the extension/contraction method.

Lemma 4 ([2, Lemma 7.47]). *Let I be an ideal in $K[x]$, If $u \subset x$ is a MIS modulo I, then I^e is a zero dimensional ideal of $K(u)[x \backslash u]$.*

Let $E \subset K[t]$, $p \in K[t]$ and $G \subset K[t][x]$. Assume that a triple $(E, \{p\}, G)$ satisfies conditions: for all $\bar{t} \in \mathbf{V}_{\bar{K}}(E) \backslash \mathbf{V}_{\bar{K}}(p)$, $\dim(\langle \mathrm{lt}(G) \rangle) \neq 0$. Set u a MIS modulo $\langle \mathrm{lt}(G) \rangle$. Then, for all $\bar{t} \in \mathbf{V}_{\bar{K}}(E) \backslash \mathbf{V}_{\bar{K}}(p)$, $\langle \sigma_{\bar{t}}(G) \rangle$ a zero dimensional ideal in $\overline{K}(u)[x \backslash u]$.

To compute a parametric radical system of a non-zero dimensional ideal with parameters, we first compute a parametric radical system of $\langle G \rangle^e$ in $K(u)[t][x \backslash u]$. Essentially, this algorithm is the same as Algorithm 6 (**PRS_ZERO**). However, since the coefficient domain is $K(u)$, it is necessary to compute a CGS over $\overline{K(u)}$ of $\langle G \rangle^e$. This requires using the algorithm **CGS_RATIONAL** again.

The following algorithm, which modifies Algorithm 2 (**SQUARE_FREE**) using **CGS_RATIONAL**, outputs the squarefree parts of a parametric polynomial in $\overline{K(u)}[t][x_i]$.

Algorithm 10 (Squarefree part of f in $K(u)[t][x_i]$)

Specification: SQUARE_RATIONAL(E, p, f, u, x_i)
Computation of squarefree parts of f in $K(u)[t][x_i]$.
Input: $E \subset K[t]$: finite set, $p \in K[u][t]$, $f \in (K[u][t])[x_i]$, $u \subset x$, $x_i \in x \backslash u$.
For all $\bar{t} \in \mathbf{V}_{\overline{K}}(E) \backslash \mathbf{V}_{\overline{K}}(p)$, $\sigma_{\bar{t}}(f) \neq 0$. ($\mathrm{char}(K) = 0$)
Output: $\mathcal{P} = \{(E_1, \{p_1\}, h_1), \ldots, (E_\ell, \{p_\ell\}, h_\ell)\}$: For all $\bar{t} \in \mathbf{V}_{\overline{K}}(E_i) \backslash \mathbf{V}_{\overline{K}}(p_i)$ $(1 \leq i \leq \ell)$, $\sigma_{\bar{t}}(h_i)/\sigma_{\bar{t}}(\mathrm{lc}(h_i))$ is the squarefree part of $\sigma_{\bar{t}}(f)/\mathrm{lc}(\sigma_{\bar{t}}(f))$ where $\mathbf{V}_{\overline{K}}(E) \backslash \mathbf{V}_{\overline{K}}(p) = \bigcup_{i=1}^{\ell} \left(\mathbf{V}_{\overline{K}}(E_i) \backslash \mathbf{V}_{\overline{K}}(p_i) \right)$.
BEGIN
$\mathcal{P} \leftarrow \emptyset$; $\mathcal{G} \leftarrow$ **CGS_RATIONAL**$(E, p, \{f, \frac{\partial f}{\partial x_i}\}, u, \prec)$;
for each $(E', \{p'\}, \{g\}) \in \mathcal{G}$ **do**
$q \leftarrow$ Compute q s.t. $\mathrm{lc}(g)^{1+\deg(f)-\deg(g)} f = qg + r$ $(\deg(r) < \deg(g))$;
(by pseudo-division)
$\mathcal{P} \leftarrow \mathcal{P} \cup \{(E', \{p'\}, q)\}$
end-for
return $\mathcal{P}$;
END

Algorithm 11, which modifies **PRS_ZERO** using the **CGS_RATIONAL** algorithm, computes a parametric radical system in $K(u)[t][x\backslash u]$.

Algorithm 11 (Parametric radical system of $\langle F\rangle^e$)

Specification:PRS_MIS(E, p, F, u)
Computation of a parametric radical system of $\langle F\rangle^e$ in $K(u)[x\backslash u]$.
Input: $E \subset K[t]$: finite set, $p \in K[u][t]$, $F \subset K[t][x]$ finite set,
$u \subset x$: MIS modulo $\langle \mathrm{lt}(F)\rangle$.
Output: $\mathcal{P}$: parametric radical system of $\langle F\rangle \subset K(u)[t][x\backslash u]$ on $\mathbf{V}_{\overline{K}}(E)\backslash\mathbf{V}_{\overline{K}}(p)$.
BEGIN
$\mathcal{P} \leftarrow \{(E, \{p\}, F)\}$; $y = \{y_1, \ldots, y_\rho\} \leftarrow x\backslash u$;
for each $i = 1$ to ρ **do** /*ρ variables */
  $\mathcal{H} \leftarrow \emptyset$; $\prec\leftarrow$ Set a block term order with $y_i \ll y\backslash\{y_i\}$;
  $\mathcal{G} \leftarrow$ **CGS_RATIONAL**$(E, p, F, u, \prec)$;
  for each $(E', \{p'\}, G') \in \mathcal{G}$ **do**
    $g \leftarrow$ Select the polynomial g of minimal degree in $G' \cap K(u)[t][y_i]$;
    $\mathcal{B} \leftarrow$**SQUARE_RATIONAL**(E', p', g, u, y_i);
    for each $(E'', \{h\}, b) \in \mathcal{B}$ **do**
      $\mathcal{W} \leftarrow \mathcal{P}$;
      for each $(D, \{d\}, H) \in \mathcal{W}$ **do**
        if $(\mathbf{V}_{\overline{K}}(E'')\backslash\mathbf{V}_{\overline{K}}(h)) \cap (\mathbf{V}_{\overline{K}}(D)\backslash\mathbf{V}_{\overline{K}}(d)) \neq \emptyset$ **then**
          $\mathcal{H} \leftarrow \mathcal{H} \cup \{(E'' \cup D, \{\sqrt{hd}\}, H \cup \{b\})\}$;
        end-if
      end-for
    end-for
  end-for
  $\mathcal{P} \leftarrow \mathcal{H}$;
end-for
return $\mathcal{P}$;
END

Let us execute **PRS_MIS**(E, p, G, u), where E, p, G are taken from the discussion immediately after Lemma 4, and u is a MIS modulo $\langle \mathrm{lt}(G)\rangle$. Then, the output $\mathcal{P}$ satisfies: $\forall(E', \{p'\}, G') \in \mathcal{P}$ and $\forall\bar{t} \in \mathbf{V}_{\overline{K}}(E')\backslash\mathbf{V}_{\overline{K}}(p')$,

$$rad_{\overline{K}(u)[x\backslash u]}(\langle\sigma_{\bar{t}}(G)\rangle^e) = \langle\sigma_{\bar{t}}(G')\rangle \text{ in } \overline{K}(u)[x\backslash u].$$

Let us apply our contraction method to $(E', p', G', u, \prec)$, i.e., **PARA_CONT** $(E', p, u, \prec)$, where $\prec$ is a term order on $Term(x)$. Then, the output $\mathcal{C}$ satisfies: $\forall(D, \{d\}, H) \in \mathcal{C}$ and $\forall\bar{a} \in \mathbf{V}_{\overline{K}}(D)\backslash\mathbf{V}_{\overline{K}}(d)$, $(rad_{\overline{K}(u)[x\backslash u]}(\langle\sigma_{\bar{a}}(G)\rangle^e))^c = \langle\sigma_{\bar{a}}(H)\rangle$ in $\overline{K}[x]$. In fact, by the following lemma, we have $rad_{\overline{K}[x]}(\langle\sigma_{\bar{a}}(G)\rangle^{ec}) = \langle\sigma_{\bar{a}}(H)\rangle$ in $\overline{K}[x]$.

Lemma 5 ([2, Lemma 8.97]). *(i) If I is an ideal in $K(u)[x\backslash u]$, then* $(rad_{K(u)[x\backslash u]}(I))^c = rad_{K[x]}(I^c)$.

(ii) I_1 *and* I_2 *are ideals of* $K[x]$*, then* $rad_{K[x]}(I_1 \cap I_2) = rad_{K[x]}(I_1) \cap rad_{K[x]}(I_2)$.
(iii) If I *is an ideal of* $K[x]$*, then* $(rad_{K[x]}(I))^e = rad_{K(u)[x\setminus u]}(I^e)$.

Recall Proposition 4 and Lemma 5. There exists $q \in K[t][u]$ such that $\forall \bar{a} \in \mathbf{V}_{\overline{K}}(D)\setminus\mathbf{V}_{\overline{K}}(d)$,

$$rad_{\overline{K}[x]}(\langle\sigma_{\bar{a}}(G)\rangle) = rad_{\overline{K}[x]}(\langle\sigma_{\bar{a}}(G \cup \{q\})\rangle) \cap rad_{\overline{K}[x]}(\langle\sigma_{\bar{a}}(G)\rangle^{ec}).$$

By applying the algorithm **PARA_EXTCONT**, the polynomial q can be obtained. Therefore, if we have a basis of $rad_{\overline{K}[x]}(\langle\sigma_{\bar{a}}(G \cup q)\rangle)$, we can obtain the basis of $rad_{\overline{K}[x]}(\langle\sigma_{\bar{a}}(G)\rangle)$ by computing their intersection.

Since the same computation can be done recursively for $\langle G \cup \{q\}\rangle$, we can devise an algorithm for computing a parametric radical system of a parametric ideal as follows.

Algorithm 12 (Parametric radical system of non-zero dim. ideal)

Specification: PRS_NONZERO($E, p, F, \prec$**)**
Computation of a parametric radical system of a non-zero dim. ideal.
Input: $E \subset K[t]$: finite set, $p \in K[u][t]$, $F \subset K[t][x]$ finite set,
$\prec$: term order on $Term(x)$.
($\forall \bar{t} \in \mathbf{V}_{\overline{K}}(E)\setminus\mathbf{V}_{\overline{K}}(p)$, $\dim(\langle\sigma_{\bar{t}}(F)\rangle) \neq 0$, $\langle\sigma_{\bar{t}}(F)\rangle \neq \{0\}$ and $\langle\sigma_{\bar{t}}(F)\rangle \neq \langle 1\rangle$.)
Output: $\mathcal{N}Z$: parametric radical system of $\langle F\rangle$ on $\mathbf{V}_{\overline{K}}(E)\setminus\mathbf{V}_{\overline{K}}(p)$.
BEGIN
$\mathcal{N}Z \leftarrow \emptyset$; $\mathcal{G} \leftarrow$ Compute a CGS of $\langle F\rangle$ over $\overline{K}$ on $\mathbf{V}_{\overline{K}}(E)\setminus\mathbf{V}_{\overline{K}}(p)$;
for each $(E', \{p'\}, G') \in \mathcal{G}$ **do**
  $u \leftarrow$ Compute a MIS modulo $\langle \mathrm{lt}(G')\rangle$;
  $\mathcal{Z} \leftarrow$**PRS_MIS**(E', p', G', u);
  for each $(E_z, \{p_z\}, Z) \in \mathcal{Z}$ **do**
    $\mathcal{C} \leftarrow$ **PARA_CONT**$(E_z, p_z, Z, u, \prec)$;
    $\mathcal{D} \leftarrow$**PARA_EXTCONT**(E', p', G', u);
    for each $(E_d, \{p_d\}, q_d) \in \mathcal{D}$ **do**
      for each $(E_c, \{p_c\}, G_c) \in \mathcal{C}$ **do**
        if $\mathbf{V}_{\overline{K}}(E_d \cup E_c)\setminus\mathbf{V}_{\overline{K}}(\sqrt{p_d p_c}) \neq \emptyset$ **then**
          $\mathcal{L} \leftarrow$**PRS_NONZERO**$(E_c \cup E_d, \sqrt{p_c p_d}, G_c \cup \{q_d\}, \prec)$;
        end-if
        for each $(E_l, \{p_l\}, L) \in \mathcal{L}$ **do**
        $\mathcal{A} \leftarrow$**PARA_INTERSECTION**(E_l, p_l, L, G_c);
        $\mathcal{N}Z \leftarrow \mathcal{N}Z \cup \mathcal{A}$;
        end-for
      end-for
    end-for
  end-for
end-for
return $\mathcal{N}Z$;
END

Remark 5. (i) As $\left(\mathbf{V}_{\overline{K}}(E_l)\setminus\mathbf{V}_{\overline{K}}(p_l)\right) \subset \left(\mathbf{V}_{\overline{K}}(E_c)\setminus\mathbf{V}_{\overline{K}}(p_c)\right)$, thus we have

$$\big(\mathbf{V}_{\overline{K}}(E_l)\backslash\mathbf{V}_{\overline{K}}(p_l)\big)\cap\big(\mathbf{V}_{\overline{K}}(E_c)\backslash\mathbf{V}_{\overline{K}}(p_c)\big)=\big(\mathbf{V}_{\overline{K}}(E_l)\backslash\mathbf{V}_{\overline{K}}(p_l)\big).$$

Hence, we adopted **PARA_INTERSECTION**(E_l, p_l, L, G_c) in the algorithm.

(ii) Since algorithms for computing a CGS output a finite number of strata, the stratum $\mathbf{V}_{\overline{K}}(E)\backslash\mathbf{V}_{\overline{K}}(p)$ is divided into a finite number of strata. We note that by the MIS u, we have $\langle G'\rangle \cap K(t)[u]=0$. It follows that the inclusion $\langle G_c\rangle \subset \langle G_c \cup \{q_d\}\rangle$ is proper in $K(t)[x]$. We observe that the recursive calls of **PRS_NONZERO** gives rise to a strictly ascending chain of ideals, which cannot be infinite since $K(t)[x]$ is Noetherian. This occurs for each stratum $\mathbf{V}_{\overline{K}}(E_c\cup E_d)\backslash\mathbf{V}_{\overline{K}}(\sqrt{p_cp_d})$. Therefore, the algorithm terminates.

Example 5. Let $F=\{ax^2z+xy^2,(y+xz)^2+ax^3z^2\}\subset\mathbb{C}[a][x,y,z]$ and $\prec$ the graded reverse lexicographic term order with $x\prec y\prec z$ where a is a parameter and x,y,z are variables. A CGS of $\langle F\rangle$ over $\mathbb{C}$ w.r.t. $\prec$ is

$$\{(\{0\},\{a\},G),(\{a\},\{1\},\{y^4,z^2x^2+2zyx+y^2,y^2x\})\}$$

where $\{az^2x^3+z^2x^2+2zyx+y^2,-a^2z^2x^2+y^4,azx^2+y^2x\}$.

Let us consider the first segment $(\{0\},\{a\},G)$. Then, a MIS modulo $\langle \mathrm{lt}(G)\rangle$ is $\{x\}$. Thus, $\langle G\rangle$ is not zero dimensional on $\mathbb{C}\backslash\mathbf{V}_{\mathbb{C}}(a)$. Then, **PRS_MIS**$(\{0\},a,G,\{x\})$ outputs $\{(\{0\},\{a\},G\cup Z)\}$ where

$$Z=\{ay^3x+y^3-2ay^2+a^2y,a^2z^3x^4+2az^3x^3+(z^3-2a^2z^2)x^2+2az^2x+a^2z\}.$$

Next, **PARA_CONT**$(\{0\},a,Z,\{x\},\prec)$ outputs $\{(\{0\},\{a\},\{azx+y^2,(az^2y+2a^2z^2)x^2+z^2yx+3azy-2a^2z,-az^2x^3+(2azy-z^2)x^2-3azx-2ay\})\}$, and **PRS_EXTCONT**$(\{0\},a,G)$ outputs $\{(\{0\},\{a\},\{a^2x^4+2ax^3+x^2\})\}$.

Due to the page limitation, the computation process from here is omitted. After computing **PARA_NONZERO**$(\{0\},a,G\cup\{a^2x^4+2ax^3+x^2\},\prec)$, we obtain a parametric radical system $\mathcal{P}$ of $\langle G\rangle$ on $\mathbb{C}\setminus\mathbf{V}_{\mathbb{C}}(a)$ as follows.

$$\mathcal{P}=\{(\{0\},\{a\},\{azx+y^2,az^2x^3+(-2azy+z^2)x^2+3azx+2ay\})\}.$$

Repeat the same procedure for $(\{a\},\{1\},\{y^4,z^2x^2+2zyx+y^2,y^2x)$. Then, we obtain a parametric radical system of $\langle F\rangle$ as follows

$$\{(\{0\},\{a\},\{azx+y^2,az^2x^3+(-2azy+z^2)x^2+3azx+2ay\}),(\{a\},\{1\},\{y,zx\})\}.$$

The following is the algorithm for computing a parametric radical system of a parametric ideal.

Algorithm 13

Specification: PRS$(F,\prec)$

Computation of a parametric radical system of a parametric ideal.

Input: $F\subset K[t][x]$: finite set, $\prec$: term order on *Term*(x).
Output: $\mathcal{L}$: parametric radical system of $\langle F\rangle$.
BEGIN
$(\mathcal{Z},\mathcal{N},\mathcal{W})\leftarrow$ **PARA_DIM**(F);
$\mathcal{P}\leftarrow\bigcup_{(E,\{p\},G)\in\mathcal{Z}}$ **PRS_ZERO**(E,p,G);

$\mathcal{Q} \leftarrow \bigcup_{(E',\{p'\},G')\in\mathcal{N}} \textbf{PRS\_NONZERO}(E',\{p'\},G',\prec)$;
$\mathcal{L} \leftarrow \{(E'',\mathrm{Coef}(p''),G'') \mid (E'',\{p''\},G'')\in\mathcal{Q}\}\cup\mathcal{P}\cup\mathcal{W}$;
return $\mathcal{L}$;
END

Algorithm 13 has been implemented in the computer algebra system Risa/Asir. The code is available on the web:
`https://www.rs.tus.ac.jp/~nabeshima/softwares.html`.

Example 6. Let $F = \{ax^2z + xy^4, (x + y)^3 + bx^3z^2, y^2 + bxy\} \subset \mathbb{Q}[a, b][x, y, z]$ where a, b are parameters and x, y, z are variables. Then, our implementation outputs the following parametric radical system of $\langle F\rangle$.
$\{(\{b^2 - 3b + 3\}, \{ab\}, \{3ax + (-b + 3)ay, 3yz^3 - byz + 3yz\}), (\{0\}, \{(b^4 - 4b^3 + 6b^2 - 3b)a\}, \{(b^4 - 4b^3 + 6b^2 - 3b)ax + (b^3 - 4b^2 + 6b - 3)ay, (b^3 - 4b^2 + 6b - 3)azx + (3az^3 + (-2b^2 + 5b - 3)az)y\}), (\{b - 1\}, \{(b^3 - 3b^2 + 3b)a\}, \{y, x\}), (\{a\}, \{b^3 - 3b^2 + 3b\}, \{y, (bz^2 + 1)x\}), (\{a, b^2 - 3b + 3\}, \{b^2 - 3b\}, \{y, (3z^2 - b + 3)x\}), (\{a, b\}, \{1\}, \{y, x\}), (\{b\}, \{a\}, \{x, y]\})\}$.

Acknowledgements: This work has been partly supported by JSPS Grant-in-Aid for Scientific Research(C)(No. 23K03076).

References

1. Abbott, J. Bigatti, A.M., Palezzato, E. and Robbiano, L.: Computing and using minimal polynomials. *J. Symb. Comp.*, **100**, 137–163, (2020).
2. Becker, T. and Weispfenning, V.: *Gröbner Bases, A Computational Approach to Commutative Algebra (GTM 141)*. Springer, (1993)
3. Cox, D., Little, J. and O'Shea, D.: *Ideal, Varieties, and Algorithm (2nd edition)*. Springer, (1997)
4. Gianni, P., Trager, B. and Zacharias, G.: Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comp.*, **6**, 149–167, (1988)
5. Kapur, D., Sun, Y. and Wang, D.: A new algorithm for computing comprehensive Gröbner systems. *Proc. ISSAC 2010*, 29–36, ACM, (2010)
6. Kapur, D., Sun, Y. and Wang, D.: An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial system. *J. Symb. Comp.*, **49**, 74–44, (2013)
7. Montes, A. : *The Gröbner Cover*. Springer Nature Switzerland AG 2018
8. Nabeshima, K.: Stability conditions of monomial bases and comprehensive Gröbner systems. *Proc. CASC 2012, LNCS*, **7442**, 248–259, Springer, (2012)
9. Nabeshima, K. and Tajima, S.: CSSg method for several genericities of parametric systems. *Japan J. Industrial and Applied Mathematics*, **40**, 315–337, (2023)
10. Nabeshima, K.: Generic Gröbner basis of a parametric ideal and its application to a comprehensive Gröbner systems. *Applicable Algebra in Engineering, Communication and Computing*, **35**, 55–70, (2024)
11. Noro, M. and Takeshima, T.: Risa/Asir - A computer algebra system. *Proc. ISSAC 1992*, 387–396, ACM, (1992) `http://www.math.kobe-u.ac.jp/Asir/asir.html`
12. Suzuki, A. and Sato, Y. : A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases. *Proc. ISSAC 2006*, 326–331, ACM, (2006)
13. Weispfenning, V. : Comprehensive Gröbner bases. *J. Symb. Comp.*, **14**, 1-29, (1992)