Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Algorithms for computing greatest common divisors of parametric multivariate polynomials ☆

Deepak Kapur [a], Dong Lu [b,c], Michael Monagan [d], Yao Sun [e], Dingkang Wang [f,g]

[a] *Department of Computer Science, University of New Mexico, Albuquerque, NM, USA*
[b] *Beijing Advanced Innovation Center for Big Data and Brain Computing, Beihang University, Beijing 100191, China*
[c] *School of Mathematics and Systems Science, Beihang University, Beijing 100191, China*
[d] *Department of Mathematics, Simon Fraser University, Burnaby, B.C., V5A 1S6, Canada*
[e] *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[f] *KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China*
[g] *School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China*

ARTICLE INFO

Article history:
Received 23 October 2018
Accepted 4 July 2019
Available online xxxx

Keywords:
Parametric multivariate polynomials
Gcd system
Minimal comprehensive Gröbner system
Ideal intersection
Ideal quotient

ABSTRACT

Two new efficient algorithms for computing greatest common divisors (gcds) of parametric multivariate polynomials over $k[U][X]$ are presented. The key idea of the first algorithm is that the gcd of two non-parametric multivariate polynomials can be obtained by dividing their product by the generator of the intersection of two principal ideals generated by the polynomials. The second algorithm is based on another simple insight that the gcd can be extracted using the generator of the ideal quotient of a polynomial with respect to the second polynomial. Since the ideal intersection and ideal quotient in these cases are also principal ideals, their generators can be obtained by computing minimal Gröbner bases of the ideal intersection and ideal quotient, respectively. To avoid introducing new variables which can adversely affect the efficiency, minimal Gröbner bases computations are performed on modules. Both of these constructions generalize to the parametric case as shown in the paper. Comprehensive Gröbner system constructions are used for the parametric ideal intersection and ideal quotient using the Kapur-Sun-Wang's algorithm. It is proved that whether in a minimal comprehensive Gröbner system of a parametric ideal

☆ This paper is an extended version of the paper entitled "An Efficient Algorithm for Computing Parametric Multivariate Polynomial GCD", which was presented at ISSAC 2018 (Kapur et al., 2018).

E-mail addresses: kapur@cs.unm.edu (D. Kapur), donglu@amss.ac.cn (D. Lu), mmonagan@cecm.sfu.ca (M. Monagan), sunyao@iie.ac.cn (Y. Sun), dwang@mmrc.iss.ac.cn (D. Wang).

https://doi.org/10.1016/j.jsc.2019.10.006

intersection or in that of a parametric ideal quotient, each branch of the specializations corresponds to a principal parametric ideal with a single generator. Using this generator, the parametric gcd of that branch is obtained by division. For the case of more than two parametric polynomials, we can use the above two algorithms to compute gcds recursively, and get an extended algorithm by generalizing the idea of the second algorithm. Algorithms do not suffer from having to apply expensive steps such as ensuring whether parametric polynomials are primitive w.r.t. the main variable as used in both the algorithms proposed by Nagasaka (ISSAC, 2017). The resulting algorithms are not only conceptually simple to understand but are more efficient in practice. The proposed algorithms and both of Nagasaka's algorithms have been implemented in Singular, and their performance is compared on a number of examples.

1. Introduction

Multivariate polynomial gcd computation is one of the most important operations in computer algebra as it is used in many algorithms and applications. The problem has been extensively investigated and numerous algorithms have been developed to compute the gcd efficiently beyond Euclid's algorithm using division for univariate polynomials and its extension to multivariate polynomials using pseudo-division. The modular gcd algorithm from Brown (1971) was the first gcd algorithm that avoided intermediate expression swell. For sparse polynomials Moses and Yun (1973) developed the EZ GCD algorithm which is based on Hensel lifting. Zippel's sparse modular gcd algorithm (Zippel, 1979) used sparse interpolation. It is currently used in Maple, Magma, and Mathematica. We mention also algorithms of Gianni and Trager (1985) and Sasaki and Suzuki (1992) which compute a gcd from a Gröbner basis. For sparse multivariate polynomials, Sanuki et al. (2016) utilized Extended Hensel Construction to compute gcd and found that their algorithm to be comparable in performance to Maple's gcd routine.

Using the concept of parametric polynomials, there have also been many publications studying how to compute the gcd of parametric polynomials. Abramov and Kvashenko (1993) used the subresultant chain to compute a parametric univariate polynomial gcd. Ayad (2010) presented three algorithms based on parametrization of the Gaussian elimination procedure to compute gcd of a finite set of parametric univariate polynomials. At ISSAC 2017, Nagasaka (2017) extended the ideas of Gianni and Trager (1985) as well as Sasaki and Suzuki (1992) to polynomials with parameters for computing the gcd of parametric multivariate polynomials. The main tool used in Nagasaka's algorithms is the comprehensive Gröbner system which is the parametric extension of Gröbner basis, introduced by Weispfenning (1992) (and independently by Kapur (1995) as parametric Gröbner basis) and was improved by Suzuki and Sato (2006), Kapur et al. (2010, 2013) and Nabeshima (2012). In Nagasaka's paper, the algorithms to compute the gcd of parametric multivariate polynomials need to consider whether parametric polynomials are primitive w.r.t. the main variable under different parametric constraints. Moreover, he had to construct an ideal that is maximal for any specialization based on extending Gianni and Trager's results (Gianni and Trager, 1985). Both of these steps in his algorithms can be extremely time consuming.

This paper presents two new efficient algorithms for the gcd computation of parametric multivariate polynomials. We first consider the non-parametric case, and then generalize to the parametric case.

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

Let k be a field, $k[U][X]$ be the polynomial ring over $k[U]$ in the variables $X = \{x_1, \ldots, x_n\}$.[1] Assume that f_1 and f_2 are two nonzero polynomials in $k[X]$. The first algorithm is based on a simple insight that the gcd of f_1 and f_2 is equal to the product of f_1 and f_2 divided by the least common multiple (lcm) of f_1 and f_2. Since the intersection of $\langle f_1\rangle$ and $\langle f_2\rangle$ is generated by the principal ideal generated by $\text{lcm}(f_1, f_2)$, computing a minimal Gröbner basis of $\langle f_1\rangle \cap \langle f_2\rangle$ gives $\text{lcm}(f_1, f_2)$. Then, $\gcd(f_1, f_2) = \frac{f_1 \cdot f_2}{\text{lcm}(f_1, f_2)}$. The main idea of the second algorithm is based on computing a minimal Gröbner basis G for the ideal quotient $\langle f_1\rangle : \langle f_2\rangle$, which is also a principal ideal with G including only one polynomial $\bar{f}_1$. Then, $\gcd(f_1, f_2) = \frac{f_1}{\bar{f}_1}$. In order to avoid introducing new variables for intersection and quotient computation, we use computations on modules to compute the generators of ideal intersection and ideal quotient.

Most importantly, these constructions extend to the case of parametric polynomials in which Gröbner bases computations for modules of the ideal intersection and ideal quotient are replaced by comprehensive Gröbner systems constructions for modules of parametric polynomials, respectively. In Nabeshima (2010), algorithms based on the results in Suzuki and Sato (2006) are given for computing parametric Gröbner bases for modules and parametric syzygies. In this paper, we extend the algorithms in Kapur et al. (2010, 2013) to the cases of parametric modules and syzygies.

To compute the gcd of more than two parametric polynomials, the above methods are repeated as in the case of computing the gcd of a family of numbers. We also generalize the idea of the second algorithm and obtain an algorithm which use a single comprehensive Gröbner system to compute gcds for a system of more than two parametric polynomials.

Compared with Nagasaka's algorithms, the proposed algorithms have two advantages: there is no need to check whether parametric polynomials are primitive w.r.t. main variable in each iteration, and further, it is guaranteed that a parametric polynomial $f_1 f_2$ is divisible by the result of the associated ideal intersection as well as f_1 is divisible by the result of the associated ideal quotient. The algorithms have been implemented and compared with Nagasaka's algorithms and are shown to be superior in performance.

This paper is organized as follows. In Section 2, we provide background about the gcd and the comprehensive Gröbner system computations for parametric multivariate polynomials. Nagasaka's algorithms are reviewed in Section 3. The two proposed algorithms are presented in Section 4. To provide intuition and make the presentation simple, for each algorithm we first briefly discuss how the gcd of non-parametric two polynomials can be computed using a minimal Gröbner basis of a principal ideal; then this is followed by extending this method to parametric polynomials, and the new algorithm is presented. In Section 5, a non-trivial example is given to illustrate the key steps of the two proposed algorithms. Some remarks and an algorithm which is an extension of the second algorithm about computing the gcds for a system of more than two parametric polynomials are given in Section 6. Experimental data and a comparison with Nagasaka's algorithms are presented in Section 7. We end with some concluding remarks in Section 8.

2. Preliminaries

Let k be a field, L be an algebraic closed field containing k, $k[X]$ be the polynomial ring in the variables $X = \{x_1, \ldots, x_n\}$, $k[U]$ be the parameter ring in the parameters $U = \{u_1, \ldots, u_m\}$, and $k[U][X]$ be the polynomial ring over $k[U]$ in X. It is assumed that $X \cap U = \emptyset$, i.e., X and U are disjoint sets. In some cases, we abbreviate $\{x_i, x_{i+1}, \ldots, x_n\}$ to X_i $(2 \le i \le n)$.

We introduce some notations and definitions for non-parametric multivariate polynomials. Two polynomials $f, g \in k[X]$ are associate if $\exists c \in L$ such that $f = c \cdot g$; we denote this equivalence relation by $f \sim g$. For a polynomial $f \in k[X]$, the leading term, leading coefficient, leading monomial and the total degree of f w.r.t. a monomial order $\prec$ are denoted by $\text{lt}(f)$, $\text{lc}(f)$, $\text{lm}(f)$ and $\text{tdeg}(f)$ respectively. We have $\text{lt}(f) = \text{lc}(f) \cdot \text{lm}(f)$. The ideal in $k[X]$, generated by $f_1, \ldots, f_s$, is denoted by $\langle f_1, \ldots, f_s\rangle$.

[1] When $n = 1$, we compute a minimal comprehensive Gröbner system of parametric univariate polynomials, and then the generator of each branch is the gcd of these polynomials. Hence, we only consider the case of $n \ge 2$ in this paper.

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

Definition 1. Let $f_1, \ldots, f_s \in k[X]$. Then $h \in k[X]$ is called a **greatest common divisor** (gcd) of $f_1, \ldots, f_s$, denoted $h = \gcd(f_1, \ldots, f_s)$, if

1. $\forall i$ $(1 \leq i \leq s)$, h divides f_i and
2. if g is any polynomial which divides $f_1, \ldots, f_s$, then g divides h.

Particularly, we define $\gcd(f_1, \ldots, f_s) = \gcd(f_2, \ldots, f_s)$ if $f_1 = 0$, and $\gcd(0, 0) = 0$, for convenience.

A gcd of polynomials is defined modulo associates. For any given polynomials $f_1, \ldots, f_s \in k[X]$, there exist $\bar{f}_1, \ldots, \bar{f}_s \in k[X]$ such that $f_i = \gcd(f_1, \ldots, f_s) \cdot \bar{f}_i$ for each $i = 1, \ldots, s$, then $\bar{f}_1, \ldots, \bar{f}_s$ are called the **cofactors** of $f_1, \ldots, f_s$.

Definition 2. Let $f_1, \ldots, f_s \in k[X]$. Then $g \in k[X]$ is called a **least common multiple** (lcm) of $f_1, \ldots, f_s$, denoted $g = \mathrm{lcm}(f_1, \ldots, f_s)$, if

1. $\forall i$ $(1 \leq i \leq s)$, f_i divides g and
2. g divides any polynomial which all $f_1, \ldots, f_s$ divide.

Definition 3. Let $f \in k[X]$. f is said to be primitive w.r.t. x_1 if it is primitive as a polynomial in $k[X_2][x_1]$. That is, its coefficients in $k[X_2]$ are co-prime.

Definition 4. A **minimal Gröbner basis** for a polynomial ideal $I \subseteq k[X]$ is a Gröbner basis G for I such that $\mathrm{lm}(p) \notin \langle \mathrm{lm}(G - \{p\}) \rangle$ for all $p \in G$.

Definition 5. If I, J are ideals in $k[X]$, then $I : J$ is the set

$$I : J = \{f \in k[X] \mid fg \in I \text{ for all } g \in J\}$$

and is called the **ideal quotient** (or **colon ideal**) of I divided by J. If J is generated by one element g, we use $I : g$ instead of $I : \langle g \rangle$ for convenience.

For example, in $k[x_1, x_2, x_3]$ we have $\langle x_1x_3, x_2x_3 \rangle : x_3 = \{f \in k[x_1, x_2, x_3] \mid x_3 f \in \langle x_1x_3, x_2x_3 \rangle\} = \{f \in k[x_1, x_2, x_3] \mid x_3 f = h_1x_1x_3 + h_2x_2x_3\} = \{f \in k[x_1, x_2, x_3] \mid f = h_1x_1 + h_2x_2\} = \langle x_1, x_2 \rangle$, where $h_1, h_2 \in k[x_1, x_2, x_3]$.

Next we introduce some notations for parametric multivariate polynomials. For a parametric polynomial $g \in k[U][X]$, the leading term, leading coefficient, leading monomial and total degree of g w.r.t. a monomial order $\prec_X$ are denoted by $\mathrm{lt}_X(g)$, $\mathrm{lc}_X(g)$, $\mathrm{lm}_X(g)$ and $\mathrm{tdeg}_X(g)$ respectively. Whether $g \in k[X]$ or $g \in k[U][X]$, we use $\mathrm{lc}_{x_i}(g)$ to denote the leading coefficient of g w.r.t. x_i.

A **specialization** of $k[U]$ is a homomorphism $\sigma : k[U] \to L$. In this paper, we only consider the specializations induced by elements in L^m. That is, for $\bar{\alpha} = (\alpha_1, \ldots, \alpha_m) \in L^m$, the induced specialization $\sigma_{\bar{\alpha}}$ is defined as

$$\sigma_{\bar{\alpha}} : \varphi \to \varphi(\bar{\alpha}),$$

where $\varphi \in k[U]$. Every specialization σ: $k[U] \to L$ extends canonically to a specialization σ: $k[U][X] \to L[X]$ by applying σ coefficient-wise.

For a set $E \subset k[U]$, the variety defined by E in L^m is denoted by $\mathbf{V}(E) = \{\bar{\alpha} \in L^m \mid f(\bar{\alpha}) = 0 \text{ for all } f \in E\}$. In this paper, an **algebraically constructible set** A is defined as follows: $A = \mathbf{V}(E) \setminus \mathbf{V}(N)$, where E, N are subsets of $k[U]$. It is easy to see that the algebraically constructible set A is not empty by ensuring that at least one $f \in N$ is not in the radical of $\langle E \rangle$.

For a parametric polynomial system, the definitions of comprehensive Gröbner system and minimal comprehensive Gröbner system are given below.

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

Definition 6. Let F be a set in $k[U][X]$, and S be a subset of L^m. Assume that $G_1, \ldots, G_l$ are subsets of $k[U][X]$, and $A_1, \ldots, A_l$ are algebraically constructible subsets of L^m such that $S = \bigcup_{i=1}^{l} A_i$ and $A_i \cap A_j = \emptyset$ for $i \neq j$. A finite set $\mathcal{G} = \{(A_1, G_1), \ldots, (A_l, G_l)\}$ is called a **comprehensive Gröbner system** (CGS) on S for F if $\sigma_{\bar{\alpha}}(G_i)$ is a Gröbner basis for $\langle \sigma_{\bar{\alpha}}(F) \rangle \subset L[X]$ with $\bar{\alpha} \in A_i$ and $i = 1, \ldots, l$. Each (A_i, G_i) is called a branch of $\mathcal{G}$. In particular, if $S = L^m$, then $\mathcal{G}$ is called a comprehensive Gröbner system for F.

Definition 7. A comprehensive Gröbner system $\mathcal{G} = \{(A_1, G_1), \ldots, (A_l, G_l)\}$ on S for F is said to be **minimal**, if for each $i = 1, \ldots, l$,

1. $A_i \neq \emptyset$;
2. $\sigma_{\bar{\alpha}}(G_i)$ is a minimal Gröbner basis for $\langle \sigma_{\bar{\alpha}}(F) \rangle \subset L[X]$ with $\bar{\alpha} \in A_i$;
3. if $G_i \neq \{0\}$, then for each $g \in G_i$, $\sigma_{\bar{\alpha}}(\mathrm{lc}_X(g)) \neq 0$ for any $\bar{\alpha} \in A_i$.

Abramov and Kvashenko (1993) studied the parametric gcd of univariate polynomials with one parameter. The definition of parametric gcd (one parameter) can be easily extended to the case m ($m \geq 1$).

Definition 8. Let F be a subset of $k[U][X]$, and S be a subset of L^m. Assume that $g_1, \ldots, g_r$ are parametric polynomials in $k[U][X]$, and $A_1, \ldots, A_r$ are algebraically constructible subsets of L^m such that $S = \bigcup_{i=1}^{r} A_i$ and $A_i \cap A_j = \emptyset$ for $i \neq j$. A finite set $\{(A_1, g_1), \ldots, (A_r, g_r)\}$ is called a **gcd system** on S for F, if for each $i = 1, \ldots, r$, $\sigma_{\bar{\alpha}}(g_i)$ is a gcd of $\sigma_{\bar{\alpha}}(F)$ for any specialization $\sigma_{\bar{\alpha}}$ with $\bar{\alpha} \in A_i$. Moreover, if $g_i \neq 0$, then we have $\sigma_{\bar{\alpha}}(\mathrm{lc}_X(g_i)) \neq 0$ for any $\bar{\alpha} \in A_i$. In particular, if $S = L^m$, we simply call it a gcd system for F.

3. Nagasaka's algorithms

As stated in the introduction, the gcd of non-parametric polynomials have been extensively studied in the literature because of the enormous importance of this operation in many symbolic computation algorithms and applications; see Brown (1971); Moses and Yun (1973); Zippel (1979) for instance. The main issue in the gcd computation is that of intermediate expression swell as analyzed in Knuth vol. 2.

Gianni and Trager (1985) and Sasaki and Suzuki (1992) studied the gcd of non-parametric polynomials by computing a Gröbner basis. Nagasaka (2017) extended their results to polynomials with parameters and proposed two algorithms to compute a gcd system of parametric multivariate polynomials. In the following, we provide an overview of Nagasaka's algorithms and illustrate their shortcomings; more details about the algorithms can be found in Nagasaka (2017).

3.1. Extending Gianni and Trager's algorithm

Nagasaka extended Proposition 2 in Gianni and Trager (1985) to state:

Lemma 9. *Let $f_1, \ldots, f_s, g \in k[X]$ be primitive w.r.t. x_1, J be a maximal ideal in $k[X_2]$ such that $1 \in \langle f_1, \ldots, f_s, J \rangle$ and $1 \in \langle \mathrm{lc}_{x_1}(gf_i), J \rangle$ for some i. Let G be a Gröbner basis for $\langle gf_1, \ldots, gf_s, J^r \rangle$ w.r.t. any total degree order, where r is a positive integer. Then, the polynomial $\hat{g}$ in G of least total degree is an associate of g if the least total degree of the elements in J^r is larger than $\mathrm{tdeg}(g)^2$.*

Nagasaka further extended Lemma 9 to the case of parametric polynomials for which additional conditions on the ideal $J \subset k[U][X_2]$ for each specialization $\sigma_{\bar{\alpha}}$ must be satisfied:

1. $\sigma_{\bar{\alpha}}(f_1), \ldots, \sigma_{\bar{\alpha}}(f_s)$ are primitive w.r.t. x_1;
2. $\sigma_{\bar{\alpha}}(J)$ is a maximal ideal in $L[X_2]$;

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

3. $1 \in \langle \mathrm{lc}_{x_1}(\sigma_{\bar{\alpha}}(f_i)), \sigma_{\bar{\alpha}}(J)\rangle$ for some i;
4. $1 \in \langle \bar{f}_1, \ldots, \bar{f}_s, \sigma_{\bar{\alpha}}(J)\rangle$, where each $\bar{f}_i \in L[X]$ is the cofactor of $\sigma_{\bar{\alpha}}(f_i)$.

To satisfy these conditions, the parametric space L^m needs to be decomposed into branches such that $F \subset k[U][X]$ and each J have the following properties.

Definition 10. For any given $F = \{f_1, \ldots, f_s\} \subset k[U][X]$ with $S \subset L^m$ and $J \subset k[U][X_2]$, we introduce the following.

1. F is said to be S-**primitive** if $\forall \bar{\alpha} \in S$, $\sigma_{\bar{\alpha}}(f_1), \ldots, \sigma_{\bar{\alpha}}(f_s)$ are primitive w.r.t. x_1;
2. J is said to be S-**maximal** if $\forall \bar{\alpha} \in S$, $\sigma_{\bar{\alpha}}(J)$ is a maximal ideal in $L[X_2]$;
3. F is said to be S-**nonvanishlc** if $\forall \bar{\alpha} \in S$, $\mathrm{lc}_{x_1}(\sigma_{\bar{\alpha}}(f_i)) = \sigma_{\bar{\alpha}}(\mathrm{lc}_{x_1}(f_i))$ for each i;
4. F is said to be S-**nondegenerate** if $\forall \bar{\alpha} \in S$, $1 \in \langle \mathrm{lc}_{x_1}(\sigma_{\bar{\alpha}}(f_i)), \sigma_{\bar{\alpha}}(J)\rangle$ for some i;
5. J is said to be S-**luckyprime** if $\forall \bar{\alpha} \in S$, $1 \in \langle \bar{f}_1, \ldots, \bar{f}_s, \sigma_{\bar{\alpha}}(J)\rangle$, where each $\bar{f}_i \in L[X]$ is the cofactor of $\sigma_{\bar{\alpha}}(f_i)$.

Under these conditions, Nagasaka proposed an algorithm to compute a gcd system for F by combining Lemma 9 and Definition 10, which we call henceforth, the Nagasaka-GT algorithm.

Step 1: compute the S-primitive part of F w.r.t. x_1;
Step 2: decompose S such that F is S-nonvanishlc;
Step 3: construct a maximal ideal $J \subset k[U][X_2]$ such that F is S-nondegenerate;
Step 4: compute a minimal CGS for $\langle F \cup J^r\rangle$ on S, where r satisfies the condition of Lemma 9;
Step 5: check whether J is a S-luckyprime, if not, return to the Step 3;
Step 6: obtain the gcd system for F on S.

As the reader will notice, the above conditions are complicated and not easy to appreciate. Further, while implementing the Nagasaka-GT algorithm in Singular, we discovered the following shortcomings. We assume in the following examples that $U = \{a, b\}$, $X = \{x_1, x_2, x_3\}$ and consider the lexicographic order $\succ_X$ with $x_1 > x_2 > x_3$.

- In Step 1, Nagasaka needs to call this algorithm repeatedly to compute the primitive part of each parametric polynomial. For example, computing the primitive part of $f = (1-a)x_1^3x_2^2 + a(b-1)x_1^3x_2x_3 + (a^2-a)x_1x_2^2 + (a-b)x_1x_3 + (a-1)x_2^2 + a(b-1)x_2x_3^3 + ax_3$ w.r.t. x_1 on $\mathbb{C}^2$, we must know a gcd system for the coefficients of f w.r.t. x_1 on $\mathbb{C}^2$, i.e., we have to call this algorithm to compute the gcd system of f_{11}, f_{12}, f_{13}, where $f_{11} = (1-a)x_2^2 + a(b-1)x_2x_3$, $f_{12} = (a^2-a)x_2^2 + (a-b)x_3$ and $f_{13} = (a-1)x_2^2 + a(b-1)x_2x_3^3 + ax_3$. As the number of variables increases, this becomes more and more tedious, resulting in computational inefficiency.
- Step 2 is not necessary. Step 1 has ensured that the leading coefficient of f w.r.t. x_1 is not zero on each branch S_j, i.e., $\mathrm{lc}_{x_1}(\sigma_{\bar{\alpha}}(f)) = \sigma_{\bar{\alpha}}(\mathrm{lc}_{x_1}(f))$ for any $\bar{\alpha} \in S_j$. Therefore, Step 2 can be removed.
- If the parameter space S is divided into many small areas, more and more maximal ideals need to be constructed in Step 3. Although Nagasaka proved that a maximal ideal $J \subset k[U][x_2, x_3]$ which is S-nondegenerate and S-luckyprime can be constructed in a finite number of steps, we do not know how much time it takes to construct so many maximal ideals.
- Since we do not know the polynomial g in Lemma 9, we need to estimate the value of r in Step 4. Without any loss of generality, we often let $r = \min\{\mathrm{tdeg}_X(f_i)^2 + 1 \mid f_i \in F\}$. For instance, let $F = \{f_1, f_2\}$ and $J = \langle x_2 - c_2, x_3 - c_3\rangle$, where $f_1 = ax_1^3x_2^2x_3 + (1-b)(x_2^2 + x_3)$, $f_2 = (1-a)x_1^3x_2^2x_3 + b(x_2^2 + x_3)$. Then, $r = 37$. There are two problems: first, it will take more time to compute the minimal CGS of $\langle F \cup J^{37}\rangle$ which sometimes does not terminate in an hour; second, since $c_2, c_3 \in \mathbb{C}$ are chosen randomly, sometimes c_i^{37} is a large integer.

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

3.2. Extending Sasaki and Suzuki's algorithm

Sasaki and Suzuki (1992) also used a Gröbner basis construction to compute the gcd of non-parametric polynomials, by improving upon Gianni and Trager's results. They obtained a similar theorem, but did not need to use a maximal ideal $J \subset k[X_2]$.

Theorem 11. (Theorem 1 in Sasaki and Suzuki (1992)) *Let $f_1, f_2 \in k[X]$ be primitive w.r.t. x_1, and G be the Gröbner basis for $\langle f_1, f_2 \rangle$ w.r.t. any block order such that $x_1 \gg X_2$. Then, there exists a polynomial $h \in k[X_2]$ such that $\hat{g} = h \cdot \gcd(f_1, f_2)$, where $\hat{g}$ is the polynomial in G of least degree in x_1.*

Using the insight in Theorem 11, Nagasaka proposed an other algorithm (henceforth called, Nagasaka-SS algorithm) to compute a gcd system for $F \subset k[U][X]$.

Step 1: compute an S-primitive decomposition of F;
Step 2: compute a minimal CGS for an S-primitive of F;
Step 3: compute a gcd system for the coefficients of candidate factor;
Step 4: compute the primitive part in each branch;
Step 5: obtain the gcd system for F on S.

There are similarities between Nagasaka-SS algorithm and Nagasaka-GT algorithm which are also sources of inefficiency: both need to compute S-primitive decompositions and make recursive calls to compute a gcd system for the coefficients of parametric polynomials in F. Nagasaka-SS algorithm has been observed to be more efficient than Nagasaka-GT algorithm, since Nagasaka-SS algorithm does not need to construct many maximal ideals and only needs to compute the minimal CGS of $\langle F \rangle$ rather than $\langle F \cup J^r \rangle$.

4. New parametric GCD algorithms

As stated above, there are many well-known algorithms for computing the gcd of non-parametric multivariate polynomials starting from Euclid's algorithm improved by Collins using reduced polynomial remainder sequences (PRS), Brown and Traub and Brown's subresultant PRS with EZGCD algorithm in MACSYMA for non-parametric polynomials in general and Zippel's algorithm based on sparse interpolation which is more efficient for sparse polynomials. There are also algorithms based on Gröbner basis computations. We are, however, interested in algorithms which generalize to parametric multivariate polynomials. To our knowledge, algorithms based on the Gröbner bases are most suited to generalize to the parametric case.

In this section, we propose two new algorithms which are based on comprehensive Gröbner systems for computing a gcd system of two parametric multivariate polynomials. To present the key ideas, in each subsection we first give the method for the non-parametric case and then we extend it to the parametric case.

4.1. Algorithm based on ideal intersection

The main idea of the first algorithm is that compute the least common multiple (lcm) of two non-parametric polynomials by computing the intersection of two principal ideals generated by one polynomial and another polynomial respectively. Since the intersection of two principal ideals is also a principal ideal, the generator can be obtained by a minimal Gröbner basis computation. This generator is the lcm of the two polynomials, and the gcd of the two polynomials is equal to the product of the two polynomials divided by this generator. To avoid introducing a new variable, we use the technique of module to compute the generator of the intersection of two principal ideals. For the parametric case, we only need to extend the results in non-parametric case to parametric case, and obtain a gcd system for two parametric polynomials by computing a minimal CGS of a module in $k[U][X]^3$.

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

4.1.1. Computing intersection of principal ideals

We first introduce the following proposition which plays an important role in the first proposed algorithm.

Proposition 12. *(pp. 189-190, Cox et al. (1992))*

1. *The intersection $I \cap J$ of two principal ideals $I, J \subset k[X]$, is a principal ideal.*
2. *If $I = \langle f_1 \rangle$, $J = \langle f_2 \rangle$ and $I \cap J = \langle f \rangle$, then $f = \text{lcm}(f_1, f_2)$.*
3. *Let $f_1, f_2 \in k[X]$, then $\text{lcm}(f_1, f_2) \cdot \text{gcd}(f_1, f_2) = f_1 \cdot f_2$.*

When $f_1 \cdot f_2 \neq 0$, it follows immediately from Proposition 12 that

$$\text{gcd}(f_1, f_2) = \frac{f_1 \cdot f_2}{\text{lcm}(f_1, f_2)}.$$

This gives an algorithm for computing the gcd of f_1 and f_2. Namely, we first compute $\text{lcm}(f_1, f_2)$ and then divide it into the product of f_1 and f_2 using the division algorithm. Proposition 12 tells us that the generator of the intersection of $\langle f_1 \rangle$ and $\langle f_2 \rangle$ is $\text{lcm}(f_1, f_2)$. The following is an important theorem for dealing with the computation of ideal intersection.

Theorem 13. *(pp. 187, Cox et al. (1992)) Let I, J be ideals in $k[X]$, then*

$$I \cap J = (\upsilon \cdot I + (1 - \upsilon) \cdot J) \cap k[X],$$

where υ is a new variable which is different from X.

The above theorem and Elimination Theorem (Theorem 2, pp. 116, in Cox et al. (1992)) lead to the following method for computing $\text{lcm}(f_1, f_2)$: introduce a new variable υ and consider the ideal $\langle \upsilon f_1, (1 - \upsilon) f_2 \rangle$, compute a minimal Gröbner basis w.r.t. a monomial order in which υ is greater than X, then the element of this Gröbner basis which do not contain the variable υ is the lcm of f_1 and f_2.

Given that the complexity of Gröbner basis computations is heavily influenced by the number of variables and the total degrees of polynomials (Mayr and Meyer, 1982; Möller and Mora, 1984; Dubé, 1990; Bayer and Mumford, 1993), we believe that the computation of ideal intersection over modules in the Chapter 5 of Cox et al. (2005) is likely to be more efficient. This has also been verified by the performance of comparing our implementations.

Let $\mathbf{e}_1 = (1, 0, 0)^T$, $\mathbf{e}_2 = (0, 1, 0)^T$ and $\mathbf{e}_3 = (0, 0, 1)^T$, then $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ is a free basis of $k[X]^3$, where ^{T} stands for transposition. That is, for any element $\vec{v}$ in $k[X]^3$, it can be expressed as $\vec{v} = h_1 \cdot \mathbf{e}_1 + h_2 \cdot \mathbf{e}_2 + h_3 \cdot \mathbf{e}_3$ where $h_1, h_2, h_3 \in k[X]$. For any submodule W of $k[X]^3$, we can also compute the Gröbner basis of W. The module case follows the ideal case almost exactly. However, we need to extend the notion of monomial orders to the free module $k[X]^3$. Let $\prec$ be a term order on $k[X]$, then extend $\prec$ to the $k[X]^3$ in a position over term fashion with $\mathbf{e}_3 \prec \mathbf{e}_2 \prec \mathbf{e}_1$.

Theorem 14. *Let f_1, f_2 be two nonzero polynomials in $k[X]$ and $\prec$ be a monomial order on $k[X]$. Suppose $W \subset k[X]^3$ is a $k[X]$-module generated by $\{\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3, f_1 \cdot \mathbf{e}_1, f_2 \cdot \mathbf{e}_2\}$ and G is a* **minimal** *Gröbner basis of W w.r.t. an order extended from $\prec$ in a position over term fashion with $\mathbf{e}_3 \prec \mathbf{e}_2 \prec \mathbf{e}_1$. Then there exists a unique nonzero polynomial $f \in k[X]$ such that $f \cdot \mathbf{e}_3 \in G$ and $\langle f \rangle = \langle f_1 \rangle \cap \langle f_2 \rangle$.*

Proof. Let $F = \{f \in k[X] \mid f \cdot \mathbf{e}_3 \in G\}$. As f_1 and f_2 are both nonzero by assumption, it is easy to verify that the set F is not empty. We prove $\langle F \rangle = \langle f_1 \rangle \cap \langle f_2 \rangle$ below.

We first show $\langle f_1 \rangle \cap \langle f_2 \rangle \subset \langle F \rangle$. For any given polynomial f in $\langle f_1 \rangle \cap \langle f_2 \rangle$, there exists two polynomials $p, q \in k[X]$ such that $f = pf_1 = qf_2$. Then, $f \cdot \mathbf{e}_3 = f(\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3) - p(f_1 \cdot \mathbf{e}_1) - q(f_2 \cdot \mathbf{e}_1)$ implies $f \cdot \mathbf{e}_3 \in W$. Since G is a minimal Gröbner basis of W, it follows that $f \in \langle F \rangle$.

For the converse, suppose $f' \in \langle F \rangle$. Then there exist polynomials $p_1, \ldots, p_r, g_1, \ldots, g_r \in k[X]$ such that $f' = \sum_{i=1}^{r} (p_i g_i)$ and $g_i \cdot \mathbf{e}_3 \in G$ for $1 \leq i \leq r$. Thus, we have $f' \cdot \mathbf{e}_3 \in \langle G \rangle$, which implies $f' \cdot \mathbf{e}_3 =$

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

$h_1(\mathbf{e}_1+\mathbf{e}_2+\mathbf{e}_3)+h_2(f_1\cdot\mathbf{e}_1)+h_3(f_2\cdot\mathbf{e}_2)$ for some polynomials $h_1,h_2,h_3\in k[X]$. From this equation we can obtain the following equations:

$$\begin{cases} 0=h_1+h_2f_1,\\ 0=h_1+h_3f_2,\\ f'=h_1. \end{cases}$$

It can easily be seen that $f'\in\langle f_1\rangle\cap\langle f_2\rangle$.

Therefore, we have $\langle F\rangle=\langle f_1\rangle\cap\langle f_2\rangle$. Proposition 12 implies that $\langle F\rangle$ is a principal ideal and $\langle F\rangle=\langle f\rangle$, where $f=\mathrm{lcm}(f_1,f_2)$. Besides, G is a Gröbner basis of W, there must exist a polynomial $g\in k[X]\setminus\{0\}$ such that $g\cdot\mathbf{e}_3\in G$ and $\mathrm{lm}(g)=\mathrm{lm}(f)$. Moreover, we have $g=f$ as G is minimal, because otherwise there should exist another element in G that divides $(g-\frac{\mathrm{lc}(g)}{\mathrm{lc}(f)}f)\cdot\mathbf{e}_3$ and has a smaller leading monomial than $\mathrm{lm}(f)\cdot\mathbf{e}_3$. □

Based on the results of Proposition 12 and Theorem 14, we can get the gcd of f_1 and f_2 by using the following corollary.

Corollary 15. *Let f_1, f_2 be two polynomials in $k[X]$ and $\prec$ be a monomial order on $k[X]$. Suppose $W\subset k[X]^3$ is a $k[X]$-module generated by $\{\mathbf{e}_1+\mathbf{e}_2+\mathbf{e}_3, f_1\cdot\mathbf{e}_1, f_2\cdot\mathbf{e}_2\}$ and G is a* **minimal** *Gröbner basis for W w.r.t. an order extended from $\prec$ in a position over term fashion with $\mathbf{e}_3\prec\mathbf{e}_2\prec\mathbf{e}_1$. Let $F=\{f\in k[X]\mid f\cdot\mathbf{e}_3\in G\}$. Then*

1. *If F is empty, then $f_1\cdot f_2=0$. In this case, $\gcd(f_1,f_2)$ is equal to 0 or f' which satisfies $f'\cdot(0,1,\star)^T\in G$, where $\star$ stands for 0 or 1.*
2. *If F is not empty, then $F=\{\mathrm{lcm}(f_1,f_2)\}$ and $\gcd(f_1,f_2)=\frac{f_1\cdot f_2}{\mathrm{lcm}(f_1,f_2)}$.*

Proof. If $f_1=f_2=0$, then $G=\{\mathbf{e}_1+\mathbf{e}_2+\mathbf{e}_3\}$ and F is empty. In this case, $\gcd(f_1,f_2)=0$. If $f_1=0$ and $f_2\neq0$, then $G=\{\mathbf{e}_1+\mathbf{e}_2+\mathbf{e}_3, f_2\cdot\mathbf{e}_2\}$ and F is empty. In this case, $\gcd(f_1,f_2)=f_2$. If $f_1\neq0$ and $f_2=0$, then $G=\{\mathbf{e}_1+\mathbf{e}_2+\mathbf{e}_3, f_1\cdot(\mathbf{e}_2+\mathbf{e}_3)\}$ and F is empty. In this case, $\gcd(f_1,f_2)=f_1$. In the case of f_1 and f_2 being nonzero, the result follows Theorem 14. □

4.1.2. Algorithm 1 for computing a gcd system of two parametric polynomials

The nice thing about using the intersection of two principal ideals for computing the gcd is that Corollary 15 generalizes easily to the parametric case.

Theorem 16. *Given $f_1,f_2\in k[U][X]$ and an algebraically constructible set $A=\mathbf{V}(E)\setminus\mathbf{V}(N)\subset L^m$. Let $\mathcal{G}=\{(A_i,G_i)\}_{i=1}^l$ be a* **minimal** *comprehensive Gröbner system of the module $W=\langle\mathbf{e}_1+\mathbf{e}_2+\mathbf{e}_3, f_1\cdot\mathbf{e}_1, f_2\cdot\mathbf{e}_2\rangle$ on A w.r.t. an order extended from $\prec_X$ in a position over term fashion with $\mathbf{e}_3\prec\mathbf{e}_2\prec\mathbf{e}_1$. For each branch (A_i,G_i), let $F_i=\{f\in k[U][X]\mid f\cdot\mathbf{e}_3\in G_i\}$. Then we have the following results:*

1. *If F_i is empty, then $\gcd(\sigma_{\bar\alpha}(f_1),\sigma_{\bar\alpha}(f_2))$ is equal to 0 or $\sigma_{\bar\alpha}(f')$ which satisfies $f'\cdot(0,1,\star)^T\in G_i$ for any $\bar\alpha\in A_i$, where $\star$ stands for 0 or 1.*
2. *If F_i is not empty, then $F_i=\{f\}$ and $\gcd(\sigma_{\bar\alpha}(f_1),\sigma_{\bar\alpha}(f_2))=\frac{\sigma_{\bar\alpha}(f_1\cdot f_2)}{\sigma_{\bar\alpha}(f)}$ for any $\bar\alpha\in A_i$.*

Proof. Since $\mathcal{G}$ is a **minimal** comprehensive Gröbner system, for each branch (A_i,G_i), the set $\sigma_{\bar\alpha}(G_i)$ is a minimal Gröbner basis of $\langle\sigma_{\bar\alpha}(W)\rangle$ for any $\bar\alpha\in A_i$. Besides, there are no elements in G_i that can specialize to 0 because the leading coefficients of all elements in G_i are nonzero under specialization. Therefore, it is easy to derive the results from Corollary 15. □

Note that in Theorem 16 (2), the expression $\frac{\sigma_{\bar\alpha}(g)}{\sigma_{\bar\alpha}(f)}$ is a polynomial in $L[X]$ for any $\bar\alpha\in A_i$, but the expression g/f is not necessarily a parametric polynomial in $k[U][X]$, where $g=f_1\cdot f_2$. However, since $\mathrm{lc}_X(f)$ is a nonzero polynomial in $k[U]$ that does not vanish for any specialization σ in the branch, we can use the following division in $k[U][X]$ to compute an associate of $\frac{\sigma_{\bar\alpha}(g)}{\sigma_{\bar\alpha}(f)}$.

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

To compute $q \in k[U][X]$ such that $\sigma_{\bar{\alpha}}(q) \sim \sigma_{\bar{\alpha}}(g)/\sigma_{\bar{\alpha}}(f)$, g is multiplied by $\mathrm{lc}_X(f)$ repeatedly during division so that

$$(\mathrm{lc}_X(f))^{\lambda} g = q \cdot f + h,$$

and no monomial in h is divisible by the leading monomial $\mathrm{lm}_X(f)$, where λ is a non-negative integer. Theorem 16 can guarantee that $\sigma_{\bar{\alpha}}(h)$ is zero for any $\bar{\alpha} \in A_i$. This operation is similar to the division algorithm in Montes (2002); Montes and Schoenemann (2016).

The pseudo-division algorithm in polynomial rings requires a main variable to be specified. Obviously, the above division is not the same as the pseudo-division, so we call it **special division algorithm** in $k[U][X]$, and denote by $\mathrm{Quo}(g, f)$ the quotient q.

We use a simple example to illustrate this algorithm. Let $g = x^2 - by + b$, $f = ax$ with $q = \mathrm{Quo}(g, f)$ and an algebraically constructible set $A = \mathbf{V}(ab) \setminus \mathbf{V}(a)$. Using the lexicographic order on X, where $X = \{x, y\}$ and $x > y$, f special-divides g in $k[U][X]$, giving $\mathrm{lc}_X(f) \cdot g = x \cdot f + h$, where $h = -aby + ab$. It is obvious that h is zero on A. Thus $q = x$. Moreover, for any $\bar{\alpha} \in A$, $\frac{\sigma_{\bar{\alpha}}(g)}{\sigma_{\bar{\alpha}}(f)} = \frac{1}{a}x$. Therefore, $\sigma_{\bar{\alpha}}(q) \sim \sigma_{\bar{\alpha}}(g)/\sigma_{\bar{\alpha}}(f)$.

Now, the first algorithm is given below and is called "Ideal Intersection Based GCD".

Proposition 17. *Algorithm 1 works correctly.*

Proof. The proof follows directly from Theorem 16. □

Algorithm 1 Ideal Intersection Based GCD

Input : $f_1, f_2 \in k[U][X]$, a constructible set $A \subset L^m$, and two monomial orders $\prec_X, \prec_U$.
Output: a gcd system $\{(A_i, h_i)\}_{i=1}^{l}$, where $\gcd(\sigma_{\bar{\alpha}}(f_1), \sigma_{\bar{\alpha}}(f_2)) = \sigma_{\bar{\alpha}}(h_i)$ for any $\bar{\alpha} \in A_i$ and $\cup_{i=1}^{l} A_i = A$.

```
1  begin
2      compute a minimal CGS {(A_i, G_i)}_{i=1}^l on A for ⟨e1 + e2 + e3, f1 · e1, f2 · e2⟩ ⊂ k[U][X]^3 in a position over term with
         e3 ≺ e2 ≺ e1;
3      for i from 1 to l do
4          F_i := {f ∈ k[U][X] | f · e3 ∈ G_i};
5          if F_i is not empty then
6              F_i := {f};
7              h_i := Quo(f1 · f2, f) on A_i;
8          else
9              h_i := 0 or f' which satisfies f' · (0, 1, ⋆)^T ∈ G_i on A_i;
10     return {(A_i, h_i)}_{i=1}^l.
```

4.2. Algorithm based on ideal quotient

The key idea of the second algorithm is well-known: compute the cofactor by computing the ideal quotient of one polynomial with respect to the other polynomial. This ideal quotient is known to be principal and has a single generator which can be computed by a single minimal Gröbner basis computation. This generator, which is the cofactor of the first polynomial, is used to obtain the gcd by dividing the polynomial by its cofactor. For the parametric case, a minimal comprehensive Gröbner system of a module in $k[U][X]^2$ is computed, leading to multiple branches for different specializations; for each branch, the generator is used to obtain the gcd for the associated parametric specializations.

4.2.1. Computing ideal quotient

The second algorithm is based on the following theorem.

Theorem 18. *Consider two polynomials $f_1, f_2 \in k[X] \setminus \{0\}$ such that $f_1 = d \cdot \bar{f}_1$ and $f_2 = d \cdot \bar{f}_2$, where $d = \gcd(f_1, f_2)$ and $\gcd(\bar{f}_1, \bar{f}_2) = 1$. Then, $\langle \bar{f}_1 \rangle = \langle f_1 \rangle : f_2$ and $\langle \bar{f}_2 \rangle = \langle f_2 \rangle : f_1$.*

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

Proof. We only prove $\langle \bar{f}_1 \rangle = \langle f_1 \rangle : f_2$, the proof of $\langle \bar{f}_2 \rangle = \langle f_2 \rangle : f_1$ follows in a similar manner.

Since $f_2 \bar{f}_1 = d \bar{f}_2 \bar{f}_1 = \bar{f}_2 f_1 \in \langle f_1 \rangle$, then $\langle \bar{f}_1 \rangle \subseteq \langle f_1 \rangle : f_2$. In the other direction, if there exists a polynomial $g \in \langle f_1 \rangle : f_2$ such that $\bar{f}_1 \nmid g$, then by division algorithm in $k[X]$, g is written as $g = p\bar{f}_1 + r$, where $p, r \in k[X]$, and none of the monomials in r is divisible by $\mathrm{lm}(\bar{f}_1)$. Note that $g f_2 \in \langle f_1 \rangle$ implies $(p\bar{f}_1 + r) f_2 = h f_1$, where $h \in k[X]$. Hence, $(h - p\bar{f}_2)\bar{f}_1 = r\bar{f}_2$ by dividing both sides by d and $\gcd(\bar{f}_1, \bar{f}_2) = 1$. This would require that $\bar{f}_1 \mid r$ giving a contradiction. Hence $\langle f_1 \rangle : f_2 \subseteq \langle \bar{f}_1 \rangle$. □

Theorem 18 implies that $\langle f_1 \rangle : f_2$ is a principal ideal. A minimal Gröbner basis G of $\langle f_1 \rangle : f_2$ w.r.t. a monomial order $\prec$ is $\{g\}$ such that $\gcd(f_1, f_2) = f_1/g$. Depending upon the structure of f_1, f_2 and the degree of their gcd relative to the degrees of f_1 and f_2, computing $\langle f_1 \rangle : f_2$ or $\langle f_2 \rangle : f_1$ can have varied performance.

A ideal quotient can be computed using ideal intersection which involves introducing a new variable to construct a new ideal in a bigger polynomial ring. In the following, we introduce a new method to compute the ideal quotient $\langle f_1 \rangle : f_2$.

Theorem 19. *Let f_1, f_2 be two polynomials in $k[X] \setminus \{0\}$ and $\prec$ be a monomial order on $k[X]$. Suppose $W \subset k[X]^2$ is a $k[X]$-module generated by $\{f_1 \cdot \vec{e}_1, f_2 \cdot \vec{e}_1 - \vec{e}_2\}$ and G is a* **minimal** *Gröbner basis of W w.r.t. an order extended from $\prec$ in a position over term fashion with $\vec{e}_2 \prec \vec{e}_1$, where $\vec{e}_1 = (1, 0)^T$ and $\vec{e}_2 = (0, 1)^T$. Then there exists a unique polynomial $g \in k[X] \setminus \{0\}$ such that $g \cdot \vec{e}_2 \in G$ and $\langle g \rangle = \langle f_1 \rangle : f_2$.*

Proof. Let $H = \{h \in k[X] \mid h \cdot \vec{e}_2 \in G\}$. As f_1 and f_2 are both nonzero by assumption, it is easy to check that the set H is not empty. We prove $\langle H \rangle = \langle f_1 \rangle : f_2$ below.

We first show $\langle f_1 \rangle : f_2 \subset \langle H \rangle$. For any given polynomial p in $\langle f_1 \rangle : f_2$, there exists a polynomial $q \in k[X]$ such that $p f_2 = q f_1$. Then, $p \cdot \vec{e}_2 = q(f_1 \cdot \vec{e}_1) - p(f_2 \cdot \vec{e}_1 - \vec{e}_2)$ implies $p \cdot \vec{e}_2 \in W$. Since G is a minimal Gröbner basis of W, it follows that $p \in \langle H \rangle$.

For the converse, suppose $h \in \langle H \rangle$. Then there exist polynomials $g_1, \ldots, g_s, p_1, \ldots, p_s \in k[X]$ such that $h = \sum_{i=1}^{s} (p_i g_i)$ and $g_i \cdot \vec{e}_2 \in G$ for $1 \le i \le s$. Thus, we have $h \cdot \vec{e}_2 \in \langle G \rangle$, which implies $h \cdot \vec{e}_2 = h_1(f_1 \cdot \vec{e}_1) + h_2(f_2 \cdot \vec{e}_1 - \vec{e}_2)$ for some polynomials $h_1, h_2 \in k[X]$. From this equation we can obtain the following equations:

$$\begin{cases} 0 = h_1 f_1 + h_2 f_2, \\ h = -h_2. \end{cases}$$

Therefore, we have $h \in \langle f_1 \rangle : f_2$.

In sum, we have $\langle H \rangle = \langle f_1 \rangle : f_2$. By Theorem 18, we obtain $\langle H \rangle = \langle \bar{f}_1 \rangle$, where $\bar{f}_1$ is the cofactor of f_1. Besides, G is a Gröbner basis of W, there must exist a polynomial $g \in k[X] \setminus \{0\}$ such that $g \cdot \vec{e}_2 \in G$ and $\mathrm{lm}(g) = \mathrm{lm}(\bar{f}_1)$. Moreover, we have $g = \bar{f}_1$ as G is minimal, because otherwise there should exist another element in G that divides $(g - \frac{\mathrm{lc}(g)}{\mathrm{lc}(f_1)} \bar{f}_1) \cdot \vec{e}_2$ and has a smaller leading monomial than $\mathrm{lm}(\bar{f}_1) \cdot \vec{e}_2$. □

Theorem 19 only discusses the case when f_1 and f_2 are both nonzero polynomials. We can extend the result to more general cases.

Corollary 20. *Let f_1, f_2 be two polynomials in $k[X]$ and $\prec$ be a monomial order on $k[X]$. Suppose $W \subset k[X]^2$ is a $k[X]$-module generated by $\{f_1 \cdot \vec{e}_1, f_2 \cdot \vec{e}_1 - \vec{e}_2\}$ and G is a* **minimal** *Gröbner basis for W w.r.t. an order extended from $\prec$ in a position over term fashion with $\vec{e}_2 \prec \vec{e}_1$. Let $H = \{h \in k[X] \mid h \cdot \vec{e}_2 \in G\}$. Then*

1. *If H is empty, then $f_1 = 0$ and $f_2 \neq 0$. In this case, $\gcd(f_1, f_2) = f_2$.*
2. *If H is not empty, then $H = \{\bar{f}_1\}$ and $\gcd(f_1, f_2) = f_1/\bar{f}_1$.*

Proof. If $f_1 = 0$, $f_2 \neq 0$, then H can be checked to be empty. If $f_1 = f_2 = 0$, then $H = \{1\}$. If $f_1 \neq 0$ and $f_2 = 0$, then $H = \{1\}$ and $\gcd(f_1, f_2) = f_1$. In the case of f_1 and f_2 being nonzero, the result follows Theorem 19. □

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

Table 1
The comparison of two new algorithms.

	Algorithm 1	Algorithm 2
approach	ideal intersection	ideal quotient
gcd in $k[X]$	$f_1 f_2/\text{lcm}(f_1, f_2)$	$f_1/\tilde{f}_1$
$k[U][X]$-module	$k[U][X]^3$	$k[U][X]^2$
minimal CGS	$\langle \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3, f_1 \cdot \mathbf{e}_1, f_2 \cdot \mathbf{e}_2 \rangle$	$\langle f_1 \cdot \vec{e}_1, f_2 \cdot \vec{e}_1 - \vec{e}_2 \rangle$

By Corollary 20, the gcd of f_1 and f_2 can be obtained from the Gröbner basis G directly without any knowledge of f_1 or f_2 being zero or not.

4.2.2. Algorithm 2 for computing a gcd system of two parametric polynomials

Now, we generalize Corollary 20 to the parametric case.

Theorem 21. *Given $f_1, f_2 \in k[U][X]$ and an algebraically constructible set $A = \mathbf{V}(E) \setminus \mathbf{V}(N) \subset L^m$, let $\mathcal{G} = \{(A_i, G_i)\}_{i=1}^{l}$ be a* **minimal** *comprehensive Gröbner system of the module $W = \langle f_1 \cdot \vec{e}_1, f_2 \cdot \vec{e}_1 - \vec{e}_2 \rangle$ on A w.r.t. an order extended from $\prec_X$ in a position over term fashion with $\vec{e}_2 \prec \vec{e}_1$. For each branch (A_i, G_i), let $H_i = \{h \in k[U][X] \mid h \cdot \vec{e}_2 \in G_i\}$. Then we have the following results.*

1. *If H_i is empty, then $\gcd(\sigma_{\bar{\alpha}}(f_1), \sigma_{\bar{\alpha}}(f_2)) = \sigma_{\bar{\alpha}}(f_2)$ for any $\bar{\alpha} \in A_i$.*
2. *If H_i is not empty, then $H_i = \{g_i\}$ and $\gcd(\sigma_{\bar{\alpha}}(f_1), \sigma_{\bar{\alpha}}(f_2)) = \frac{\sigma_{\bar{\alpha}}(f_1)}{\sigma_{\bar{\alpha}}(g_i)}$ for any $\bar{\alpha} \in A_i$.*

Proof. The proof is similar to that of Theorem 16. □

Now, the second algorithm based on ideal quotient construction is given below.

Algorithm 2 Ideal Quotient Based GCD

Input : $f_1, f_2 \in k[U][X]$, a constructible set $A \subset L^m$, and two monomial orders $\prec_X, \prec_U$.
Output: a gcd system $\{(A_i, h_i)\}_{i=1}^{l}$, where $\gcd(\sigma_{\bar{\alpha}}(f_1), \sigma_{\bar{\alpha}}(f_2)) = \sigma_{\bar{\alpha}}(h_i)$ for any $\bar{\alpha} \in A_i$ and $\cup_{i=1}^{l} A_i = A$.

```
1  begin
2      compute a minimal CGS {(A_i, G_i)}_{i=1}^l on A for ⟨f_1·e_1, f_2·e_1 − e_2⟩ ⊂ k[U][X]^2 in a position over term with e_2 ≺ e_1;
3      for i from 1 to l do
4          H_i := {h ∈ k[U][X] | h·e_2 ∈ G_i};
5          if H_i is not empty then
6              H_i has exactly one polynomial, say g_i;
7              h_i := Quo(f_1, g_i) on A_i;
8          else
9              h_i := f_2 on A_i;
10     return {(A_i, h_i)}_{i=1}^l.
```

Proposition 22. *Algorithm 2 works correctly.*

Proof. The proof follows directly from Theorem 21. □

4.3. Comparison of ideal intersection and ideal quotient GCD algorithms

As we see in the above two subsection, we proposed two algorithms to compute a gcd system of two parametric polynomials. Comparing the two proposed algorithms, we get the following results.

Table 1 shows the differences between the two proposed algorithms. Obviously, they have the following similarities: we use the method of module instead of introducing a new variable to compute the ideal intersection and quotient ideal, thus reducing the computation cost; use the special

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

division algorithm proposed in subsection 4.1.2 to compute the gcd system on different algebraically constructible sets. In Algorithm 1 and Algorithm 2, if f_1 (or f_2) vanishes on the constructible set A, we only need to compute a minimal comprehensive Gröbner system $\{(A_i, h_i)\}_{i=1}^{l}$ of f_2 (or f_1), and then the gcd of $\sigma_{\bar{\alpha}}(f_1)$ and $\sigma_{\bar{\alpha}}(f_2)$ on each branch A_i is $\sigma_{\bar{\alpha}}(h_i)$.

To experimentally compare the two proposed algorithms with both of Nagasaka's algorithms, we have implemented them all in Singular on a single platform so that their comparative performance can be fairly analyzed (Section 7).

4.4. Gcd systems for more than two parametric polynomials

Given parametric polynomials $f_1, \ldots, f_s \in k[U][X]$ with $s \geq 3$ and a constructible set A, their gcd system can also be computed by successively computing the gcd systems of two polynomials at a time. That is, given a monomial order, we first compute a gcd system $\{(A_i, h_i)\}_{i=1}^{l}$ of f_1 and f_2 on A, where $A = \cup_{i=1}^{l} A_i$. Then, for each branch we compute a gcd system $\{(A_{ij}, h_{ij})\}_{j=1}^{l_i}$ of h_i and f_3 on A_i, where $A_i = \cup_{j=1}^{l_i} A_{ij}$. Repeating the above process, we can get a gcd system of $f_1, f_2, \ldots, f_s$ on the different branch of A.

We recognize that many tricks can be applied to the both proposed algorithms. For example, when we get the gcd system $\{(A_i, h_i)\}_{i=1}^{l}$ of f_1 and f_2, then we can compute the gcd systems of h_i and f_3 on A_i for $i = 1, \ldots, l$ at the same time. The difference in polynomial selection can make a big difference in Algorithm 2, we often choose the polynomial with the lowest total degree w.r.t. X as the first polynomial. This is because the total degree of intermediate gcds goes down substantially as computations proceed.

5. An illustrative example

We illustrate the two proposed algorithm with a simple example.

Example 23. Let $f_1, f_2, f_3 \in \mathbb{C}[U][X]$ be as follows:

$$\begin{cases} f_1 = ax^2 + bxy + a^2xz + abx + abyz + b^2y, \\ f_2 = ax^2 + bxy + (ab - a)xz - a^2x + (b^2 - b)yz - aby, \\ f_3 = ax^2 + bxy + a^2xz + (a^2 - ab)x + abyz + (ab - b^2)y, \end{cases}$$

where $U = \{a, b\}$, $X = \{x, y, z\}$, $\prec_X$ and $\prec_U$ are all lexicographic orders with $z < y < x$ and $b < a$, respectively.

5.1. Algorithm 1 for Example 23

Step 1: compute a minimal CGS $\mathcal{G}_1$ for $\langle \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3, f_1 \cdot \mathbf{e}_1, f_2 \cdot \mathbf{e}_2 \rangle$ on $\mathbb{C}^2$.

There are six branches in $\mathcal{G}_1$. The first branch of $\mathcal{G}_1$ is $(A_1, G_1) = (\mathbb{C}^2 \setminus \mathbf{V}(a(a - b + 1)), \{(ax + by)(x + az + b)(x + (b - 1)z - a) \cdot \mathbf{e}_3, (f_1 - f_2) \cdot \mathbf{e}_2 + f_1 \cdot \mathbf{e}_3, f_2 \cdot \mathbf{e}_2, \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3\})$. Then, $F_1 = \{(ax + by)(x + az + b)(x + (b - 1)z - a) \cdot \mathbf{e}_3 \in \mathbb{C}[U][X] \mid (ax + by)(x + az + b)(x + (b - 1)z - a) \cdot \mathbf{e}_3 \in G_1\}$ and the gcd of f_1 and f_2 on A_1 is $h_1 = \mathrm{Quo}(f_1 \cdot f_2, (ax + by)(x + az + b)(x + (b - 1)z - a)) = ax + by$. Similarly, we can get the gcds of f_1 and f_2 on other five branches.

Step 2: compute a minimal CGS $\mathcal{G}_2$ for $\langle \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3, h_1 \cdot \mathbf{e}_1, f_3 \cdot \mathbf{e}_2 \rangle$ on A_1.

There is only one branch: $(A_1, G_2) = (\mathbb{C}^2 \setminus \mathbf{V}(a(a - b + 1)), \{f_3 \cdot \mathbf{e}_3, (ax + by) \cdot (\mathbf{e}_2 + \mathbf{e}_3), \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3\})$. Then $H_2 = \{f_3\}$ and the gcd of h_1 and f_3 on A_1 is $h_2 = \mathrm{Quo}(h_1 \cdot f_3, f_3) = ax + by$. It follows that the gcd of f_1, f_2 and f_3 on A_1 is $ax + by$.

Step 3: repeat Step 2 and obtain the following result.

5.2. Algorithm 2 for Example 23

Step 1: Computing a minimal CGS $\mathcal{G}_1$ for $\langle f_1 \cdot \vec{e}_1, f_2 \cdot \vec{e}_1 - \vec{e}_2 \rangle$ on $\mathbb{C}^2$.

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

Table 2
The gcd system of f_1, f_2, f_3.

No.	A_i	gcd
1	$\mathbb{C}^2 \setminus \mathbf{V}(a(a-b+1))$	$ax+by$
2	$\mathbf{V}(a-b+1) \setminus \mathbf{V}((2b-1)(b-1))$	$(b-1)x+by$
3	$\mathbf{V}(2a+1, 2b-1)$	$x-y$
4	$\mathbf{V}(a) \setminus \mathbf{V}(b(b-1))$	y
5	$\mathbf{V}(a, b-1)$	y
6	$\mathbf{V}(a, b)$	0

There are six branches in $\mathcal{G}_1$. The first branch of $\mathcal{G}_1$ is $(A_1, G_1) = (\mathbb{C}^2 \setminus \mathbf{V}(a(a-b+1)), \{(x + az + b) \cdot \vec{e}_2, ((a^2 - ab + a)xz + (a^2 + ab)x + (ab - b^2 + b)yz + (ab + b^2)y) \cdot \vec{e}_1 + \vec{e}_2, f_2 \cdot \vec{e}_1 - \vec{e}_2\})$. Then, $H_1 = \{x + az + b \in \mathbb{C}[U][X] \mid (x + az + b) \cdot \vec{e}_2 \in G_1\}$ and the gcd of f_1 and f_2 on A_1 is $h_1 = \mathrm{Quo}(f_1, x + az + b) = ax + by$. Similarly, we can get the gcds of f_1 and f_2 on other five branches.

Step 2: Computing a minimal CGS $\mathcal{G}_2$ for $\langle h_1 \cdot \vec{e}_1, f_3 \cdot \vec{e}_1 - \vec{e}_2 \rangle$ on A_1.

There is only one branch: $(A_1, G_2) = (\mathbb{C}^2 \setminus \mathbf{V}(a(a-b+1)), \{\vec{e}_2, h_1 \cdot \vec{e}_1\})$. Then $H_2 = \{1\}$ and the gcd of h_1 and f_3 on A_1 is $h_2 = \mathrm{Quo}(h_1, 1) = ax + by$. It follows that the gcd of f_1, f_2 and f_3 on A_1 is $ax + by$.

Step 3: Repeat Step 2 and obtain the gcds of f_1, f_2 and f_3 on other five branches. The result is the same as that in Table 2.

6. Extending ideal quotient to a system of more than two polynomials

Currently, we compute a gcd system of a pair of parametric polynomials whose output is a finite set of constructible sets with the corresponding gcds. For each such branch, the gcd is used to compute its gcd with the next polynomial leading to more branches. However, we can use a single comprehensive Gröbner system to compute a gcd system of more than two parametric polynomials.

In general, the equation $\gcd(f_1, \ldots, f_s) = \frac{f_1 \cdots f_s}{\mathrm{lcm}(f_1, \ldots, f_s)}$ does not hold for $s \geq 3$. For example, let $f_1 = x_1^2 x_2 x_3^2$, $f_2 = x_2^3 x_3$, and $f_3 = x_1^3 x_3^4$. Then, $\mathrm{lcm}(f_1, f_2, f_3) = x_1^3 x_2^3 x_3^4$, $\gcd(f_1, f_2, f_3) = x_3$, and $\mathrm{lcm}(f_1, f_2, f_3) \cdot \gcd(f_1, f_2, f_3) \neq f_1 f_2 f_3$. Hence, we cannot extend Algorithm 1 directly to the case of more than two parametric polynomials. However, we can generalize the method of Algorithm 2 to the case of more than two parametric polynomials. We first consider the gcd of non-parametric polynomials.

Theorem 24. *Let $I = \langle f_1 \rangle$ and $J = \langle f_2, \ldots, f_s \rangle$ be ideals in $k[X]$, where $f_1 \neq 0$ and $s \geq 3$. Then the ideal quotient $I : J$ is a principal ideal. If $I : J$ generated by a polynomial $g \in k[X]$, then $\gcd(f_1, \ldots, f_s)$ is an associate of $\frac{f_1}{g}$.*

Proof. According to Theorem 18 and Proposition 12, it follows from $I : J = \bigcap_{i=2}^{s} (\langle f_1 \rangle : f_i)$ that $I : J$ is a principal ideal. Suppose that $I : J = \langle g \rangle$, then $g \neq 0$ by the assumption. Since $I \subset I : J$, we have $f_1 \in \langle g \rangle$. This implies that $g \mid f_1$. Let $\gcd(f_1, \ldots, f_s) = d$, in the following we prove that $\frac{f_1}{g} \mid d$ and $d \mid \frac{f_1}{g}$.

Let $\langle f_1 \rangle : f_i = \langle f_{1i} \rangle$, where $f_{1i} \in k[X] \setminus \{0\}$ and $i = 2, \ldots, s$. Then $\langle g \rangle = \bigcap_{i=2}^{s} \langle f_{1i} \rangle$. This implies that for each i, we have $f_{1i} \mid g$ and $\frac{f_1}{g} \mid \frac{f_1}{f_{1i}}$. From the equation

$$\gcd(f_1, \ldots, f_s) = \gcd(\gcd(f_1, f_2), \ldots, \gcd(f_1, f_s)),$$

we have $d = \gcd(\frac{f_1}{f_{12}}, \ldots, \frac{f_1}{f_{1s}})$ and $\frac{f_1}{g} \mid d$. On the other hand, since $d \mid \frac{f_1}{f_{1i}}$ we have $f_{1i} \mid \frac{f_1}{d}$ for $i = 2, \ldots, s$. This implies that $\frac{f_1}{d} \in \bigcap_{i=2}^{s} \langle f_{1i} \rangle = \langle g \rangle$. Hence, $g \mid \frac{f_1}{d}$ implies that $d \mid \frac{f_1}{g}$. □

The most important thing in Theorem 24 is to compute the generator of the ideal quotient $\langle f_1 \rangle : \langle f_2, \ldots, f_s \rangle$. Theorem 19 cannot be generalized to the case of $s \geq 3$ directly. For example, let $f_1 =$

x^2yz^2, $f_2 = xy^2$, $f_3 = y^3z$, $\succ$ be the lexicographic order with $x > y > z$, and $\succ_3$ denotes the position over term extension of $\succ$ to $k[X]^3$. A minimal Gröbner basis for the module $\langle f_1 \cdot \vec{e}_1, f_2 \cdot \vec{e}_1 - \vec{e}_2, f_3 \cdot \vec{e}_1 - \vec{e}_3\rangle$ w.r.t. $\succ_3$ has an element $x^2z \cdot \vec{e}_3$. However, the ideal quotient $\langle x^2yz^2\rangle : \langle xy^2, y^3z\rangle$ is generated by x^2z^2, which leads to a contradiction. Next, we use syzygies to compute the ideal quotient $I : J$.

Theorem 25. *Let $I = \langle f_1\rangle$ and $J = \langle f_2, \ldots, f_s\rangle$ be ideals in $k[X]$, where $f_1 \neq 0$ and $s \geq 3$. A polynomial $h_1 \in k[X]$ is an element of $I : J$ if and only if h_1 appears as the first component of a syzygy $(h_1, \ldots, h_s)^T \in k[X]^s$ in the module $\mathrm{Syz}(M) = \{\vec{u} \in k[X]^s \mid M \cdot \vec{u} = \vec{0}\}$, where M is a polynomial matrix as follows:*

$$\begin{pmatrix} f_2 & f_1 & 0 & \cdots & 0 \\ f_3 & 0 & f_1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ f_s & 0 & 0 & \cdots & f_1 \end{pmatrix}.$$

Proof. Let $\vec{v}_i \in k[X]^{s-1}$ be the i-th **column** of matrix M, where $i = 1, \ldots, s$. Suppose that $h_1\vec{v}_1 + h_2\vec{v}_2 + \cdots + h_s\vec{v}_s = \vec{0}$. From the j-th component, we obtain an equation $h_1f_{j+1} + h_{j+1}f_1 = 0$, so $h_1 \in \langle f_1\rangle : f_{j+1}$, where $j = 1, \ldots, s-1$. Therefore, $h_1 \in \bigcap_{j=1}^{s-1}(\langle f_1\rangle : f_{j+1}) = I : J$.

On the other hand, for any given polynomial $g \in I : J$, we have $g \in \bigcap_{j=1}^{s-1}(\langle f_1\rangle : f_{j+1})$. That is, $\forall j \ (1 \leq j \leq s-1)$, $g \in \langle f_1\rangle : f_{j+1}$. This implies that there exists a polynomial $\varphi_j \in k[X]$ such that $gf_{j+1} = \varphi_j f_1$. Let $\vec{u} = (g, -\varphi_1, \ldots, \varphi_{s-1})^T$, then $M \cdot \vec{u} = \vec{0}$. It follows that $g \in I : J$ appears as the first component in $\mathrm{Syz}(M)$. □

Remark 26. In Cox et al. (2005), Proposition 3.11 (pp. 230, Chapter 5, Modules) uses syzygies to compute the intersection of two ideals. Theorem 25 is similar to Proposition 3.11 and is an answer to Exercise 10 in Cox et al. (2005) (pp. 232) which uses Proposition 3.11 to give an algorithm for computing $I : J$. Furthermore, according to Exercise 15 in Cox et al. (2005) (pp. 233), we have the following method to compute $\mathrm{Syz}(M)$. Let $\mathfrak{e}_1, \ldots, \mathfrak{e}_{2s-1}$ be the standard basis of the free module $k[X]^{2s-1}$, and consider the submodule $W \subset k[X]^{2s-1}$ generated by

$$\mathbf{w}_i = (\vec{v}_i^T, 0, \ldots, 0, 1_{s-1+i}, 0, \ldots, 0)^T, \quad i = 1, \ldots, s,$$

where $\mathbf{w}_i \in k[X]^{2s-1}$ and 1_{s-1+i} in $\mathbf{w}_i$ stands for 1 in the $(s-1+i)$-th component. Let G be a minimal Gröbner basis of W w.r.t. $\succ_{2s-1}$, where $\succ_{2s-1}$ denotes the position over term extension of $\succ$ to $k[X]^{2s-1}$. Then, the set $G_0 = \{\vec{u} \in k[X]^s \mid (\vec{0}^T, \vec{u}^T)^T \in G\}$ is a minimal Gröbner basis w.r.t. $\succ_s$ for the syzygy module $\mathrm{Syz}(M)$. Since $\langle f_1\rangle : \langle f_2, \ldots, f_s\rangle$ is a principal ideal, G_0 has only one element $\vec{u}$. Then the first component of $\vec{u}$ is the generator of $\langle f_1\rangle : \langle f_2, \ldots, f_s\rangle$. The computer algebra system Singular command **syz** makes use of this idea (Decker and Lossen, 2006).

Now, we extend Theorem 24 and Theorem 25 to the case of parametric polynomials.

Theorem 27. *Given $f_1, \ldots, f_s \in k[U][X]$ and an algebraically constructible set $A = \mathbf{V}(E) \setminus \mathbf{V}(N) \subset L^m$, where for any specialization $\sigma_{\bar{\alpha}}$ the polynomial $\sigma_{\bar{\alpha}}(f_1)$ is nonzero with $\bar{\alpha} \in A$. Let $\mathcal{G} = \{(A_j, G_j)\}_{j=1}^{l}$ be a* **minimal** *comprehensive Gröbner system of the module $W \subset k[U][X]^{2s-1}$ generated by $\{\mathbf{w}_i\}_{i=1}^{s}$ on A w.r.t. an order extended from $\succ_X$ in a position over term fashion with $\mathfrak{e}_{2s-1} < \cdots < \mathfrak{e}_1$. For each branch (A_j, G_j), let $H_j = \{\vec{u} \in k[U][X]^s \mid (\vec{0}^T, \vec{u}^T)^T \in G_j\}$. Then we have the following results.*

1. *H_j has only one element $\vec{u}_j \in k[U][X]^s$; and*
2. *let $g_j \in k[U][X]$ be the first component of $\vec{u}_j$, then $\gcd(\sigma_{\bar{\alpha}}(f_1), \ldots, \sigma_{\bar{\alpha}}(f_s)) = \frac{\sigma_{\bar{\alpha}}(f_1)}{\sigma_{\bar{\alpha}}(g_j)}$ for any $\bar{\alpha} \in A_j$.*

Proof. The proof is similar to that of Theorem 16. □

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

Remark 28. When we check whether f_1 is nonzero on A, we only need to check whether the intersection of A and the variety generated by the coefficients of f_1 w.r.t. X is empty. For example, $f_1 = ax + by \in \mathbb{C}[a,b][x,y]$ and $A = \mathbb{C}^2$. Let A_{f_1} be the variety generated by the coefficients of f_1 w.r.t. x, y, then $A_{f_1} = \mathbf{V}(a,b)$. Therefore, for any specialization $\sigma_{\bar{\alpha}}$ the polynomial $\sigma_{\bar{\alpha}}(f_1)$ is nonzero with $\bar{\alpha} \in \mathbb{C}^2 \setminus A_{f_1}$, and we can use Theorem 27 to compute the gcd system of $f_1, \ldots, f_s$ on $\mathbb{C}^2 \setminus A_{f_1}$. For any $\bar{\alpha} \in A_{f_1}$, we have $\gcd(\sigma_{\bar{\alpha}}(f_1), \sigma_{\bar{\alpha}}(f_2), \ldots, \sigma_{\bar{\alpha}}(f_s)) = \gcd(\sigma_{\bar{\alpha}}(f_2), \ldots, \sigma_{\bar{\alpha}}(f_s))$.

According to Theorem 27, we can obtain an extended algorithm for computing gcd systems of more than two parametric polynomials. Of course, the extended algorithm is still valid when the number of parametric polynomials is two. We can get the same result by using the extended algorithm to solve Example 23. We implemented the extended algorithm and compared it with other four algorithms in the following section.

7. Comparative performance with Nagasaka's algorithms

The two proposed algorithms, the extended algorithm and Nagasaka's algorithms (Nagasaka-GT algorithm and Nagasaka-SS algorithm) have been implemented by us in the computer algebra system *Singular (4-0-3)* (Decker et al., 2016). The implementations of five algorithms have been tried on a number of examples including the examples in Nagasaka (2017). The following table compares our implementations with Nagasaka's two algorithms for computing gcd systems of parametric multivariate polynomials. The parametric polynomials for the examples are given below:

- $F_1 = \{ax^3 + (a^3 - a + 1)x^2y + (a^2 + 2)xy^2 + (3a^2 - 3)y^3, ax^3 + (a+1)x^2y + 4xy^2 + 3y^3\}$, $X = \{x, y\}$, $U = \{a\}$;
- $F_2 = \{(x + ay + bz)^3 + c(x + ay + bz) + d, 3(x + ay + bz)^2 + c, 3a(x + ay + bz)^2 + ac, 3b(x + ay + bz)^2 + bc\}$, $X = \{x, y, z\}$, $U = \{a, b, c, d\}$;
- $F_3 = \{axz + (a-1)yz, (a-1)x^2 + axy\}$, $X = \{x, y, z\}$, $U = \{a\}$;
- $F_4 = \{ax^3y^2z + (1-b)(y^2 + z), (1-a)x^3y^2z + b(y^2 + z)\}$, $X = \{x, y, z\}$, $U = \{a, b\}$;
- $F_5 = \{(1-a)y^2 - bx^2 - cxy, (1-b)x^2 - ay^2 - cxy\}$, $X = \{x, y\}$, $U = \{a, b, c\}$;
- $F_6 = \{ax^2 + bxy + a^2xz + abx + abyz + b^2y, ax^2 + bxy + (ab - a)xz - a^2x + (b^2 - b)yz - aby, ax^2 + bxy + a^2xz + (a^2 - ab)x + abyz + (ab - b^2)y\}$, $X = \{x, y, z\}$, $U = \{a, b\}$;
- $F_7 = \{ax^2y + bx + y^3, ax^2y + bxy + cx, y^2 + bx^2y + cxy\}$, $X = \{x, y\}$, $U = \{a, b, c\}$;
- $F_8 = \{ax^3y + cxz^2, x^2y + 3dy + z, cx^2 + bxy, x^2y^2 + ax^2\}$, $X = \{x, y, z\}$, $U = \{a, b, c, d\}$;
- $F_9 = \{(ax + by)(x + a)(y - b), (aby^2 + b - 1)(bx + ay)(x + b)(y - a), (axy + a^2x - 3a)(ax + by)(x + b), (bx + ay)(ax + by)(ax + b)(by + a)\}$, $X = \{x, y\}$, $U = \{a, b\}$;
- $F_{10} = \{(1-a)x^2y + bx^2 + y^2, ax^2y + (1-b)xy + cx, y^2 + bx^2y + (1-c)xy\}$, $X = \{x, y\}$, $U = \{a, b, c\}$.

For all these examples, the monomial orders used on U and X are lexicographic orders, respectively. For interested readers, more comparative examples can be generated by the codes at: http://www.mmrc.iss.ac.cn/~dwang/software.html.

In Table 3, entry labeled "E-Algorithm" is for the extended algorithm of Algorithm 2. Timings were obtained on an Intel(R) Xeon(R) CPU E7-4809 v2 @ 1.90 GHz and 756 GB of RAM. As is evident from Table 3, our algorithms perform better than Nagasaka's algorithms. Since our algorithms are quite different from Nagasaka's algorithms, it is hard to analyze in theory where the improvements come from. In our opinion, the avoidance of checking primitive part contributes to most of the improvements.

The reasons that Algorithm 2 performs better than Algorithm 1 are as follows: choosing the polynomial with lowest total degree w.r.t. X as the first polynomial in each iteration, which can reduce the computations of $\mathrm{Quo}(f_1, \bar{f}_1)$; computing $\mathrm{Quo}(f_1, \bar{f}_1)$ takes less time than computing $\mathrm{Quo}(f_1 \cdot f_2, f)$; computing a minimal CGS for $\langle f_1 \cdot \vec{e}_1, f_2 \cdot \vec{e}_1 - \vec{e}_2 \rangle$ in $k[U][X]^2$ is faster than that for $\langle \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3, f_1 \cdot \mathbf{e}_1, f_2 \cdot \mathbf{e}_2 \rangle$ in $k[U][X]^3$. When the number of polynomials in F_i is greater than two, E-Algorithm is the fastest. This is because under the assumption of $f_1 \neq 0$, we only need to compute a minimal CGS for the module constructed by $f_1, f_2, \ldots, f_s$ $(s > 2)$. Since Nagasaka-SS algorithm does not need to construct maximal ideals in different parameter spaces, it performs better in practice than Nagasaka-GT algorithm for most of the examples.

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

Table 3
Comparative Performance of Parametric GCD Algorithms(sec).

Examples	Algorithm 1	Algorithm 2	E-Algorithm	Nagasaka-GT	Nagasaka-SS
F_1	0.134	0.127	0.129	1.428	0.442
F_2	0.889	0.391	0.135	30.985	12.771
F_3	0.151	0.145	0.146	6.159	1.836
F_4	0.271	0.183	0.190	$>$ 1h	7.148
F_5	0.843	0.561	0.572	6.210	2.426
F_6	0.615	0.571	0.327	$>$ 1h	8.401
F_7	0.755	0.605	0.361	$>$ 1h	$>$ 1h
F_8	1.188	1.005	0.537	$>$ 1h	20.407
F_9	1.669	1.487	1.173	$>$ 1h	5.105
F_{10}	1.426	1.164	0.893	$>$ 1h	$>$ 1h

8. Concluding remarks

Two new algorithms for computing gcd systems of parametric polynomials have been proposed. Using module comprehensive Gröbner system, the gcd systems of multivariate polynomials can be computed. The experimental data in Table 3 suggests that the two proposed algorithms are superior in practice in comparison with both the algorithms proposed by Nagasaka. We think this is because our methods do not compute the primitive part of polynomials in different parameter spaces, and our theorem guarantees that a parametric polynomial is special divisible by another parametric polynomial on various algebraically constructible sets. Since the computational efficiency of our algorithms depends on the number of branches in a module comprehensive Gröbner system, we believe that the two proposed algorithms can be further improved by removing inessential polynomials from comprehensive Gröbner system computations as discussed in Kapur and Yang (2014). This will be further studied in the future along with heuristics to minimize the number of branches to be considered for computing gcd systems of parametric multivariate polynomials.

Declaration of competing interest

Authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research was supported in part by the National Natural Science Foundation of China under Grant No. 11371356 and No. 61877058, the Chinese Academy of Sciences Key Project QYZDJ-SSW-SYS022, the National Science Foundation DMS-1217054, the CAS-SAFEA International Partnership Program for Creative Research Teams, the Strategy Cooperation Project AQ-1701, and the Beijing Advanced Innovation Center for Big Data and Brain Computing, Beihang University.

References

Abramov, S., Kvashenko, K., 1993. On the greatest common divisor of polynomials which depend on a parameter. In: Proceedings of the 1993 ACM International Symposium on Symbolic and Algebraic Computation, pp. 152–156.

Ayad, A., 2010. Complexity of algorithms for computing greatest common divisors of parametric univariate polynomials. Int. J. Algebra 4 (4), 173–188.

Bayer, D., Mumford, D., 1993. What can be computed in algebraic geometry? In: Eisenbud, D., Robbiano, L. (Eds.), Computational Algebraic Geometry and Commutative Algebra. Cambridge University Press, Cambridge, pp. 1–48.

Brown, W., 1971. On Euclid's algorithm and the computation of polynomial greatest common divisors. J. ACM 18, 478–504.

Cox, D., Little, J., O'shea, D., 1992. Ideals, Varieties, and Algorithms, third edition. Undergraduate Texts in Mathematics. Springer, New York.

Cox, D., Little, J., O'shea, D., 2005. Using Algebraic Geometry, second edition. Undergraduate Texts in Mathematics. Springer, New York.

Decker, W., Greuel, G.-M., Pfister, G., Schoenemann, H., 2016. SINGULAR 4.0.3. a computer algebra system for polynomial computations, fb mathematik der universitaet, d-67653 kaiserslautern https://www.singular.uni-kl.de/.

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006

Decker, W., Lossen, C., 2006. Computing in Algebraic Geometry: A Quick Start Using SINGULAR. Algorithms and Computation in Mathematics (AACIM), vol. 16. Springer, New York.

Dubé, T., 1990. The structure of polynomial ideals and Gröbner bases. SIAM J. Comput. 19, 750–775.

Gianni, P., Trager, B., 1985. GCDs and factoring multivariate polynomials using Gröbner bases. In: Proceedings of EUROCAL '85, European Conference on Computer Algebra. In: Lecture Notes in Computer Science, vol. 204. Springer, Berlin, Heidelberg, pp. 409–410.

Kapur, D., 1995. An approach for solving systems of parametric polynomial equations. In: Saraswat Hentenryck, V. (Ed.), Principles and Practices of Constraint Programming. MIT Press, pp. 217–244.

Kapur, D., Lu, D., Monagan, M., Sun, Y., Wang, D., 2018. An efficient algorithm for computing parametric multivariate polynomial GCD. In: Proceedings of the 2018 ACM on International Symposium on Symbolic and Algebraic Computation, pp. 239–246.

Kapur, D., Sun, Y., Wang, D., 2010. A new algorithm for computing comprehensive Gröbner systems. In: Proceedings of the 2010 ACM International Symposium on Symbolic and Algebraic Computation, pp. 29–36.

Kapur, D., Sun, Y., Wang, D., 2013. An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial system. J. Symb. Comput. 49, 27–44.

Kapur, D., Yang, Y., 2014. An algorithm for computing a minimal comprehensive Gröbner basis of a parametric polynomial system. In: Proceedings of Conference Encuentros de Algebra Computacionaly Aplicaciones (EACA).

Mayr, E., Meyer, A., 1982. The complexity of the word problems for commutative semigroups and polynomial ideals. Adv. Math. 46 (3), 305–329.

Möller, H., Mora, F., 1984. Upper and lower bounds for the degree of Gröbner bases. In: Fitch, J. (Ed.), EUROSAM 1984. In: Lecture Notes in Computer Science, vol. 174. Springer-Verlag, New York, pp. 172–183.

Montes, A., 2002. A new algorithm for discussing Gröbner bases with parameters. J. Symb. Comput. 33 (2), 183–208.

Montes, A., Schoenemann, H., 2016. grobcov.lib http://www.singular.uni-kl.de/Manual/latest/sing_900.htm.

Moses, J., Yun, D., 1973. The EZ GCD algorithm. In: Proceedings of ACM'73. ACM Press, New York, pp. 159–166.

Nabeshima, K., 2010. On the computation of parametric Gröbner bases for modules and syzygies. Jpn. J. Ind. Appl. Math. 27 (2), 217–238.

Nabeshima, K., 2012. Stability Conditions of Monomial Bases and Comprehensive Gröbner Systems. Proceedings of the International Conference on Computer Algebra in Scientific Computing, vol. 7442. Springer-Verlag, pp. 248–259.

Nagasaka, K., 2017. Parametric greatest common divisors using comprehensive Gröbner systems. In: Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, pp. 341–348.

Sanuki, M., Inaba, D., Sasaki, T., 2016. Computation of GCD of sparse multivariate polynomials by extended hensel construction. In: Proceedings of the 2016 IEEE International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, pp. 34–41.

Sasaki, T., Suzuki, M., 1992. Three new algorithms for multivariate polynomial GCD. J. Symb. Comput. 13 (4), 395–411.

Suzuki, A., Sato, Y., 2006. A simple algorithm to compute comprehensive Gröbner bases using gröbner bases. In: Proceedings of the 2006 ACM International Symposium on Symbolic and Algebraic Computation, pp. 326–331.

Weispfenning, V., 1992. Comprehensive Gröbner bases. J. Symb. Comput. 14 (3), 669–683.

Zippel, R., 1979. Probabilistic algorithms for sparse polynomials. In: Proceedings of EUROSAM'79. Springer-Verlag, pp. 216–226.

Please cite this article in press as: Kapur, D., et al. Algorithms for computing greatest common divisors of parametric multivariate polynomials. J. Symb. Comput. (2019), https://doi.org/10.1016/j.jsc.2019.10.006