J Syst Sci Complex (2017) 30: 196–233

Comprehensive Gröbner Basis Theory for a Parametric Polynomial Ideal and the Associated Completion Algorithm*

KAPUR Deepak

DOI: 10.1007/s11424-017-6337-8
Received: 29 December 2016

Abstract Gröbner basis theory for parametric polynomial ideals is explored with the main objective of mimicking the Gröbner basis theory for ideals. Given a parametric polynomial ideal, its basis is a comprehensive Gröbner basis if and only if for every specialization of its parameters in a given field, the specialization of the basis is a Gröbner basis of the associated specialized polynomial ideal. For various specializations of parameters, structure of specialized ideals becomes qualitatively different even though there are significant relationships as well because of finiteness properties. Key concepts foundational to Gröbner basis theory are reexamined and/or further developed for the parametric case: (i) Definition of a comprehensive Gröbner basis, (ii) test for a comprehensive Gröbner basis, (iii) parameterized rewriting, (iv) S-polynomials among parametric polynomials, (v) completion algorithm for directly computing a comprehensive Gröbner basis from a given basis of a parametric ideal. Elegant properties of Gröbner bases in the classical ideal theory, such as for a fixed admissible term ordering, a unique Gröbner basis can be associated with every polynomial ideal as well as that such a basis can be computed from any Gröbner basis of an ideal, turn out to be a major challenge to generalize for parametric ideals; issues related to these investigations are explored. A prototype implementation of the algorithm has been successfully tried on many examples from the literature.

Keywords Comprehensive Gröbner basis, minimal comprehensive Gröbner basis, parametric polynomial system, parametric S-polynomial, redundancy.

1 Introduction

The concept of a comprehensive Gröbner basis (CGB) was introduced by Weispfenning[1] to associate Gröbner basis like objects for parametric polynomial systems (see also the notion of a related concept of a parametric Gröbner basis independently introduced by Kapur[2]). For a specialization of parameters, a Gröbner basis of the specialized ideal is the specialized CGB.

KAPUR Deepak
Department of Computer Science, University of New Mexico, Albuquerque, NM, USA.
Email: kapur@cs.unm.edu.
*This research was supported by the National Science Foundation under Grant No. DMS-1217054.
◇ *This paper was recommended for publication by Editor-in-Chief GAO Xiao-Shan.*

These properties of a CGB make it very attractive in applications where a family of related problems can be parameterized and specified using a parametric polynomial system. For various specializations, they can be solved by specializing a parametric solution without having to repeat computations; see [1] for a discussion of application of parametric ideals in algebraic geometry and [2–6] for applications other than mathematics.

Because of their many applications, the topics of comprehensive Gröbner basis and system have been well investigated by researchers and a number of algorithms have been proposed to construct such objects for parametric polynomial systems[3–5, 7–15]. An algorithm for simultaneously generating a comprehensive Gröbner system (CGS) and a comprehensive Gröbner basis (CGB) by Kapur, et al. (KSW)[4] is particularly noteworthy because of its many nice properties: (i) Fewer segments (branches) in the resulting CGS, (ii) all polynomials in the CGS and CGB are faithful meaning that they are from the input ideal, and more importantly, (iii) the algorithm has been found efficient in practice[6].

There is however no algorithm to directly compute a minimal faithful CGB of a parametric ideal. Weispfenning's paper[1] and Kapur's paper[2] appear to be the only attempts to compute a CGB directly but the outputs in both cases are polynomials relative to segments or constrained polynomials†. Since Suzuki and Sato's paper[13] where they showed how the reduced Gröbner basis construction over $K[U][X]$ could be effectively used to compute a CGS, all known algorithms for computing a comprehensive Gröbner basis of a parametric ideal are indirect in the sense that they first compute a CGS and then extract from it an associated CGB. Even Weispfenning's algorithm[1] constructed a reduced Gröbner system, which is like a CGS; it however obtained a comprehensive Gröbner basis by collecting all polynomials generated and ignoring segments.

In this paper we give the first completion algorithm for directly computing a minimal faithful CGB of a parametric polynomial. It is patterned after Buchberger's algorithm. A parametric polynomial f can be viewed as a family of specialized polynomials generated from it with different leading terms, $\{f_{\alpha_1}, f_{\alpha_2}, \cdots, f_{\alpha_n}\}$ with $\alpha_1, \alpha_2, \cdots, \alpha_n$ being the associated segments of specializations on parameters. The algorithm computes a set of parametric S-polynomials of two parametric polynomials f and g from the critical pairs between the specialized tuples of f and g for various segments.

Like Buchberger's algorithm, the proposed completion algorithm depends upon a direct CGB test. Each parametric S-polynomial of every pair of distinct polynomials in a given basis must be reduced to 0 in its associated segment for the test to succeed. When the test fails, new polynomials generated from parametric S-polynomials with non-zero normal forms are added to the current basis. An important distinction of this algorithm is that reduction of a parametric

†In Section 4 entitled Reduced Gröbner Systems of his paper[1], Weispfenning discussed reduced comprehensive Gröbner basis as well as globally reduced comprehensive Gröbner basis which suggest that he was thinking along similar lines in defining minimal faithful comprehensive Gröbner basis; his notions were dependent upon global reduction algorithm which he never included in the paper but commented that it could be obtained by a slight modification of the usual non-parametric reduction algorithm by Buchberger!!! We beg to disagree with Weispfenning's assessment that such a global reduction algorithm could be easily designed.

S-polynomial is performed under a given segment: The leading term of an S-polynomial under the segment is simplified by a given basis under the the same segment.

The proposed completion algorithm has another nice feature that its output is always a minimal faithful CGB, in the sense that every polynomial in it is essential for the basis to be a CGB as well as every polynomial is in simplified form and in the parametric ideal generated by the input basis. In other words, every polynomial is needed for some specialization to ensure that the specialized CGB is indeed a Gröbner basis of the associated specialized ideal.

More importantly, the completion algorithm can be used to generate minimal faithful CGB for certain parametric ideals which cannot be obtained using other indirect algorithms proposed in the literature for computing a CGB.

The paper is organized as follows. After an overview of basic definitions in the next section, how specializations of parametric polynomials affect the behavior of polynomials is reviewed; notions of redundancy of a polynomial with respect to a basis and the associated minimality of a basis are discussed. Section 4 analyzes relationships among the reduced Gröbner basis, comprehensive Gröbner system, comprehensive Gröbner basis of a parametric polynomial ideal and redundancy for such bases. Methods for checking redundancy of a polynomial with respect to a comprehensive Gröbner basis as well as a comprehensive Gröbner system are presented. Section 5 proposes two ways to demonstrate existence of a canonical comprehensive Gröbner basis of a parametric ideal once a term ordering is fixed. The rest of the paper focuses on testing whether a given basis of a parametric ideal is a CGB as well as a Buchberger like completion algorithm for generating a minimal CGB from a given basis. Section 6 is on a decidable test for a given basis to be a CGB. Concepts of a family of parametric S-polynomials generated from a pair of parametric polynomials as well as reduction of a parametric polynomial by a finite basis of parametric polynomials with respect to a set of specializations are presented; they are closely related to the associated concepts discussed in [1, 2]. Section 7 introduces new operations on a CGB to make it smaller in our quest for generating a canonical CGB. Section 8 discusses the performance of a prototypical implementation of these operations on top of an implementation of the KSW algorithm in SINGULAR. Particularly, it is shown that much smaller CGBs can be generated from CGBs output by the KSW algorithm. Section 9 is a detailed discussion of the completion algorithm using concepts presented in Section 6. It is shown that the completion algorithm computes a minimal comprehensive Gröbner basis (MCGB). Section 10 is a detailed comparison with other algorithms proposed in the literature for computing a CGB. Section 11 presents some experimental observations from the prototypical implementation of the proposed completion algorithm in SINGULAR. In particular, two illustrative examples are given for which the algorithm computes MCGBs different from those given by algorithms including another indirect algorithm proposed by us. Section 12 comments on possible complications in designing an algorithm for computing a canonical CGB. The paper ends with concluding remarks and discusses topics for future research.

2 Preliminaries

Let K be a field, L an algebraically closed field extension of K, U and X are the sets of parameters and variables respectively. Let $>$ be an admissible total block term order in which $X \gg U$ (which implies that the terms in variables and parameters $U \cup X$ are bigger than terms in U). In a ring of parametric polynomials $K[U][X]$, where K is a field, for a polynomial $f \in K[U][X]$, $\mathrm{LC}(f) \in K[U]$, $\mathrm{LT}(f)$ is a term in X and $\mathrm{LM}(f) \in K[U][X]$ are defined as its leading coefficient, leading term and leading monomial with respect to a given term order $>$ respectively. For example, let $f = 32(u-1)x^2 + 4uy$, where $U = \{u\}$, $X = \{x, y\}$, and $>$ is a lexicographic term order with $x > y \gg u$. Then $\mathrm{LC}(f) = 32(u-1)$, $\mathrm{LT}(f) = x^2$ and $\mathrm{LM}(f) = \mathrm{LC}(f) \cdot \mathrm{LT}(f) = 32(u-1)x^2$. If a polynomial f is viewed without making distinction among parameters and variables (i.e., treating each symbol in $U \cup X$ as a variable, then the leading term in $U \cup X$, leading coefficient in K and leading monomial of f are defined appropriately; for the above f, they would be ux^2, 32 and $32ux^2$, respectively.

An admissible term ordering $>$ can be extended in a natural way to polynomials f, g: $f > g$ iff (i) $\mathrm{LT}(f) > \mathrm{LT}(g)$, (ii) $\mathrm{LT}(f) = \mathrm{LT}(g)$ and $\mathrm{LC}(f) > \mathrm{LC}(g)$, or (iii) $\mathrm{LM}(f) = \mathrm{LM}(g)$ and $f - \mathrm{LM}(f) > g - \mathrm{LM}(g)$. Unless an ordering on leading coefficients is total, a polynomial ordering so defined need not be total.

Similarly, two finite sets of polynomials S and S' can be compared using the polynomial ordering on their elements: $S > S'$ if (i) S is a proper superset of S' or (ii) otherwise, for every polynomial $g \in S' - S$, there is a polynomial $f \in S - S'$ such that $f > g$. Again if the underlying polynomial ordering is not total, then the ordering so induced on finite subsets of polynomials is also not total.

2.1 Gröbner Basis of a Polynomial Ideal

In his Ph.D. dissertation[16], Buchberger introduced special bases for polynomial ideals over a field and called them Gröbner bases; he also gave an algorithm for computing such bases from a given basis of an ideal. Over the last four decades, Gröbner basis theory have been extensively studied because of numerous applications of Gröbner bases in many theoretical domains including algebra, number theory, combinatorics, logic, etc., as well as in many practical domains in engineering, sciences, AI, formal methods and software design, cryptography, etc. Gröbner basis construction has been generalized along numerous directions. There are a number of books devoted to the topic as well as several implementations available in computer algebra systems including commercial systems such as Maple, Mathematica, as well as in research platforms such as MAGMA, SINGULAR.

Below we briefly review some key concepts in Gröbner basis theory for polynomial ideals. More details can be found in [17].

Definition 1 Given an ideal $I \subseteq K[U, X]$ and an admissible term ordering $>$, $GB \subseteq I$ is a Gröbner basis of I iff for every polynomial $p \in I, p$ rewrites (reduces) to 0 using GB. Equivalently, any polynomial $p \in K[U, X]$ has a unique normal form (also called its canonical form) with respect to GB.

A Gröbner basis is reduced iff (i) it is minimal (to mean all its elements are essential), (ii)

the head coefficient of each polynomial in it is monic, and (iii) no term in it can be reduced any further by another polynomial in the basis.

A polynomial p rewrites to p' using another polynomial q iff there is a term t in p with nonzero coefficient c such that $\mathrm{LT}(q)|t$ (to mean $t = s\ \mathrm{LT}(q)$ for some term s) and $p' = p - (\frac{c}{\mathrm{LC}(q)}) * s * q$. A term t in p is irreducible (or cannot rewritten) using a basis B if no polynomial $q \in B$ can rewrite p at t; similarly p is irreducible (as well as in normal form) iff no term in p can be reduced by B. Admissibility of a term ordering $>$ ensures that $p > p'$ and the rewriting process always terminates giving normal forms.

Proposition 2 *Given an ideal $I \subseteq K[U, X]$ and $>$, its reduced monic Gröbner basis, henceforth called RGB, is unique, where a Gröbner basis is reduced iff every polynomial in it is normal form.*

Such a Gröbner basis of an ideal is also called the canonical (Gröbner) basis of the ideal with respect to $>$.

Buchberger's algorithm can be used to test whether a given basis of an ideal I is a Gröbner basis or not as well as to compute a Gröbner basis of I if its basis is not a Gröbner basis. Further, the RGB of I can be computed from any Gröbner basis by rewriting.

Corollary 3 *No two distinct polynomials in the RGB of I have head terms which are multiple of each other.*

Further, no polynomial contains a non head term that is a multiple of the head term of some other polynomial in RGB.

2.2 Parametric or Comprehensive Gröbner Basis

The above concepts were extended independently by Weispfenning[1] and Kapur[2] to parametric ideals.

A specialization σ is a ring homomorphism from $K[U]$ to L, where L is usually an algebraically closed field extension of K. It can be canonically extended to $K[U][X] \to L[X]$ with the identity on variables. For a polynomial $f \in K[U][X]$, σ is given by $f \to f(v_1, v_2, \cdots, v_m)$, where $m = |U|$ and $v_1, v_2, \cdots, v_m \in L$. This image of f is denoted as $\sigma_{\overline{v}}(f)$ for brevity, where $\overline{v} = (v_1, v_2, \cdots, v_m) \in L^m$, or simply $\sigma(f)$ if it's clear from the context.

Definition 4 Let E, N be subsets of $K[U]$; the tuple (E, N) is called a **parametric segment** (or **segment**). An associated **constructible set** α is given by $\mathbb{V}(E) - \mathbb{V}(N)$, where $\mathbb{V}(E)$ is the algebraic variety (zero set) of E in L. (E, N) is consistent if $\alpha \neq \emptyset$.

The concept of a Gröbner basis associated with a polynomial ideal is generalized to the ring $K[U][X]$ as a CGB of a parametric ideal:

Definition 5 Given an ideal $I \subseteq K[U][X]$, $S \subseteq L^m$ the parameter space, and an admissible term order $>$, a finite set $\mathcal{G} \subseteq K[U][X]$ is called a **comprehensive Gröbner basis (CGB)** of I on S with respect to $>$, if for $\forall \sigma \in S$, $\sigma(\mathcal{G})$ is a Gröbner basis of the ideal $\sigma(I)$ on $L[X]$. Specifically, if $S = L^m$, $\mathcal{G}$ is a CGB of I.

A CGB $\mathcal{G}$ of a parametric ideal I is called minimal if no proper subset of $\mathcal{G}$ is also a CGB of I.

In contrast to a Gröbner basis of a polynomial ideal I which is a subset of I, the above

definition of a CGB does not require it to be a subset of I, Consider, for illustration, **EX1:** $I = \langle a^2x \rangle$; it can be verified that I has infinitely many CGBs $\{a^ix\}$ for each $i > 0$, among others. A CGB of I is called faithful if and only if the CGB is a subset of I[‡]. The significance of the faithfulness property of CGBs is extensively discussed in [1].

For the above example, most CGBs are faithful including $\{a^2x\}$ as well as $\{a^jx\}$ for every $j > 2$, which are also minimal. But $\{ax\}$ is not faithful as $a\ x \notin \langle a^2\ x \rangle$. The CGB $\{a^2x\}$ is the least among minimal faithful CGBs.

Definition 6 A minimal comprehensive Gröbner basis $\mathcal{G}$ of a parametric ideal I is **canonical** iff it is faithful, minimal as well as the least among all CGBs with a natural extension of the polynomial ordering $>$ to finite sets of polynomials.

For the above example, $\{a^2x\}$ is the canonical CGB of $\langle a^2x \rangle$. The main objective for defining the canonical CGB of an ideal is to associate a unique object with the ideal, given an admissible total term ordering $>$, independent of any algorithm used to compute CGBs. Equality of two parametric ideals can thus be checked by selecting an admissible term order $>$ and computing canonical CGBs of each of the ideals and see whether they are identical. The above definition parallels the definition of a canonical Gröbner basis of an ideal once a polynomial ordering $>$ is fixed.

A related but perhaps more useful concept for applications is that of a comprehensive Gröbner system (CGS) defined below.

Definition 7 Given an ideal $I = \langle F \rangle \subseteq K[U][X]$, where F is finite, and an admissible term order $>$, let $A_1, A_2, \cdots, A_l$ be constructible sets of L^m, and $G_1, G_2, \cdots, G_l$ subsets of $K[U][X]$, and S a subset of L^m such that $S \subseteq A_1 \cup A_2 \cup \cdots \cup A_l$. Then a **comprehensive Gröbner system (CGS)** of I on S with respect to $>$ is a finite set $CGS = \{(A_1, G_1), (A_2, G_2), \cdots, (A_l,$
$G_l)\}$, where for $\forall 1 \leq i \leq l$, $\sigma_i(G_i)$ is a Gröbner basis of the ideal $\sigma_i(I)$ on $L[X]$ under $\forall \sigma_i \in A_i$.

Each (A_i, G_i) is called a branch of CGS. Specifically, if $S = L^m$, then CGS is called a comprehensive Gröbner system (CGS) of I. Typically, segments of branches are disjoint.

Much like the definition of a CGB, the above definition of a CGS does not require that G_i be a subset of I; in fact, there are algorithms (see [3, 7, 8, 13]) for computing a CGS of an I in which G_i need not be a subset. A CGS is called faithful if and only if each $G_i \subseteq I$.

Proposition 8 *Given a faithful CGS of a parametric ideal I, the set of all polynomials appearing in various branches of the CGS constitute a CGB of I.* The CGB so generated is also faithful.

In [3, 4], algorithms are discussed for computing a CGS and CGB of a parametric polynomial ideal I; these algorithms first compute a reduced Gröbner basis (RGB) of I and use it as the starting point for generating a CGS.

As observed in [1] (see also [3]), the size of a CGB is often much smaller than that of the corresponding CGS especially if duplicate and redundant entries are removed from the CGB; in

[‡]It is easy to see that for a principal ideal with a single polynomial as a basis B, B also serves as its Gröbner basis as well as its CGB.

that sense, the CGB contains the same information in a condensed form. A constructible partition of the parameter space together with corresponding Gröbner bases can be easily recovered from a CGB as well.

3 Specializations of a Parametric Polynomial

Unlike a (non-parametric) polynomial, a parametric polynomial when specialized can have different structure. Even for a fixed admissible term ordering $>$, its head term, head coefficient, the number of nonzero terms in it can change under different specializations. Certain parametric polynomials can be specialized to zero even when they are not identically 0. Because of different possible structures of a parametric polynomial, computing using parametric polynomials can be complex, subtle as well as counter-intuitive. As observed in [1], construction of Gröbner bases is "extremely unstable" for different specializations.

Even though a parametric polynomial can stand for a family of infinitely many polynomials because of infinitely many possible specializations, it can be characterized by a finite set of polynomials based on the coefficients of terms appearing in it. Infinitely many specializations can be partitioned into a finite set of disjoint segments: Consider the coefficient of each term in descending term order in the polynomial by making the specialization of the coefficient of the term to be 0 or nonzero. This ensures that that the leading terms of the polynomials under the corresponding segment are distinct, and parametric segments are disjoint and nonempty (by performing a check).

3.1 Tuple Representation

Given an non-empty segment α, a parametric polynomial $f \in K[U][X]$ with respect to α, written as f_α, is represented by a tuple: $f_\alpha = ([\overline{f},\ \underline{f}],\ \alpha)$, where $\overline{f}$ and $\underline{f}$ are the non-zero and zero parts of f under α, and $f = \overline{f} + \underline{f}$. That is, every term in $\underline{f}$ has coefficient determined to be 0 under α, whereas the head coefficient of $\overline{f}$ is determined to be non-zero. Such a polynomial f is called unambiguous under α, since $\mathrm{LC}(\overline{f}) \neq 0$ under α. On the contrary, a polynomial is ambiguous under α if its leading coefficient is not determined under α. An ambiguous polynomial with respect to a segment can be made unambiguous by refining the segment using the coefficient of the largest term which is not determined with respect to the segment (see later the subsection titled Branch Partition and Segment Splitting for more details). Since we need to compute the leading term and leading coefficient of a polynomial f under a segment α, we will abuse the terminology and denote them by $\mathrm{LT}(f, \alpha)$ and $\mathrm{LC}(f, \alpha)$ respectively.

Let Φ_f be a finite set of such tuples $\{f_{\alpha_1}, f_{\alpha_2}, \cdots, f_{\alpha_n}\}$ of f under disjoint segments $\alpha_1, \alpha_2, \cdots, \alpha_n$ respectively, where these segments form a partition of the parameter space. Related concepts were introduced in [1, 2].

We will use the following example, called **EX2**, which is complex enough consisting of nonlinear polynomials but still manageable by hand. Let $U = \{a, b\}$ be parameters, $X =$

$\{x, y, z\}$ be variables; consider a degree term order such that $x > y > z \gg a > b$. Given a basis

$$\mathcal{F} = \{f_1 = ab^2y^2 + b^3 - 1,\ f_2 = (a^3b^2 + b^3 - 1)x^2 + 3ab^2y - 3a^2b^2,$$
$$f_3 = a(a^3b^2 + b^3 - 1)x^4 - 6a^3b^2x^2 + 9a^2b^2\},$$

with specializations in the segment $(\mathcal{E}, \mathcal{N}) = (\{\}, \{1\})$. For f_1, its specializations are:

$$\Phi_{f_1} = \{(f_{11} = [ab^2y^2 + b^3 - 1,\ 0],\ \alpha_1 = (\emptyset,\ \{ab^2\})),$$
$$(f_{12} = [b^3 - 1,\ ab^2y^2],\ \alpha_2 = (\ \{ab^2\},\ \{b^3 - 1\}\ ))\}.$$

Notice that in the first tuple, the leading term is y^2 which is ensured by enforcing the leading coefficient of f_1 to be nonzero in the specializations. In the second tuple, the leading coefficient of f_1 is enforced to be 0 in specializations; so for these specializations, the leading term is not y^2 any more. The next possible leading term is 1; to enforce that, its leading coefficient should be made nonzero. Finally, when the coefficients of both the terms y^2 and 1 are 0 in f_1, then f_1 is specialized to 0; this trivial tuple is omitted.

3.2 Essentiality, Redundancy, Minimality

Given an ideal I and its basis B, B is minimal iff for any polynomial $p \in B$, the ideal generated by $B - \{p\}$ is a proper subideal of I. In other words, a polynomial $p \in B$ is redundant iff p is in the ideal generated by $B - \{p\}$, i.e., is not a linear combination of other polynomials in B; otherwise it is called essential for I. In the absence of a Gröbner basis of I, this check can be quite nontrivial. The facilitation of ideal membership check is one of the key properties of a Gröbner basis of an ideal: A polynomial is in the ideal iff it reduces to 0 using its Gröbner basis.

There is however another stronger kind of redundancy that is defined using rewriting (with respect to a term ordering $>$) of a polynomial with respect to other polynomials: A polynomial p is redundant with respect to a basis B under a term ordering $>$ iff p reduces to 0 using B ($>$ is used to define rewrite rules from polynomials). Assuming a term ordering $>$, a basis B is called minimal if no polynomial $p \in B$ reduces to 0 using polynomials $B - \{p\}$; a basis B is called reduced iff every polynomial in $p \in B$ is in normal form with respect to $B - \{p\}$.

A redundant polynomial $p \in B$ with respect to rewriting under $>$ is redundant in the stronger sense, since p is in the ideal generated by $B - \{p\}$ but not vice versa. For instance, an S-polynomial generated from a pair of polynomials in a basis B is redundant with respect to the ideal generated by B but it need not be redundant with respect to rewriting under $>$; every S-polynomials is redundant with respect to rewriting under $>$ if the basis is already a Gröbner basis.

Many steps in a Gröbner basis computation can be saved if an algorithm keeps a basis to be minimal and reduced; however, see [18] for a different perspective since rewriting can be expensive. It should also be easy to see that the order in which redundancy of polynomials in a given basis B is checked can lead to many different minimal subsets of B as bases of the ideal.

For a parametric ideal I, the above definition can be generalized: Given a parametric basis B of I, $p \in B$ is essential iff there is a specialization σ of parameters such that $\sigma(p) \in \sigma(B)$ is

essential for $\sigma(I)$. In other words, $p \in B$ is redundant for I iff for every specialization σ, $\sigma(p)$ is redundant in $\sigma(B)$ for $\sigma(I)$. In that case, p is also said to be covered by $B - \{p\}$. As in the nonparametric case, this check is nontrivial to perform. In fact, even with an RGB and/or a CGB, the check is not easy to implement because of complex nature of parametric rewriting as discussed below. It is these aspects of parametric polynomials and their specializations which make development of Gröbner basis theory for parametric ideals to be counter-intuitive as well as difficult.

4 Relationships: RGB, CGS, CGB, Redundancy and Essentiality

Possible relationships of the reduced Gröbner basis (RGB) of a parametric ideal I over $K[U][X]$ using a block ordering in which $X \gg U$ to its CGS and CGB were brought to prominence by Suzuki and Sato[13] in which they advocated using a reduced Gröbner basis of a parametric ideal as the starting point for constructing its CGS. This was in contrast to Weispfenning's approach as well as Kapur's approach in which the construction of the RGB of a parametric ideal I was totally bypassed. In this section, we highlight possible relationships between the RGB (recall that it is unique) and a CGB of a parametric polynomial ideal I assuming a fixed admissible term order $>$ as well as issues related to CGBs and minimal CGBs.

4.1 RGB and CGB

As discussed in [3, 4] as well as stated above, a CGB can be easily extracted from a CGS. However, a CGB so constructed can have many redundant polynomials as discussed in [19]. For some parametric ideals, an RGB itself is a CGB. In general, RGB need not be a CGB. As an illustration, consider a very simple example[14] with **EX3** : $\{f : uy + x, g : vz + x + 1\}$ as a basis with u, v as parameters, which can be analyzed even by hand. Even though all polynomials in x, y are linear, this example is quite illustrative exhibiting most of the complexities of parametric polynomials. The RGB of the ideal generated by f, g with respect to $x > y > z \gg u > v$ is $\{f, g\}$. However, its CGB is $\{f, g, h : vz - uy + 1\}$ including another polynomial $h = g - f$ which reduces to 0 using classical rewriting; that is why it is not in the RGB.

More interestingly, even if an RGB of I is a CGB, it need not be minimal, i.e., it may have redundant elements–both polynomials purely in parameters as well as in parameters and variables. As also evident from **EX3**, a CGB of I need not be a subset of RGB or vice versa. Further, every polynomial p in a faithful CGB reduces to 0 by the RGB, whereas every $p \in I$ need not reduce to 0 using a faithful CGB since it need not be a Gröbner basis. Recall however that for every specialization σ and $p \in I$, $\sigma(p)$ reduces to 0 using σ(CGB).

As a simple case, for any $I \subset K[U][X]$, consider the subideal $I_U = I \cap K[U]$; assuming $I_U \neq \{0\}$, the subset of the RGB of I only in parameter set U, i.e., $G' = \text{RGB} \cap K[U]$ is a Gröbner basis of I_U. G' almost always contains redundant elements as often a proper subset of G' suffices to generate I and characterize its zero set. This is illustrated later by **EX5**. The whole G' need not be a subset of every CGB since many polynomials in G' may be redundant. Instead it need to include a minimal basis that generates I_U. However, other polynomials with variables can also cover specializations for which polynomials in I_U may be needed; it may thus

be enough to include only a subset of a minimal basis thus further complicating such bottom up constructions.

The following example (**EX4**) illustrates some of these subtleties. Let $I = \langle f_1 : bc^2 - b, f_2 : ac^2 - a, f_3 : ax - b\rangle$ with $x \gg a > b > c$. It is easy to see that $\{f_1, f_2, f_3\}$ is the RGB of I; it is also a CGB. A minimal CGB is CG $= \{f_2, f_3\}$, which is a proper subset of its RGB. However, $\{f_1, f_2\}$ are both needed to characterized the zero set of $I \cap K[a, b, c]$. The zero set of f_1 is either covered by f_2 (when $c^2 - 1 = 0$) or f_3 (when $c^2 - 1 \neq 0 \wedge a = 0$). And $G' = \{f_1, f_3\}$ is not a CGB since for the specializations $b = 0, c^2 - 1 \neq 0, a \neq 0$, I specializes to $\{1\}$, whereas G' specializes to x. This example illustrates that a minimal faithful CGB (and hence a canonical CGB) need not include the least polynomial in the ideal for every minimal head term; particularly, for the specialization $a = 0, b \neq 0, c^2 - 1 = 0$, the least polynomial in the ideal with the head term 1 is $bc^2 - b$ whereas in the least minimal CGB, the polynomial f_3 accounts for it. In general, every minimal CGB need not include the least element of G' as it may not be needed in a minimal basis of I_U

The above example shows that even if G'' is the smallest subset (in the ordering) of G' that characterizes all zeros of I_U, i.e, $V(G'') = V(G') = V(I_U)$, G'' is not necessarily a subset of CCGB.

4.2 CGB and Essentiality Check

The essentiality of a polynomial p in a CGB is checked by determining whether it can be covered by polynomials in CGB $- \{p\}$ over a subset of parameter specializations for which p is needed. In the absence of such information about specializations, p can be checked for every specialization irrespective of whether it is needed or not. This check can be performed relatively easily in case of a CGB and even further optimized if a CGS from which CGB is constructed is also available; from such a CGS,

Proposition 9 *Given a CGB, a polynomial p is redundant iff for every specialization σ, the head term of $\sigma(p)$ is a multiple of the head term of some polynomial in CGB$-\{p\}$.*

In other words it is sufficient to focus in a CGB only on the head terms of specialized polynomials, much like in the case of a Gröbner basis. The above proposition can be used to generate a CGB without any redundant polynomials. However, the order in which redundancy check is perormed makes a difference leading to possibly many distinct minimal CGBs can be generated from a given CGB (see [19]). Consider a slight variation on **EX4**; call it **EX5**: Let $J = \langle f_1 : bc^2 - b, f_2 : ac^2 - a, f_3 : ax - b, f_4 : bx - a\rangle$ with $x \gg a > b > c$. Its RGB includes an additional polynomial $f_5 : a^2 - b^2$. RGB itself is a CGB which is not minimal. $C_1 = \{f_1, f_5, f_4\}$ is a minimal CGB, so is $C_2 = \{f_1, f_5, f_3\}$. Its CCGB is $\{f_1, f_5, f_4\}$.

Lemma 10 *If polynomials in a CGB $\mathcal{G}$ are checked for redundancy in a descending order induced by an admissible polynomial ordering and redudant polynomials are removed from $\mathcal{G}$, the resulting subset $\mathcal{G}'$ of $\mathcal{G}$ is minimal and least, in the polynomial ordering induced on finite set of polynomials, among all CGBs which are subsets of $\mathcal{G}$.*

Using Proposition 9, it follows:

Proposition 11 *If there are two polynomials p and q in a CGB such that $q = A * p$, where*

A is a polynomial in parameters, then q is not essential with respect to CGB $- \{q\}$.

It is not necessarily the case that all CGBs of a parametric polynomial ideal can be computed from its RGB, partly because there are infinitely many CGBs. Consider $I = \langle ax \rangle$; its RGB is $\{ax\}$. Since it is a CGB also, it is the CCGB. However, there are infinitely many CGBs, including $\{a^i x\}$ for any $i > 0$; further they are all minimal.

Lemma 12 *Let* $A * p$ *be in a CGB, where A is a polynomial purely in parameters;* $A * p$ *can be replaced by* $A * B * p$ *in the CGB still preserving CGBness where B is purely in parameters and* $Ap \neq 0 \implies B \neq 0$.

A corollary of the above property is:

Corollary 13 *Given* $A * p$ *in a CGB, where A is a polynomial purely in parameters,* $A * p$ *can be replaced by* $A^i * p$ *in the CGB still preserving CGBness.*

Proof For any specialization σ such that $\sigma(Ap) = 0, \sigma(A^i p) = 0$; further any specialization in which $\sigma(Ap) \neq 0$ implying $\sigma(A) \neq 0$ implies $\sigma(A^i p) \neq 0$. The property also follows from the fact that $\sigma(HT(Ap)) = \sigma(HT(A^i p)) \neq 0$.

The above properties enable generating infinitely many CGBs from a given CGB such as $\{ax\}$. This is also the justification for the check discussed later to reduce a faithful CGB to get an even smaller faithful CGB: If $A^i p$ in a CGB, then check whether any $A^k * p \in I, 0 \leq k < i$, (this check can be performed using the RGB of I) in which case replace $A^i * p$ in the CGB by $A^j * p$ where j is the least such k. If the faithfullness property is not required of a CGB, then $A^i * p$ can be replaced by $A * p$. The inverse of this step can be used to generate infinitely many minimal CGBs from a given minimal CGB.

Given that a canonical CGB is the least among all CGBs, factoring a polynomial p in a CGB to check whether it has factors purely in parameters is useful in making CGBs smaller. If $p = A * p' \in$ CGB for some polynomial A in parameters only and further $p' \in I$ (which can be checked using its RGB), $p \in$ CGB can be replaced by p'.

Corollary 14 *Given* $A * p$ *in a CGB, where A is a polynomial purely in parameters,* $A * p$ *can be replaced by p in the CGB still preserving CGBness if* $p \in I$.

4.3 CGS and Essentiality Check

In case a CGS of I is available from which the given CGB is constructed, we can possibly optimize the check for redundant polynomials in the CGB by identifying other polynomials in the CGB which can possibly cover p. Since p in the CGB may be contributed by many branches in the CGS, for every such branch and its associated segment, we need to check whether polynomials appearing in other branches of CGS can cover p. In a branch with an associated segment A_i in which p appears, only those polynomials in the CGB can cover p that have terms which can possibly reduce the leading term of p with respect to A_i. The structure of the associated CGS computed by the KSW algorithm (particularly that each branch (A_j, G_j) is for a disjoint subset of specialization defined by A_j and G_j is a minimal Gröbner basis under these specializations) can be exploited to perform this check efficiently.

Let $B_p = \{(A_j, G_j)\}_{j \in J}$ be the set of branches in CGS with $p \in G_j$ for each $j \in J$. Then it is enough to consider specializations corresponding to A_j's in B_p, since p is guaranteed to

be covered over all the others[§]. Other polynomials in the same branch as p cannot cover p. Further, we only need to consider polynomials which have a term under the segment under consideration appearing with a possibly nonzero coefficient of which the leading term of p is a multiple. This can reduce the number of candidate polynomials which can cover p. Let G_{cand} be the subset of CGB $- G_j$ such that each $g \in G_{cand}$ contains some term in X dividing the leading term of p with respect to A_j in X. If there is some $g \in G_{cand}$ such that $\forall \sigma \in A_j$, $\mathrm{LT}(\sigma(g)) \mid \mathrm{LT}(\sigma(p))$, then p is covered over this branch and replaced by $g \in G_j$. If a single polynomial q covers p for the branch under consideration, then q can replace p in the branch (A_j, G_j) as well as q can replace p in G_j. For different branches in which p appears, there may be different such q's covering p. If for at least one branch in the CGS in which p appears, it cannot be covered, then p is declared essential and kept in the CGB. If p can be covered in all branches of the CGS in which it appears, then p is not essential and can thus be discarded from the CGB (and the CGS); further, p is replaced by the corresponding q's in respective branches in the CGS).

4.3.1 Branch Partition and Segment Splitting

Even for a particular branch in which p appears, multiple polynomials may be needed to cover p. If $\mathrm{LT}(\sigma(g)) \mid \mathrm{LT}(\sigma(p))$ for $\sigma \in A_{jc} \subsetneqq A_j$, then A_j is partitioned into A_{jc} and A_{jn}, and then specializations in A_{jn} needs to be considered for covering of p using $G'_{cand} = G_{cand} - \{g\}$. The branch (i.e., segment of specializations) needs to be split into multiple sub-branches so that multiple polynomials can cover p.

Consider an example (**EX6**) in $K[u,v][y,x]$ and a lexicographic term order with $y > x \gg u > v$; in a branch $A_j = (\{u^2 - v^2\},\ \{u\}) \in CGS$ of an ideal, $G_j = \{p = (u^2 - v^2)y + ux\}$ and $Q = \{q_1 = (u+v)x,\ q_2 = (u-v)x\}$. To check if Q can cover p in $A_j = \{\langle u, v\rangle | u \neq 0, u^2 - v^2 = 0\}$, it is easy to see that both q_1 and q_2 partially cover p, since neither of their leading coefficients is determined with respect to A_j. So A_j is partitioned with respect to $u + v$ where q_1 covers p in $A_{j1} = \{\langle u, v\rangle | u \neq 0, u^2 - v^2 = 0, u + v \neq 0\}$ and q_2 covers p in $A_{j0} = \{\langle u, v\rangle | u \neq 0, u^2 - v^2 = 0, u + v = 0, u - v \neq 0\}$. $Q = \{q_1, q_2\}$ is a covering of p in A_j. Splitting of a segment deals with the case when the leading term of p with respect to the segment appears in q but with the coefficient that is not determined to be nonzero.

Definition 15 Given a CGB $\mathcal{G}$ of an ideal I, a finite set $Q = \{q_1, q_2, \cdots, q_n\} \subseteq \mathcal{G} - \{p\}$ is said to be a **covering** of a polynomial $p \in \mathcal{G}$ over a set A of specializations, if for $\forall \sigma \in A$, there is some $q_i \in Q$ such that $\mathrm{LT}(\sigma(q_i)) \mid \mathrm{LT}(\sigma(p))$.

The covering check on A_j continues until either some $A_{ess} \subseteq A_j$ is generated such that $\mathrm{LT}(\sigma(p))$ is not divisible by $\mathrm{LT}(\sigma(G_{cand}))$ and hence cannot be covered, thus declaring p to be essential and the procedure terminates. Otherwise, a partition of A_j is generated such that $(\sigma(p))$ is divisible by $\mathrm{LT}(\sigma(G_{can}))$ for $\forall \sigma \in A_j$, with possibly different polynomials in G_{can} with respect to the respective subsets of A_j. This is followed by the next branch in B_p. If p is covered for every branch in B_p, the procedure terminates declaring p as redundant.

Lemma 16 *Given a polynomial p in a CGB CG of I, p is not essential (or redundant)*

[§]A nonminimal CGS can also be used in a similar way.

with respect to CG if and only if for every branch (A_j, G_j) in the associated CGS of I such that $p \in G_j$, and for every specialization $\sigma \in A_j$, $LT(\sigma(p))$ is divided by $LT(\sigma(q))$ for some $q \in CG\backslash\{p\}$; in that case p has a covering $Q_j = \{q_1, q_2, \cdots, q_n\} \subseteq \mathcal{G} - G_j$, such that for $\forall \sigma_k \in A_j$, there is some $q_k \in Q$ with $LT(\sigma_i(q_k)) = LT(\sigma_i(p))$.

4.4 Minimal CGB

Given a CGB of a parametric ideal, a polynomial in it is called essential because of the following property of minimal CGBs.

Proposition 17 *Given a CGB $\mathcal{G}$ of an ideal $I \subseteq K[U][X]$ with respect to a term order $>$, a polynomial $f \in \mathcal{G}$ is essential with respect to $\mathcal{G}$, iff $\mathcal{G} - \{f\}$ is not a CGB of I.*

A minimal CGB (MCGB) can be defined as follows:

Definition 18 A CGB $\mathcal{G}$ of an ideal $I \subseteq K[U][X]$ with respect to a term order $>$ is minimal if the following conditions are satisfied:

1) No proper subset of $\mathcal{G}$ is a CGB of I with respect to $>$;

2) For $\forall g \in \mathcal{G}$, LC$(g)$ is monic in $K[U]$.

The second requirement is technical; it is introduced to enable comparison among different minimal CGBs of the same ideal I using the extension of $>$ on polynomials to finite sets of polynomials since I can have multiple minimal CGBs.

Consider a slight variation of **EX1** discussed in Section 2.2: $I' = \langle B' \rangle$ where $B' = \{a^3, a^2x\}$; its RGB is the basis itself: $\{a^3, a^2x\}$. It is a CGB but a^2x is redundant since for $a = 0$ it specializes to 0, and for specializations in which $a \neq 0$, it can be reduced by $\{a^3\}$. This implies $\{a^3\}$ is a minimal CGB as well as it is canonical. From KSW algorithm's branch 1 a^3 is a Gröbner basis; in the second branch in which $a^3 = 0$ implying $a = 0$, the specialized ideal is $\{0\}$ with the empty set as the Gröbner basis. The CGB generated from the KSW algorithm is indeed the canonical CGB in this case.

Consider yet another variation: $I'' = \langle B'' \rangle$ where $B'' = \{a^2, (a+b)x\}$ with respect to $x \gg a > b$. B'' is neither the RGB nor a CGB of I'', since the S-polynomial between a^2 and $(a+b)x$ does not reduce to 0. The set $\{a^2, ab\, x\}$ is its RGB as well as a CGB, but it is not minimal since $ab\, x$ is redundant. Its canonical CGB is $\{a^2\}$. The KSW algorithm generates the canonical CGB from the CGS in this case also.

Essentiality can be used to characterize minimal CGBs as follows:

Corollary 19 *A finite basis $\mathcal{G} \subseteq K[U][X]$ is a minimal CGB, iff $\forall g \in \mathcal{G}$, g is essential with respect to $\mathcal{G}$.*

5 Canonical Comprehensive Gröbner Basis: Existence

There are at least two different ways the existence of a canonical comprehensive Gröbner basis (CCGB) for every parametric polynomial ideal I can be established once a total admissible polynomial ordering is fixed.

All minimal CGBs are finite; without any loss of generality, they can be assumed to be minimal as a canonical CGB must be minimal. They can be compared with each other using the polynomial ordering extended to finite sets of polynomials. In general, this ordering is

partial. However, assuming Zorn's lemma, K and L can be totally ordered as well, leading to a total ordering on finite subsets of polynomials.

Using Zorn's lemma, the least minimal CGB among all CGBs exists and satisfies the definition of CCGB.

There is yet another (perhaps less nonconstructive) way to show that a canonical CGB exists for every parametric ideal; it is likely to provide some insights to construct such as a CGB. The construction is inspired by a construction in the nonparametric case for computing the RGB of an ideal with respect to $>$.

Recall that an RGB of a polynomial ideal I is a finite subset of I that can be constructed by considering all minimal head terms using divisibility among terms ordering (i.e., of polynomials in I and then picking from I, the least polynomial in I with these minimal head terms)[17]. It can be shown that such a basis is a Gröbner basis and further it is the least among all Gröbner bases of I. And, it is also a reduced Gröbner basis.

Similar to various characterizations for a RGB of a polynomial ideal, the existence of a canonical comprehensive Gröbner basis can be established as follows:

Given a parametric ideal I, for each specialization σ, for every minimal head term of specialized polynomials in $\sigma(I)$, pick the least polynomials in I which under σ specializes to have this head term. Consider all such polynomials and call the set S.

Definition 20 Let $S = \bigcup_\sigma \{\text{the least } p \in I \mid \text{LT}(\sigma(p)) \text{ is minimal} \in \text{LT}(\sigma(I))\}$.

Proposition 21 *S is finite.*

Proposition 22 *S is a CGB.*

Both of the above properties are easy to prove. But S may have redundant polynomials:

Consider yet another variation on **EX1**: $J = \langle a * b * x, a^2 * x\rangle$ with $x \gg a > b$; with lexicographic ordring or degree ordering, $a^2 * x > a * b * x$. For the subset of specializations $a \neq 0, b \neq 0$, the associated reduced Gröbner basis is $\{a*b*x\}$ and the least polynomial with the head term x is $a*b*x$; for the subset of specializations $a \neq 0, b = 0$ the reduced Gröbner basis is $\{a^2*x\}$ and the least polynomial with the head term is a^2*x. So using the above construction, $S = \{a * b * x, a^2 * x\}$. But $a * b * x$ is redundant since it is covered by $a^2 * x$ whereas $a^2 * x$ is not covered by $a * b * x$ for specializations when $a \neq 0 \wedge b = 0$.

After redundant polynomials have been removed from S by performing the essentiality check in the descending order, the result S' is unique and the least CGB as proved below.

Theorem 23 *Let $C \subseteq S$ be a subset of polynomials after removing from S all redundant polynomials in descending order. Then C is the least CGB among all CGBs of I (and is unique).*

Proof By definition of redundancy, C is a CGB. Let D be another CGB of I that is smaller than C or noncomparable to C. So there exists f in $D - C$ which is smaller than every polynomial in $C - D$.

It should be noted that a canonical CGB does not necessarily only include the polynomial with the same head term from the ideal for every minimal head term; redundancy check on S takes care of such cases. In fact, there can be another polynomial included for bigger head term

in the canonical CGB which also accounts for small head terms for certain specializations. A case in point is the example **EX4:** $I = \langle f_1 : bc^2 - b, f_2 : ac^2 - a, f_3 : ax - b\rangle$ with $x \gg a > b > c$ discussed above. There are two minimal head terms of Gröbner bases for various specializations: $1, x$. The least polynomial with x as its head term is indeed $ax - b$ for specializations in which $a \neq 0, c^2 - 1 = 0$ and x is the minimal head term of the specialized ideals; for other specializations, particularly $b \neq 0, c^2 - 1 \neq 0$, the minimal head term of the specialized ideals is 1 and the least polynomial is $f_1 : bc^2 - b$; however, $ax - b$ covers it for the case when $a = 0$ whereas for $a \neq 0$, $f_2 : ac^2 - a$ covers it.

An algorithmic construction of a canonical CGB remains a challenge however, as it is unclear how such a CGB can be generated directly, or from a CGS or from a CGB constructed using various algorithms proposed in the literature.

In the next section, we present a method for checking whether a given basis B of a parametric ideal I is a CGB. Following that section, we discuss operations on a given CGB to get a smaller CGB in the polynomial ordering.

6 Test for a Comprehensive Gröbner Basis

Example **EX1** above showed that a reduced Gröbner basis (RGB) of a parametric ideal over $K[U, X]$ with the block ordering under which $X \gg U$, need not be its CGB. Specializations of parameters can change the leading term, total degree and the kind of terms appearing in a specialization of a parametric polynomial. In contrast, in the reduced Gröbner basis algorithm over $K[U, X]$ there is an implicit assumption that the head coefficient of each polynomial is nonzero. Concepts of S-polynomial and reduction used in Buchberger's algorithm must be adapted for parametric polynomials to take into consideration the fact that under specializations, the same polynomial has different head terms. In the RGB construction, two distinct polynomials may not have a nontrivial S-polynomial because their head terms are co-prime, but that need not be true when they are specialized. This is first illustrated using a simple example below.

Consider the example **EX2** discussed in Subsection 3.1. We check if $\mathcal{F}$ is a CGB for the whole space of specialization of parameters:

Step 1 Parametric Specializations of a Polynomial with Different Leading Terms.

$$\begin{aligned}\Phi_{f_1} = \{&(f_{11} = [ab^2y^2 + b^3 - 1,\ 0],\ \alpha_1 = (\emptyset,\ \{ab^2\})),\\ &(f_{12} = [b^3 - 1,\ ab^2y^2],\ \alpha_2 = (\ \{ab^2\},\ \{b^3 - 1\}\ ))\},\end{aligned}$$

The tuple $([0,\ ab^2y^2 + b^3 - 1],\ (\{ab^2, b^3 - 1\},\ \{1\}))$ corresponding to the specialized polynomial 0 is omitted.

Similar to f_1, the associated finite sets of tuples are computed for f_2, f_3; let $\psi = a^3b^2 + b^3 - 1$.

$$\begin{aligned}\Phi_{f_2} = \{&(f_{21} = [\psi x^2 + 3ab^2y - 3a^2b^2,\ 0],\ \beta_1 = (\ \emptyset,\ \{\psi\}\ )),\\ &(f_{22} = [3ab^2y - 3a^2b^2,\ \psi x^2],\ \beta_2 = (\ \{\psi\},\ \{3ab^2\}))\};\\ \Phi_{f_3} = \{&(f_{31} = [a\psi x^4 - 6a^3b^2x^2 + 9a^2b^2,\ 0],\ \gamma_1 = (\ \emptyset,\ \{a\psi\}\ )),\\ &(f_{32} = [6a^3b^2x^2 - 9a^2b^2,\ a\psi x^4],\ \gamma_2 = (\ \{a\psi\},\ \{6a^3b^2\}\ ))\}.\end{aligned}$$

Step 2 Compute Parametric S-polynomials.

For each pair of parametric polynomials, a set of S-polynomials is computed using their specialization. For example, for f_1 and f_2, construct all possible critical pairs as $(\Phi_{f_1} \times \Phi_{f_2}) = \{(f_{11}, f_{21}), (f_{11}, f_{22}), (f_{12}, f_{21}), (f_{12}, f_{22})\}$. By Buchberger's first criterion, we can ignore the unnecessary critical pairs with coprime leading terms as such an S-polynomial always reduces to 0. So among the above set, only (f_{11}, f_{22}) needs further consideration.

Compute the parametric S-polynomial from it. The segment $\delta_1 = \alpha_1 \cap \beta_2 = (\ \{\psi\},\ \{ab^2\}\ )$ is not empty. Under δ_1, the parametric S-polynomial is $h_1 = 3f_{11} - yf_{22} = [3a^2b^2y + 3b^3 - 3,\ -\psi x^2 y]$. If a segment is empty for a critical pair, the associated S-polynomial also does not have to be considered.

Step 3 Reduction under a Segment.

Parametric reduction is defined below and illustrated using the example. Reduce h_1 by the basis $\mathcal{F}$ under the segment δ_1: Both h_1 and $\mathcal{F}$ are unambiguous under δ_1. h_1 is reduced in one step to $h_1' = h_1 - af_2 = [3\psi,\ -3\psi x^2 y - a\psi x^2]$. So h_1 is reduced to 0 by $\mathcal{F}$ under δ_1 since $\overline{h_1} = 3\psi = 0$.

Repeat Steps 2 and 3 for other pairs.

The other two pairs, (f_2, f_3) and (f_1, f_3), must be checked using steps 2 and 3. For f_2 and f_3, after removing unnecessary critical pairs, there are two left: (f_{21}, f_{31}) and (f_{21}, f_{32}). Further, since $\beta_1 \cap \gamma_2 = \emptyset$, we only need to consider the first one:

The segment $\delta_2 = \beta_1 \cap \gamma_1 = (\emptyset,\ \{a\psi\}))$. Under δ_2, the S-polynomial is $h_2 = ax^2 f_{21} - f_{31} = [3a^2b^2x^2y + 3a^3b^2x^2 - 9a^2b^2,\ 0]$. Reduce it by $\mathcal{F}$ under δ_2. h_2 is unambiguous, but $f_1 \in \mathcal{F}$ is ambiguous. So partition δ_2 into δ_{20} and δ_{21} to make $\mathcal{F}$ unambiguous:

i) $\delta_{20} = \delta_2 \cup \{ab^2 = 0\}$: $h_2 = [0,\ 3a^2b^2x^2y + 3a^3b^2x^2 - 9a^2b^2]$, which is already reduced to 0.

ii) $\delta_{21} = \delta_2 \cup \{ab^2 \neq 0\}$: $h_2' = \psi h_2 + 2a^2b^2 f_1 - (a^2b^2y + a^3b)f_2 = [0,\ 3a^2b^2x^2y + 3a^3b^2x^2 - 9a^2b^2]$.

This implies that f_2 reduces to 0.

Finally, since all critical pairs from f_1 and f_3 are unnecessary, the algorithm terminates declaring $\mathcal{F}$ to be a CGB.

In the next subsections, parametric S-polynomials and parametric rewriting are defined.

6.1 Parametric S-Polynomial

Two key concepts are used in the check for CGB: Parametric S-polynomial and reduction under segment, both of which are generalizations of S-polynomial and reduction in Buchberger's algorithm from $K[X]$ to $K[U][X]$. They are also related to similar concepts introduced in [1, 2].

Since a parametric polynomial f stands for many specialized polynomials under various segments, denoted by Φ_f, a distinct pair of parametric polynomials can have multiple parametric S-polynomials for different segments, in contrast to exactly one S-polynomial defined in Buchberger's algorithm.

Definition 24 Given two distinct parametric polynomials $f, g \in K[U][X]$, let $f_\alpha = ([\overline{f}, \underline{f}], \alpha)$ and $g_\beta = ([\overline{g}, \underline{g}], \beta)$ be the unambigous forms of f under segment α and g under

segment β respectively. Then a **parametric S-polynomial** of f and g under a non-empty segment $\alpha \cap \beta$ is

$$\text{S-PolyP}_{\alpha\cap\beta}(f_\alpha, g_\beta) = \frac{\text{lcm}(\text{LM}(\overline{f}), \text{LM}(\overline{g}))}{\text{LM}(\overline{f})} f - \frac{\text{lcm}(\text{LM}(\overline{f}), \text{LM}(\overline{g}))}{\text{LM}(\overline{g})} g.$$

There are a lot more unnecessary S-polynomials of parametric polynomials which will trivially reduce to 0 especially for the parametric case. Many of them can be discarded by the Buchberger's criterion if the leading terms of the polynomials are coprime (Proposition 4 in [17]), or if the segment in the associated critical pair is empty, or the leading term of one of the polynomials is 1. In Example **EX2**, for instance, only h_1 and h_2 are necessary out of 12 possible parametric S-polynomials.

6.2 Reduction of a Parametric Polynomial by a Parametric Basis Under a Segment

There are many trade offs in generalizing the definition of rewriting of a parametric polynomial by a basis of parametric polynomials. An important requirement is that if for some specialization, the specialization of a polynomial does not reduce to 0 using the same specialization of a basis, then that polynomial should not reduce to 0 using the basis by parametric rewriting for segments that include the specialization. It will also be desirable to check redundancy using parametric rewriting, like in the classical theory, where if a polynomial in a basis rewrites to 0 using the rest of the polynomials in the basis, then it can be dropped. Of course, there is another desirable property of a Gröbner basis identified by Buchberger: every polynomial p in an ideal I reduces to 0 using any of its Gröbner bases if and only if $p \in I$, and further, every polynomial is a unique normal form with respect to a Gröbner basis. In our view, parametric rewriting is the most nontrivial concept for parametric polynomials. We first illustrate these desired properties before proposing the definition of parametric rewriting with respect to a segment α.

As illustrated above, a CGB is neither a subset of RGB nor a superset of RGB. Thus classical rewriting cannot reduce every element of the ideal to 0 using any of its CGB unless it is a Gröbner basis. We have also seen examples for which it is essential to include in a CGB, extra polynomials from an ideal along with a subset of RGB. For such polynomials which are in the ideal, it should not be possible to reduce them to 0 by parametric rewriting using the remaining polynomials in a CGB.

Here are some desired properties of parametric reduction. A polynomial, even if in the ideal, should not parametrically reduce to 0 using a basis if there is some specialization for which it does not reduce to 0 using the associated specialized basis.

For **EX3**, $h : vz - uy + 1$ while classically reduces to 0 using $\{f, g\}$, does not reduce to 0 using the specializations of $\{f, g\}$, particularly when $u = 0 \wedge v = 0$. So h should not parametrically reduce to 0 using $\{f, g\}$.This indicates that parametric rewriting is stronger than classical rewriting in the sense that a polynomial p may classically reduce to 0 using a basis B but need not parametrically reduce to 0, whereas the vice versa must hold. h should be a normal form with respect to the basis $\{f, g\}$ by parametric rewriting.

For the example, $J = \langle a * b * x, a^2 * x\rangle$, the basis itself is a CGB but is not minimal, as discussed above. Since $a*b*x$ is redundant, can parametric rewriting so defined that it reduces it to 0 using the basis $\{a^2 * x\}$? The definition proposed in [20] indeed does so. However, there are issues with that definition also.

Consider **EX1:** $\{a^2x\}$ is a faithful CGB of $I = \langle a^2x\rangle$; $a^i\ x$ reduces to 0 for every $i \geq 2$, since it is in I, but what about ax? ax is not in I; however, for every specialization σ, $\sigma(ax)$ reduces to 0 using $\sigma(\{a^2x\})$ even though it is not in I. $\{a^3x\}$, for instance, is also a faithful CGB of I. Should $a^2x \in I$ reduce to 0 using $\{a^3x\}$? This is one of the dilemmas. The definition given in [20] will parametrically reduce a^2x to 0 using CGBs $\{a^2x\}$ as well as $\{a^3x\}$ but the definition would also reduce ax to 0 even though $ax \notin I$. It should be noted that for every specialization σ of a, $\sigma(a * x)$ does reduce to 0 using $\sigma(\{a^2 * x\})$. So should we abandon a property that if a polynomial p parametrically reduces to 0 using a basis B, then p must be in the ideal generated by B?

Our objective in defining (parametric) rewriting is to mimic classical writing as much as possible so as to ensure that as many polynomials from the subideal generated by a CGB of an ideal reduce to 0 using the CGB.

Definition 25 Given two distinct parametric polynomials $f, p \in K[U][X]$ and a non-empty segment α such that $f_\alpha = ([\overline{f}, \underline{f}], \alpha)$ and $p_\alpha = ([\overline{p}, \underline{p}], \alpha)$. f parametrically reduces to f' by p under α in one step if there is a term t in $\overline{f}$ with coefficient c such that $\mathrm{LT}(\overline{p}) \mid t$ and $\mathrm{LC}(\overline{(p)}) \mid c$, and

$$f' = f - \frac{c}{\mathrm{LC}(\overline{p})} * \frac{t}{\mathrm{LT}(\overline{p})} * p.$$

We write it as $f \xrightarrow{\alpha}_p f'$. Unless unclear from context, we will drop the adjective parametric in parametric rewriting on parametric polynomials.

Even though the above definition of parametric reduction is closely related (essentially the same) to the classical reduction when no distinction between parameters and non-parameters is made, the results are different because of the requirement that the head term of p is with respect to a segment. Consider **EX3**: h in its CGB, which is the same as $f - g$, classically reduces to 0 using f and g, but does not reduce to 0 using the above parametric rewriting using f and g; for the segment $u = 0 \wedge v = 0$, the leading term of h is 1, whereas the leading term of both f and g are x. This indeed captures our intent.

Lemma 26 *Given a basis $B \subset K[U][X]$, if p parametrically reduces to 0, then p classically reduces to 0 over $K[U, X]$ using B. And not necessarily, vice versa.*

It is possible for a polynomial f to be such that for for all specializations σ, $\sigma(p)$ reduces to 0 using $\sigma(B)$ but f neither classically nor parametrically reduce to 0 using a basis B. Consider $f = ax$ and $B = \{a^2x\}$; under every specialization in which $a \neq 0$, the head term of f is x as well as that of the singleton element in the basis; for $a = 0$, $\sigma(f) = 0$. However, f does not classically reduce to 0; further it also does not parametrically reduce to 0 since for the segment $a^2 \neq 0$, $\mathrm{LT}(f) = x, \mathrm{LC}(f) = a$, $\mathrm{LT}(a^2x) = x$, but $\mathrm{LC}(a^2x) = a^2$ does not divide a. The above definition does not reduce $a * b * x$ to 0 using

Proof Suppose f does not classically reduce to 0 using B; this implies that there is a

sequence of rewrites $f = f_0, f_1, \cdots, f_k$ using elements of B such that $f_k \neq 0$ cannot classically reduce any further using any polynomial in B (implying that there is no term in f_k which is a multiple of the head term of any polynomial in B). Since $\sigma(f)$ reduces to 0 for every specialization σ, construct the segment taking the conjunction of $\bigwedge_{p\in B} \mathrm{LC}(p) = 0$ and the conjunction of the coefficient of the term in f_i reduced by B to be not zero. Under every specialization σ in this segment (assuming that it is consistent), $\sigma(f)$ reduces to 0 since it is possible to mimic the rewriting sequence on $\sigma(f)$ using $\sigma(B)$. Such a segment is consistent follows from:

$\sigma(f_k)$ can be reduced using by some polynomial $\sigma(p) \in \sigma(B)$, thus implying that $\mathrm{LT}_X(\sigma(p)) \neq \mathrm{LT}_X(p)$

The second part of the statement is illustrated using the counter example of h in **EX3** classically reducing to 0 using $\{f, g\}$ but not parametrically reducing to 0 since under the specialization $u = 0 \wedge v = 0$, $\sigma(h)$ does not reduce using $\{\sigma(f), \sigma(g)\}$.

The above definition is different from the definition introduced in [20] where f can be multiplied by an appropriate polynomial in parameters in case the coefficient of t is not a multiple of the $\mathrm{LC}(\overline{p})$ (this multiplier is a factor of $\mathrm{LC}(\overline{p})$); in this sense, that definition was closer to pseudo-division. It is easy to see that the above definition is stronger than the one[20] in the sense that if $f \xrightarrow{\alpha}_p f'$ then it also reduces using the definition in [20] but not vice versa. The definition of rewriting given in [1] is even weaker than in [20]; it multiplies the polynomial f being rewritten by the head coefficient of the polynomial p under α so that the result can be classically rewritten using p: $f' = \mathrm{LC}(\overline{p}) * f - c * \frac{t}{\mathrm{LT}(\overline{p})} * p$.

This definition has the desired property vis a vis ideal membership using parametric rewriting. For certain CGBs of an ideal, ideal membership can be decided using parametric rewriting but not for all CGBs. But if a polynomial is not in an ideal, then it does not reduce to 0 using any faithful CGB. Revisiting EX1, the polynomial $p = ax$ is not in the ideal J generated by a^2x and p does not parametrically rewrite to 0 using a^2x which is in a CGB of J.

If the weaker definition given in [20] is used for parametric rewriting, then it can be proved that for any $p \in I$, p parametrically reduces to 0 using a faithful CGB of I. However, there are other polynomials not in I which also reduce to 0 using a CGB. The weaker definition however will be able to reduce more redundant polynomials in a basis to 0 in contrast to the proposed definition above as was observed in the case of $a * b * x$ with respect to $\{a^2 * x\}$.

Given a finite basis $\mathcal{B} \subseteq K[U][X]$ and a segment α, $f \xrightarrow{\alpha}_{\mathcal{B}} f'$ if there is an unambiguous polynomial $p \in \mathcal{B}$ under α such that $f \xrightarrow{\alpha}_p f'$. Then $f \xrightarrow{\alpha}{}^*_{\mathcal{B}} f'$ is the transitive closure of $\xrightarrow{\alpha}_{\mathcal{B}}$ such that $\forall p \in \mathcal{B}$, $\mathrm{LM}(\overline{p})$ cannot divide any monomial in $\overline{f'}$. In case, f is ambiguous with respect to α, then α needs to be split into multiple segments in order to make f unambiguous with respect to those segments.

Proposition 27 *Given* $f \xrightarrow{\alpha}_{\mathcal{B}} f'$,

(i) $\overline{f'} < \overline{f}$ *under* α;

(ii) f' *is in the ideal generated by* $\mathcal{B} \cup \{f\}$;

(iii) $\xrightarrow{\alpha}_{\mathcal{B}}$ *terminates for fixed* $\mathcal{B}$ *and* α.

In general, f and/or $\mathcal{B}$ can be ambiguous under α. In such a case, to perform reduction, α

is partitioned into a number of subsegments such that f and $\mathcal{B}$ are unambiguous under each of them. After that reduction is applied in each subsegment separately. The reduction of h_2 by $\mathcal{F}$ under δ_2 in Example **EX2** is such a case.

6.3 Algorithm

The algorithm below tests whether a given basis is a CGB or not.

Algorithm CGBTest($\mathcal{G}, \mathcal{E}, \mathcal{N}$)
Input: $\mathcal{G}$: a finite basis in $K[U][X]$; $(\mathcal{E}, \mathcal{N})$: The given parameter space, where $\mathcal{E}, \mathcal{N} \subseteq K[U]$.
Output: True if $\mathcal{G}$ is a CGB on $(\mathcal{E}, \mathcal{N})$; False otherwise.

1. **if** $|\mathcal{G}| \leq 1$ **return** True; **endif**
2. **for each** $f \in \mathcal{G}$:
3. $\quad \Phi_f :=$ SpecializedTuple$(f, \mathcal{E}, \mathcal{N})$;
   endfor
4. **for each** $f, g \in \mathcal{G}$ where $f \neq g$:
5. $\quad \mathcal{P} := \{(f_\alpha, g_\beta, \delta = \alpha \cap \beta) \mid (f_\alpha, \alpha) \in \Phi_f,\ (g_\beta, \beta) \in \Phi_g, \delta \neq \emptyset\}$;
6. $\quad$ **for each** $(f_i, g_j, \delta_{ij}) \in \mathcal{P}$:
7. $\quad\quad$ **if** necessary(f_i, g_j, δ_{ij}) **then**
8. $\quad\quad\quad h_{ij} :=$ S-PolyP$_{\delta_{ij}}(f, g)$;
9. $\quad\quad\quad h_{ij} \xrightarrow{\delta_{ij}}{}^{*}_{\mathcal{F}} h'_{ij}$;
10. $\quad\quad\quad$ **if** h'_{ij} not determined to be 0 under δ_{ij} **then**
11. $\quad\quad\quad\quad$ **return** $False$;
    $\quad\quad\quad$ **endif**
    $\quad\quad$ **endif**
    $\quad$ **endfor**
    endfor
12. **return** True.

Proposition 28 *Given a finite basis $\mathcal{F} \subseteq K[U][X]$ and a parameter space $S = (\mathcal{E}, \mathcal{N})$, the* CGBTest *algorithm terminates, and returns $True$ iff $\mathcal{F}$ is a CGB on S.*

7 Making a CGB Smaller

In this section, we discuss operations on a given CGB to generate a smaller CGB from it. The most critical operation is the redundancy check discussed above. Removing redundant polynomials from a CGB clearly makes it smaller. Below we discuss how redundancy check can be made more efficient by using parametric rewriting. For instance, the redundancy check can be used to generate minimal subsets that are CGBs from the CGB generated by the KSW

algorithm. As shown above, if the redundancy check is performed in ascending order, then the resulting minimal CGB is the least among all subsets of the input CGB that are CGBs. In addition, an essential polynomial in a CGB can be made smaller in multiple ways: (i) Removing factors which are polynomials in parameters and (ii) using classical rewriting insofar as CGBness is preserved.

7.1 Redundancy Check Using Parametric Rewriting Using a Basis

The normal form of a polynomial with respect to a basis varies for different segments. In the illustrative example discussed later in Subsection 9.1, g_4 can be reduced to 0 under η_1, but it is not even reducible under η_2. The parametric ideal generated without g_4 is a proper subideal of $\mathcal{G}$ for many specializations. However, if a polynomial p can be reduced to 0 for every possible specialization by a basis B, then p is redundant with respect to B; in that case, p can be proved to be covered by B; further, for every specialization, the ideal generated by $B \cup \{p\}$ is equal to the ideal generated by B. However, if for some specialization, p does not reduce to 0, then it may or may not be redundant implying that for those specializations, the ideal generated by $B \cup \{p\}$ is in general a superset of the ideal generated by B. This check is equivalent to checking in the nonparametric case whether a normal form of a polynomial p is 0 with respect to a basis in which case p is redundant for the basis; however, a normal form is not 0, then it may or may not be redundant since the basis may not be locally confluent.

As illustrated above, the redundancy of polynomials in a basis is based relative to specializations (segments):

Definition 29 Given a finite basis $\mathcal{F} \subseteq K[U][X]$, a polynomial $f \in \mathcal{F}$ may not be redundant (or is **essential**) with respect to $\mathcal{F}$, if there is a non-empty segment α such that f is reduced by $\mathcal{F} - \{f\}$ to a non-zero normal form under α.

The reader should note that a parametric p may not be redundant with respect to a parametric basis B, but is still in the ideal generated by B just as in the classical case.

Definition 30 Given a finite basis $\mathcal{F} \subseteq K[U][X]$, F is **minimal** if and only if no polynomial $p \in F$ is redundant with respect to $F - \{p\}$.

Keeping a basis minimal can reduce unnecessary computations; there is however a trade-off because this operation can be expensive. As we show later, this check can be relatively easily performed for a CGB. For a given basis, there can in general be many subsets of the basis which may be minimal depending upon the order in which polynomials are checked for redundancy. To generate a least (with respect to the term order $>$ when extended to finite sets of polynomials) minimal basis, the redundancy check must be performed in descending order of polynomials in the basis.

In the nonparametric case, S-polynomials generated from different pairs of polynomials in a Gröbner basis are redundant with respect to the Gröbner basis. In the parametric case also, this property holds as well, suggesting that redundancy check is equivalent to computing a normal form and checking its nonzeroness. That is why for the parametric case, if an S-polynomials generated from specializations of a pair of parametric polynomials is checked for redundancy with respect to the parametric basis in lines 9 and 10 even when it is in the ideal.

7.2 Removing Factors in Parameters

Using results in Subsection 4.1, a minimal CGB can have a polynomial that can be factored with an factor purely in parameters. An example discussed above illustrates this. Consider the ideal $I = \langle ax \rangle$ where a is a parameter. I has along with $\{ax\}$, $\{a^2x\}$ $\{(a^3 + a)x\}$ as CGBs among infinitely many CGBs. In such a case, if a CGB of I includes $A * p$ such that $p \in I$ and $A \neq 1$ is a nonzero polynomial in $K[U]$, then $A * p$ in the CGB can be replaced by p giving a smaller CGB.

7.3 Simplification: Classical Rewriting Preserving CGBness

As illustrated above for **EX3**, classical rewriting does not preserve CGBness of a basis. A polynomial may reduce to 0 with respect to a basis using classical rewriting, but may not reduce to 0 using parametric rewriting. Classical rewriting implicitly assumes the coefficient of the head term of a polynomial used for rewriting is nonzero under all specializations but does not necessarily ensure it. A parametric polynomial $uy + x$ has y as the head term for all specializations in which $u \neq 0$ except for $u = 0$ in which case rewriting done by reducing a term that is a multiple of uy is not generally valid but rather valid only as long as $u \neq 0$.

Identifying conditions under which rewriting and parametric rewriting coincide has been a challenge. A conservative operation, called simplification is introduced in [19] which combines rewriting and checking for CGBness in which case the result can replace the rewritten polynomial. This is illustrated below.

Example 31 For $I = \langle ux^2 - 2y + (4u + 4v)z, (-2u + 2v)x^2 - 2y + 4vz \rangle \subseteq K[u, v][x, y, z]$ and a lexicographic term order $>$ with $x > y > z \gg u > v$, the CGS computed by the KSW algorithm is:

Table 1

	branch	basis	LT
1	$(\ \emptyset,\ \{v(3u - 2v)\}\ )$	$\{f_1, f_2\}$	$\{y, x^2\}$
2	$(\ \{3u - 2v\},\ \{v\}\ )$	$\{f_4, f_3\}$	$\{z, x^2\}$
3	$(\ \{u,\ v\},\ \{1\}\ )$	$\{f_2\}$	$\{y\}$
4	$(\ \{v\},\ \{u\}\ )$	$\{f_2, f_4\}$	$\{y, x^2\}$

and the CGB is:

$$\mathcal{G} = \left\{ f_1 = \left(u - \frac{2}{3}v\right)y + \left(-\frac{4}{3}u^2 - \frac{2}{3}uv + \frac{4}{3}v^2\right)z,\ f_2 = vx^2 - 3y + (4u + 6v)z, \right.$$
$$\left. f_3 = \left(u - \frac{10}{13}v\right)x^2 + \frac{4}{13}y + \frac{12u - 8v}{13}z,\ f_4 = \left(u - \frac{2}{3}v\right)x^2 + \frac{4}{3}uz \right\}.$$

A minimal CGB using essentiality check in descending order gives $\mathcal{M}_1 = \{f_1, f_2, f_3\}$. However, even a smaller MCGB can be obtained from $\mathcal{M}_1$ by simplifying f_3 further to i_1 : $ux^2 - 2y + 4(u + v)z$, the first polynomial in the input basis.

Simplification for parametric polynomials can be extremely tricky however; particularly, replacing a parametric polynomial in a CGB by another parametric polynomial obtained in general after simplifying using the CGB need not preserve CGBness.

An obvious way to ensure that replacing a polynomial by its simplified form preserves CGBness is to check that the simplified form covers the original polynomial along with other polynomials in the CGB as defined in the previous section. That means essentiality check must be performed after simplification to maintain the correctness. This simplification step can be performed after a minimal CGB has been generated using essentiality check in the ascending order.

It will be useful to identify conditions under which simplification using classical rewriting preserves CGBness so that the expensive essentiality check can be avoided.

8 Performance of Algorithm for Generating Minimal CGBs

Table 2 Results about computing MCGB and CGS

Example	$\|KCGS\|$	$\|MCGS\|$	$\|\mathcal{KM}\|$	$\|\mathcal{M}\|$	% reduced
bad test	6	6	8	6	33%
KSW51	6	5	7	6	17%
higher 1	4	4	9	6	50%
higher 3	6	6	6	4	50%
linear	4	4	4	3	33%
montes 3	12	10	11	6	83%
GBCover	7	5	12	7	71%
SS 1	4	4	12	10	20%
SS 3	19	17	36	27	41%
Sit 21	5	5	6	3	100%
Weispfenning 4	4	4	3	2	50%
Principal	6	5	3	1	200%
CTD	5	5	6	4	50%
S 10	4	4	14	12	17%
S 12	18	15	15	8	88%
S 13	11	10	9	6	50%
S 16	19	19	15	9	67%
S 53	7	5	13	6	117%
Nonlinear 1	6	6	9	4	125%

Below we show the performance of some of the algorithms discussed earlier; they are implemented in SINGULAR[21]. We tested the implementation on a large suite of examples including those from [4, 6, 7, 9, 13, 14, 22]. For instance, there are 70 out of 100 examples which have redundant polynomials in the CGBs generated by the KSW algorithm, which is considered the best algorithm so far for computing smaller CGSs and CGBs[6]. Below we list some of the results. Even though the worst-case complexity of computing CGS, CGB, MCGB is very high, the table below demonstrates that on many problems, results can be effectively obtained.

The complexity of a problem is given by the size of its CGS (i.e., the number of branches) and CGB, which are the columns with labels KCGS and $|\mathcal{KM}|$, with the prefix K suggesting that the KSW implementation was used . The size of an MCGB computed by removing redundant polynomials is shown in the column with label $|\mathcal{M}|$, with the percentage of how many non-essential polynomials are removed from $\mathcal{KM}$ calculated as $(|\mathcal{KM}| - |\mathcal{M}|)/|\mathcal{M}|$. The column with label —MCGS— shows the size of CGS reconstructed from minimal CGB $\mathcal{M}$. As the table illustrates, a minimal CGB can reduce the size of an input CGB by as much as 100% sometimes.

9 Computing Minimal CGB Directly: Completion Algorithm

A completion algorithm for computing a comprehensive Gröbner basis of a parametric ideal is presented in this section. It is similar in spirit to Buchberger's completion algorithm for computing a Gröbner basis of a polynomial ideal. It closely parallels any completion procedure in which when the result of a critical pair checking (local) confluence fails, then the result is added to a given basis to eliminate that lack of non-confluence of the basis.

If the check for CGB (CGBTest) fails on a given basis of a parametric ideal, the current basis can be augmented with (normal forms of) S-polynomials that do not reduce to 0 during the CGB check; this process is repeated until a basis is obtained that passes the CGB check. Since parametric rewriting can be expensive, there is a trade off about how much rewriting should be performed. The performance of the completion algorithm is governed by many factors including the order in which S-polynomials are processed, whether polynomials in the current basis are normalized using the new polynomial(s) generated and redundant polynomials in the basis are discarded.

Before discussing the details of the completion algorithm, we illustrate its key ideas.

9.1 An Illustrative Example

Consider an ideal $I = \langle \mathcal{F} \rangle = \langle g_1 = ab^2y^2 + b^3 - 1,\ g_2 = ax^2y + a^2x^2 - 3a \rangle \subseteq K[a,b][x,y,z]$.We wish to compute a CGB of I for all values of a and b with respect to the degree order induced by $x > y > z \gg a > b$. The initial basis is $\mathcal{G} = \{g_1, g_2\}$.

Step 1 Parametric Specializations of Polynomials and Redundancy Check.

Compute Φ_{g_1} and Φ_{g_2} as the sets of all possible specializations of g_1 and g_2:

$$\begin{aligned}\Phi_{g_1} = \{&(g_{11} = [ab^2y^2 + b^3 - 1, 0],\ \alpha_1 = (\emptyset,\ \{ab^2\})),\\ &(g_{12} = [b^3 - 1,\ ab^2y^2],\ \alpha_2 = (\{ab\},\ \{b^3 - 1\}))\};\\ \Phi_{g_2} = \{&(g_{21} = [ax^2y + a^2x^2 - 3a,\ 0],\ \beta_1 = (\emptyset,\ \{a\}))\}.\end{aligned}$$

None of g_1, g_2 is redundant since each of them has a non-zero normal form after reduction by the other polynomial under some segment.

Step 2 Reduce Parametric S-polynomial.

Let $\mathcal{P}$ be the set of critical pairs constructed from Φ_{g_1} and Φ_{g_2}; there is only one necessary pair: $(g_{11},\ g_{21},\ \delta_1 = \alpha_1 \cap \beta_1 = (\emptyset,\ \{ab\}))$. Under δ_1, the parametric S-polynomial is $h_1 =$

S-PolyP$_{\delta_1}(g_{11}, g_{21}) = x^2 g_{11} - b^2 y g_{21} = [-a^2b^2x^2y + (b^3-1)x^2 + 3ab^2y,\ 0]$.

Both h_1 and the basis $\mathcal{G}$ are unambiguous under δ_1. h_1 can be reduced using $\mathcal{G}$ leading to its normal form: $h_1' = [\psi x^2 + 3ab^2y - 3a^2b^2,\ 0]$ under δ_1, where $\psi = a^3b^2 + b^3 - 1$. Since $\overline{h_1'} \neq 0$ under δ_1, $\mathcal{G}$ fails to be a CGB.

This normal form $g_3 = \psi x^2 + 3ab^2y - 3a^2b^2$ is added to $\mathcal{G}$, making it $\{g_1, g_3, g_2\}$, where $g_1 < g_3 < g_2$.

Step 3 Redundancy Check.

It is checked whether adding g_3 can make any of g_1, g_2 redundant, which is not the case. g_3 contributes new critical pairs both with g_1 and g_2 using Φ_{g_3}.

$$\Phi_{g_3} = \{(g_{31} = [g_3,\ 0],\ \gamma_1 = (\emptyset,\ \{\psi\})),\\ (g_{32} = [3ab^2y - 3a^2b^2,\ \psi x^2],\ \gamma_2 = (\{\psi\},\ \{3ab^2\}))\}.$$

There are 3 new necessary critical pairs: $(g_{11}, g_{32}, \alpha_1 \cap \gamma_2)$, $(g_{31}, g_{21}, \gamma_1 \cap \beta_1)$ and $(g_{32}, g_{21}, \gamma_2 \cap \beta_1)$.

Repeat Step 2. $(g_{11},\ g_{32},\ \alpha_1 \cap \gamma_2)$: $\delta_2 = (\{\psi\},\ \{3a^2b^4\})$ gives $h_2 = $ S-PolyP$_{\delta_2}(g_{11}, g_{32}) = [3a^2b^2y + 3b^3 - 3,\ -\psi x^2 y]$. Both h_2 and the basis $\mathcal{G}$ is unambiguous under δ_2. A normal form is $h_2' = h_2 - a g_{32} = [0,\ -\psi x^2 y - a\psi x^2 + 3\psi]$, which is 0 under δ_2. No new polynomial is added in $\mathcal{G}$.

The next critical pair is $(g_{32},\ g_{21},\ \gamma_2 \cap \beta_1)$. $\delta_3 = (\{\psi\},\ \{3a^2b^2\})$ resulting in $h_3 = $ S-PolyP$_{\delta_3}(g_{32}, g_{21}) = x^2 g_{32} - 3b^2 g_{21} = [-6a^2b^2x^2 + 9ab^2,\ \psi x^4]$. Both h_3 and the basis $\mathcal{G}$ are unambiguous under δ_3. h_3 is already reduced, with $\overline{h_3} \neq 0$ under δ_3. So $h_3 = \psi x^4 - 6a^2b^2x^2 + 9ab^2$ is added as g_4 to the current basis: $\mathcal{G} = \{g_1, g_3, g_2, g_4\}$, where $g_1 < g_3 < g_2 < g_4$.

Repeat Step 3.

It is checked whether adding g_4 can make polynomials g_1, g_2, g_3 in $\mathcal{G}$ redundant. First consider g_2, which has only one specialized tuple (g_{21}, β_1). The set $\mathcal{G} - \{g_2\}$ is ambiguous under $\beta_1 = (\emptyset,\ \{a\})$, so partition β_1 into β_{11}, β_{12} and β_{13}:

(i) $\beta_{11} = \beta_1 \cup \{ab^2 \neq 0,\ \psi \neq 0\}$: g_{21} has a normal form $g_{21}' = \psi g_{21} + 3a g_1 - (ay + a^2) g_2 = 0$.

(ii) $\beta_{12} = \beta_1 \cup \{ab^2 = 0\}$: LT$(\mathcal{G} - \{g_2\}, \beta_{12}) = \{1, x^2, x^4\}$. The normal form of g_{21} is 0 using g_1

(iii) $\beta_{13} = \beta_1 \cup \{\psi = 0,\ ab^2 \neq 0\}$: LT$(\mathcal{G} - \{g_2\}, \beta_{13}) = \{x, y, y^2\}$. The normal form of g_{21} by $\mathcal{G} - \{g_2\}$ under this segment is also 0.

Since g_2 reduces to 0 under all subsegments of β_1, g_2 is redundant; it is removed from $\mathcal{G}$. Neither of the remaining polynomials g_1 and g_3 is redundant. The current basis is thus $\mathcal{G} = \{g_1, g_3, g_4\}$. Since g_2 is no more in the current basis, all critical pairs due to g_2 are removed from $\mathcal{P}$ making $\mathcal{P} = \emptyset$.

Compute critical pairs due to Φ_{g_4}:

$$\Phi_{g_4} = \{(g_{41} = [g_4,\ 0],\ \eta_1 = (\emptyset,\ \{\psi\}),\\ (g_{42} = [6a^2b^2x^2 - 9ab^2,\ -\psi x^4],\ \eta_2 = (\{\psi\},\ \{6a^2b^2\}))\}.$$

There is only one necessary pair: $(g_{31},\ g_{41},\ \gamma_1 \cap \eta_1)$.

The segment associated with this critical pair is: $\delta_4 = \gamma_1 \cap \eta_1 = (\emptyset, \{\psi\})$, and $h_4 = \text{S-Poly}_{\delta_4}(g_{31}, g_{41}) = 3ab^2x^2y + 3a^2b^2x^2 - 9ab^2$. The basis $\mathcal{G}$ is ambiguous under δ_4, since $\text{LC}(g_1, \delta_4)$ is not determined. Segment δ_4 is thus partitioned as follows:

(i) $\delta_{40} = \delta_4 \cup \{ab^2 = 0\}$: g_1 becomes 0, so $\text{LT}(\mathcal{G}, \delta_{40}) = \{x^2, x^4\}$.

(ii) $\delta_{41} = \delta_4 \cup \{ab^2 \neq 0\}$: $\text{LT}(\mathcal{G}, \delta_{41}) = \{y^2, x^2, x^4\}$.

h_4 reduces to 0 by $\mathcal{G}$ under both the segments. Since that is the only critical pair in $\mathcal{P}$, the algorithm terminates with a CGB of I:

$$\mathcal{G} = \{g_1 : ab^2y^2 + b^3 - 1,\ g_3 : \psi x^2 + 3ab^2y - 3a^2b^2,\ \ g_4 : \psi x^4 - 6a^2b^2x^2 + 9ab^2\},$$

where $\psi = a^3b^2 + b^3 - 1$.

9.2 Algorithm

Algorithm Redundant$(f, \mathcal{G}, \mathcal{E}, \mathcal{N})$

Input: f: A parametric polynomial in $\mathcal{G}$; $\mathcal{G}$: A finite basis in $K[U][X]$; $(\mathcal{E}, \mathcal{N})$: Segment, where $\mathcal{E}, \mathcal{N} \subseteq K[U]$.

Output: True if f is redundant in $\mathcal{G}$ on $(\mathcal{E}, \mathcal{N})$; False otherwise.

if $|\mathcal{G}| \leq 1$ **then return** $\mathcal{G}$ **endif**

Let $\Phi_f :=$ SpecializedTuple$(f, \mathcal{E}, \mathcal{N})$;

for each $(f_\alpha, \alpha) \in \Phi_f$:

$f \xrightarrow{\alpha}{}^{*}_{\mathcal{G}-\{f\}} f'$;

if f' is not determined to be 0 under α **then** **return** False;

endfor

return True;

As illustrated above, the Completion algorithm is closely related to the algorithms given in [1, 2] except for the integration of the redundancy check. During the CGB check (CGBTest), if an S-polynomial does not reduce to 0 for the associated segment of specializations, its normal form[¶] is added to the current basis; this process is repeated until the CGB check succeeds implying that all S-polynomials generated from all distinct pairs of parametric polynomials in the current basis reduce to 0. The definitions of S-polynomials and reduction above ensure that every new polynomial added to the current basis is in the parametric ideal, thus preserving the faithfulness of the current basis as an invariant property of the completion algorithm.

In Buchberger's algorithm, a minimal Gröbner basis (MGB) is obtained by always using the newly added polynomial in normal form to simplify other polynomials in the current basis (particularly by eliminating their leading terms). A reduced Gröbner basis (RGB) is generated when full reduction is used for simplification and polynomials in the current basis are kept in their normal forms. Such a minimal reduced Gröbner basis can be made unique for a given

[¶]As the reader would have seen in the above illustration, the concept of a normal form for a parametric polynomial is more complex than the classical definiton of a normal form of a polynomial by a basis.

ideal I for a given term order $>$ by making the leading coefficient of every polynomial in the basis to be a unit.

The properties of MGB and RGB are however a lot more difficult to achieve for the Completion algorithm for the parametric case because of complications due to specializations. While the minimality check on a CGB was first proposed in [19] and the first completion algorithm for generating a minimal CGB algorithm was proposed in [20], an algorithm for generating a canonical CGB (CCGB) is elusive and to our knowledge, is still an open question.

To keep a basis in the completion algorithm to be minimal, Redundant algorithm is used to delete, from a current basis, polynomials that are not essential. Assuming that every polynomial in the input basis is essential (which can be checked at the start of the algorithm) and by applying the Redundant algorithm on the basis every time a new polynomial is added to the basis, the Completion algorithm has another invariant property as stated below.

Proposition 32 *The basis $\mathcal{G}$ in the main loop of* Completion *algorithm* (*Line* 8 *to* 21) *contains only essential polynomials at the end of each iteration.*

Invariant properties of a basis $\mathcal{G}$ at every iteration of the main loop of the Completion algorithm ensure that the basis always consists of faithful and essential polynomials.

The correctness and termination of the Completion algorithm can be established by a proof similar to the proofs of correctness of Buchbeger's algorithm and the algorithm for computing a Gröbner system given in [1]; the proposed algorithm is structurally similar to the algorithm Gröbner system in [1] except for the redundancy check which only eliminates polynomials from a basis. The only place a polynomial — a non-zero normal form of an S-polynomial with respect to a segment, is added to a basis in the algorithm is at Line 21.

We use an argument similar to the one in [1] for showing termination. The main loop is from 8–21. To show termination, consider a tree of 4-tuples of the form $\langle \alpha, B, f, g\rangle$, where α is a segment, B is a basis, $f \neq g, f, g \in B$ (these are tuples for generating S-polynomials). A parent $\langle \delta_{i,j}, \mathcal{G}, f_i, g_j\rangle$ at Line 9 of the algorithm is followed in the tree after an iteration of the loop body, by the immediate descendents $\langle \delta', \mathcal{G}', f', g'\rangle$, depending upon a normal form r computed from $S\text{-Poly}_{\delta_{i,j}}(f_i, g_j)$ with respect to $\delta_{i,j}$ (Lines 10 and 11): (i) $r = 0$: $\mathcal{G}' = \mathcal{G}$; there can only be finitely many such descendants on a path since $\mathcal{G}$ is finite, (ii) $r \neq 0$: $\mathcal{G}'$ includes r but the rest of it is a subset of $\mathcal{G}$ since polynomials made redundant due to r in Lines 16 and 17 are removed; however $\text{LT}(r)$ with respect to $\delta_{i,j}$ is not multiple of any head term of the other polynomials with respect to $\delta_{i,j}$ in $\mathcal{G}'$; such a path is also finite as there cannot be infinitely many polynomials with respect to $\delta_{i,j}$ with noncomparable head terms (using divisibility relation among terms) because of Dickson's Lemma (like in Buchberger's algorithm). Since this tree is finitely branching, for it to be infinite, there must exist an infinite branch by König Lemma, which gives a contradiction. Also, there can only be finitely many segments refining the segment $\delta_{i,j}$.

Proposition 33 *Given a finite basis $\mathcal{F} \subseteq K[U][X]$ and a parameter space $S = (\mathcal{E}, \mathcal{N})$, the* Completion *algorithm terminates, and outputs a faithful minimal CGB of an ideal $I = \langle \mathcal{F}\rangle$ on S.*

Algorithm Completion($\mathcal{F},\mathcal{E},\mathcal{N}$)
Input $\mathcal{F}$: a finite basis in $K[U][X]$; $(\mathcal{E},\mathcal{N})$: the given parameter space, where $\mathcal{E},\mathcal{N}\subseteq K[U]$.
Output An MCGB $\mathcal{G}$ of ideal $I=\langle F\rangle$.

1. $\mathcal{G}:=\mathcal{F}$;
2. **if** $|\mathcal{G}|\leq 1$ **then return** $\mathcal{G}$; **endif**
3. **for each** $f\in\mathcal{G}$:
4. **if** Redundant$(f,\mathcal{G},\mathcal{E},\mathcal{N})$ **then**
5. $\mathcal{G}:=\mathcal{G}-\{f\}$;
6. **else** $\Phi_f:=$ SpecializedTuple$(f,\mathcal{E},\mathcal{N})$;
endif
endfor
7. $P:=\{\pi=(f_\alpha,g_\beta,\alpha\cap\beta)\mid \alpha\cap\beta\neq\emptyset,\ f,g\in\mathcal{G},\ (f_\alpha,\alpha)\in\Phi_f,\ (g_\beta,\beta)\in\Phi_g,\text{necessary}(\pi)\}$;
8. **while** $\mathcal{P}\neq\emptyset$ **do**
9. Choose $\pi=(f_i,g_j,\delta_{ij})\in\mathcal{P}$;
10. $h_{ij}=\text{S-Poly}_{\delta_{ij}}(f,g)$;
11. $h_{ij}\xrightarrow{\delta_{ij}}{}^{*}_{\mathcal{G}}\ r$;
12. **if** r is determined to be 0 under $\delta_{i,j}$ **then**
13. $\mathcal{P}:=\mathcal{P}-\{\pi\}$;
else
15. **for each** $q\in\mathcal{G}$:
16. **if** Redundant$(q,\mathcal{G}\cup\{r\},\mathcal{E},\mathcal{N})$ **then**
17. $\mathcal{G}:=\mathcal{G}-\{q\}$;
18. $\mathcal{P}:=\mathcal{P}-\{(\phi_\gamma,\psi_\eta,\gamma\cap\eta)\mid \phi=q \text{ or } \psi=q\}$;
endif
endfor
19. $\Phi_r:=$ SpecializedTuple$(r,\mathcal{E},\mathcal{N})$;
20. $\mathcal{P}:=\mathcal{P}\cup\{(r_\gamma,\phi_\eta,\gamma\cap\eta)\mid \gamma\cap\eta\neq\emptyset,\phi\in\mathcal{G},$
$(r_\gamma,\gamma)\in\Phi_r,\ (\phi_\eta,\eta)\in\Phi_\phi\}$;
21. $\mathcal{G}:=\mathcal{G}\cup\{r\}$;
endif
endwhile
22. **return** $\mathcal{G}$;

In the illustrative example in Subsection 9.1, the Completion algorithm indeed computes an minimal CGB $\mathcal{G}=\{g_1,g_3,g_4\}$ of I. Further, by performing the Redundant algorithm every time when adding a new polynomial to the basis, unnecessary critical pairs related to redundant polynomials are discarded. For example, after removing g_2 from the basis in the illustrative example in Subsection 9.1, the pair $(g_{32},\ g_{21},\ \gamma_2\cap\beta_1)$ in $\mathcal{P}$ is removed without consideration.

A normal selection strategy[25] is applied on triples in $\mathcal{P}$ to improve the efficiency. For instance, in the illustrative example in Subsection 9.1, when $\mathcal{P}$ has 3 triples: $\pi_1=(g_{11},\ g_{32},\ \alpha_1\cap\gamma_2)$, $\pi_2=(g_{31},\ g_{21},\ \gamma_1\cap\beta_1)$ and $\pi_3=(g_{32},\ g_{21},\ \gamma_2\cap\beta_1)$, π_1 is chosen first, since lcm(LT(g_{11}),

$\mathrm{LT}(g_{32})) = y^2$ is the least, while those of the other two are both x^2y.

While the proposed Completion algorithm is deterministic and computes a unique minimal CGB from a basis of any given ideal, different bases of the same ideal can lead the Completion algorithm to generate different minimal CGBs. Further the order in which polynomials in the current basis are checked for redundancy can also lead to the Completion algorithm producing different minimal CGBs. We have implemented a strategy in which polynomials in the current basis are checked for redundancy in descending order thus generating the smallest minimal basis at any time in the ordering on finite sets of polynomials induced by an admissible term ordering. This is quiet a contrast from the non-parametric case where a unique reduced Gröbner basis is computed if the elements of a basis are always in normal form and the head coefficients are made monic. This also illustrates the difficulty in computing a canonical CGB in the parametric case.

10 Comparison with Other CGB Algorithms

To our knowledge, the proposed completion algorithm is the first direct algorithm for computing a minimal faithful comprehensive Gröbner basis of a given parametric ideal as we are unaware of any other algorithm that computes a CGB directly from a given basis. All existing algorithms proposed in the literature instead first compute a comprehensive Gröbner system (CGS) (or an object similar to it) of a given parametric ideal, which is a finite set of branches, with each branch consisting of a segment and a corresponding Gröbner basis under it. A CGB can be recovered from such a CGS if it is faithful, by taking the union of these Gröbner bases. If branches in a CGS do not have faithful Gröbner bases, then the union of the Gröbner bases need not even be a CGB since for some specialization, the Gröbner basis of the specialized ideal may be 1 or include a polynomial not in the ideal. Faithfulness is thus a crucial property desired in constructions for CGBs. Below we discuss other algorithms proposed in the literature from the stand point of whether they produce a minimal and/or faithful and/or unique comprehensive Gröbner basis.

Weispfenning's Gröbner system as well as Reduced Gröbner System (RGS) algorithms in [1] and the parametric Gröbner basis (PGB) algorithm by Kapur in [2] are patterned after the Buchberger's algorithm much like the proposed completion algorithm. RGS is defined using S-polynomials and reduction relative to a condition γ (equivalent to a segment); similarly, PGB has constrained polynomials (γ, f), where f is a parametric polynomial and γ is a set of constraints, which is also equivalent to a segment. In Weispfenning's algorithms, reduction relative to a segment is defined similar to that in [20] and is thus less restricted than the definition given in this paper. In other words, the polynomial $a\ x$ reduces to 0 using a basis $\{a^u\ x\}$ for any $i > 1$ even though $a\ x$ is not in the ideal generated by the basis. Both algorithms enforce the Gröbner basis under each segment to be reduced. Weispfenning's RGS looked similar to CGS. Weispfenning defined a CGB to be the union of all polynomials generated during RGS computation after dropping the segments associated with the polynomials. The faithful CGS and CGB computed by the (KSW) algorithm proposed by Kapur, et al. in [4] has the property

that under each segment γ, the corresponding Gröbner basis G_γ is minimal of the specialized ideal. The KSW algorithm thus computes a minimal CGS. However, the CGB recovered by taking the union of these corresponding Gröbner bases fails to be minimal as illustrated by numerous examples above. That is despite the fact that all segments in the KSW are disjoint whereas that need not be the case for other algorithms. The main difference between the methods proposed in this paper in contrast to [1, 2] is performing the redundancy check and including only essential polynomials in a basis. In the redundancy check as discussed above, all specialized tuples of a polynomial f are used together for determining whether f is redundant for efficiency and completeness, while such tuples are considered independent of each other in RGS and PGB.

Weispfenning's definition of a reduced comprehensive Gröbner basis in [1] using the concept of a reduced Gröbner system appears to be particularly complicated. As stated in [1], whereas a reduced Gröbner basis in the classical sense is unique for an ideal for a fixed term ordering and further, has the smallest number of polynomials among all Gröbner bases of the ideal for that ordering, a reduced comprehensive Gröbner basis of a parametric ideal in [1] neither has fewer elements nor is unique. In fact, such as reduced CGB often has many redundant polynomials which can be eliminated using the essentiality check discussed above.

Weispfenning's CCGB algorithm[14] achieves the algorithm-dependent uniqueness of the resulting CGB, but it fails to be minimal or canonical in the sense that it is a unique minimal CGB associated with a parametric ideal for a given admissible term ordering. Consider Example 8.2 in [14] on $\mathbb{Q}[v,u][z,y,x]$ using a lexicographic term order such that $z > y > x \gg v > u$: $I = \langle f : uy + x,\ g : vz + x + 1\rangle$. The CCGB algorithm computes CGB $\mathcal{G} = \{f, g, h, -h\}$, where $h = vz - uy + 1$. It is easy to check that both $\{f, g, h\}$ and $\{f, g, -h\}$ are also CGBs of I, so $\mathcal{G}$ is neither minimal nor unique.

Algorithms proposed by Kapur, et al. in [3, 4] compute faithful CGSs, whereas algorithms of Suzuki and Sato[13] as well as the MCCGS[7] and Gröbner cover[9] algorithms of Montes and his collaborators do not compute faithful CGSs. The Gröbner cover uses regular functions, rather than polynomials, for the representation of segments.

Montes' MCCGS algorithm also achieves an algorithm-dependent definition of uniqueness. It was later extended by Montes and Wibmer as the Gröbner cover algorithm to compute an algorithm-independent unique Gröbner cover for a given parametric ideal for a given admissible term ordering. It first homogenizes the given basis to the projective space, then computes a canonical CGS of this homogeneous ideal, and finally maps it back to the affine space. However, Gröbner cover is not faithful, thus no CGB is generated from it.

11 Implementation of Completion Algorithm

The proposed algorithm has been implemented on top of Singular system 4.0[21]. Except for using basic polynomial operations of Singular, we had to reimplement S-polynomials and reduction of a polynomial with an associated segment by a basis of polynomials from scratch since all computations must be done with respect to segments. We were unable to use any

of the available infrastructure such as computing normal forms, reduction of a polynomial by a basis of polynomials, computing a Gröbner basis, etc. This has made our implementation slower compared to implementations for computing reduced Gröbner basis supported by Singular. Despite this disadvantage/handicap, we have successfully computed minimal CGBs of all examples of parametric ideals reported in [7, 9, 13, 14].

We have also compared the output generated by the proposed algorithm with a two-phase algorithm MCGBMain of computing MCGBs proposed in [19]: Recall that in that algorithm, first a faithful CGS and the associated CGB are computed using the KSW algorithm which is considered the fastest algorithm available for computing CGSs[6]; subsequently, an MCGB is generated from the CGB by removing redundant polynomials (similar to redundancy check discussed in Section 4) and performing simplification of polynomials using MCGBSimpl discussed in [19]. In many examples, the Completion algorithm generates MCGBs smaller than MCGBMain and MCGBSimpl.

We have also compared the output generated by the proposed algorithm with a two-phase algorithm *MCGBMain* of computing MCGBs proposed in [19]: recall that in that algorithm, first get a faithful CGS and the associated CGB are computed using the KSW algorithm which is considered the fastest algorithm available for computing CGSs[6], and an MCGB is generated this CGB by removing redundant polynomials (similar to redundancy check discussed in Section 4) and then performing simplification of polynomials using *MCGBSimpl*. For many examples, the proposed *Completion* algorithm generates MCGBs even smaller than *MCGBMain* and *MCGBSimpl*.

The most surprising observation has been that using the proposed completion algorithm, we are able to generate minimal faithful CGBs for some parametric ideals which cannot be obtained using any other algorithm including our two-phase algorithm reported in [19]. Below we give two such examples.

Consider the illustrative example in Subsection 9.1. The KSW algorithm gives a CGB

$$\begin{aligned}\mathcal{G} = \{&g_1 : ab^2y^2 + b^3 - 1,\ g_2 : \psi x^2 + 3ab^2y - 3a^2b^2,\\ &g_3 : a^2\psi x^2 + 3a^3b^2y - 3a^4b^2,\ g_4 : a\psi x^4 - 6a^3b^2x^2 + 9a^2b^2\},\end{aligned}$$

where $\psi = a^3b^2 + b^3 - 1$.

The two-phase algorithm in [19] generates an MCGB $\mathcal{M}' = \{g_1, g_2, g_4\}$.

The Completion algorithm gives a smaller MCGB $\mathcal{M} = \{g_1, g_2, g_5\}$, where $g_5 = \psi x^4 - 6a^2b^2x^2 + 9ab^2$.

For the second example, consider an ideal $I = \langle (a-b)x^2 - by^2 + ay,\ axy - ay^2 - by\rangle \subseteq K[a,b][x,y]$ and a graded lexicographic term order such that $x > y \gg a > b$. The KSW algorithm gives a CGB

$$\begin{aligned}\mathcal{G} = \Big\{ &g_1 : axy - ay^2 - by,\\ &g_2 : (a-b)x^2 - by^2 + ay,\\ &g_3 : (a-b)x^2 - axy + (a-b)y^2 + (a+b)y,\end{aligned}$$

$$g_4 : (a^2 - 2ab)y^3 - b^2xy + (a^2 + 2ab - b^2)y^2 + b^2y,$$
$$g_5 : axy^2 - ay^3 + (-a + b)x^2 - ay,$$
$$g_6 : (a - 2b)x^2y + (a - 2b)y^3 + \frac{1}{2}(-a + 2b)xy + \frac{1}{2}(5a + 2b)y^2 + \frac{1}{2}by,$$
$$g_7 : (a - 2b)x^2y + (a - 2b)y^3 + \frac{1}{2}(5a + 2b)xy + \frac{1}{2}(-a + 2b)y^2 - \frac{5}{2}by,$$
$$g_8 : (a - 2b)x^2y + (a - 2b)y^3 + (6a - 6b)x^2 + \frac{1}{2}(-a + 2b)xy + \frac{1}{2}(5a - 10b)y^2 + \frac{1}{2}(12a + b)y\Big\}.$$

After removing redundant polynomials g_3, g_5, g_7, g_8, MCGBMain algorithm gives an MCGB $\mathcal{M}_1 = \{g_1, g_2, g_4, g_6\}$.

Interestingly, the proposed completion algorithm gives an MCGB $\mathcal{M}_2 = \{g_1, g_2, g_9\}$ using a new polynomial g_9:

$$g_9 = (a^3 - 2a^2b)y^3 + (a^3 + 2a^2b - 2ab^2)y^2 + (ab^2 - b^3)y.$$

$\mathcal{M}_2$ not only reduces the size of $\mathcal{G}$ by half, but it's the least MCGB with a smaller size and simpler polynomials than $\mathcal{M}_1$.

12 Issues in Designing an Algorithm for Computing a CCGB

Even though the existence of a canonical CGB of a parametric ideal with respect to an admissible term ordering, was proved above, its algorithimic construction is a challenge. There are a number of obstacles. Below we provide some additional insights.

We have recently observed a phenomenon in CGB constructions which may not be easy to compute. It is best illustrated by the following example:

Let $B = \{f_1 : b*y-(a+1)*v+b), f_2 : (a+1)*y+b*v-a-1, f_3 : b*x-(a-1)*u-b, f_4 : (a-1)*x+b*u+(a-1)\}$ be a basis of a parametric ideal I in which a, b are parameters and x, y, u, v are indeterminates. Using degree, reverse lex or lexicographic term orderings in which $x > y \gg u > v$ as a block (such distinctions among ordering do not matter in case of linear polynomials), it can be shown that the RGB of I is also a CGB, however it contains many redundant elements.

The smallest MCGB we have been able to find so far is: $M_{\min} = \{g_1 : (a^2+2a+b^2+1)*v-2ab-2b, g_2 : (a^2-2a+b^2+1)*u+2ab-2b, f_1 : b*y+(-a-1)*v+b, f_2 : (a+1)*y+b*v+(-a-1), f_3 : b*x+(-a+1)*u-b, f_4 : (a-1)*x+b*u+(a-1)\}$ which includes the input basis. However, there is an MCGB of smaller size which is however bigger than $M_{\min}$ in the set ordering on polynomials: $M_s = \{g_1 : (a^2 + 2a + b^2) * v - 2ab - 2b, g_2 : (a^2 - 2a + b^2) * u + 2ab - 2b, g_3 : (a^2 + 2a + b^2 + 1) * y + (-a^2 - 2a + b^2 - 1), g_4 : (a^2 - 2a + b^2 + 1) * x + (a^2 - 2a - b^2 + 1)\}$. It turns out all the MCGBs we were able to compute using different methods include g_1, g_2. Apparently, f_1, f_2, which are smaller than g_3 replace it; similarly f_3, f_4 replace g_4. Notice that the $\mathrm{LC}(g_3) = \mathrm{LC}(f_1)^2 + \mathrm{LC}(f_2)^2$; similarly $\mathrm{LC}(g_4) = \mathrm{LC}(f_3)^2 + \mathrm{LC}(f_4)^2$. $\mathrm{LC}(g_3) = 0$ is

equivalent to $\mathrm{LC}(f_1) = 0 \wedge \mathrm{LC}(f_2) = 0$ except for the case when $\mathrm{LC}(f_1) = \mathrm{LC}(f_2)$ i given that the field of specializations is algebraically closed (complex numbers for example). A curious reader can work out the details of the case when $\mathrm{LC}(g_3) = 0$ but $\mathrm{LC}(f_1) = \mathrm{LC}(f_2) * i \neq 0$ which makes $a = -1 + b * i$; for such family of specializations, the above two different specializations of CGBs lead to the same RGB.

The above example seems to suggest the need of yet another operation on polynomials and CGBs to generate a smaller CGB from a given CGB. In particular, when the leading coefficient can be expressed as a sum of square expressions, perhaps it can be replaced by multiple polynomials with the same leading term, but with smaller coefficients, as that of the polynomial being replaced insofar as they are in the ideal. But this operation does not seem local but appears relative to the whole basis just like redundancy check. Perhaps the following may work: Given a polynomial p in a CGB such that $\mathrm{LC}(p)$ can be decomposed into smaller polynomials in parameters, say $A_1, A_2, \cdots, A_k$ such that $\mathrm{LC}(p) = A_1^2 + A_2^2 + \cdots + A_k^2$, then p can be replaced by a set of polynomials with the same head term as that of p but with A_i's as head coefficients (perhaps in general B_i's as head coefficients assuming $A_i = B_i^m$ for some $m > 0$ or $A_i = B_{i,1} * B_{i,2} * \cdots * B_{i,l}$) insofar as such polynomials are in the ideal. For the above example $((a+1)^2 + b^2)$ is replaced by $a + 1$ and b for g_3 whose head term is y; similarly, for g_4, the coefficient of x can be made smaller by finding replacements for g_3. This information is available in the RGB of I. Integrating such an operation efficiently into the proposed completion algorithm is a challenge.

The simplification[19] operation discussed in Section 7.3 which integrates classical rewriting with essentiality check is also needed for generating smaller CGBs as illustrated above. It may be possible to replace coefficients of terms in a polynomial in a CGB by smaller coefficients using classical rewriting but still preserving CGBness but that is not true in general as illustrated above. Consider an ideal J generated by a basis $B = \langle (a+b)x, (a-b)x \rangle$, with $x \gg a > b$, a, b are parameters and x is a non-parameter. It can be easily checked that the basis B is a CGB which is also minimal since both polynomials are essential. To verify essentiality, under the segment $(a - b) \neq 0$, which makes $(a-b)x$ unambiguous, $(a+b)x$ is still ambiguous, so it is split into two parts: $(a + b) \neq 0$ and $(a + b) = 0$; In the first case, $(a + b)x$ is covered by $(a - b)x$; in the second case, when $a + b = 0$, $(a + b)x$ specializes to 0. However, if $a - b = 0$ but $a + b \neq 0$, then $(a + b)x$ is not covered and hence essential. A similar argument can be made to show that $(a - b)x$ is essential as well, especially when $a + b = 0$. The Completion algorithm also returns $\{(a+b)x, (a-b)x\}$ as the minimal CGB: the specialized tuples of $(a+b)x$ are $\{([(a + b)x, 0], (\emptyset, \{a + b\})), ([0, (a + b)x], (\{a + b\}, \{1\}))\}$; similarly, for $(a - b)x$, they are $\{([(a - b)x, 0], (\emptyset, \{a - b\})), ([0, (a - b)x], (\{a - b\}, \{1\}))\}$. There is only necessary critical pair, which is for the segment $(\emptyset, \{(a + b)(a - b)\})$ generating the S-polynomial 0.

When the KSW algorithm for generating a CGS and CGB is run on this example, first RGB is generated, which is $CG = \{ax, bx\}$, which is also a minimal faithful CGB. Clearly this CGB is smaller than the one above generated by completion which suggests that the current version of the Completion algorithm is not likely to generate a canonical CGB; if its input is already a CGB, then besides removing redundant polynomials in the input, it also needs

to make polynomials smaller by simplification insofar as CGBness is preserved. Parametric rewriting does not help in generating a smaller minimal CGB $\{ax, bx\}$, which is also canonical.

Simplification operation also checks whether after simplification, the result preserves CGBness of the original ideal; if yes, this operation produces a smaller CGB; otherwise the result is discarded and the original polynomial is kept as is in the CGB. $(a+b)x$ can be classically rewritten using $(a-b)x$ to $2bx$ and CGBness is preserved since $(a+b)x$ is covered by $\{(a-b)x, bx\}$ declaring $(a+b)x$ to be redundant; bx can then rewrite $(a-b)x$ to ax again preserving CGBness. The result of simplification thus is $\{ax, bx\}$ which is smaller as well as canonical.

The completion procedure presented above does not implement simplification and decomposition operations during intermediate steps or on a minimal CGB generated by it. These issues are left for future investigations.

13 Concluding Remarks and Future Work

We have proposed a theoretical framework for parametric polynomial ideals with a particular focus on Gröbner basis computations on parametric ideals. The focus of the study is the concept of a comprehensive Gröbner basis (CGB) of a parametric ideal particularly, faithful minimal CGBs that only have polynomials from a parametric ideal necessary for it to be a CGB. The existence of the canonical CGB of a parametric ideal for a given total admissible polynomial ordering has been proved.

Several issues related to CGBs of a parametric ideal and their relationship to reduced Gröbner basis and comprehensive Gröbner systems have been investigated. Particularly it is shown the a RGB need not be a CGB or a subset of a CGB, or a CGB is not a subset of the RGB; further additional polynomials from the ideal which classically reduce to 0 by RGB may need to be included in a CGB. It was also observed that almost all algorithms for computing CGBs, including the KSW algorithm considered the most efficient, generate in their output, redundant polynomials. The dual concepts of an essential polynomial and a redundant polynomial with respect to a CGB are introduced; methods for checking these properties are discussed. These checks must be performed to generate minimal CGBs.

A test for checking whether a given basis of a parametric ideal is a CGB or not, is given. The concepts of rewriting of a parametric polynomial by a basis of parametric polynomials is defined for a subset of specializations of the parameters as characterized by a segment. S-polynomials on such specializations of a pair of parametric polynomials are presented. They serve as the build blocks for the CGBness check.

A completion algorithm to generate a minimal CGB from a given basis that is not a CGB is presented. If a given basis fails the test of CGBness, a minimal CGB can be generated using the completion algorithm; this algorithm falls in the framework of the famous Knuth-Bendix completion procedure for arbitrary first-order equational theories[23] as well as Buchberger's Gröbner basis algorithm for a polynomial ideal over a field (see also [24] for a direction relationship between Buchberger's algorithm and the Knuth-Bendix procedure).

While the Completion algorithm may have lots of similarities in using constructions proposed in [1, 2], it is the first algorithm to compute a comprehensive Gröbner basis directly

without having to go through a comprehensive Gröbner system like object. The output of the algorithm is a finite set of faithful minimal polynomials; these properties are ensured by keeping intermediate bases faithful and minimal. Because of these nice properties, the completion algorithm has been able to generate minimal faithful CGBs for some parametric ideals which cannot be computed using any other algorithm for computing a CGB.

Eliminating redundant polynomials from a CGB can only produce minimal CGBs which are subsets of an input CGB. Redundancy check can generate different minimal CGBs depending upon the order in which polynomials are checked for redundancy. The concept of simplification of an essential polynomial by other essential polynomials in a CGB is introduced using which minimal CGBs that are not necessarily subsets of an input CGB can be generated. Such CGBs cannot be generated using any algorithm in the literature.

From a minimal CGB, an algorithm to compute a CGS from it has been developed; the output CGS of this algorithm is often simpler and more compact from the original CGS used to generate a minimal CGB. A CGB generated from faithful Gröbner bases for various specializations can have redundant polynomials; on the other hand, a CGS generated from a minimal CGB need not be reduced for various specializations. To illustrate this, let $I = \langle f = uz + x,\ g = (u+1)y - x\rangle \subseteq K[u][z, y, x]$ with a lexicographic term order $>$ such that $z > y > x \gg u$. The KSW algorithm computes its CGS as

Table 3

i	branch	basis	$\sigma_i(G_i)$
1	$u \neq 0, u+1 \neq 0$	$\{f, g\}$	$\{(u+1)y - x,\ uz + x\}$
2	$u + 1 = 0$	$\{g, h\}$	$\{x, z\}$
3	$u = 0$	$\{f, h\}$	$\{x, y\}$

From the above CGS, the CGB $\mathcal{G} = \{f,\ g,\ h = f + g = uz + (u+1)y\}$ is not minimal, while $\sigma_1(G_1)$, $\sigma_2(G_2)$ and $\sigma_3(G_3)$ are all reduced. The minimal CGB from it is $\mathcal{M} = \{f, g\}$. If a CGS is generated from this minimal CGB, we get each of $G_1, G_2, G_3 = \{f, g\}$; then $\sigma_2(G_2) = \{x, z - x\}$ and $\sigma_3(G_3) = \{x, y - x\}$ are larger than the specialized Gröbner bases from the above CGS.

Consider how the construction for a canonical CGB given in Section 5 works. Various specializations of the parameter u can be partitioned into three segments presented above: For $u = 0$, the least faithful polynomials with the minimal head terms $\{y, x\}$ are g, f, respectively; they are also the least faithful polynomials for the segments $u = -1$ as well as $(u \neq 0 \wedge u \neq -1)$, resulting in a CGB $\{f, g\}$ which happens to be minimal as well. But as illustrated above, a CGB using this construction need not be minimal. This indicates specializations do not preserve canonicity or reducedness of specialized Gröbner basis generated from the canonical CGB.

The algorithms discussed in the paper have been implemented and their effectiveness is demonstrated on examples.

Future work could be done at least in two directions. Given that the current implementation of the Completion algrorithm is computationally intensive, a lot can be done to improve its performance. Rewriting and redundancy check are the most expensive operations. And, the number of times these operations are performed is governed by the number of S-polynomials generated during the Completion. We plan to explore additional criteria for avoiding S-polynomials given that there are multiple S-polynomials generated from a pair of polynomials due to their different specializations. We plan to explore Buchberger's second criterion as well as possible criteria arising from considering various specializations arising from a single parametric polynomial. Different selection strategies for considering S-polynomials are also worth investigating in which it is not necessary to consider all S-polynomials arising from a pair of polynomials due to different specializations. When reduction should be performed and interleaved with S-polynomial generation is also an important research topic worth investigation. Essentiality check can be quite expensive given that it is performed every time a new polynomial is added to a basis in Completion. Heuristics need to be developed to make the essentiality check more efficient, particularly to use information from previous checks.

We plan on integrating factoring and decomposition as possible additional operations on a minimal basis insofar as its CGBness is preserved. All such investigations would hopefully lead to a more efficient implementation of the completion algorithm.

We are also interested in adapting signature-based algorithms for computing Gröbner basis to the parametric case. We however consider such an extension to be quite challenging.

Our ultimate goal remains to develop a constructive method for generating a canonical comprehensive Gröbner basis from a basis of a parametric ideal, no matter how challenging it may be.

Acknowledgment

This paper is an expanded version of an invited talk at EACA, 2014 in Barcelona, in June 2014[19] and a paper in ISSAC 2015[20]. These papers result from a collaboration with Yiming Yang. He is not a coauthor of this paper as he chose to drop out of the project. The author would like to thank Prof. Yao Sun for many helpful discussions on this topic. The help provided by Prof. Montes through emails is appreciated.

Many of the concepts in this paper are closely related to similar concepts proposed in [1, 2].

Some of this work was done during the author's sabbatical at the Institute of Software, the Chinese Academy of Sciences in Beijing, China.

References

[1] Weispfenning V, Comprehensive Gröbner bases, *Journal of Symbolic Computation*, 1992, **14**(1): 1–29.

[2] Kapur D, An approach for solving systems of parametric polynomial equations, Eds. by Saraswat Vijay, Van Hentenryck Pascal, *Principles and Practices of Constraints Programming*, MIT Press, 1995, 217–224.

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

[4] Kapur D, Sun Y, and Wang D, An efficient method for computing comprehensive Gröbner bases, *Journal of Symbolic Computation*, 202, **52**: 124–142.

[5] Manubens M and Montes A, Improving the DISPGB algorithm using the discriminant ideal, *Journal of Symbolic Computation*, 2006, **41**(11): 1245–1263.

[6] Montes A, Using Kapur-Sun-Wang algorithm for the Gröbner cover, *Proceedings of EACA* 2012, Ed. by Sendra J R, Villarino C, Universidad de Alcalá de Henares, 2012, 135–138.

[7] Manubens M and Montes A, Minimal canonical comprehensive Gröbner systems, *Journal of Symbolic Computation*, 2009, **44**(5): 463–478.

[8] Montes A, A new algorithm for discussing Gröbner bases with parameters, *Journal of Symbolic Computation*, 2002, **33**(2): 183–208.

[9] Montes A and Wibmer M, Gröbner bases for polynomial systems with parameters, *Journal of Symbolic Computation*, 2010, **45**(12): 1391–1425.

[10] Nabeshima K, A speed-up of the algorithm for computing comprehensive Gröbner systems, *Proceedings of the* 2007 *International Symposium on Symbolic and Algebraic Computation*, 2007, 299–306, ACM.

[11] Suzuki A and Sato Y, An alternative approach to comprehensive Gröbner bases, *Journal of Symbolic Computation*, 2003, **36**(3): 649–667.

[12] Suzuki A and Sato Y, Comprehensive Gröbner bases via ACGB, *ACA*, 2004, 65–73.

[13] Suzuki A and Sato Y, A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases, *Proceedings of the* 2006 *International Symposium on Symbolic and Algebraic Computation*, 2006, 326–331.

[14] Weispfenning V, Canonical comprehensive Gröbner bases, *Journal of Symbolic Computation*, 2003, **36**(3): 669–683.

[15] Wibmer M, Gröbner bases for families of affine or projective schemes, *Journal of Symbolic Computation*, 2007, **42**(8): 803–834.

[16] Buchberger B, An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal: A translation, *A Special Issue of Journal of Symbolic Computation*, Ed. by Kapur D, 2006, **41**(4): 475–511.

[17] Cox D, Little J, and OSHEA D, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer, 2007.

[18] Eder C and Faugere J C, A survey on signature-based algorithms for computing Gröbner bases, *J. of Symbolic Computation*, 2017, **80**(3): 719–784.

[19] Kapur D and Yang Y, An algorithm for computing a minimal comprehensive Gröbner basis of a parametric polynomial system, Invited Talk, *Proc. Conference Encuentros de Algebra Comptacional y Aplicaciones* (*EACA*), Barcelona, Spain, June, 2014, 21–25.

[20] Kapur D and Yang Y, An algorithm to check whether a basis of a parametric polynomial system is a comprehensive Gröbner basis and the associated completion algorithm, *Proc. Intl. Symp. on Symbolic and Algebraic Computation* (*ISSAC*), Bristol, July, 2015.

[21] Decker W, Greuel G M, Pfister G, et al., Singular 3-1-6 — A computer algebra system for polynomial computations, http://www.singular.uni-kl.de, 2012.

[22] Sit W, An algorithm for solving parametric linear systems, *Journal of Symbolic Computation*, 1992, **13**(4): 353–394.

[23] Knuth D and Bendix P, Simple word problems in universal algebras, *Computational Problems in Abstract Algebra*, Pergamon Press, 1970, 263–297.

[24] Kandri-Rody A, Kapur D, and Winkler F, Knuth-Bendix procedure and Buchberger algorithm: A synthesis, *Proceedings of International Symposium on Symbolic and Algebraic Computation* (*ISSAC*), 1989, 55–67.

[25] Buchberger B, A criterion for detecting unnecessary reductions in the construction of Gröbner-bases, *Symbolic and Algebraic Computation*, Springer, Berlin Heidelberg, 1979, 3–21.

[26] Giovini A, Mora T, Niesi G, et al., "One sugar cube, please" or selection strategies in the Buchberger algorithm, *Proceedings of the* 1991 *International Symposium on Symbolic and Algebraic Computation*, 1991, 49–54.