Gröbner basis detection with parameters (extended abstract)*

Kosaku Nagasaka[1] and Ryo Oshimatani

[1] Kobe University, 3-11 Tsurukabuto, Nada-ku, Kobe 657-8501, Japan
nagasaka@main.h.kobe-u.ac.jp

1 Introduction

Gröbner basis plays one of the most significant roles in computer algebra, and there are many studies on computing it faster as possible, after the Buchberger algorithm[1]. In those studies, basically the term order is fixed first and then the Gröbner basis is computed with respect to the term order. On the other hand, since many applications of Gröbner basis do not depend on any certain term order, one may want to make the resulting Gröbner basis as small (short) as possible without any specified term order in advance (e.g. the term order is automatically selected and may change during the computation). Moreover, in some cases, there may exist a term order $\prec$ such that a given polynomial set F (a generator of the ideal) is already a Gröbner basis of the ideal $\langle F \rangle$ with respect to $\prec$. The problem to find such a term order is called the *Gröbner basis detection* (GBD in short), that is proposed by Gritzmann and Sturmfels[2]. Their algorithm is an application of Minkowski addition of polytopes, and is given as a special case of dynamic approach version of the Buchberger algorithm. A few years later, Sturmfels and Wiegelmann[8] proposed a related problem called *structural Gröbner basis detection* (SGBD in short). In this extended abstract, we are interested in solving variants of GBD and SGBD for parametric polynomials.

1.1 Notations and Definitions

Let K be a field, L be the algebraic closure of K, R be the polynomial ring $K[\vec{u}]$ in the parameters $\vec{u} = \{u_1, \ldots, u_m\}$, and $R[\vec{x}]$ be the polynomial ring over R in the variables $\vec{x} = \{x_1, \ldots, x_n\}$ where $\vec{u} \cap \vec{x} = \phi$. We consider a specialization $\sigma_{\vec{a}} : R \to L$ that is a homomorphism induced by $\vec{a} \in L^m$, and extend canonically to a specialization $\sigma_{\vec{a}} : R[\vec{x}] \to L[\vec{x}]$ by applying $\sigma_{\vec{a}}$ coefficient-wise.

For a given term order $\prec$ on $L[\vec{x}]$ (note that $\prec$ is also a term order on $R[\vec{x}]$), we denote the leading power product of $f \in L[\vec{x}]$ with respect to $\prec$ by $\mathrm{lpp}_{\prec}(f)$. We may abbreviate it to $\mathrm{lpp}(f)$ if it is clear which term order is considered. We note that the term order in this extended abstract is only depending on $\vec{x}$ and not $\vec{u}$. Moreover, we extend this notation to a set of polynomials F by applying it element-wise. For example, $\mathrm{lpp}(F) = \{\, \mathrm{lpp}(f) \mid f \in F \,\}$.

* This work was originally started by the second author, continued by the first author and then supported by JSPS KAKENHI Grant Number 19K11827.

Any term order on any finite subset of $L[\vec{x}]$ can be represented by a positive weight vector $\vec{w} \in \mathbb{R}_+^n$ (e.g. the proof can be found in [6]). By $\prec_{\vec{w}}$ we denote the term order represented by $\vec{w} \in \mathbb{R}_+^n$. This means that for any power products $\vec{x}^{\vec{\alpha}}, \vec{x}^{\vec{\beta}} \in L[\vec{x}]$, we have

$$\vec{x}^{\vec{\alpha}} \prec_{\vec{w}} \vec{x}^{\vec{\beta}} \Longleftrightarrow \vec{w}^T \vec{\alpha} < \vec{w}^T \vec{\beta}$$

where $\vec{w}^T$ denotes the transpose of $\vec{w}$. We note that it is easily extensible to a term order on $L[\vec{x}]$ by adding some linearly independent weight vectors (see [7]).

For a given finite subset $F \subset L[\vec{x}]$, the *Gröbner basis detection*[2] and the *structural Gröbner basis detection*[8] problems are defined as follows.

Definition 1 (Gröbner basis detection (GBD)). *This problem is to decide if there exists — and if "yes" find — a term order $\prec_{\vec{w}}$ with $\vec{w} \in \mathbb{R}_+^n$ such that F is a Gröbner basis of $\langle F \rangle$ with respect to $\prec_{\vec{w}}$.* ◁

Definition 2 (structural Gröbner basis detection (SGBD)). *This problem is to decide if there exists — and if "yes" find — a term order $\prec_{\vec{w}}$ with $\vec{w} \in \mathbb{R}_+^n$ such that $\mathrm{lpp}_{\prec_{\vec{w}}}(F)$ is a set of pairwise coprime power products.* ◁

In this extended abstract, we are interested in a Gröbner basis of polynomials with parameters (i.e. $F \subset R[\vec{x}]$), and basically follow the notations in [3,4]. For subsets $E, N \subset R = K[\vec{u}]$, we call a pair (E, N) a *parametric constraint*, and it is said to be *consistent* (*inconsistent*) if the set $V(E) \setminus V(N)$ is not empty (is empty, respectively) where $V(P)$ denotes the affine variety of $P \subset K[\vec{u}]$ (i.e. $V(P) = \{ \vec{a} \in L^m \mid \forall p(\vec{u}) \in P, p(\vec{a}) = 0 \}$). Moreover, we call a subset $A \subseteq L^m$ a *algebraically constructible subset* if it is represented by $A = V(E) \setminus V(N)$ with $(E, N) \subset K[\vec{u}] \times K[\vec{u}]$ (e.g. $L^m = V(\phi) \setminus V(\{1\})$).

1.2 Problems to be Solved

We consider extending the GBD and SGBD problems to polynomials with parameters in the same way that the Gröbner basis is extended to the comprehensive Gröbner system. Therefore we define the following system of term orders as a representation of solutions of extended problems.

Definition 3 (system of term orders). *Let S be a subset of L^m. We call a finite set $\mathcal{W} = \{(A_1, \overrightarrow{w_1}), \ldots, (A_\ell, \overrightarrow{w_\ell})\}$ a system of term orders on S if $A_1, \ldots, A_\ell$ are algebraically constructible subsets of L^m satisfying $S \subseteq A_1 \cup \cdots \cup A_\ell$ and $\overrightarrow{w_1}, \ldots, \overrightarrow{w_\ell}$ are in $\mathbb{R}_+^m$ or "not exist". Each $(A_i, \overrightarrow{w_i})$ is called a branch of $\mathcal{W}$. Particularly, if $S = L^m$, then $\mathcal{W}$ is called simply a system of term orders.* ◁

With this definition, we propose the following problems.

Problem 1 (comprehensive GBD (CGBD)). Let F be a finite subset of $R[\vec{x}]$ and S be a subset of L^m. This problem is to compute a system of term orders $\mathcal{W} = \{(A_1, \overrightarrow{w_1}), \ldots, (A_\ell, \overrightarrow{w_\ell})\}$ on S, such that $\overrightarrow{w_i}$ is a solution of the Gröbner basis detection of $\sigma_{\vec{a}}(F) \subseteq L[\vec{x}]$ for any $\vec{a} \in A_i$ and $i = 1, \ldots, \ell$. ◁

Problem 2 (comprehensive SGBD (CSGBD)). Let F be a finite subset of $R[\vec{x}]$ and S be a subset of L^m. This problem is to compute a system of term orders $\mathcal{W} = \{(A_1, \overrightarrow{w_1}), \ldots, (A_\ell, \overrightarrow{w_\ell})\}$ on S, such that $\overrightarrow{w_i}$ is a solution of the structural Gröbner basis detection of $\sigma_{\vec{a}}(F) \subseteq L[\vec{x}]$ for any $\vec{a} \in A_i$ and $i = 1, \ldots, \ell$. ◁

2 How to Solve Comprehensive GBD and SGBD

The algorithms for GBD and SGBD are basically depending on the support of the given polynomial. We denote the support of a polynomial $f \in L[\vec{x}]$ by $\mathrm{supp}(f)$, that is the set of power products of f whose coefficients are non-zero hence we have $f = \sum_{t \in \mathrm{supp}(f)} c_t t$ for some non-zero $c_t \in L$ for each t. We also extend the notation of support $\mathrm{supp}(\cdot)$ to a set of polynomials $F = \{f_1, \ldots, f_r\} \subset R[\vec{x}]$ by applying it element-wise, such that $\mathrm{supp}(F) = \{\mathrm{supp}(f_1), \ldots, \mathrm{supp}(f_r)\}$ in this order. Then the support (the coefficients are non-zero) can be defined as follows.

Definition 4 (system of supports).
Let $F = \{f_1, \ldots, f_r\}$ be a finite subset of $R[\vec{x}]$ and S be a subset of L^m. A finite set $\mathcal{T} = \{(A_1, T_1), \ldots, (A_\ell, T_\ell)\}$ where $A_1, \ldots, A_\ell$ are algebraically constructible subsets of L^m satisfying $S \subseteq A_1 \cup \cdots \cup A_\ell$ and $T_1, \ldots, T_\ell$ are subsets of $K[\vec{x}]^r$, is called a system of supports on S for F, if $T_i = \mathrm{supp}(\sigma_{\vec{a}}(F))$ for any $\vec{a} \in A_i$ and $i = 1, \ldots, \ell$. Each (A_i, T_i) is called a branch of $\mathcal{T}$. Particularly, if $S = L^m$, then $\mathcal{T}$ is called simply a system of supports for F. ◁

At first, our algorithm computes a system of supports, and then computes a solution of GBD or SGBD for each branch. We show some examples as follows.

Example 1 (comprehensive GBD).
For $F = \{ax^2 + by,\ cw^2 + z,\ (y-w)^2 + (x-z)^2,\ 2dwx - 2by\} \subset K[\vec{u}][\vec{x}]$ ($F8$ in [5], and see also [4]) where $\vec{u} = \{a, b, c, d\}$ and $\vec{x} = \{x, y, z, w\}$, we have the following system of term orders as a solution of comprehensive GBD for F.

$$\begin{array}{ll}
\{\quad (\{\}, \{bd\}), \text{“not exist”}), & (\{\{b\}, \{cd\}), (6, 11, 8, 3)), \\
(\{\{d\}, \{abc\}), (48, 56, 108, 81)), & (\{\{a, d\}, \{c\}), (8, 4, 4, 5)), \\
(\{\{b, c\}, \{d\}), (1, 2, 1, 1)), & (\{\{b, d\}, \{ac\}), (4, 8, 4, 5)), \\
(\{\{c, d\}, \{ab\}), (24, 28, 27, 54)), & (\{\{a, c, d\}, \{1\}), (2, 1, 1, 1)), \\
(\{\{b, c, d\}, \{a\}), (1, 2, 1, 1)) & \}.
\end{array}$$

Our implementation deletes the redundant constraints by computing quotient ideals (i.e. by using the fact $V(E) \setminus V(f) = V(\langle E \rangle : f^\infty) \setminus V(f)$ as noted in [4]), and merges some redundant constraints (i.e. $((E \cup \{f\}, N), \overrightarrow{w})$ and $((E, N \times \{f\}), \overrightarrow{w})$ are merged as $((E, N), \overrightarrow{w})$). ◁

Example 2 (comprehensive SGBD).
We have the following system of term orders as a solution of comprehensive SGBD for F in the example 1.

$$\begin{array}{ll}
\{\quad (\{\}, \{bd\}), \text{“not exist”}), & (\{\{b\}, \{ad\}), \text{“not exist”}), \\
(\{\{d\}, \{abc\}), (7, 8, 13, 8)), & (\{\{a, b\}, \{cd\}), (1, 8, 4, 1)), \\
(\{\{a, d\}, \{b\}), \text{“not exist”}), & (\{\{b, d\}, \{ac\}), (3, 6, 6, 4)), \\
(\{\{c, d\}, \{a\}), (1, 1, 1, 2)), & (\{\{a, b, c\}, \{d\}), (1, 2, 1, 1)),
\end{array}$$

$$(\{\{a,b,d\},\{c\}\},(3,3,3,2)),\ (\{\{a,b,c,d\},\{1\}\},(1,1,1,2))\ \}.$$

We note that each computed term order is just a representative of corresponding equivalence class and our algorithm does not guarantee the minimum representation hence they can be different from the result of the example 1. ◁

3 More Efficient Algorithms

In our improved algorithms, we use some strategy of cut off the redundant branches in system of supports, and also we use some early termination strategy in CSGBD. As the result, the resulting system of term orders for F in the example 1 has the following 9 branches while there are 10 branches if with only the cut off strategy (Example 2) and there are 16 branches if without any strategy.

$$\begin{array}{ll}
\{\quad (\{\},\{bd\}),\text{“not exist”}), & (\{\{b\},\{ad\}\},\text{“not exist”}),\\
(\{\{d\},\{abc\}\},(7,8,13,8)), & (\{\{a,b\},\{d\}\},(1,8,4,1)),\\
(\{\{a,d\},\{b\}\},\text{“not exist”}), & (\{\{b,d\},\{ac\}\},(3,6,6,4)),\\
(\{\{c,d\},\{a\}\},(1,1,1,2)), & (\{\{a,b,d\},\{c\}\},(3,3,3,2)),\\
(\{\{a,b,c,d\},\{1\}\},(1,1,1,2)) & \}.
\end{array}$$

Moreover, we also propose an alternative way to compute a system of supports, by using CGS computation over modules. This may be useful if the computer algebra system in use (e.g. Risa/Asir, Maple, Mathematica, Singular and so on) has some efficient implementation of CGS over modules.

References

1. Buchberger, B.: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. J. Symbolic Comput. **41**(3-4), 475–511 (2006), translated from the 1965 German original by Michael P. Abramson
2. Gritzmann, P., Sturmfels, B.: Minkowski addition of polytopes: computational complexity and applications to Gröbner bases. SIAM J. Discrete Math. **6**(2), 246–269 (1993)
3. Kapur, D., Sun, Y., Wang, D.: A new algorithm for computing comprehensive Gröbner systems. In: ISSAC 2010—Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation. pp. 29–36. ACM, New York (2010)
4. Kapur, D., Sun, Y., Wang, D.: An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial system. J. Symbolic Comput. **49**, 27–44 (2013)
5. Nabeshima, K.: A speed-up of the algorithm for computing comprehensive Gröbner systems. In: ISSAC 2007—Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation, pp. 299–306. ACM, New York (2007)
6. Ostrowski, A.M.: On multiplication and factorization of polynomials. I. Lexicographic orderings and extreme aggregates of terms. Aequationes Math. **13**(3), 201–228 (1975)
7. Robbiano, L.: Term orderings on the polynomial ring. In: EUROCAL '85, Vol. 2 (Linz, 1985), Lecture Notes in Comput. Sci., vol. 204, pp. 513–517. Springer, Berlin (1985)
8. Sturmfels, B., Wiegelmann, M.: Structural Gröbner basis detection. Appl. Algebra Engrg. Comm. Comput. **8**(4), 257–263 (1997)