7th International Conference on
Combinatorics, Cryptography, Computer Science and Computing
November. 16-17, 2022

# Zero-dimensional Parametric Gröbner Bases Conversion

Mahdi Dehghani Darmian[1]
Department of Mathematics, Technical and Vocational University (TVU),
Tehran, Iran

Amir Hashemi
Department of Mathematical Sciences, Isfahan University of Technology,
Isfahan, 84156-83111, Iran

Abstract

In this paper we consider the non-trivial problem of converting a zero-dimensional parametric Gröbner basis. In many applications of Gröbner bases theory, one needs to compute a lexicographical Gröbner basis of a given ideal. On the other hand, computing Gröbner bases w.r.t the lexicographic monomial ordering is typically more expensive, however it is more efficient to work with other monomial orderings like degree reverse lexicographic ordering. Faugère et al. proposed the FGLM algorithm to compute first a Gröbner basis of a zero-dimensional ideal w.r.t. degree reverse lexicographic ordering and then convert it (using linear algebra techniques) into a Gröbner basis w.r.t the lexicographic monomial ordering. In this paper, we introduce the needed parametric linear algebra tools to describe a varaint of FGLM algorithm to convert a parametric zero-dimensional Gröbner basis w.r.t. a source monomial ordering into Gröbner basis w.r.t. a target monomial ordering.

Keywords: Gröbner bases, FGLM algorithm, Parametric Gröbner bases, Parametric linear algebra.
AMS Mathematical Subject Classification [2010]: 13P10, 68W30.

## 1 Introduction

Th concept of Gröbner bases is a powerful tool in computational algebra. There are many literatures concerning history of Gröbner bases and their applications (see [1]). Solving polynomial systems may be considered as the most important applications of Gröbner bases. So, converting a Gröbner basis w.r.t. degree reverse lexicographical ordering, $\prec_{drl}$, (which is known to be fast in practice) to a Gröbner basis w.r.t. lexicographical ordering, $\prec_{lex}$, (which may lead to nice properties of the ideal) is quite applicable. In this direction, FGLM algorithm was proposed by Faugère et al. in 1993 in [3] which concerns zero-dimensional ideals and uses linear algebra techniques. In this paper, we adapt FGLM algorithm to convert a given zero-dimensional parametric Gröbner basis w.r.t. a given monomial ordering and also a given pair of null and non-null conditions sets for parameters, to a of Gröbner systems w.r.t. another monomial ordering. The concept of Gröbner system (and also the first algorithm to compute them) was introduced by Weispfenning in [7]. From 2002 to 2010 big developments were made by Weispfenning, Montes and Suzuki-Sato et al

[1] speaker

[5, 6, 8]. In 2010 Kapur et al. proposed the most efficient algorithm (PGBMain algorithm) for computing them [4]. Gröbner systems have numerous applications. In connection with these applications, we present in this paper parametric FGLM algorithm to convert a zero-dimensional parametric Gröbner basis to a Gröbner system w.r.t. a target monomial ordering. It is worth noting that the full paper on this subject was published in [2]. In the following, we give a very brief review of the basic notations and definitions relating to Gröbner bases and Gröbner systems.

Throughout this paper, we consider $\mathbb{K}$ a field and $\mathcal{R} = \mathbb{K}[\mathbf{x}]$ the polynomial ring in $\mathbf{x} = x_1, \ldots, x_n$ over $\mathbb{K}$. Let $\mathcal{I} = \langle f_1, \ldots, f_k \rangle$ be the ideal of $\mathcal{R}$ generated by the $f_i$'s. Also let $f \in R$ and $\prec$ be a monomial ordering on the set of all monomials of $\mathcal{R}$. The leading monomial of $f$, denoted by $\mathrm{LM}_{\prec}(f)$, is the greatest monomial (with respect to $\prec$) appearing in $f$ and its coefficient is the leading coefficient of $f$ and we denote it by $\mathrm{LC}_{\prec}(f)$. The leading term of $f$ is the product $\mathrm{LT}_{\prec}(f) = \mathrm{LC}_{\prec}(f)\mathrm{LM}_{\prec}(f)$. The leading term ideal of $\mathcal{I}$ is defined to be $\mathrm{LT}_{\prec}(\mathcal{I}) = \langle \mathrm{LT}_{\prec}(f) \mid f \in \mathcal{I} \rangle$. For a finite set $F = \{f_1, \ldots, f_k\} \subset \mathcal{R}$, LT(F) stands for the set $\{\mathrm{LT}(\mathrm{f}_1), \ldots, \mathrm{LT}(\mathrm{f}_k)\}$. A finite subset $\{g_1, \ldots, g_m\} \subset \mathcal{I}$ is called a Gröbner basis for $\mathcal{I}$ w.r.t. $\prec$ if $\mathrm{LT}_{\prec}(\mathcal{I}) = \langle \mathrm{LT(G)} \rangle$. We refer e.g. to [1] for more details. Now, let $\mathcal{S} = \mathbb{K}[\mathbf{a}, \mathbf{x}]$ be a polynomial ring where $\mathbf{a} = a_1, \ldots, a_m$ is a sequence of parameters and $\mathbf{x} = x_1, \ldots, x_n$ is a sequence of variables. Let $\prec_{\mathbf{x}}$ (resp. $\prec_{\mathbf{a}}$) be a monomial ordering on the variables (resp. parameters). The product of $\prec_{\mathbf{x}}$ and $\prec_{\mathbf{a}}$ is a monomial ordering on $\mathcal{S}$, denoted by $\prec_{\mathbf{x},\mathbf{a}}$ which is defined as follows:

$$\mathbf{x}^{\alpha}\mathbf{a}^{\gamma} \prec_{\mathbf{x},\mathbf{a}} \mathbf{x}^{\beta}\mathbf{a}^{\delta} \text{ if either } \mathbf{x}^{\alpha} \prec_{\mathbf{x}} \mathbf{x}^{\beta} \text{ or } (\mathbf{x}^{\alpha} = \mathbf{x}^{\beta} \text{ and } \mathbf{a}^{\gamma} \prec_{\mathbf{a}} \mathbf{a}^{\delta}), \text{ for all } \alpha, \beta \in \mathbb{N}^n \text{ and } \gamma, \delta \in \mathbb{N}^m.$$

Definition 1.1. Let $F \subset \mathcal{S}$ and $\mathcal{G} = \{(N_i, W_i, G_i)\}_{i=1}^{\ell}$ be a finite triple set where $N_i, W_i \subset \mathbb{K}[\mathbf{a}]$ and $G_i \subset \mathcal{S}$ are finite for $i = 1, \ldots, \ell$. The set $\mathcal{G}$ is called a Gröbner system for $\langle F \rangle$ w.r.t. $\prec_{\mathbf{x},\mathbf{a}}$ if for any $i$ and for any specialization $\sigma : \mathbb{K}[\mathbf{a}] \to \bar{\mathbb{K}}$ with $\bar{\mathbb{K}}$ the algebraic closure of $\mathbb{K}$, the following conditions hold

- $\sigma(G_i) \subset \bar{\mathbb{K}}[\mathbf{x}]$ is a Gröbner basis for $\sigma(\langle F \rangle) \subset \bar{\mathbb{K}}[\mathbf{x}]$ w.r.t. $\prec_{\mathbf{x}}$
- $\sigma(p) = 0$ for each $p \in N_i$ and $\sigma(q) \neq 0$ for some $q \in W_i$.

Example 1.2. Let $F = \{ax - b, by - a, cx^2 - y, cy^2 - x\} \subset \mathbb{K}[a, b, c, x, y]$ where $a, b, c$ are parameters and $x, y$ are variables. Using our implementation of PGBMain algorithm in Maple, we obtain the following CGS for $\langle F \rangle$ w.r.t. the product ordering $y \prec_{lex} x$ and $c \prec_{lex} b \prec_{lex} a$. $\langle F \rangle \mid_{a=2} = \langle x + y^2, 2y + 2 \rangle$.

$$\mathcal{G} = \begin{cases} ( \quad [\,], [bc^2 - b, ac^2 - a, -a^3 + b^3c, -b^3 + a^3c, -b^6 + a^6], & [1] \quad ) \\ ( \quad [bc^2 - b, ac^2 - a, -a^3 + b^3c, -b^3 + a^3c, -b^6 + a^6], [b], & [bx - acy, by - a] \quad ) \\ ( \quad [a, b], [c], & [cx^2 - y, cy^2 - x] \quad ) \\ ( \quad [a, b, c], [\,], & [x, y] \quad ) \end{cases}$$

For instance, if $a = 0, b = 0, c = 2$ then the third branch corresponds to this value of parameter. Therefore, $\{2x^2 - y, 2y^2 - x\}$ will be a Gröbner basis for the ideal $\langle F \rangle \mid_{a=b=0,c=2} = \langle 2x^2 - y, 2y^2 - x \rangle$.

## 2 Main results

In this section, we present the parametric FGLM algorithm which can be considered as a generalization of FGLM algorithm to parametric zero-dimensional ideals.

Definition 2.1. Let $\mathcal{I}, G \subset \mathcal{S}$ and $(N, W)$ a conditions pair. The triple $(N, W, G)$ is called a parametric zero-dimensional Gröbner basis for $\mathcal{I}$ if for any specialization $\sigma : \mathbb{K}[\mathbf{a}] \to \bar{\mathbb{K}}$ satisfying $(N, W)$, $\sigma(G)$ is a zero-dimensional Gröbner basis for $\sigma(\mathcal{I})$. Furthermore, $\mathcal{I}$ is called zero-dimensional ideal if for any specialization $\sigma$ we have $\sigma(\mathcal{I})$ is zero-dimensional.

Example 2.2. Let us consider $F = [ax^2 - bx, y^3, z^3 + cy] \subset \mathcal{S} = \mathbb{K}[a,b,c][x,y,z]$. A CGS of $F$ w.r.t. the product of $z \prec_{drl} y \prec_{drl} x$ and $c \prec_{lex} b \prec_{lex} a$ is computed using our implementation of PGBMain algorithm in Maple as follow:

$$S = \begin{cases} ([\,], & [a], & [ax^2 - bx, z^3 + cy, y^3]) \\ ([a], & [b], & [bx, z^3 + cy, y^3]) \\ ([b,a], & [\,], & [z^3 + cy, y^3]). \end{cases}$$

The variable $S$ contains three segments and scince any triple is a parametric zero-dimensional Gröbner basis so, $F$ is a zero-dimensional ideal.

A crucial tool that we use in the PFGLM algorithm is the parametric linearly dependency check. More precisely, let us consider a triple $(N, W, G)$ s.t. $G \subset \mathcal{S}$ is a linear reduced Gröbner basis w.r.t. the constraint sets $N, W \subset \mathbb{K}[\mathbf{a}]$. Let $g \in \mathcal{S}$ be a parametric linear polynomial. The question that may arise is: how one could characterize the dependency of $g$ on the triple $(N, W, G)$? In this direction, we describe the LDS algorithm to determine the dependency of a linear parametric polynomial on a given set of parametric polynomials without the use of Gröbner systems. This algorithm plays an important role in the design and efficiency of the PFGLM algorithm.

Algorithm 1 LDS (Linearly Dependency System)

Require: $G \subset \mathcal{S}$; a linear set which is a reduced Gröbner basis w.r.t. the product of the monomial orderings $\prec_{\mathbf{x}}$ and $\prec_{\mathbf{a}}$ provided that a conditions pair $(N, W)$ is satisfied and $g \in \mathcal{S}$; a parametric linear polynomial
Ensure: A linearly dependency system of $g$ on $(N, W, G)$
  $f, Q$ :=NormalForm($g$,GröbnerBasis($N, \prec_{\mathbf{a}}$), $\prec_{\mathbf{a}}$)
  $f', Q'$ :=NormalForm($f, G, \prec_{\mathbf{x}}$)
  if $f' = 0$ then
    Sys:=Sys $\bigcup\{(N, W, [true, Q', 0])\}$
  else
    $A := \{a_{i_1}, \ldots, a_{i_t}\}$ where $f' = a_{i_1} x_{i_1} + \cdots + a_{i_t} x_{i_t}$ with $a_{i_j} \neq 0$ and $x_{i_1} \succ_{\mathbf{x}} \cdots \succ_{\mathbf{x}} x_{i_t}$
    for $j$ from 1 to $t$ do
      if $a_{i_j}$ is not constant then
        Sys:=Sys $\bigcup\{(N \cup \{a_{i_1}, \ldots, a_{i_{j-1}}\}, W \cup \{a_{i_j}\}, [false, Q', f'|_{a_{i_1}=0,\ldots,a_{i_{j-1}}=0}])\}$
      else
        Sys:=Sys $\bigcup\{(N \cup \{a_{i_1}, \ldots, a_{i_{j-1}}\}, W, [false, Q', f'|_{a_{i_1}=0,\ldots,a_{i_{j-1}}=0}])\}$
        Return(Sys)
      end if
    end for
    Sys:=Sys $\bigcup\{(N \bigcup A, W, [true, Q', 0])\}$
  end if
  Return(Sys)

Theorem 2.3. LDS algorithm terminates and is correct.

Proof. The termination of this algorithm is trivial. The correctness of LDS algorithm comes from the fact that $g$ is dependent on $G$ iff either $f' = 0$ or all the coefficients of $f'$ are null. If $f' \neq 0$, we add the coefficients of $f'$ (which are polynomials in $\mathbb{K}[\mathbf{a}]$) into $N$ and verify the consistency of the new conditions pairs. □

We are willing now to present the parametric FGLM slgorithm, so called PFGLM algorithm. The PFGLM algorithm receives as input a parametric zero-dimensional Gröbner basis w.r.t. a given monomial ordering $\prec_1$, and outputs a zero-dimensional Gröbner system w.r.t. the target monomial ordering $\prec_2$. Below, we let Sys be a variable which is initialized to empty set, and finally it is the output linearly dependency system.

Algorithm 2 PFGLM (Parametric FGLM)

Require: $(N, W, G)$; a parametric zero-dimensional Gröbner basis w.r.t. $\prec_1$ and $\prec_2$; a monomial ordering
Ensure: $\{(N_i, W_i, G_i)\}_{i=1}^{\ell}$; a Gröbner system for $\langle G\rangle$ w.r.t. $\prec_2$ s.t. $(N, W) = \bigcup_{i=1}^{\ell}(N_i, W_i)$
  Sys:= {} and $A := \{(false, 1, \{\}, [\ ], [\ ], \{\}, N, W, 1, [1], 1)\}$
  while $A \neq [\ ]$ do
    Select and remove the first element, say $a$, from $A$
    if $a[1] = true$ then
      $T := a[3]$, $NF := a[4]$, $B_{new} := a[5]$
      $g := a[9].a[2] - \sum_{i=1}^{|a[5]|} a[5][i].a[10][i]$ and $G_{new} := a[6] \bigcup \{g\}$
    else
      $T := a[3] \bigcup \{x_i a[2] \mid i = 1, \ldots, n\}$ and $G_{new} := a[6]$
      $NF :=$ The new list by adding $a[11] - \sum_{i=1}^{|a[4]|} a[4][i].a[10][i]$ in order into $a[4]$
      $B_{new} :=$ The new list by adding $a[9].a[2] - \sum_{i=1}^{|a[5]|} a[5][i].a[10][i]$ in order into $a[5]$
    end if
    $T := \{t \in T \mid t \notin \langle \mathrm{LM}_{\prec_2}(\mathrm{G_{new}})\rangle\}$
    if $T = [\ ]$ then
      Sys:=Sys $\bigcup \{(a[7], a[8], G_{new})\}$
    else
      Select and remove the minimum element $t$ of $T$ w.r.t. $\prec_2$
      $f :=$ The normal form of $t$ w.r.t. $G$ according to $\prec_1$ and $dn :=$ denominator of $f$ and $nu :=$ numerator of $f$
      $S :=$LDS$(a[7], a[8], NF, nu)$
      for $s \in S$ do
        $s = (N_1, W_1, [flag, Q])$ and $A := A \bigcup \{(flag, t, T, NF, B_{new}, G_{new}, N_1, W_1, dn, Q, nu)\}$
      end for
    end if
  end while
  Return(Sys)

Theorem 2.4. PFGLM algorithm terminates and is correct.

Proof. The termination of the algorithm is guaranteed by the facts that $(N, W, G)$ is a parametric zero-dimensional Gröbner basis. We conclude with the correctness of the algorithm. We consider a branch $(N_i, W_i, G_i)$ computed by the main algorithm. The above construction shows that for each selected monomial $t \in T$ two cases may occur: If the normal form of $t$ is linearly dependent on $NF$ then the corresponding polynomial has been added into $G_i$. Otherwise, we record the corresponding normal form in $NF$ and we add the multiplications of $t$ into $T$. Therefore, the structure is quite similar to the case of the classical FGLM algorithm and this proves the correctness of the algorithm. □

Now, if we want to compute a Gröbner system of a parametric zero-dim ideal $\mathcal{I}$ w.r.t. $\prec_{lex}$ ordering on variables, we can compute a Gröbner system of $\mathcal{I}$ w.r.t. $\prec_{drl}$ ordering and the union of outputs of PFGLM for each branch is a Gröbner system of $\mathcal{I}$ w.r.t. $\prec_{lex}$ ordering. We call this procedure as the Gröbner System Conversion (GSC). Below, we present a simple algorithm which takes as input a parametric zero-dimensional ideal and returns a CGS of the ideal w.r.t. lexicographical ordering.

Algorithm 3 GSC (Gröbner System Conversion)

Require: A parametric zero-dimensional ideal $\mathcal{I}$
Ensure: A CGS of $\mathcal{I}$ w.r.t. lexicographical ordering
  Sys:={}
  $S :=$ A CGS of $\mathcal{I}$ w.r.t. degree reverse lexicographical ordering
  for $(N, W, G) \in S$ do
    Sys:= Sys $\bigcup$ PFGLM$(N, W, G, \prec_{lex})$
  end for
  Return(Sys)

Theorem 2.5. GSC algorithm terminates and is correct.

Proof. The termination and correctness of the algorithm are direct consequences of Theorem 2.4. □

We have implemented all the algorithms of this paper in Maple 15 [2] and we compare the performance of GSC algorithm with the performance of PGBMain algorithm by the following parametric zero-dimensional ideals in parametric polynomial ring $\mathbb{K}[a,b,c,d,m,n,r,t][x,y,z,u]$.

- EX.1: $[x^3+ay-bz+m, y^3+dx+n, z^2-c+tx^3]$
- EX.2: $[ax^2+tcu+(a-3)x, y^3+abxy+cz, bz^3+(1-b)z^2+n, (t-3)u^3+tu+m]$
- EX.3: $[u^3+(a-1)yu, y^3+(m-2)xy, x^2+c+dyz, z^3+bz]$
- EX.4: $[x^3+d^4yx, u^2+(a^8-1)x+n, y^3+n(m-2)xy+ax, z^3+t(1-b^7)z^2+x^2]$
- EX.5: $[x^2+a^2b(c-1)y^2+a, y^3+bx+c(a^3-8), z^3+ay^2+b(c^4-1)]$
- EX.6: $[y^2+(nm-1)x+a, z^2+cx, x^2+(ad-1)yx+b, u^2+(a^4-4)x+n]$
- EX.7: $[x^4+(ab-c)z-n, y^2+(ac-b)x+d, z^3-(bc-a)y+t]$
- EX.8: $[z^3+acy^2+b, x^3+bcy^2+a, y^3+abx+c]$
- EX.9: $[(a-1)x^2+bcy^2+ax, y^4+abx+cz, (b-2)z^3+bz^2+ay]$
- EX.10: $[z^2-c+tx^3+ry, x^3+ay-bz+m, y^3+dx+n]$

| Example | Method | Time (sec.) | Used Memory (GB) |
|---|---|---|---|
| EX.1 | GSC | 1.40 | 0.1 |
| | PGBMain | 18.91 | 1.78 |
| | First GB | 17.72 | 1.77 |
| EX.2 | GSC | 8.32 | 0.79 |
| | PGBMain | 16.90 | 1.67 |
| | First GB | 2.37 | 0.26 |
| EX.3 | GSC | 11.14 | 0.74 |
| | PGBMain | 12.01 | 1.22 |
| | First GB | 7.57 | 0.92 |
| EX.4 | GSC | 10.45 | 0.73 |
| | PGBMain | 13.04 | 1.20 |
| | First GB | 8.86 | 0.87 |
| EX.5 | GSC | 1.65 | 0.12 |
| | PGBMain | — | — |
| | First GB | 54.78 | 7.49 |
| EX.6 | GSC | 1.87 | 0.15 |
| | PGBMain | — | — |
| | First GB | 31.89 | 3.28 |
| EX.7 | GSC | 3.14 | 0.29 |
| | PGBMain | 18.85 | 2.18 |
| | First GB | 9.19 | 1.04 |
| EX.8 | GSC | 14.12 | 1.08 |
| | PGBMain | — | — |
| | First GB | 15.37 | 1.33 |
| EX.9 | GSC | 13.11 | 0.79 |
| | PGBMain | — | — |
| | First GB | 2.83 | 0.31 |
| EX.10 | GSC | 4.78 | 0.25 |
| | PGBMain | 345 | 31.70 |
| | First GB | 56.73 | 5.68 |

The results are shown in this table where the timings were conducted on a personal computer with 7 core, 8 GB RAM and 64 bits under the windows 7 operating system. The monomial ordering is always the product of monomial orderings $t \prec_{lex} r \prec_{lex} n \prec_{lex} m \prec_{lex} d \prec_{lex} c \prec_{lex} b \prec_{lex} a$ and $u \prec_{lex} z \prec_{lex} y \prec_{lex} x$. The, "First

[2]The Maple code the algorithms are available at http://amirhashemi.iut.ac.ir/softwares

GB" stands for the computation of the first reduced Gröbner basis of a parametric ideal w.r.t. the product ordering which is needed in the PGBMain algorithm and we use Basis function of Maple to compute Gröbner bases. We note that the time for GSC algorithm includes also the time for computing the Gröbner system of the input ideal w.r.t. degree reverse lexicographical ordering.

## References

[1] Cox, D., Little, J., and O'Shea, D. Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra. 3rd ed. New York, NY: Springer, 2007.

[2] Dehghani Darmian, M., and Hashemi, A. Parametric fglm algorithm. J. Symb. Comput. 82 (2017), 38–56.

[3] Faugère, J., Gianni, P., Lazard, D., and Mora, T. Efficient computation of zero-dimensional Gröbner bases by change of ordering. J. Symb. Comput. 16, 4 (1993), 329–344.

[4] Kapur, D., Sun, Y., and Wang, D. A new algorithm for computing comprehensive Gröbner systems. In Proceedings of the 35th international symposium on symbolic and algebraic computation, ISSAC 2010, Munich, Germany, July 25–28, 2010. New York, NY: ACM Press, 2010, pp. 29–36.

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

[6] Suzuki, A., and Sato, Y. A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases. In Proceedings of the international symposium on symbolic and algebraic computation, ISSAC 06, Genova, Italy, July 9–12, 2006. New York, NY: ACM Press, 2006, pp. 326–331.

[7] Weispfenning, V. Comprehensive Gröbner bases. J. Symb. Comput. 14, 1 (1992), 1–29.

[8] Weispfenning, V. Canonical comprehensive Gröbner bases. J. Symb. Comput. 36 (2003), 669–683.

e-mail: m.dehghanidarmian@gmail.com
e-mail: amir.hashemi@ipm.ir