Bulletin of the Iranian Mathematical Society Vol. 38 *No. 3* (*2012*), *pp 715-724.*

APPLYING BUCHBERGER'S CRITERIA ON MONTES'S DISPGB ALGORITHM

A. HASHEMI* AND M. DEHGHANI DARMIAN AND B. M.-ALIZADEH

Communicated by Teo Mora

Abstract. The concepts of comprehensive Gröbner bases and Gröbner systems were introduced by Weispfenning in [13]. Montes in [9] has proposed DisPGB algorithm for computing Gröbner systems. But he has not explicitly used Buchberger's criteria in his algorithm. In this paper, we show how to apply these criteria on Montes algorithm, and we propose an improved version of DisPGB.

Introduction

The theory of Gröbner bases is a key computational tool to study polynomial ideals. This theory was introduced and developed by Buchberger in 1965 (see his PhD thesis [1]). His two criteria (to detect the redundant critical pairs) and the implementation methods (see [2]) made the Gröbner bases a powerful tool to solve many important problems in polynomial ideal theory. In 1988, Gebauer and Möller have installed Buchberger's two criteria on Buchberger's algorithm in an efficient way (see [4] or [3] page 230). The concept of comprehensive Gröbner bases can be considered as an extension of Gröbner bases of polynomials over fields to polynomials with parametric coefficients. This extension plays

MSC(2010): Primary: 13P10; Secondary: 68W30, 14Q20.
Keywords: Gröbner bases, comprehensive Gröbner bases, DisPGB algorithm.
Received: 17 July 2010, Accepted: 21 April 2011.
*Corresponding author
© 2012 Iranian Mathematical Society.

an important role in the applications such as constructive algebraic geometry, robotics, electrical network, automatic theorem proving and so on (see [6, 7, 9, 11] for example). Comprehensive Gröbner bases and its equivalent; Gröbner systems were introduced by Weispfenning in [13]. He has proved that any parametric polynomial ideal has a comprehensive Gröbner basis and has described an algorithm to compute them. Montes in [9] has then proposed a more efficient algorithm (DisPGB) for computing Gröbner systems. Weispfenning in [14] has proved the existence of a canonical comprehensive Gröbner basis. In 2003, Sato and Suzuki in [12] have introduced the concept of alternative comprehensive Gröbner basis. Manubens and Montes in [6], using discriminant ideal, have improved DisPGB algorithm and in [7] have introduced an algorithm for computing minimal canonical comprehensive Gröbner system. Recently, Montes and Wibmer in [10] has presented GröbnerCover algorithm which gives a finite partition of the parameter space into locally closed subsets together with polynomial data, from which the reduced Gröbner basis for a given parameter point can immediately be determined.

Montes in his DisPGB algorithm has not explicitly used Buchberger's criteria (see also [8]). In this paper, we improve DisPGB algorithm by a non trivial use of Buchberger's two criteria. Also, we show explicitly how to use the computations already done in DisPGB (see [8]). Finally, we propose a new strategy for the selection of polynomials in this algorithm.

Now, we give the structure of the paper. Section 1 contains the basic definitions and notations. In Section 2, we describe Improved DisPGB; to apply Buchberger's criteria to Montes algorithm and for other improvements of this algorithm.

1. **Preliminaries**

In the section, we recall the basic definitions and notations needed in the paper. We first give Buchberger's criteria and then we recall the definitions of comprehensive Gröbner bases and Gröbner systems.

Let $R = K[x]$ be a polynomial ring where $x = x_1, \dots, x_n$ is a sequence of variables and K is an arbitrary field. Let $I = \langle f_1, \dots, f_k \rangle$ be the ideal of R generated by the polynomials $f_1, \dots, f_k$. Also let $f \in R$ and $\prec$ be a monomial ordering on R. The *leading monomial* of f is the greatest monomial (w.r.t. $\prec$) appeared in f, and we denote it by $\mathrm{LM}(f)$. The *leading coefficient* of f, written $\mathrm{LC}(f)$, is the coefficient of $\mathrm{LM}(f)$. The *leading term* of f is $\mathrm{LT}(f) = \mathrm{LC}(f)\mathrm{LM}(f)$. The *leading term ideal* of I

is defined to be

$$\mathrm{LT}(I) = \langle \mathrm{LT}(f) \ \mid \ f \in I \rangle.$$

A finite subset $G = \{g_1, \ldots, g_k\} \subset I$ is called a *Gröbner basis* of I w.r.t. $\prec$ if $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_k) \rangle$. Buchberger in 1965 has introduced an algorithm to compute Gröbner bases (see [3], pages 213–214). He has proposed the following two criteria to improve his algorithm (see [2]). Below, we denote by $\overline{g}^G_\prec$ a remainder of the division of a polynomial g by a set G w.r.t $\prec$.

Lemma 1.1. (*Buchberger's first criterion*) *Let $f, g \in R$ be two polynomials such that* $\gcd(\mathrm{LM}(f), \mathrm{LM}(g)) = 1$. *Then* $\overline{\mathrm{Spol}(f,g)}^{\{f,g\}}_\prec = 0$.

Proof 1.2. *See* [3]*, Lemma 5.66.*

Definition 1.3. *Let $0 \neq f \in R$, $F \subset R$ be a finite set of polynomials and $t \in R$ be a monomial. A representation $f = \sum_{i=1}^k m_i f_i$ where m_i are terms and $f_i \in F$ (not necessarily pairwise disjoint) is called a t-*representation *of f if* $\mathrm{LM}(m_i f_i) \preceq t$ *for all i. If $t = \mathrm{LM}(f)$, such a representation is called a* standard representation.

Proposition 1.4. (*Buchberger's second criterion*) *Let $F \subset R$ be a finite set of polynomials and $p_1, p_2, p \in R$ such that*

- $\mathrm{LM}(p) \mid \mathrm{lcm}(\mathrm{LM}(p_1), \mathrm{LM}(p_2))$
- $\mathrm{Spol}(p_i, p)$ *has a t_i-representation for $t_i \prec$* $\mathrm{lcm}(\mathrm{LM}(p_i), \mathrm{LM}(p))$ *where $i = 1, 2$*

then $\mathrm{Spol}(p_1, p_2)$ *has a t-representation for $t \prec$* $\mathrm{lcm}(\mathrm{LM}(p_1), \mathrm{LM}(p_2))$.

Proof 1.5. *See* [3]*, Proposition 5.70.*

Gebauer and Möller in [4] have installed Buchberger's two criteria on Buchberger's algorithm. Weispfenning and Becker in [3], page 230, have described Update algorithm which is a variant of Gebauer and Möller algorithm.

Now consider $F = \{f_1, \ldots, f_k\} \subset S = K[a, x]$ where $a = a_1, \ldots, a_m$ is a sequence of parameters. Let $\prec_x$ (resp. $\prec_a$) be a monomial ordering involving the x_i's (respectively a_i's). We also need a compatible elimination product ordering $\prec_{x,a}$. It is defined as follows: For all $\alpha, \gamma \in \mathbb{Z}^n_{\geq 0}$ and $\beta, \delta \in \mathbb{Z}^m_{\geq 0}$

$$x^\gamma a^\delta \prec_{x,a} x^\alpha a^\beta \quad \text{iff} \quad \begin{cases} x^\gamma \prec_x x^\alpha & \text{or} \\ x^\gamma = x^\alpha & \text{and} \quad a^\delta \prec_a a^\beta. \end{cases}$$

A finite set $G \subset S$ is called a *comprehensive Gröbner basis* for $\langle F\rangle$ w.r.t. $\prec_{x,a}$ if for all homomorphism $\sigma : K[a] \to K'$, $\sigma(G)$ is a Gröbner basis for $\langle\sigma(F)\rangle$ w.r.t. $\prec_x$ where $K' \supseteq K$ is a field extension of K. The above homomorphism σ is called a *specialization* of S. Now, we recall the definition of a Gröbner system for a parametric ideal.

Definition 1.6. *A triple set* $\{(G_i, N_i, W_i)\}_{i=1}^{\ell}$ *is called a* Gröbner system *for* $\langle F\rangle$ *w.r.t* $\prec_{x,a}$ *if*

- $\sigma(G_i)$ *is a Gröbner basis for* $\sigma(\langle F\rangle)$ *w.r.t.* $\prec_x$
- $\sigma(p) = 0$ *for each* $p \in N_i \subset K[a]$
- $\sigma(q) \neq 0$ *for each* $q \in W_i \subset K[a]$

for any homomorphism $\sigma : K[a] \to K'$, *where* K' *is a field extension of* K.

Remark that DisPGB computes a Gröbner system for a parametric ideal, and from such a system one can compute a comprehensive Gröbner basis for the ideal (for more details we refer to [13, 9]). The set N_i (respectively W_i) is called the (respectively non) null conditions set. The pair (N_i, W_i) is called the *actual specification* of a homomorphism σ (and we write $\sigma \in \sum(N_i, W_i)$ for simplification) if the second and third items of the above definition are satisfied.

2. **Improved** DisPGB **algorithm**

Montes in [9] has proposed an efficient algorithm (DisPGB) for computing Gröbner systems. But, he has not explicitly used Buchberger's criteria in his algorithm, and he has only indicated the use of these criteria (see also [8]). In this section, we prove that we can use Buchberger's criteria for computing Gröbner systems. Also, we show explicitly how to use the computations already done in DisPGB to speed up the new algorithm (see [8]).

To describe DisPGB, Montes has used five subalgorithms Canspec, Newcond, CondPGB, Branch and Newvertex. In the following, we explain how to improve (some of) these algorithms to apply Buchberger's criteria (see CondPGB) and to use the computations already done in DisPGB. The Maple code of our algorithms are available at `http://amirhashemi.iut.ac.ir/software.html`.

Note that the algorithms that we do not improve here are the same as in [9]. Below we use the notations of the previous section. We use Improved Newvertex function which is similar to Newvertex. The only difference between them is that the former gets a set of critical pairs and at the end, transfers it to Improved Branch without any change.

It is worth noting that the correctness and termination of our new algorithms are followed by Theorem 2.1, [3], Theorem 5.73 and [9], Theorem 16.

To modify DisPGB algorithm, we propose first the OrderedSet algorithm. In DisPGB, the polynomials are chosen by the order of the input. Then, each polynomial can refine the data at the corresponding vertex by Newcond algorithm, and therefore the bad choice of polynomials may lead to different outputs and timing. Thus, we propose a selection strategy in the following and we then use it in DisPGB algorithm.

Algorithm 1 OrderedSet

Require: B; set of polynomials in S
Ensure: B'; ordered version of B
B':= The ordered set of B w.r.t. $\prec_a$, increasingly and according to the leading coefficient of the elements of B w.r.t. $\prec_x$
Return(B')

Algorithm 2 Improved DISPGB

Require: $F \subset S$
Ensure: A Gröbner system for $\langle F \rangle$
List:={ } (a global variable)
flag:=false (a global variable)
B:=`InterReduce`($F, \prec_{x,a}$)
G :=OrderedSet(B)
Improved Branch($[\,], G, [\,], [\,], \{\,\}$)
Return(List);

The `InterReduce` function is a Maple function which inter-reduces a list of polynomials w.r.t. the given monomial ordering. For example, let $F = \{x^2 + xy - 2, x^2 - xy\}$. Then `InterReduce`$(F, \prec)$ returns $\{xy - 1, x^2 - 1\}$ where $\prec$ is the lexicographical ordering with $y \prec x$.

Algorithm 3 Improved Branch

Require: v; label of the vertex, B; specializing basis at the vertex v, N; set of null conditions, W; set of non-null conditions and J; set of critical pairs

Ensure: It stores the refined (B', N', W', J') at the vertex v, and create two new vertices when necessary or make the vertex as terminal

```
if flag then
    B := [f̄^N_{≺a} | ∀f ∈ B]
    f := B[−1] (the last element of B)
    (cd, f', N', W') =Newcond(f, N, W)
    if f' = 0 then
        remove f' from B and the critical pairs containing f' from J
    else
        B[−1] := f'
    end if
    if cd ≠ ∅ then
        pivot:= |B|
    end if
else
    for i from 1 to |B| while cd = ∅ do
        f := B[i]
        (cd, f', N', W') :=Newcond(f, N, W)
        if f' = 0 then
            remove f' from B and the critical pairs containing f' from J
        else
            B[i] := f'
        end if
        if cd ≠ ∅ then
            pivot:= i
        end if
    end for
end if
T[v] := (−, B, N', W')(cond is already stored in T(v). Refinement of data)
if cd = ∅ then
    (test, B', N', W', J') :=CondPGB(B, N', W', J)
    if test then
        T[v] := (−, B', N', W', terminal vertex)
        List:=List ∪ {T[v]}
    else
        Improved Branch(v, B', N', W', J')(further refinement is needed)
    end if
else
    Improved Newvertex(1, v, cd, B', N', W', J', pivot)
    Improved Newvertex(0, v, cd, B', N', W', J', pivot)
end if
```

Algorithm 4 Improved CondPGB

Require: B; specializing basis, N; the set of null conditions, W; the set of non-null conditions (where $\sigma \in \sum(N, W)$) and J; the set of critical pairs

Ensure: test; if test = true then $\sigma(B')$ is yet the Gröbner basis, B'; the new completed specializing basis, (N', W'); the refined specification of (N, W)

test := true
flag := true (a global variable)
$N' := N$
$W' := W$
if $J = [\ ]$ **then**
  $B' := [\ ]$
  $J' := [\ ]$
  for i **from** 1 **to** $|B|$ **do**
    $(B', J') :=$Update$(B[i], B', J')$
  end for
else
  $(B', J') :=$Update$(B[-1], [B[1], \ldots, B[|B|-1]], J)$
end if
sort J' by the normal strategy
while $J' \neq \emptyset$ **and** test **do**
  select and remove (i, j) from J'
  $S := \overline{\mathrm{PSpol(B'[i], B'[j], \prec_x)}}^{B'}_{\prec_x}$;
  $S := \overline{S}^{N'}_{\prec_{x,a}}$;
  if $S \neq 0$ **then**
    $(cd, S, N', W') :=$Newcond(S, N', W');
    if $cd = \emptyset$ **then**
      if $S \neq 0$ **then**
        $(B', J') :=$Update(S, B', J')
      end if
    else
      test:=false
      B' :=adding S at the end of B'
    end if
  end if
end while
if test **then**
  $B' :=$`InterReduce`$(B', \prec_{x,a})$
end if
Return((test,B', N', W', J'))

For more details on the normal strategy and UPDATE algorithm, we refer to [3], page 225 and 230 respectively. In IMPROVED CONDPGB, in order to avoid denominators and unnecessary factors in S-polynomial for two polynomials $f, g \in S$, we use

$$\mathrm{PSpol}(f,g) = \frac{\Gamma x^\gamma}{\mathrm{LT}(f)} f - \frac{\Gamma x^\gamma}{\mathrm{LT}(g)} g$$

where $\Gamma = \mathrm{lcm}(\mathrm{LC}(f), \mathrm{LC}(g))$ and $x^\gamma = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$.

Theorem 2.1. IMPROVED CONDPGB *algorithm determines a quintuple* $(test, B', N', W', J')$ *where if test=true,* $\sigma(B')$ *is the reduced Gröbner basis of* $\langle \sigma(F) \rangle$ *for* $\sigma \in \sum(N', W')$ *and if test=false,* B' *is an extended set of* B *and contains at least one polynomial such that the actual specification* (N, W) *cannot decide if its leading coefficient specializes to zero or not. In this case, it returns also a non-empty set* J' *of the critical pairs remaining to study to complete the Gröbner basis process.*

Proof. The proof of termination of IMPROVED CONDPGB is similar to that of CONDPGB (see [9], pages 197–198). Its correctness is deduced also from that of CONDPGB, but, we have to prove the correctness of using UPDATE algorithm. Indeed, we must prove that we do not delete any undecidable parameters. Let $p, p_1, p_2 \in B$ be three polynomials s.t. $\mathrm{LM}_{\prec_x}(p) \mid \mathrm{lcm}\big(\mathrm{LM}_{\prec_x}(p_1), \mathrm{LM}_{\prec_x}(p_2)\big)$ and the pairs (p, p_1) and (p, p_2) have been (will be) treated during IMPROVED DISPGB algorithm. According to IMPROVED BRANCH, IMPROVED CONDPGB is applied when all the leading coefficients of the elements of B are decided. From [3], page 224, we can write

$$b\mathrm{Spol}(p_1, p_2) = cs_1 \mathrm{Spol}(p_1, p) + as_2 \mathrm{Spol}(p, p_2)$$

where $a = \mathrm{LC}_{\prec_x}(p_1), b = \mathrm{LC}_{\prec_x}(p), c = \mathrm{LC}_{\prec_x}(p_2)$, $s_1 = \frac{\mathrm{lcm}(\mathrm{LM}(p_1), \mathrm{LM}(p_2))}{\mathrm{lcm}(\mathrm{LM}(p_1), \mathrm{LM}(p))}$ and $s_2 = \frac{\mathrm{lcm}(\mathrm{LM}(p_1), \mathrm{LM}(p_2))}{\mathrm{lcm}(\mathrm{LM}(p), \mathrm{LM}(p_2))}$. From our assumption $\mathrm{Spol}(p_1, p)$ and $\mathrm{Spol}(p, p_2)$ have non-zero leading coefficients w.r.t. (N, W), and have also standard representations. Therefore, the pair (p_1, p_2) has a standard representation, and we can delete it by UPDATE algorithm (see [3] Proposition 1.3). We can prove in the same way that if a pair (p_1, p_2) satisfies Buchberger's first criterion, we can delete it. □

Acknowledgments

The authors would like to thank the anonymous referee for helpful comments.

References

[1] B. Buchberger, Ein Algorithms zum Auffinden der Basiselemente des Restklassenrings nach einem nuildimensionalen Polynomideal. PhD thesis, Universität Innsbruck, 1965.

[2] B. Buchberger, A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Bases, In symbolic and algebraic computation (EUROSAM'79, Internat. Sympos., Marseille, 1979), 3–21, Lecture Notes in Compute. Sci. **72**, Springer, Berlin-New York, 1979.

[3] T. Becker and V. Weispfenning, Gröbner Bases, A Computational Approach to Commutative Algebra, Springer-Verlag, New York, 1993.

[4] R. Gebauer and H. Möller, On an Installation of Buchberger's algorithm, *J. Symbolic Comput.* **6** (1988), no. 2-3, 275–286.

[5] K. Nabeshima, *Comprehensive Gröbner Bases in Various Domains*, PhD Thesis, Johannes Kepler Universität, Linz, 2007.

[6] M. Manubens and A. Montes, Improving the DisPGB algorithm using the discriminant ideal, *J. Symbolic Comput.* **41** (2006), no. 11, 1245–1263.

[7] M. Manubens and A. Montes, Minimal canonical comprehensive Gröbner systems, *J. Symbolic Comput.* **44** (2009), no. 5, 463–478.

[8] M. Manubens and A. Montes, Improving DisPGB Algorithm for Parametric Gröbner Bases, Actas de EACA, 2004.

[9] A. Montes, A new algorithm for discussing Gröbner bases with parameters, *J. Symbolic Comput.* **33** (2002), no. 2, 183–208.

[10] A. Montes and M. Wibmer, Gröbner bases for polynomial systems with parameters, *J. Symbolic Comput.* **45** (2010), no. 12, 1391–1425.

[11] A. Montes, Solving the load flow problem using Gröbner bases, *SIGSAM Bull.* **29** (1995), 1–13.

[12] Y. Sato and A. Suzuki, An alternative approach to comprehensive Gröbner bases, *J. Symbolic Comput.* **36** (2003), no. 3-4, 649–667.

[13] V. Weispfenning, Comprehensive Gröbner bases, *J. Symbolic Comput.* **14** (1992), no. 1, 1–29.

[14] V. Weispfenning, Cannonical comprehensive Gröbner bases, *J. Symbolic Comput.* **36** (2003), no. 3-4, 669–683.

Amir Hashemi

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

Email: `Amir.Hashemi@cc.iut.ac.ir`

Mahdi Dehghani Darmian
Department of Mathematical Sciences, Isfahan University of Technology, 84156-83111, Isfahan, Iran
Email: mahdi_math_63@yahoo.com

Benyamin M.-Alizadeh
Department of Mathematical Sciences, Isfahan University of Technology, 84156-83111, Isfahan, Iran
Email: benyamin.m.alizadeh@googlemail.com