An Algorithm for Computing Relative Groebner Bases

Huang Guanli
School of Mathematics and System Science, LMIB
Beihang University; Beijing Polytechnic
Beijing, China
e-mail: huangguanli@sina.com

Zhou Meng
School of Mathematics and System Science, LMIB
Beihang University
Beijing(100191), China
e-mail: zhoumeng1613@hotmail.com

Abstract—In this paper we improve the computer algorithm of Zhou and Winkler for computing relative Groebner bases which used in Computer aided design and Robotics, etc. We introduce the concept of difference differential degree compatibility on generalized term orders. Then we prove that in the process of the algorithm the polynomials with higher and higher degree wouldn't be produced, if the term orders are difference differential degree compatibility. We present a condition on the generalized orders and prove that under the condition the algorithm for computing relative Groebner bases will terminate. And then the relative Groebner bases exist under the condition. Due to the algorithm is used as the main tool for algorithmic computation of many engineering and technique problems, we conclude that our result improve the algorithm and guarantee the algorithm effective works in solving verious problems of science and technology.

Keywords- Computer aided design; relative Groebner basis; difference differential module; dimension polynomials; termination of algorithm.

I. INTRODUCTION

Commutative Groebner basis theory and its computer algorithm software are well known and have found numerous applications both inside mathematics as well as in science and technology. They are widely used in solving equations, cryptosystems and cryptoanalysis, Geometric modeling, proving theorems in geometries, computer aided design, robotics, and other engineering technique fields. For non-commutative case, the theory of Groebner bases in free modules over various rings of differential operators or difference-differential operators has been developed. See [1-8]. Relative Groebner bases were introduced by Zhou and Winkler[9] in order to compute bivariate dimension polynomials in difference-differential modules. The algorithm for computing relative Groebner bases and bivariate dimension polynomials also were presented in [9]. Christian Donch [10] made Maple software of the algorithm. By now it is used as the main tool for the algorithmic computation of dimension polynomials in difference differential modules.

Recently Christian Donch[10] presented an example where the algorithm provided by Zhou and Winkler[9]does not terminate. From the counterexample Donch pointed out that it is questionable whether a relative Grobner basis always exists.

In this paper we improve the results of Zhou and Winkler[8] about relative Groebner bases. We introduce the concept of difference-differential degree compatibility on generalized term orders. Then we prove that in the process of the algorithm the polynomials with higher and higher degree wouldn't be produced, if the two term orders are difference-differential degree compatibility. So we present a condition on the generalized orders and prove that under the condition the algorithm for computing relative Groebner bases will terminate. Also the relative Groebner bases exist under the condition. Finally we prove the algorithm for computation of the bivariate dimension polynomials in difference-differential modules.

II. DEGREE COMPATIBILITY

In this paper Z, N, Z- and Q will denote the sets of all integers, all nonnegative integers, all non-positive integers, and all rational numbers, respectively. By a ring we always mean an associative ring with a unit. By the module over a ring A we mean a unitary left A-module. Let R be a field with character 0, $\Delta = \{\delta_1, \cdots, \delta_m\}$ a set of derivations and $\Sigma = \{\sigma_1, \cdots, \sigma_n\}$ a set of automorphisms of the ring R, Λ will denote the commutative semigroup of terms, i.e. elements of the form

$$\lambda = \delta_1^{k_1} \cdots \delta_m^{k_m} \sigma_1^{l_1} \cdots \sigma_n^{l_n} \quad \text{.....(2.1)}$$

where $(k_1, \cdots, k_m) \in N^m$ and $(l_1, \cdots, l_n) \in Z^n$.

Let D = $\{\sum_{\lambda \in \Lambda} a_\lambda \lambda \mid a_\lambda \in R\}$ .....(2.2)

There are only finitely many coefficients a_λ in (2.2) are different from zero. D is called the ring of difference differential operators over R.

Let F be a finitely generated free D-module (we call it a finitely generated free difference-differential module) with a set of free generators E={ $e_1, \cdots, e_q$ }. Zhou and Winkler[8] introduced the notion of relative Groebner bases and the algorithm for computation of a relative Groebner bases in difference-differential module F.

THEOREM 2.1. ([9]) Let F be a free D-module, "$\prec$" and "$\prec'$" be two generalized term orders on F, G be a finite subset of F \ {0} and W be the submodule in F generated by G. Then G is a $\prec$ -Groebner basis of W relative to $\prec'$ if and only if G is a Grobner basis with

respect to $\prec'$ of W and for all Λ_j, for all $g_i, g_k \in G$, for all $v \in V(j, g_i, g_k)$, the S-polynomials $S(j, g_i, g_k, v)$ with respect to $\prec$ can be $\prec$-reduced to 0 modulo G relative to $\prec'$.

Christian Donch[11] gave a counterexample pointing out that the algorithm does not terminate in some cases. He pointed out that in the process of the algorithm some polynomials with higher and higher degree will be produced, and then the algorithm will not terminate. This motivates us to give the concept of degree compatibility.

DEFINITION 2.1. Let F be a free D-module, "$\prec$" and "$\prec'$" be two generalized term orders on F, for $t = \delta_1^{k_1} \cdots \delta_m^{k_m} \sigma_1^{l_1} \cdots \sigma_n^{l_n} e_j$ denote $\deg_\delta t = \sum_{j=1}^{m} k_j$, $\deg_\sigma t = \sum_{j=1}^{n} |l_j|$, we call term orders "$\prec$" and "$\prec'$" are of difference-differential degree compatibility, if

(i) $t_1 \prec t_2$ when $\deg_\delta t_1 < \deg_\delta t_2$, or $\deg_\delta t_1 = \deg_\delta t_2$ and $\deg_\sigma t_1 < \deg_\sigma t_2$, for any t_1, t_2;

(ii) $t_1 \prec' t_2$ when $\deg_\sigma t_1 < \deg_\sigma t_2$, or $\deg_\sigma t_1 = \deg_\sigma t_2$ and $\deg_\delta t_1 < \deg_\delta t_2$, for any t_1, t_2;

(iii) $t_1 \prec t_2 \Leftrightarrow t_1 \prec' t_2$ when $\deg_\delta t_1 = \deg_\delta t_2$ and $\deg_\sigma t_1 = \deg_\sigma t_2$, for any t_1, t_2.

Form the algorithm described in Theorem 2.1, let G be a $\prec'$-Groebner basis of W, if there exist $f, g \in G$ and $v \in V(j, f, g)$ such that $S(j, f, g, v)$ is $\prec$-reduced to $r_1 \neq 0$ by G relative to $\prec'$, we put $G_1 = G \cup \{r_1\}$, and so on will get a sequence $G_i, i = 1,2,\cdots$. Then the algorithm in Theorem 2.1 for computing a $\prec$-Groebner basis relative to $\prec'$ of W will terminate if the sequence $G_i, i = 1,2,\cdots$, is a finite sequence, i.e., there exist k ∈ N such that $G_{k+1} = G_k$ for all i ∈ N.

THEOREM 2.2. Let F be a free D-module, "$\prec$" and "$\prec'$" be two generalized term order on F, $G_i = \{g_1, \cdots, g_p, r_1, \cdots, r_i\} \subseteq F \setminus \{0\}$, $i = 1,2,\cdots$, such that r_{i+1} is $\prec$-reduced modulo G_i relative to $\prec'$. Denote $lt_{\prec}(h)$ as u_h and $lt_{\prec'}(h)$ as v_h for $h \in F$. If $u_{r_{i+1}} \neq u_{th}$ for any t ∈ Λ, h ∈ G_i, then sequence G_i is a finite sequence.

PROOF. Since r_{i+1} is $\prec$-reduced modulo G_i relative to $\prec'$ and $u_{r_{i+1}} \neq u_{th}$ for any t ∈ Λ, h ∈ G_i, it follows that r_{i+1} is $\prec$-reduced modulo G_i in usual meaning. Then the sequence G_i is just the produced sequence from the algorithm for computing $\prec$-Groebner bases of W= $\langle g_1, \cdots, g_p \rangle$ (see [7], Theorem 3.3). Therefore the sequence G_i is a finite sequence.

THEOREM 2.3. Let F be the free D-module and let U be an infinite sequence of terms from the set ΛE. Then there exists an index j (1 ≤ j ≤ q) and an infinite subsequence $u_1 e_j, u_2 e_j, \cdots, u_k e_j \cdots$ of the sequence U, such that any two elements of the sequence are in the same orthant of Λ ,and for all $i = 1,2,\cdots$, $u_{i+1} = \lambda_i u_i$ for some $\lambda_i \in \Lambda$ which is in the same orthant of Λ as u_i.

PROOF. The statement is just Lemma 4.1 in [6]. The proof can be found in ([12],Chap.0,section 17).

THEOREM 2.4. Let F be a free D-module, $\prec'$ be a generalized term order on F. If v= $lt_{\prec'}(h)$ and $lt_{\prec'}(\lambda h)$ is in the same orthant of Λ as v, where h ∈ F and $\lambda \in \Lambda$, then $lt_{\prec'}(\lambda h)$)= λv.

PROOF. By [9] Lemma 3.3, for each j there exists some $\lambda \in \Lambda$ and a term u_j of h such that $lt(\lambda h) = \lambda u_j \in \Lambda_j E$, Furthermore, the term u_j of h is unique: if $lt(\lambda_1 h) = \lambda_1 u_{j_1} \in \Lambda_j E$ and $lt(\lambda_2 h) = \lambda_2 u_{j_2} \in \Lambda_j E$ then $u_{j_1} = u_{j_2}$. The term u_j is called j-th leading term of h and denoted by $lt_j(h)$. The coefficient of u_j is denoted by $lc_j(h)$.

Now suppose v= $lt_{\prec'}(h) \in \Lambda_j E$, then for $\lambda_1 \in \Lambda_j$ we have $lt_{\prec'}(\lambda_1 h) = \lambda_1 v \in \Lambda_j E$ (because in the same orthant, $\prec'$ is a usual term order). So for any $\lambda \in \Lambda$, if $lt_{\prec'}(\lambda h) = \lambda u_j \in \Lambda_j E$ for a term u_j of h, then u_j=v.

THEOREM 2.5. $\deg_\sigma \lambda v \leq \deg_\sigma \lambda + \deg_\sigma v$ for $\lambda \in \Lambda$, v ∈ ΛE. If λ and v are in the same orthant, then $\deg_\sigma \lambda v = \deg_\sigma \lambda + \deg_\sigma v$.

PROOF. Since $\deg_\sigma v = \sum_{j=1}^{n} |l_j|$ for $v = \delta_1^{k_1} \cdots \delta_m^{k_m} \sigma_1^{l_1} \cdots \sigma_n^{l_n} e_j$, it is clear that $\sum_{j=1}^{n} |l_j + l'_j| \leq \sum_{j=1}^{n} |l_j| + \sum_{j=1}^{n} |l'_j|$ for $\lambda = \delta_1^{k_1'} \cdots \delta_m^{k_m'} \sigma_1^{l_1'} \cdots \sigma_n^{l_n'}$. If λ and v are in the same orthant then $\sum_{j=1}^{n} |l_j + l'_j| = \sum_{j=1}^{n} |l_j| + \sum_{j=1}^{n} |l'_j|$.

III. TERMINATION OF THE ALGORITHM FOR COMPUTING RELATIVE GROEBNER BASES

THEOREM 3.1. Let F be a free D-module, "$\prec$" and "$\prec'$" be two generalized term order on F. If the term orders "$\prec$" and "$\prec'$" are of difference-differential degree compatibility, then the algorithm for computing a

$\prec$ -Groebner basis relative to $\prec'$ of W will terminate. And then there exist the relative Groebner bases.

PROOF. Let G={ $g_1,\cdots,g_p$ } be a finite subset of F\ {0} and W be the submodule in F generated by G. We may suppose that G is a $\prec'$ -Groebner basis of W, and by the algorithm for computing a $\prec$ -Groebner basis relative to $\prec'$ of W we get a series $G_i=\{g_1,\cdots,g_p,r_1,\cdots,r_i\}$, $i=1,2,\cdots$, such that r_{i+1} is $\prec$ -reduced modulo G_i relative to $\prec'$.

Denote $lt_{\prec}(h)$ as u_h and $lt_{\prec'}(h)$ as v_h for $h\in F$. Then it follows from [9] Theorem 2.1 that

(a) $u_{r_{i+1}}\neq u_{th}$ for any $t\in\Lambda$, $h\in G_i$; or

(b) $u_{r_{i+1}}=u_{th}$, $v_{r_{i+1}}\neq v_{th}$ and $v_{r_{i+1}}\prec' v_{th}$ for some $t\in\Lambda$, $h\in G_i$.

If the algorithm doesn't terminate, then the sequence $G_i=\{g_1,\cdots,g_p,r_1,\cdots,r_i\}$, $i=1,2,\cdots$, will be an infinite sequence. Because there are finitely many r_i satisfy (a) (see THEOREM 2.2), we may suppose that there are infinitely many { r_i, $i=1,2,\cdots$ } and $k\in N$ such that when i>k the following condition holds:

$u_{r_i}=u_{t_ir_j}$, $v_{r_i}\neq v_{t_ir_j}$ and $v_{r_i}\prec' v_{t_ir_j}$ for some $t_i\in\Lambda$, j<i.

Note that if $u_{r_i}=u_{r_j}$, then $v_{r_i}=v_{r_j}$. So there exists an infinite subsequence U = { $u_k \mid k=1,2,\cdots$ } of { u_{r_i} } and it does not contain two equal elements. Indeed, if this is not true, then there is an infinite subsequence U'= { $u'_l \mid l=1,2,\cdots$ } of { u_{r_i} } such that all elements of U' are equal. It follows that V'={ $v'_l \mid l=1,2,\cdots$ } is an infinite strictly descending sequence with respect to $\prec'$, i.e. $v'_1\prec' v'_2\prec'\cdots$, Since $\prec'$ is a generalized term order on F, this is impossible.

Now the set U is infinite and it does not contain two equal elements. By THEOREM 2.3, there is an infinite sequence { $u_{h_1},u_{h_2}\cdots$ } of elements of U which does not contain two equal elements, such that any two elements of the sequence are in the same orthant of Λ, and for all $i=1,2,\cdots$, $u_{h_{i+1}}=\lambda_iu_{h_i}$ for some $\lambda_i\in\Lambda$ which is in the same orthant of Λ as u_{h_i} (and $u_{h_{i+1}}$).

From that $v_{h_{i+1}}\neq v_{\lambda_ih_i}$, $v_{h_{i+1}}\prec' v_{\lambda_ih_i}$, and the term orders " $\prec$ " and " $\prec'$ " are difference-differential degree compatibility, we have $\deg_\sigma v_{h_{i+1}}<\deg_\sigma v_{\lambda_ih_i}$, or $\deg_\delta v_{h_{i+1}}<\deg_\delta v_{\lambda_ih_i}$, or $\deg_\sigma v_{h_{i+1}}=\deg_\sigma v_{\lambda_ih_i}$ and $\deg_\delta v_{h_{i+1}}=\deg_\delta v_{\lambda_ih_i}$ for some $\lambda_i\in\Lambda$ which is in the same orthant of Λ as u_{h_i} (and $u_{h_{i+1}}$).

Now we may suppose that all v_{h_i}, $i=1,2,\cdots$, are in a same orthant of Λ, this is because there are only finitely many orthant in Λ, so there exist an infinite subsequence of v_{h_i}, $i=1,2,\cdots$ such that all elements are in a same orthant of Λ. Then by THEOREM 2.4, $lt_{\prec'}(\lambda_ih_i)=\lambda_ilt_{\prec'}(h_i)$, i.e. $v_{\lambda_ih_i}=\lambda_iv_{h_i}$. It follows that

$$\deg_\sigma v_{h_{i+1}}<\deg_\sigma \lambda_iv_{h_i} \qquad (3.1)$$

or $$\deg_\delta v_{h_{i+1}}<\deg_\delta \lambda_iv_{h_i} \qquad (3.2)$$

or $$\deg_\sigma v_{h_{i+1}}=\deg_\sigma \lambda_iv_{h_i},\ \deg_\delta v_{h_{i+1}}=\deg_\delta \lambda_iv_{h_i} \qquad (3.3)$$

for some $\lambda_i\in\Lambda$ which is in the same orthant of Λ as u_{h_i} (and $u_{h_{i+1}}$). Still, we may suppose that all v_{h_i}, $i=1,2,\cdots$ satisfy (3.1)(or all v_{h_i}, $i=1,2,\cdots$ satisfy (3.2), or all v_{h_i}, $i=1,2,\cdots$ satisfy (3.3)).

If all v_{h_i}, $i=1,2,\cdots$ satisfy (3.1), let $\deg_\sigma u_{h_i}=k_i$ and $\deg_\sigma v_{h_i}=l_i$, then $l_{i+1}<\deg_\sigma \lambda_i+l_i$ (THEOREM 2.5) and then $l_{i+1}-l_i<\deg_\sigma \lambda_i$. Note that $u_{h_{i+1}}=\lambda_iu_{h_i}$ implies that $\deg_\sigma u_{h_{i+1}}=\deg_\sigma \lambda_i+\deg_\sigma u_{h_i}$ (THEOREM 2.5) and then $k_{i+1}=\deg_\sigma \lambda_i+k_i$, therefore $k_{i+1}-k_i=\deg_\sigma \lambda_i$.

So we get $l_{i+1}-l_i<k_{i+1}-k_i$ for all $i=1,2,\cdots$. This means that $l_{i+1}-k_{i+1}<l_i-k_i$ for all $i=1,2,\cdots$. Since $l_i=\deg_\sigma v_{h_i}$, $k_i=\deg_\sigma u_{h_i}$ and $u_{h_i}\prec' v_{h_i}$ so $l_i-k_i\geq 0$ by the definition of difference-differential degree compatibility in " $\prec$ " and " $\prec'$ ". Therefore we get a infinite nonnegative integer series $l_i-k_i>l_{i+1}-k_{i+1}>l_{i+2}-k_{i+2}>\ldots\ldots$, a contradiction.

If all v_{h_i}, $i=1,2,\cdots$ satisfy (3.2), then by the symmetry of " $\prec$ " and " $\prec'$ " for relative Groebner bases (see[9]) and the symmetry of difference-differential degree compatibility (DEFINITION 2.1), it is obvious that a contradiction will be reduced as in the case (3.1). If all v_{h_i}, $i=1,2,\cdots$ satisfy (3.3), then by the definition of difference-differential degree compatibility, the $\prec$ leading term and the $\prec'$ leading term of h_i will be the same one. This contradict to the definition of sequence { h_i, $i=1,2,\cdots$ }. Then the proof of the theorem is completed.

IV. CONCLUSIONS

From THEOREM 3.1 we can conclude that if the term orders " $\prec$ " and " $\prec'$ " are difference-differential degree compatibility, then the algorithm for computing a relative Groebner basis can be implemented in finite steps by computer.

THEOREM 4.1. Let F be a free D-module, " $\prec$ " and " $\prec'$ " be two generalized term order on F, which are of

difference-differential degree compatibility, G be a finite subset of F\ {0} and W be the submodule in F generated by G. For each Λ_j and f, g $\in$ F\{0} let V(j, f, g) , S(j, f, g, v) and S'(j, f, g, v) be as in [9] w.r.t. $\prec$ and $\prec'$, respectively. Then the following algorithm for computing a $\prec$ -Groebner basis of W relative to $\prec'$ will be completed in finite steps:

Input: G={ $g_1,\cdots,g_\mu$ }, a set of generators of W

$\prec$ and $\prec'$, two generalized term order on F

Output: $G''=\{g_1'',\cdots,g_\nu''\}$, a $\prec$ -Groebner basis of W relative to $\prec'$

Begin

$G' := G$;

While there exist f, g $\in$ G' and v $\in$ V(j, f, g) such that S'(j, f, g, v) is reduced (w.r.t. $\prec'$) to r $\neq$ 0 by G'

Do G' :=G'$\bigcup$ {r}

Endwhile;

G" :=G';

While there exist f, g $\in$ G" and v $\in$ V(j, f, g) such that S(j, f, g, v) is $\prec$ -reduced to r $\neq$ 0 by G" relative to $\prec'$

Do G" :=G"$\bigcup$ {r}

Endwhile

End

PROOF. In the theorem, the algorithm for computing a relative Groebner basis can be divided into two parts. The first part deals with S'(j, f, g, v) w.r.t. $\prec'$ and determines a Groebner basis G' w.r.t. $\prec'$. Then, the second part deals with S(j, f, g, v) w.r.t. $\prec$ and relative to $\prec'$, which determines a $\prec$ -Groebner basis relative to $\prec'$.

It is known that the first part for a Groebner basis G' w.r.t. $\prec'$ will be completed in finite steps [7]. By THEOREM 3.1, if G' is a $\prec'$ -Groebner basis , " $\prec$ " and " $\prec'$ " are of difference-differential degree compatibility, then the sequence $G_i=\{g_1,\cdots,g_p,r_1,\cdots,r_i\}$, $i=1,2,\cdots$, will not be an infinite sequence, and then the second part will be completed in finite steps.

Then we get the following conclusions.

(1) If the term orders " $\prec$ " and " $\prec'$ " satisfy the condition of difference-differential degree compatibility, then the algorithm for computing relative Groebner bases will be completed in finite steps.

(2) If the term orders " $\prec$ " and " $\prec'$ " satisfy the condition of difference-differential degree compatibility, then the $\prec$ -Groebner bases relative to $\prec'$ exist.

(3) The algorithm in [9] for computation of the bivariate dimension polynomials in difference differential modules can be implemented in finite steps by computer, and the Maple software in [10] can be implemented in finite time.

ACKNOWLEDGMENT

This work has been supported by the NSFC project 11271040.

.

REFERENCES

[1] M. Noumi, "Wronskima determinants and the Groebner representation of linear differential equation," In:Algebraic Analysis, Boston, Academic Press,1988, pp. 549-569.

[2] N. Takayama, "Groebner basis and the problem of contiguous relations," Japan J. Appl. Math., vol. 6, 1989, pp. 147-160.

[3] T. Oaku and T. Shimoyama, "A Groebner basis method for modules over rings of differential operators," J. Symb. Comput., vol. 18(3), 1994, pp. 223-248.

[4] M. Insa and F. Pauer, "Groebner bases in rings of differential operators," In: Groebner Bases and Applications, London Math. Soc. Lecture Note Series 251, B.Buchberger and F.Winkler (eds.), Cambridge UK, Cambridge University Press, 1998, pp.367-380.

[5] F. Pauer and A.Unterkircher, "Groebner bases for ideals in Laurent polynomial rings and their applications to systems of difference equations," AAECC, vol.9, 1999, pp. 271-291.

[6] A.B.Levin, "Reduced GroEbner bases, free difference-differential modules and difference-differential dimension polynomials," J.Symb. Comput.,vol.30(4), 2000, pp. 357-382.

[7] M. Zhou and F. Winkler, "Groebner bases in difference-differential modules," Proc. ISSAC 2006, ACM Press,pp. 353-360.

[8] A.B.Levin, "Groebner bases with respect to several orderings and multivariable dimension polynomials," J.Symb. Comput.,vol.42(5), 2007, pp. 561--578.

[9] M. Zhou and F. Winkler, "Computing difference-differential dimension polynomials by relative Groebner bases in difference-differential modules," J.Symb. Comput.,vol.43, 2008, pp. 726-745.

[10] C.Donch, "Bivariate difference-differential dimension polynomials and their computation in Maple," Proc. of the 8th International Conference on Applied Informatics, Eger, Hungary, January 27-30, 2010, pp.221-228.

[11] C.Donch, "Characterization of relative Groebner bases," J.Symb. Comput.,vol.55, 2013, pp. 19-29.

[12] E.R.Kolchin, "The notion of dimension in the theory of algebraic differential equations," Bull. Am. Math. Soc..vol.70,pp. 570-573.