Int. J. Nonlinear Anal. Appl. 4 (2013) No. 1, 59-65
ISSN: 2008-6822 (electronic)
http://www.ijnaa.semnan.ac.ir

A modified LLL Algorithm for Change of Ordering of Gröbner Basis

M. Borujeni[a], A. Basiri[a,*], S. Rahmany[a], A. H. Borzabadi[a]

[a]*School of Mathematics and Computer Science, Damghan University, Damghan, Iran*

Abstract

In this paper, a modified version of LLL algorithm, which is a an algorithm with output-sensitive complexity, is presented to convert a given Gröbner basis with respect to a specific order of a polynomial ideal I in arbitrary dimensions to a Gröbner basis of I with respect to another term order. Also a comparison with the FGLM conversion and Buchberger method is considered.

Keywords: Gröbner Basis, LLL Algorithm, Reduced Lattice Basis.
2010 MSC: Primary 13P10 ; Secondary 16G30.

1. Introduction

One of the main tools for solving nonlinear systems is the computation of Gröbner bases. Buchberger algorithm [3] computes a Gröbner basis for a polynomial ideal I with respect to an admissible term ordering $<$. There are different algorithms like F_4 and F_5 which were presented by Faugere in [5] and [6], to improve Buchberger algorithm. Runtime and memory requirements for computing a Gröbner basis is heavily dependendent on the term ordering $<$. The lexicographic term orders are enable to eliminate some variables and hence they can be used for solving polynomial systems and unfortunately, computing the consumes Gröbner basis wrt lexicographic order consumes a lot of time and memory than other orders. Changing of ordering can be given rise to overcome this problem. Among the all term orders, the total degree term order is one of the best orders, that the computing Gröbner basis respect to it, can be done by consuming reasonable time and memory and this is a intensive incentive for computing a total degree Gröbner basis and converting it to a lexicographic Gröbner basis. When the ideal is zero-dimensional, The algorithms presented in [7, 8] are efficients for converting the ordering of Gröbner basis. The aim of this paper is to introduce an algorithm to convert the ordering of a Gröbner basis when the dimension of ideal is positive.

*Corresponding author

Email addresses: m.borujeny@yahoo.com (M. Borujeni), basiri@du.ac.ir (A. Basiri), s-rahmani@du.ac.ir (S. Rahmany), borzabadi@du.ac.ir (A. H. Borzabadi)

Received: May 2012 *Revised:* January 2013

The idea of using LLL algorithm was first proposed by Basiri and Faugere [1], for change ordering of Gröbner basis in polynomial ring with two variables. In this paper, we tend to introduce an extension of this idea, considering a new modified LLL algorithm for conversion a Gröbner basis of an ideal with respect to $<_{old}$ into a Gröbner basis with respect to $<_{new}$, in polynomial rings with n variables, where $n \geq 2$.

The rest of the paper is organized as follows. Section 2 is devoted to present some requirement perliminaries. In Section 3, modified LLL algorithm along with its correctness and termination are described. Experimental results and a comparision with the FGLM and Buchberger methods are shown in Section 4.

2. Perliminaries and Definitions

In this section some requirement concepts and properties of Gröbner basis and lattice basis will be introduced. We refer to [4, 2] for basic facts and notations.

Let $K[\underline{x}]$ be a polynomial ring in variables $x_1, \cdots, x_n$ over an arbitrary field K and I be an ideal. The ideal generated by a set of polynomials $\{g_1, \cdots, g_m\} \subset K[\underline{x}]$ is denoted by $\langle g_1, \cdots, g_m \rangle$. Considering an admissible ordering $<$, we denote by $\mathrm{lt}(f)$ the leading term of a polynomial f. An element $f \in K[\underline{x}]$ is reduced by a Gröbner basis G if no element $g \in G$ has a leading term that divides some terms of f. A Gröbner basis G is reduced if each $g \in G$ is reduced by $G - \{g\}$.

Theorem 2.1. *Let $n,\ d_1, \cdots, d_n \in \mathbb{N}$ and w be not more than $d_1 d_2 \cdots d_n - 1$, then there exist unique numbers $0 \leqslant w_i \leqslant d_i - 1$, such that*

$$w = w_1 d_2 d_3 \cdots d_n + w_2 d_3 \cdots d_n + \cdots + w_{n-2} d_{n-1} d_n + w_{n-1} d_n + w_n.$$

Proof . The proof is by induction on n. For $n = 1$, let $w_1 = w$. Suppose $d_1, \cdots, d_n \in \mathbb{N}$ and $0 \leqslant w \leqslant d_1 d_2 \cdots d_n - 1$. By division algorithm, $w = w_1 d_2 \cdots d_n + r$, where $0 \leqslant r \leqslant d_2 \cdots d_n - 1$ and $w_1 \leqslant d_1 - 1$, because $w_1 \geqslant d_1$ is contrary to $w \leqslant d_1 d_2 \cdots d_n - 1$. By induction assumption, $r = w_2 d_3 \cdots d_n + \cdots + w_{n-1} d_n + w_n$, where $0 \leqslant w_i \leqslant d_i - 1$. Thus

$$w = w_1 d_2 \cdots d_n + w_2 d_3 \cdots d_n + \cdots + w_{n-1} d_n + w_n.$$

Suppose that $0 \leqslant \tilde{w}_i \leqslant d_i - 1$, for $1 \leqslant i \leqslant n$, satisfy in properties of the theorem. So

$$\sum_{i=2}^{n-1} \tilde{w}_i d_{i+1} \cdots d_{n-1} + \tilde{w}_n \leqslant d_2 d_3 \cdots d_n - 1.$$

By uniqueness of r and w_1 the proof is complete. $\square$

Let $(G = \{g_1, \cdots, g_m\},\ <)$ be a reduced Gröbner basis for I and

$$\alpha_i = \max\{deg_{x_i}(g_j)|\ 1 \leqslant j \leqslant m\},$$

and also $c = (\alpha_1 + 1) \cdots (\alpha_{n-1} + 1)$.

By Theorem 2.1, for $0 \leqslant d \leqslant c$, there exist unique numbers $0 \leqslant s_{d,j}$, $1 \leqslant j \leqslant n-1$, such that

$$d = 1 + s_{d,n-1} + s_{d,n-2}(\alpha_{n-1} + 1) + \cdots + s_{d,1}(\alpha_2 + 1) \cdots (\alpha_{n-1} + 1).$$

Let $s_d = (s_{d,1}, \cdots, s_{d,n-1})$ and $s_G = \{s_1, \cdots, s_c\} \subset {\mathbb{N}_0}^{n-1}$. For $f \in K[\underline{x}]$ we define $\alpha(f) =$ the $x_1^{\beta_1} \cdots x_{n-1}^{\beta_{n-1}}$, where $\mathrm{lt}(f) = x_1^{\beta_1} \cdots x_n^{\beta_n}$.

Definition 2.2. *Let* $(G = \{g_1, \cdots, g_m\}, <)$ *be a reduced Gröbner basis for* I *and* $\mathrm{lt}(g_i) = x_1^{\alpha i,1} \cdots x_n^{\alpha_{i,n}}$, *for* $1 \leqslant i \leqslant m$. *We can consider a change in the indices such that,* $\alpha(g_i) < \alpha(g_{i+1})$. *For integer numbers* $d_i \geq deg_{x_i}(\mathrm{lt}(g_j))$, $i = 1, \cdots, n-1$, *define*

$$B_G = \{x_1^{t_1} \cdots x_{n-1}^{t_{n-1}} g_i \mid t_j \leqslant d_j - \alpha_{i,j},\ 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n-1\},$$

$$A = \{x_1^{t_1} \cdots x_{n-1}^{t_{n-1}} g_i \notin G \mid\ \exists\ 1 \leqslant j \leqslant m,\ i < j,\ s.t.\ \alpha(x_1^{k_1} \cdots x_{n-1}^{k_{n-1}} g_j) = \alpha(x_1^{t_1} \cdots x_{n-1}^{t_{n-1}} g_i)\}$$

$$B_s(G) = B_G - A.$$

We denote by $M_s(G)$ *the* $K[x_n]$*-submodule of* $K[\underline{x}]$ *generated by* $B_s(G)$ *which is called s-th* $K[x_n]$*-module associated to ideal* I *with respect to* $<$. *In this case,* $B_s(G)$ *is called s-th basis of* $K[x_n]$*-module associated to ideal* I, *with respect to* $<$.

Let $\tilde{b}_1, \cdots, \tilde{b}_l$ be vectors in $K[x_n]^c$ which are linearly independent over $K[x_n]$, where l and c are positive integers and $l \leqslant c$. The lattice $L \subset K[x_n]^c$ of rank l spanned by $\tilde{b}_1, \cdots, \tilde{b}_l$ is defined as

$$L = \sum_{i=1}^{l} K[x_n]\tilde{b}_i = \{\sum_{i=1}^{l} \lambda_i \tilde{b}_i \mid\ \lambda_i \in K[x_n],\ 1 \leqslant i \leqslant l\}.$$

Consider the natural mapping from $K[x_n]^c$ to $K[\underline{x}]$, which corresponds the vector $\tilde{v} = (v_1, \cdots, v_c)$ to the polynomial $v = \sum_{j=1}^{c} v_j {x_1}^{s_{j,1}} \cdots {x_{n-1}}^{s_{j,n-1}}$. Under this mapping, the lattice $L \subset K[x_n]^c$ corresponding to the $K[x_n]-$submodule $M(L)$ of $K[\underline{x}]$ is denoted by

$$M(L) = \{v = \sum_{j=1}^{c} v_j {x_1}^{s_{j,1}} \cdots {x_{n-1}}^{s_{j,n-1}} \mid\ \tilde{v} = (v_1, \cdots, v_c) \in L\}.$$

Let $b_1, \cdots, b_l$ be a basis for the $K[x_n]-$submodule $M(L)$ of $K[\underline{x}]$ and let $\tilde{b}_1, \cdots, \tilde{b}_l$ be the corresponding basis for the lattice L. We denote by $B = (b_{i,j} {x_1}^{s_{j,1}} \cdots {x_{n-1}}^{s_{j,n-1}})$ the $l \times c$ matrix where $b_{i,j}$ is the coefficient of ${x_1}^{s_{j,1}} \cdots {x_{n-1}}^{s_{j,n-1}}$ in the polynomial $b_i = \sum_{j=1}^{c} b_{i,j} {x_1}^{s_{j,1}} \cdots {x_{n-1}}^{s_{j,n-1}}$. Then we define determinant $d(M(L))$ of $M(L)$ to be the maximum of the determinant of $l \times l$ sub-matrices of B with respect to $<$, and the determinant $d(L)$ of L to be the determinant $d(M(L))$ of $M(L)$. Finally, the orthogonality defect $OD(\tilde{b}_1, \cdots, \tilde{b}_l)$ of the basis $\tilde{b}_1, \cdots, \tilde{b}_l$ for the lattice L with respect to $<$, is defined as

$$\mathrm{lt}(b_1) \cdots \mathrm{lt}(b_l) - \mathrm{lt}(d(L)).$$

Definition 2.3. *The basis* $\tilde{b}_1, \cdots, \tilde{b}_l$ *is called reduced if* $OD(\tilde{b}_1, \cdots, \tilde{b}_l) = 0$.

For $1 \leqslant i \leqslant l$, ith successive minimum (non-unique) of $M(L)$ with respect to $<$ is a minimum element m_i of $M(L)$, such that m_i does not belong to the $K[x_n]$ submodule of $M(L)$, generated by $m_1, \cdots, m_{i-1}$.

Proposition 2.4. *Let* $\tilde{b}_1, \cdots, \tilde{b}_l$ *be a reduced basis for a lattice* $L \subset K[x_n]^c$ *of rank* $l \leqslant c$, *which is ordered in such a way that* $b_i \leqslant b_j$ *for* $1 \leqslant i < j \leqslant l$. *Then for* $1 \leqslant i \leqslant l$, b_i *is an ith successive minimum of* $M(L)$ *with respect to* $<$.

Proof . See [9] □

Proposition 2.5. *Let $\tilde{b}_1, \cdots, \tilde{b}_l$ be a basis for lattice $L \subset K[x_n]^c$ of rank $l \leqslant c$. If the coordinates of the vectors $\tilde{b}_1, \cdots, \tilde{b}_l$ can be permuted so that they satisfy*

- $b_i \leqslant b_j$, *for* $1 \leqslant i < j \leqslant l$,
- $b_{i,j} < b_{i,i} \geqslant b_{i,k}$, *for* $1 \leqslant i < j \leqslant l,\ i < k \leq c$,

then the basis $\tilde{b}_1, \cdots, \tilde{b}_l$ is reduced.

Proof . See [11]. □

Theorem 2.6. *Let $(G = \{g_1, \cdots, g_m\}, <)$ be a reduced Gröbner basis for I, $d_1, \cdots, d_{n-1}$ be positive integer numbers such that $d_i \geq deg_{x_i}(\mathrm{lt}(g_j))$ for $1 \leqslant i \leqslant n-1,\ 1 \leqslant j \leqslant m$, and*

$$I_s(G) = \{f \in I \mid \alpha(f) = x_1^{k_1} \cdots x_{n-1}^{k_{n-1}},\ k_1 \leqslant d_1, \cdots, k_{n-1} \leqslant d_{n-1}\},$$

then $I_s(G) = M_s(G)$.

Proof . Because $B_s(G) \subset I_s(G)$ then $M_s(G) \subset I_s(G)$. If $M_s(G) \neq I_s(G)$, let h be the minimum polynomials (with respect to $<$) in I_s which does not belong to $M_s(G)$. Let $\mathrm{lt}(h) = x_1^{\beta_1} \cdots x_n^{\beta_n}$ and $i_0 = \max\{i \mid \mathrm{lt}(g_i) | \mathrm{lt}(h)\}$, then $\alpha_{i_0,j} \leqslant \beta_j$, for $1 \leqslant j \leqslant n$. We have $\beta_j \leqslant d_j$ for $1 \leqslant j \leqslant n$, because $h \in I_s(G)$, thus $\beta_j - \alpha_{i_0,j} \leqslant d_j - \alpha_{i_0,j}$. Let $b = x_1^{\beta_1 - \alpha_{i_0,1}} \cdots x_{n-1}^{\beta_{n-1} - \alpha_{i_0,n-1}} g_{i_0}$. Choosing i_0 and $b \in B_s(G)$, we put $\tilde{h} = h - \frac{HC(h)}{HC(b)} x_n^{\beta_n - \alpha_{i_0,n}} b$. We claim that $\tilde{h}$ does not belong to $M_s(G)$, because otherwise $h = \tilde{h} + \frac{HC(h)}{HC(b)} x_n^{\beta_n - \alpha i_0,n} b$ is a member of $M_s(G)$ which is a contradiction with the choice of h. On the other hand, $\mathrm{lt}(\frac{HC(h)}{HC(b)} x_n^{\beta_n - \alpha_{i_0,n}} b) = x_1^{\beta_1} \cdots x_n^{\beta_n} = \mathrm{lt}(h)$ and so $\mathrm{lt}(\tilde{h}) < \mathrm{lt}(h)$. Therefore, $\tilde{h} < h$ that is a contradiction with the choice of h. Hence $M_s(G) = I_s(G)$. □

3. Modified LLL Algorithm

In this section we present a new version of LLL algorithm [10], which computes a Gröbner basis for term order $<_{new}$ from the Gobner basis corresponding to term order $<_{old}$) in $K[\underline{x}]$ and in the end, termination and correctness of the given algorithm will be proved. This algorithm contains two major steps: initialization step and main steps. In initialization step, a basis $B_s(G_{old})$ is produced where the $K[x_n]$-module generated by it, includes a Gröbner basis with respect to $<_{new}$. In main steps, first a matrix by the elements of $B_s(G_{old})$ is created and then using linear algebra techniques, this matrix is converted to a new matrix, where its orthogonality default is equal to zero. It will be justified that the rows of last matrix forms a Gröbner basis with respect to $<_{new}$.

LLL Algorithm.

Initialization step

Consider $(G_{old} = \{g_1, \cdots, g_m\},\ <_{old})$ as a reduced Gröbner basis for I, $<_{new}$, and $d_i,\ i = 1 \cdots, n-1$, as positive integers sufficiently large.

Set $\{b_1, \cdots, b_l\} := B_s(G_{old})$, and $k := 0$.

Main steps

1. Choose $i_0 \in \{k+1, \cdots, l\}$ *s.t.* $b_{i_0} = \min_{<_{new}}\{b_i \mid k+1 \leqslant i \leqslant l\}$ and swap$(\tilde{b}_{k+1}, \tilde{b}_{i_0})$.
2. Choose $j \in \{1, \cdots, c\}$ *s.t.* $HT_{new}(b_{k+1}) = HT_{new}(b_{k+1,j})$.
3. If $j \leqslant k$ set $\tilde{t} := \tilde{b}_{k+1} - \frac{HC_{new}(b_{k+1})}{HC_{new}(a_j)}\ x_n^{deg(\tilde{b}_{k+1,j}) - deg(\tilde{a}_{j,j})}\ \tilde{a}_j$, otherwise, $\tilde{t} := \tilde{b}_{k+1}$.
4. If $HT_{new}(t) = HT_{new}(b_{k+1})$ then $\tilde{a}_{k+1} := \tilde{t}$. Permute $(k+1, \cdots, n)$ such that $HT_{new}(a_{k+1,k+1}) = HT_{new}(a_{k+1})$.
   $k := k+1$ and if $k = l$ stop. Otherwise go to step 1.
5. If $HT_{new}(t) <_{new} HT_{new}(b_{k+1})$ then $p := \max\{0 \leqslant s \leqslant k \mid a_s <_{new} t\}$ and for $i = k+1, \cdots, p+2$ set $\tilde{b}_i := \tilde{a}_{i-1}$, $\tilde{b}_{p+1} := \tilde{t}$ and $k := p$. Go to step 1.

Theorem 3.1. *LLL algorithm computes a Gröbner basis G_{new} in $K[\underline{x}]$, such that $Id(G_{old}) = Id(G_{new})$.*

Proof . Let $d_1, \cdots, d_{n-1}$ be a positive integer such that

$$d_i \geqslant \max\{deg_{x_i}(\mathrm{lt}(g)),\ deg_{x_i}(\mathrm{lt}(h))\ for\ g \in G_{old}\ and\ h \in G\}$$

for $1 \leqslant i \leqslant n-1$, where G is a Gröbner basis for I with respect to $<_{new}$, then $G \subset I_s(G_{old})$ and by Theorem 2.6, $M_s(G_{old}) \subseteq I_s(G_{old})$. Therefore, $B_s(G_{old})$ is a Gröbner basis for I with respect to $<_{old}$, where $K[x_n]$-module generated by it, includes a Gröbner basis with respect to $<_{new}$.

Termination: There are finite numbers of passages through step 4 because k is increased by 1. Also there are finite numbers of passages through step 5, because

$$\mathrm{lt}(a_1)\cdots\mathrm{lt}(a_k)\mathrm{lt}(b_{k+1})\cdots\mathrm{lt}(b_n)$$

becomes smaller than previous step and stays unchanged in the step 4. Hence, the number of passages in the main steps are finite and algorithm terminates when $k = l$.

Correctness: Clearly, $B_s(G_{old})$ and $\{a_1, \cdots, a_l\}$ generate the same $K[x_n]$ submodule M of $K[\underline{x}]$. By Theorem 2.6, $M = I_s(G_{old})$. On the other hand, by Proposition 2.5, $\{e\tilde{a}_1, \cdots, \tilde{a}_l\}$ is a reduced basis for the lattice L with basis $\{b_1, \cdots, b_l\}$, because the following invariants are valid before steps 1 and 4

- $a_i \leqslant a_j$, for $1 \leqslant i < j \leqslant k$,
- $a_k \leqslant b_j$, for $k < j \leqslant l$,
- $a_{i,j} < a_{i,i} > a_{i,r},\ for\ 1 \leqslant j < i \leqslant k\ and\ i < r \leqslant c$.

Hence by Proposition 2.4, a_i is ith successive minimum of M and $\mathrm{lt}(a_i) < \mathrm{lt}(a_{i+1})$, (otherwise $\mathrm{lt}(a_i) = \mathrm{lt}(a_{i+1})$, and then $a^{'} = a_{i+1} - a_i \in M$ and $\mathrm{lt}(a^{'}) < \mathrm{lt}(a_{i+1})$ imply that $a^{'}$ is dependent upon the rows $a_1, \cdots, a_i$, so $a_{i+1} = a^{'} + a_i$ is also dependent with $a_1, \cdots, a_i$, which is a contradiction with the choice of a_{i+1}). Now, let g be a polynomial in $I_s(G_{old}) = M$, then there are $\lambda_1, \cdots, \lambda_l \in K[x_n]$ such that

$$g = \sum_{j=1}^{l} \lambda_j a_j.$$

But for $1 \leqslant i < j \leqslant l$, $\mathrm{lt}(\lambda_i a_i) \neq \mathrm{lt}(\lambda_j a_j)$, because otherwise there are $t_i,\ t_j$ such that $\mathrm{lt}(\lambda_i a_i) = x_n^{t_i}\mathrm{lt}(a_i)$ and $\mathrm{lt}(\lambda_j a_j) = x_n^{t_j}\mathrm{lt}(a_j)$, but $\mathrm{lt}(a_i) < \mathrm{lt}(a_j)$ implies $t_i > t_j$ (if $t_i < t_j$ then $x_n^{t_i}\mathrm{lt}(a_i) < x_n^{t_j}\mathrm{lt}(a_j)$, and if $t_i = t_j$ then $\mathrm{lt}(a_i) = \mathrm{lt}(a_j)$) and hence $a^{'} = x_n^{t_i - t_j} a_i - a_j \in M$ and $\mathrm{lt}(a^{'}) < \mathrm{lt}(a_j)$ which implies $a^{'}$ is dependent upon $a_1, \cdots, a_{j-1}$, so $a_j = x_n^{t_i - t_j} a_i - a^{'}$ depends on $a_1, \cdots, a_{j-1}$ which is a contradiction with the choice of a_j. Finally, there is a unique $1 \leqslant j \leqslant l$ such that $\mathrm{lt}(g) = \mathrm{lt}(\lambda_j a_j)$, so $\mathrm{lt}(a_j)|\mathrm{lt}(g)$. On the other hand, G is a Gröbner basis and for any polynomial $f \in I$, there exists $g \in G \subset M$ such that $\mathrm{lt}(g)|\mathrm{lt}(f)$ and thereupon $\mathrm{lt}(a_j)|\mathrm{lt}(f)$ which reveals that $\{a_1, \cdots, a_l\}$ is a Gröbner basis for I with respect to $<_{new}$. □

4. Experimental Results

To demonstrate the efficiency of the presented algorithm in previous section, a Gröbner basis with respect to DRL order in case of general and n variables, which is Gröbner basis generated by random polynomials, is considered. Results of implementing this modified algorithm and compare it with FGLM algorithm and Gröbner basis algorithm available in Maple can be observed in Tables 1 and 2, respectively. Note, here we didn't compute $B_s(G_{old})$, because there is not any gap between $\alpha(g_i)$ and $\alpha(g_{i+1})$, for $g_i,\ g_{i+1} \in G_{old}$. Output is Gröbner basis with respect to Lex order. The following notations is used in Tables: n is the number of variables, $D = \max\{\alpha_1, \cdots, \alpha_n\}$ is degree of Gröbner basis , dim is dimension of K-vector space $\frac{K[x]}{I}$, N_m is the number of multiplications for algorithm, t_1 is LLL algorithm execution time and t_2 is Gröbner basis algorithm (available in Maple) execution time.

n	D	dim	$n.dim^3$	N_m	n	D	dim	$n.dim^3$	N_m
2	3	5	250	25	3	4	20	24000	18323
2	4	10	2000	329	3	5	30	81000	120428
2	5	15	6750	1105	4	2	4	256	162
2	6	20	16000	2826	4	3	8	2048	1338
3	3	5	375	108	5	2	3	135	52
3	3	10	3000	1590	5	3	10	5000	8563

Table 1: The results of comparison between LLL and FGLM algorithms(DRL to Lex)

n	dim	t_1	t_2	n	dim	t_1	t_2
2	40	1.780	5.760	4	30	78.741	$>$ 1424.514
2	49	3.757	13.565	5	20	34.598	265.180
2	51	4.844	20.697	5	30	256.732	$>$3354.062
2	60	8.208	41.367	6	15	28.613	$>$1895.691
3	50	137.709	$>$2172.900	7	12	34.394	957.812
4	20	5.976	70.333	7	20	464.417	4043.733

Table 2: The results of comparison of LLL algorithm with Gröbner basis algorithm (available in Maple)(DRL to Lex)

5. Conclusion

The modified version of LLL algorithm converts a Gröbner basis of an ideal with respect to an arbitrary ordering into a Gröbner basis with respect to another desired ordering. Although in some cases, complexity of FGLM algorithm is less than LLL algorithm complexity, but an important feature of LLL algorithm lies in the fact that it can compute Gröbner basis for ideals of positive dimension while FGLM algorithm can compute it only for ideals of zero dimension.

Acknowledgments

The authors would like to thank Damghan university for supporting this research.

References

[1] A. Basiri and J.-C. Faugère. Changing the ordering of Grbner bases with LLL: Case of two variables. In J. R. Sendra, editor, *Proceedings of ISSAC*, pages 23–29. ACM Press, August 2003.

[2] T. Becker and V. Weispfenning. *Gröbner bases.* Springer-Verlag, NewYork-Berlin-Heidelberg, 1993.

[3] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Innsbruck, 1965.

[4] D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[5] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1–3):61–88, June 1999.

[6] J.-C. Faugère. A new efficient algorithm for computing Grbner bases without reduction to zero (F5). In T. Mora, editor, *Proceedings of ISSAC*, pages 75–83. ACM Press, July 2002.

[7] J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16:329–344, 1993.

[8] J.-C. Faugre and C. Mou. Fast Algorithm for Change of Ordering of Zero-dimensional Gröbner Bases with Sparse Multiplication Matrices. In *Proceedings of the 36th international symposium on Symbolic and algebraic computation*, ISSAC '11, pages 115–122, New York, NY, USA, 2011. ACM.

[9] A.-K. Lenstra. Factoring multivariate polynomials over finite fields. *Journal of Computer and System Sciences*, 30(2), 1985.

[10] A.-K. Lenstra, H.-W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[11] S. Paulus. Lattice basis reduction in function fields. In J. P. Buhler, editor, *Algorithmic Number Theory — ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, pages 567–575, Berlin, 1998. Springer-Verlag.