Fast computation of Gröbner bases of ideals of $\mathbb{F}[x, y]$

Yindong Chen
School of Computer Science
Fudan University
Shanghai, 200433, China
Email: chenyd@fudan.edu.cn

Yao Lu
School of Electronic and Information Engineering
Tongji University
Shanghai, 200433, China
Email: tj.luyao@gmail.com

Peizhong Lu
School of Computer Science
Fudan University
Shanghai, 200433, China
Email: pzlu@fudan.edu.cn

***Abstract*—This paper provides a fast algorithm for Gröbner bases of ideals of $\mathbb{F}[x, y]$ over a field $\mathbb{F}$. We show that only the S-polynomials of neighbor pairs of a strictly ordered finite generating set are needed in the computing of a Gröbner bases of the ideal. It reduces dramatically the number of unnecessary S-polynomials that are processed. Although the complexity of the algorithm is hard to evaluated, it obviously has a great improvement from Buchberger's Algorithm.**

Keywords: Gröbner Bases, Buchberger's Algorithm, polynomial ideal

I. Introduction

Gröbner bases is a powerful tool for solving algebraic systems [1], [2]. Nowadays, the application of Gröbner bases becomes more and more widely, e.g., coding theory, signal theory, and even algebraic attacks in cryptanalysis [3], [4]. However the computation of Gröbner bases is not as efficient as expected. Actually, for a general polynomial ideal I, the computation of Gröbner bases is always complex. Thus the computational complexity limits the scope of the applications of the theory. The upper boundary of the computational complexity is $O(N^{2^n})$, where N is the maximum degree of the generating polynomials and n is the number of variables [5]. Therefore efficient computing algorithm for Gröbner bases make a great sense.

Historically, Buchberger is the presenter of Gröbner bases theory, and Buchberger's Algorithm is the first algorithm for computing Gröbner bases [1]. Many of improved algorithms inherit the essential ideal of the classical Buchberger's Algorithm. They focus on how to eliminate unnecessary S-polynomials. Buchberger improves his classical algorithm by suggested criteria to remove the useless S-polynomials [2], so does the F_5 algorithm [7]. F_4 algorithm improves the original algorithm in another perspective [6]. It exploits sparse linear algebra to allow multiple pairs to be processed simultaneously, resulting efficient processing for huge number of S-polynomials. "FGLM" algorithm is another type of method to compute Gröbner bases for a zero dimensional ideal [8]. It can convert a Gröbner bases from one term ordering to another in $O(D^3)$ computation, where $D{=}\dim_{\mathbb{F}}\mathbb{F}[x]/I$.

Lu finds an interesting property of the Gröbner bases of homogenous ideals of $\mathbb{F}[x, y]$ [11]. The property shows that only the S-polynomials of neighbor pairs of a strictly ordered finite generating set are needed. In this paper, we generate the property to general ideals of $\mathbb{F}[x, y]$. Thus the number of S-polynomials decrease dramatically from $\frac{1}{2}r(r-1)$ to $(r-1)$, where r is the number of generating polynomials for current loop round.

II. Fast computation of Gröbner bases of ideals of $\mathbb{F}[x, y]$

A. Standard notations

We firstly recall the standard notations in the Gröbner bases theory [1], [2], [9], [10]. Let $\mathbb{F}$ be a field. $\mathbb{F}[x_1, x_2, \cdots, x_n]$ is denoted as the polynomial ring over $\mathbb{F}$ in n indeterminates, and we always write $\mathbb{F}[X]$ for short if there is no confusion in the context. For arbitrary $i{=}(i_1, i_2, \cdots, i_n){\in}\mathbb{N}^n$, we call $X^i{=}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ a power product (a monomial with coefficient ignored) of $\mathbb{F}[X]$. Let $T^n{=}\left\{x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}|i_1, i_2, \cdots, i_n{\in}\mathbb{N}\right\}$. Then T^n is the set of all power products of $\mathbb{F}[X]$. "$<$" is an admissible term order on T^n. For a given term order, every $f{\in}\mathbb{F}[X]$ can be written as

$$f = a_1X^{\alpha_1} + a_2X^{\alpha_2} + \cdots + a_rX^{\alpha_r}, \tag{1}$$

where $0{\neq}a_i{\in}\mathbb{F}, X^{\alpha_i}{\in}T^n$, and $X^{\alpha_1}{>}X^{\alpha_2}{>}\cdots{>}X^{\alpha_r}$.

Then, we define:

- $\mathrm{lp}(f) = X^{\alpha_1}$, the "leading power product" of f;
- $\mathrm{lc}(f) = a_1$, the "leading coefficient" of f;
- $\mathrm{lt}(f) = a_1X^{\alpha_1}$, the "leading term" of f.

In the sequel, any discussion related to $\mathrm{lp}, \mathrm{lc}, \mathrm{lt}$ has defaultly specified a term ordering.

Let $f, g, h \in \mathbb{F}[X]$, and $G = \{g_1, g_2, \cdots, g_r\} \subseteq \mathbb{F}[X]$.Then we say that:

- f reduces to h modulo g in one step, denoted $f \xrightarrow{g} h$, if and only if $\mathrm{lp}(g)$ divides a non-zero term X that appears in f and $h = f - \frac{X}{\mathrm{lt}(g)}g$.
- f top reduces to h modulo g, if and only if $f \xrightarrow{g} h$, and $\mathrm{lt}(f) > \mathrm{lt}(h)$. That is $h = f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(g)}g$.
- f reduces to h modulo G, denoted $f \xrightarrow{G} h$, if and only if there exists $g_i \in G$ such that $f \xrightarrow{g_i} h$.
- f top reduces to h modulo G, if and only if $f \xrightarrow{G} h$, and $\mathrm{lt}(f) > \mathrm{lt}(h)$.
- "$\xrightarrow{G}_+$" is the reflexive-transitive closure of "$\xrightarrow{G}$".

978-1-4244-4313-0/09/$25.00 ©2009 IEEE

- The S-polynomial of f and g, denoted $S(f,g)$, is defined as

$$S(f,g)=\frac{L}{\mathrm{lt}(f)}f-\frac{L}{\mathrm{lt}(g)}g, \tag{2}$$

where $L=\mathrm{lcm}(\mathrm{lp}(f),\mathrm{lp}(g))$.

Theorem 1 [2], [9], [10]. Let I be an ideal of $\mathbb{F}[X]$, and $G=\{g_1,g_2,\cdots,g_r\}$ a subset of I. Then the following statements are equivalent:

i) $f\in I$, if and only if $f\xrightarrow{G}_+0$.
ii) $f\in I$, if and only if

$$f=h_1g_1+h_2g_2+\cdots+h_rg_r, \tag{3}$$

where $h_1,\cdots,h_r\in\mathbb{F}[X], \mathrm{lp}(f)=\max_{1\le i\le r}\{\mathrm{lp}(h_i)\,\mathrm{lp}(g_i)\}$.
iii) $S(g_i,g_j)\xrightarrow{G}_+0$, for arbitrary $1\le i<j\le r$.

Definition 1. Let I be an ideal of $\mathbb{F}[X]$, and $G=\{g_1,g_2,\cdots,g_r\}$ a subset of I. Then G is called a Gröbner bases of I, if G satisfies any equivalent condition in Theorem 1. When we say "G is a Gröbner bases of $\mathbb{F}[X]$", it means that "G is a Gröbner bases of $\langle G\rangle$".

Definition 2. Let $G=\{g_1,g_2,\cdots,g_r\}$ be a Gröbner bases. Then G is called a minimal Gröbner bases, if for arbitrary $1\le i\ne j\le r$, $\mathrm{lt}(g_i)\nmid\mathrm{lt}(g_j)$.

B. Strictly ordering

From now on, we specify our discussion on the polynomial ring in two indeterminates, i.e., $\mathbb{F}[x,y]$. And the the lexicographic order $(y<x)$ is chosen as the fixed term order on $\mathbb{F}[x,y]$.

Definition 3. Let $G=\{g_1,g_2,\cdots,g_r\}$ be a subset of $\mathbb{F}[x,y]$. With a fixed term order, if $\mathrm{lp}(g_1)>\mathrm{lp}(g_2)>\cdots>\mathrm{lp}(g_r)$, and $\mathrm{lp}(g_i)\nmid\mathrm{lp}(g_j)$, $i\ne j$, then the leading terms of G are called to be strictly ordered.

Given a subset of $\mathbb{F}[x,y]$, denoted K, how can we change it into a strictly ordered one, G, such that $\langle K\rangle=\langle G\rangle$? Actually, if there exits $f_i,f_j\in K$ such that $\mathrm{lp}(f_i)|\,\mathrm{lp}(f_j)$, we can top reduce f_j by f_i, and replace f_j in K by the remainder of the reduction. We repeat the action (top reduction and replacing) until there is no more such pairs (f_i and f_j). Since the order of leading term of the replaced polynomial decreases by every replacing, the action will terminate in finite steps. And then we will get a strictly ordered polynomial set G, such that $\langle K\rangle=\langle G\rangle$.

Based on the upper analysis, we strictly present it as Algorithm 1.

Algorithm 1 : Finding a strictly ordered generator for an ideal

Input: A polynomial set $K=\{g_1,g_2,\cdots,g_r\}\subset\mathbb{F}[x,y]$.
Output: A strictly ordered generator G, such that $\langle G\rangle=\langle K\rangle$.
Initial: $G:=K$
While there exists $f,g\in G, f\ne g$, such that $\mathrm{lp}(f)|\,\mathrm{lp}(g)$
  $G:=G\setminus\{g\}$,
  $g\xrightarrow{f}h$.
  If $h\ne0$ **Then** $G:=G\cup\{h\}$
Return G

Example 1.
Let $K=\{g_1=x^8y^7+x^3y^2+1,\ g_2=x^6y^5+x^3y+x,\ g_3=x^3y^6+y^2\}$.
Step 1:
Since $\mathrm{lp}(g_3)|\,\mathrm{lp}(g_1)$,
then $g_1\xrightarrow[\text{top reduction}]{g_3}-x^5y^3+x^3y^2+1=g_1'$.
Update g_1 by g_1': $K=\{g_1',g_2,g_3\}$.
Step 2:
Since $\mathrm{lp}(g_1')|\,\mathrm{lp}(g_2)$,
then $g_2\xrightarrow[\text{top reduction}]{g_1'}x^4y^4+x^3y+xy^2+x=g_2'$.
Update g_2 by g_2': $K=\{g_1',g_2',g_3\}$.
Now, since there is no more g_i,g_j such that $\mathrm{lp}(g_i)|\,\mathrm{lp}(g_j)$, the computation terminates. And we get the strictly ordered generator $G=\{g_1',g_2',g_3\}$, such that $\langle G\rangle=\langle K\rangle$.

Proposition 1. Let $K=\{f_1,f_2,\cdots,f_k\}$ be a subset of $\mathbb{F}[x,y]$ and $G=\{g_1,g_2,\cdots,g_r\}$ the finite set resulting from Algorithm 1. Then the leading terms of G are strictly ordered, $r\le k$, and $\langle G\rangle=\langle K\rangle$.

Proof: G is obviously strictly ordered by the upper analysis. Let $G_0=K$, and we employ the subscript i to distinguish the symbols in the ith loop round in Algorithm 1.

- If $h_i=0$, then g_i is multiple of f_i. Thus $\langle G_{i+1}\rangle=\langle G_i\setminus\{g_i\}\rangle=\langle G_i\rangle$, and $|G_{i+1}|=|G_i|-1$.
- If $h_i\ne0$, then g_i can be represented as linear combination of f_i and h_i. Thus $\langle G_{i+1}\rangle=\langle G_i\setminus\{g_i\},h_i\rangle=\langle G_i\rangle$, and $|G_{i+1}|\le|G_i|$.

Therefore, $\langle G_{i+1}\rangle=\langle G_i\rangle$ and $|G_{i+1}|\le|G_i|$.
By induction, we have $\langle G\rangle=\langle K\rangle$, and $|\langle G\rangle|\le|\langle K\rangle|$. ■

C. Fast computation of Gröbner bases

Theorem 2. Let $G=\{g_1,g_2,\cdots,g_r\}$ be a subset of $\mathbb{F}[x,y]$, and strictly ordered, then G is a minimal Gröbner bases if and only if

$$S(g_i,g_{i+1})\xrightarrow{G}_+0,\quad i=1,2,\cdots,r-1.$$

Proof: By Theorem 1, the necessity is obviously holds. Now we prove the sufficiency.

Suppose that $S(g_i,g_{i+1})\xrightarrow{G}_+0 (i=1,2,\cdots,r-1)$. To prove that G is a Gröbner bases, we just need to prove that for $\forall f\in\langle g_1,g_2,\cdots,g_r\rangle$, f can be represented as

$$f=h_1g_1+h_2g_2+\cdots+h_rg_r,$$

where $h_1,h_2,\cdots,h_r\in\mathbb{F}[x,y]$, and

$$\mathrm{lp}(f)=\max_{1\le i\le r}\{\mathrm{lp}(h_i)\,\mathrm{lp}(g_i)\}. \tag{4}$$

In fact, since $f\in\langle g_1,g_2,\cdots,g_r\rangle$, it can be written as

$$f=h_1g_1+h_2g_2+\cdots+h_rg_r, \tag{5}$$

where $h_1,h_2,\cdots,h_r\in\mathbb{F}[x,y]$.
There is a representation of f as (5), such that

$$X=\max_{1\le i\le r}\{\mathrm{lp}(h_i)\,\mathrm{lp}(g_i)\}$$

is minimal, and moreover the number of elements in the set

$$S=\{i|1\le i\le r,\ \mathrm{lp}(h_i)\,\mathrm{lp}(g_i)=X\}, \tag{6}$$

namely $|S|$, is minimal.

If $\mathrm{lp}(f)\geq X$, then formula (4) is true. Now, let $\mathrm{lp}(f)<X$.

If $|S|=1$, then there is only one maximal term in the summations which is on the right side of formula (5). Thus, $\mathrm{lp}(f)=X$, which contradicts with the hypothesis.

Therefore, $|S|\geq 2$. We further suppose that the interval between the least two elements in S is minimal. That's to say, if $S=\{i_1, i_2, \cdots, i_{|S|}\}$, where $1\leq i_1<i_2<\cdots<i_{|S|}\leq r$, then $|S|$ and i_2-i_1 are both minimal.

For arbitrary $1\leq i\leq r$, let $n_i=\deg_x \mathrm{lp}(g_i)$, $m_i=\deg_y \mathrm{lp}(g_i)$. Since G is strictly ordered, thus

$$n_1>n_2>\cdots>n_r,\ m_1<m_2<\cdots<m_r. \tag{7}$$

For convenience in description, let $j=i_1$, $k=i_2$, $1\leq j<k\leq r$. Then

$$X=\mathrm{lp}(h_j)\,\mathrm{lp}(g_j)=\mathrm{lp}(h_k)\,\mathrm{lp}(g_k), \tag{8}$$

and for arbitrary $j\leq t_1, t_2\leq k$,

$$x^{n_{t_1}}y^{m_{t_2}}|X. \tag{9}$$

For $l<k$, let $\Delta=\mathrm{lc}(h_k)\,\mathrm{lc}(g_k)$, $\delta=\frac{\Delta}{\mathrm{lc}(g_l)}$.

From the definition of S-polynomial (2), there is

$$S(g_l,g_k)=\frac{1}{\mathrm{lc}(g_l)}y^{m_k-m_l}g_l-\frac{1}{\mathrm{lc}(g_k)}x^{n_l-n_k}g_k, \tag{10}$$

and then

$$h_kg_k-\Delta\frac{X}{x^{n_l}y^{m_k}}S(g_l,g_k)=(h_k-\mathrm{lt}(h_k))\,g_k+\left(\delta\frac{X}{x^{n_l}y^{m_l}}\right)g_l.$$

Let $l=k-1$, thus (5) becomes

$$\begin{aligned}
f &= h_jg_j+h_kg_k+\sum_{i\in S,i\neq j,i\neq k}h_ig_i+\sum_{i\notin S}h_ig_i\\
&= \Delta\frac{X}{x^{n_{k-1}}y^{m_k}}S(g_{k-1},g_k)-\Delta\frac{X}{x^{n_{k-1}}y^{m_k}}S(g_{k-1},g_k)\\
&\quad +h_jg_j+h_kg_k+\sum_{i\in S,i\neq j,i\neq k}h_ig_i+\sum_{i\notin S}h_ig_i\\
&= -\Delta\frac{X}{x^{n_{k-1}}y^{m_k}}S(g_{k-1},g_k)+h_jg_j+\delta\frac{X}{x^{n_{k-1}}y^{m_{k-1}}}g_{k-1}\\
&\quad +(h_k-\mathrm{lt}(h_k))\,g_k+\sum_{i\in S,i\neq j,i\neq k}h_ig_i+\sum_{i\notin S}h_ig_i,
\end{aligned}$$

Let

$$\omega=-\Delta\frac{X}{x^{n_{k-1}}y^{m_k}}S(g_{k-1},g_k)+(h_k-\mathrm{lt}(h_k))\,g_k. \tag{11}$$

Then

$$f=h_jg_j+\delta\frac{X}{x^{n_{k-1}}y^{m_{k-1}}}g_{k-1}+\sum_{i\in S,i\neq j,i\neq k}h_ig_i+\sum_{i\notin S}h_ig_i+\omega.$$

Since $S(g_{k-1},g_k)\xrightarrow{G}_+0$ and $x^{n_{k-1}}y^{m_k}|X$, thus $-\Delta\frac{X}{x^{n_{k-1}}y^{m_k}}S(g_{k-1},g_k)\xrightarrow{G}_+0$. So

$$-\Delta\frac{X}{x^{n_{k-1}}y^{m_k}}S(g_{k-1},g_k)=h'_1g_1+h'_2g_2+\cdots+h'_rg_r,$$

where

$$X>\mathrm{lp}\left(-\Delta\frac{X}{x^{n_{k-1}}y^{m_k}}S(g_{k-1},g_k)\right)=\max_{1\leq i\leq r}\{\mathrm{lp}(h'_i)\,\mathrm{lp}(g_i)\}.$$

Since $\mathrm{lp}\,(h_k-\mathrm{lt}(h_k))\,g_k<\mathrm{lp}(h_kg_k)=X$, then ω can be written as

$$\omega=h''_1g_1+h''_2g_2+\cdots+h''_rg_r,$$

where

$$X>\mathrm{lp}(\omega)=\max_{1\leq i\leq r}\{\mathrm{lp}(h''_i)\,\mathrm{lp}(g_i)\}.$$

a) If $j=k-1$, then

$$f=\left(1+\frac{\delta}{\mathrm{lc}(h_j)}\right)h_jg_j+\sum_{i\in S,i\neq j,i\neq k}h_ig_i+\sum_{i\notin S}h_ig_i+\omega.$$

Now, f can be represented as a summation in which the number of maximal monomials is not exceed $|S|-1$, which contradicts the hypothesis that $|S|$ is minimal.

b) If $j<k-1$, let $\bar{h}_{k-1}=(\delta\frac{X}{x^{n_{k-1}}y^{m_{k-1}}}+h_{k-1})$, then

$$f=h_jg_j+\bar{h}_{k-1}g_{k-1}+\sum_{i\in S,i\neq j,i\neq k}h_ig_i+\sum_{i\notin S,i\neq k-1}h_ig_i+\omega.$$

Since $X=\mathrm{lp}(\frac{X}{x^{n_{k-1}}y^{m_{k-1}}}g_{k-1})$, $X>\mathrm{lp}(h_{k-1})\,\mathrm{lp}(g_{k-1})$, then $X=\mathrm{lp}(\bar{h}_{k-1}\,\mathrm{lp}(g_{k-1}))$.

Now, the number of maximal monomials X in f equal to $|S|$, but the position set of maximum monomials X is $\{j,k-1\}\cup S\setminus\{k\}$, which contradicts with the hypothesis that $k-j$ is minimal.

Here, we have finished the proof. ■

Based on Theorem 2 and Proposition 1 above, we give algorithm 2 to compute a minimal Gröbner bases for an ideal of $\mathbb{F}[x,y]$.

Algorithm 2 : Computing a minimal Gröbner bases for an ideal of $\mathbb{F}[x,y]$

Input: A polynomial set $K=\{g_1,g_2,\cdots,g_r\}\subset\mathbb{F}[x,y]$.
Output: A minimal Gröbner bases G, such that $\langle G\rangle=\langle K\rangle$.
Initial: $i=1, G'_0=\varnothing, G_1=K$
While $K\neq\varnothing$
  $K:=\varnothing$
  Call Algorithm 1 to changed G_i into a strictly ordered set G'_i
  For every neighbor pair (g_j,g_k) of G'_i
    If g_j do not neighbored g_k in G'_{i-1} **Then**
      $S(g_j,g_k)\xrightarrow{G'_i}_+h$
      If $h\neq 0$ **Then** $K:=K\cup\{h\}$
  $G_{i+1}:=G'_i\cup K$
  $i:=i+1$
$G:=G_i$
Return G

Example 2.

$K=\{f_1=x^9+x^6y,\ f_2=x^8y+x^2y^3,\ f_3=x^5y^2+x^3y^5,\ f_4=x^2y^3+y^8\}$, $\mathbb{F}=\mathbb{Q}$.

$G_0' = \varnothing$, $G_1 = K$.

Step 1:

$G_1 \xrightarrow{\text{strictly ordered}} G_1' = \{f_1, f_2, f_3, f_4\}$

$S(f_1, f_2) = x^6y^3 - x^2y^3 \xrightarrow{G_1'}_+ xy^8 - y^{13} = f_5,$

$S(f_2, f_3) = -x^6y^5 + x^2y^4 \xrightarrow{G_1'}_+ y^{20} - y^9 = f_6,$

$S(f_3, f_4) = -x^3y^8 + x^3y^5 \xrightarrow{G_1'}_+ xy^{13} - xy^{10} = f_7,$

$G_2 = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7\}$.

Step 2:

$G_2 \xrightarrow{\text{strictly ordered}} G_2' = \{f_1, f_2, f_3, f_4, f_5, f_7' = y^{10} - y^9\}$

$S(f_4, f_5) = xy^{13} + y^{13} \xrightarrow{G_2'}_+ 2y^9 = f_8,$

$S(f_5, f_7') = xy^9 - y^{15} \xrightarrow{G_2'}_+ 0,$

$G_3 = \{f_1, f_2, f_3, f_4, f_5, f_7', f_8\}$.

Step 3:

$G_3 \xrightarrow{\text{strictly ordered}} G_3' = \{f_1, f_2, f_3, f_4, f_5, f_8\}$

$S(f_5, f_8) = -2y^{14} \xrightarrow{G_3'}_+ 0,$

$G_4 = \{f_1, f_2, f_3, f_4, f_5, f_8\}$.

Since there is no more polynomials to add to G_3', the computation stops. And we get a minimal Gröbner bases $G = G_4 = G_3' = \{f_1, f_2, f_3, f_4, f_5, f_8\}$, such that $\langle G\rangle = \langle K\rangle$.

III. Conclusion

Based on Theorem 2, we propose a fast algorithm for computing the Gröbner bases of ideals of $\mathbb{F}[x, y]$. Compared with Buchberger's Algorithm, we restrict the S-polynomials between neighbor pairs of the strictly ordered polynomials. Although there're extra computation for strictly ordering, we benefit much more from the number of S-polynomial dramatically decreasing, from $O(r^2)$ to $O(r)$, where r is the count of the polynomials in the generating set. Actually, the algorithm can be combined with other algorithm improved from Buchberger's Algorithm, e.g., F_4 Algorithm. What need to be emphasized is that the computational complexity of the Algorithm is hard to evaluate. But it does not influence the efficiency of the algorithm.

Acknowledgement

This research was supported by the National Natural Science Foundation of China (Grant No. 60673082), and the Special Funds of Authors of Excellent Doctoral Dissertation in China (Grant No. 200084).

References

[1] B. Buchberger, "in Algorithmus zum Auffinden der Basiselement des Restklassenringes nach einem nulldimensionalen Polynomideal," Ph.D. Thesis, Inst, University of Innsbruck, Innsbruck, Austria, 1965;

[2] B. Buchberger, "Gröbner bases: An algorithmic method in polynomial ideal theory," *Multidimensional Systems Theory*, Dordrecht: D. Peidel Publishing Co., pp. 184–232, 1984;

[3] B. Buchberger, "Gröbner bases and system Theory," *special Issue on Applications of Gröbner Bases in Multidimensional Systems and Signal Procesing*, Dordrecht: Kluwer Academic Publishers, 2001

[4] J. D. Golic, "Vectorial bolean functions and induced algebraic equations," *IEEE Trans inf Theory*, vol. 52, No. 2, pp. 528–537, 2006;

[5] D. Lazard, "A note on upper bounds for ideal-theoretic problems," *J. Symb. Comp*, vol. 13, No. 3, pp. 231–233, 1992;

[6] J. C. Faugére,"A new efficient algorithm for computing Gröbner bases(F_4)," *J Pure Appl Algebra*, vol. 139, pp. 61–83, 1999;

[7] J. C. Faugére, "A new efficient algorithm for computing Gröbner bases without reduction to zero(F_5)," *Proceedings of ISSAC*, ACM Press, pp. 75–83, 2002;

[8] J. C. Faugére, P. Gianni, D. Lazard, et al, "Efficient computation of zero dimensional Gröbner bases by change of ordering," *J Symb Comp*, vol. 16, pp. 329–444, 1993;

[9] W. Adams, P. Loustaunau, "An introduction to Gr obner Bases," *Graduate Studies in Mathematics American Mathematical Society*, Vol. 3, 1994;

[10] M. L. Liu, "Gröbner Basis Theory and the Applications," Beijing: Science Press, 2000;

[11] P. Z. Lu, Y. Zou, "Fast computation of Gröbner basis of homogenous ideals of $\mathbb{F}[x, y]$," *Science In China (Series F)*, vol. 51, No. 4, pp. 337–448, 2008;