2010

An F4-Style Involutive Basis Algorithm

Miao Yu
University of Southern Mississippi

AN F4-STYLE INVOLUTIVE BASIS ALGORITHM

MIAO YU
(FACULTY ADVISER: JOHN PERRY)

Abstract. This paper introduces a new algorithm for computing Gröbner bases. To avoid as much ambiguity as possible, this algorithm combines the F4 algorithm and basic algorithm of involutive bases and it replaces the symbolic precomputation of S-polynomials and ordinary division in F4 by a new symbolic precomputation of non-multiplicative prolongations and involutive division. This innovation makes the sparse matrix of F4 in a deterministic way. As an example the Cyclic-4 problem is presented.

1. Introduction

How to analyze solutions of systems of non-linear polynomial equations? We can compute a Gröbner Basis and analyze it [CLO97]. But how to compute a Gröbner Basis? There exist several ways to do it. Buchberger's algorithm is the original method [Buc65]. Gebauer-Möller algorithm [GM88] is a refined Buchberger's algorithm. The F4 algorithm [Fau99] uses matrix reduction to compute efficiently. Involutive Basis algorithm [GB98, AH05, ZB96] is an effective method avoiding much ambiguity in the other algorithms.

In Section 2 we describe Buchberger's and F4 algorithm and give a formulation of the basic Involutive Basis algorithm after we present the definition of involutive division. We will see that both in Buchberger's and F4, there exists ambiguity in each loop. In the method of Involutive Algorithm this ambiguity has been avoided. So in Section 3 we combine the F4 algorithm and Involutive algorithm.

2. Background

Definition 1. Graded Reverse Lex Order (grevlex) is a monomial ordering, in which all the terms of a polynomial are ordered first by the total degree of the monomials then determined by the smallest degree of the right-most variable. Precisely, let $\alpha, \beta \in \mathbb{N}^n$ we say $\mathbf{x}^\alpha \succ \mathbf{x}^\beta$ if $\sum_1^n \alpha_i > \sum_1^n \beta_i$ or $\sum_1^n \alpha_i = \sum_1^n \beta_i$ and in $\alpha - \beta \in \mathbb{Z}^n$, the right-most nonzero entry is negative.

Other orderings exist. A property of every monomial ordering that it is a well ordering [CLO97].

Definition 2. Let f be a nonzero polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. and let $\succ$ be a monomial order; the **leading monomial** of f is the largest monomial according to monomial ordering. We denote the leading monomial of f by $\operatorname{lm}(f)$ and its coefficient by $\operatorname{lc}(f)$.

Let $I = \langle g_1, g_2, \ldots, g_m \rangle \subset \mathbb{F}[x_1, \ldots, x_n]$. If for every $p \in I$, $\operatorname{lm}(g_k) \mid \operatorname{lm}(p)$ for some $k \in \{1, 2, \ldots, m\}$, we say that $G = (g_1, g_2, \ldots g_m)$ is a **Gröbner Basis.**

Example 3. For example, the leading monomial of $x_1x_2^2 + x_2x_3x_4 + x_3x_4^2$ is $x_1x_2^2$.

Buchberger's algorithm is the original algorithm that allows us to compute Gröbner bases, but the algorithm is quite inefficient without any optimizations. Let $p, q \in \mathbb{F}[x_1, \ldots, x_n]$, we say that (p, q) is a critical pair. We define the **S-polynomial** of p and q with respect to a monomial ordering to be

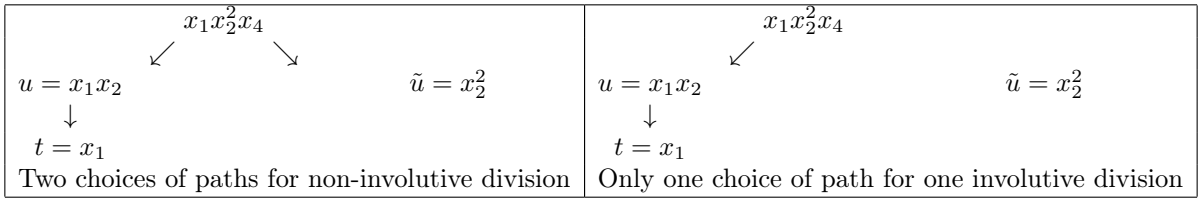
$$S(p,q) = \operatorname{lc}(q) \cdot \frac{\operatorname{lcm}(\operatorname{lm}(p), \operatorname{lm}(q))}{\operatorname{lm}(p)} \cdot p - \operatorname{lc}(p) \cdot \frac{\operatorname{lcm}(\operatorname{lm}(p), \operatorname{lm}(q))}{\operatorname{lm}(q)} \cdot q.$$

We say that q **top-reduces** p to r if $\operatorname{lm}(q) \mid \operatorname{lm}(p)$ and $r = p - \frac{\operatorname{lc}(p)\cdot\operatorname{lm}(p)}{\operatorname{lc}(q)\cdot\operatorname{lm}(q)} q$.

Theorem 4. [Buc65] *Let $G = \langle g_1, g_2, \ldots, g_n \rangle \in \mathbb{F}[x_1, \ldots, x_n]$, G is a Gröbner Basis if and only if there exists a sequence of top-reductions which reduces any S-polynomial to zero.*

Buchberger's algorithm uses critical pairs to construct S-polynomials and top-reduce one S-polynomial in each step. If all the S-polynomials top-reduce to zero, then Gröbner basis is done already; if not, add the their reduced forms to the current basis and test the new S-polynomials as well.

FIGURE 2.1. Choices of paths for non-involutive division and involutive division.



Algorithm F4 to compute a Gröbner basis was first described by Faugére in [Fau99]. F4 uses the same mathematical principles as Buchberger's algorithm, but reduces many S-polynomials in one go by forming a matrix and using linear algebra to do the reduction in parallel. Here column swaps are not allowed since it will change the ideal of the set of polynomials. In fact Faugère used F4 to compute a Gröbner basis for Cyclic-9, which had previously been intractable.

Another approach to computing a special kind of Gröbner basis is *Involutive Bases* [GB98, AH05]. This algorithm is based on a special concept of monomial multiplication.

Definition 5. Let $\mathbb{M}$ be the set of monomials of $\mathbb{F}[x_1, \ldots, x_n]$. We say that an **involutive division** L or L**-division** is given on $\mathbb{M}$ if for any finite set $U \subset \mathbb{M}$ a relation $|_L$ is defined on $U \times \mathbb{M}$ such that for any $t, u \in U$ and any $v, w \in \mathbb{M}$ the following holds:

i) $u \mid_L w$ implies $u \mid w$.
ii) $u \mid_L u$ for any $u \in U$.
iii) $u \mid_L (uv)$ and $u \mid_L (uw)$ if and only if $u \mid_L (uvw)$.
iv) If $u \mid_L w$ and $t \mid_L w$, then $u \mid_L t$ or $t \mid_L u$.
v) If $u \mid_L t$ and $t \mid_L w$, then $u \mid_L w$.
vi) If $U \subseteq V$, then $u \mid_L w$ with respect to V implies $u \mid_L w$ with respect to U.

Remark 6. The significance for property (iv) is we only have one way to do reduction by involutive division. See Figure 2.1.

Definition 7. Assume $u \mid_L w$. We say u is an **involutive divisor** of w and w is an **involutive multiple** of u. Let $v \in \mathbb{M}$ such that $w = uv$; we write $w = u \times v$ and say that v is **multiplicative** for u, denoted by $v \in \mathrm{M}(u)$. If t is a conventional divisor of w, but not an involutive divisor of w, let $v' \in \mathbb{M}$ such that $w = tv'$. We say that v' is **non-multiplicative** for t and write $w = t \cdot v'$, and we denote v' as $v' \in \mathrm{NM}_L(t)$.

Remark 8. In mathematics, $\times$ and $\cdot$ usually have the same meaning. But for involutive division, we use $\times$ instead of ordinary $\cdot$ to mean the involutive multiple of monomials.

In addition, let $t \in \mathbb{M}$. We denote $\deg_i(t)$ as $\deg_{x_i} t$.

There are three common examples of involutive division: Janet, Thomas, and Pommaret [GB98]. Here we use Janet division for the Involutive Basis algorithm.

Definition 9. Let U be a finite set. For each $1 \leq i \leq n$ divide U into groups labeled by non-negative integers $d_1, \ldots, d_i$:

$$[d_1, \ldots, d_i] = \{u \in U \mid \deg_i(u) = d_j, 1 \leqslant j \leqslant i\}.$$

A variable x_i is considered as **multiplicative in Janet Division** (or J-multiplicative) for $u \in U$ if

- $i = 1$ and $\deg_i(u) = \max\{\deg_1(v) \mid v \in U\}$, or
- $i > 1$, $u \in [d_1, \ldots, d_{i-1}]$, and $\deg_i(u) = \max\{\deg_i(v) \mid v \in [d_1, \ldots, d_{i-1}]\}$.

We will compute a Gröbner basis of Cyclic-4 using Janet division in the next section, so we conclude here by identifying the multiplicative and non-multiplicative variables of its leading terms.

Example 10. Let $F = \{f_1, f_2, f_3, f_4\}$ be the Cyclic-4 system,

$$f_1 = x_1 + x_2 + x_3 + x_4 \qquad f_2 = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1$$
$$f_3 = x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2 \qquad f_4 = x_1x_2x_3x_4 - 1.$$

Here we choose the grevlex ordering with $x_1 \succ x_2 \succ x_3 \succ x_4$ and the Janet division. Let

$$U = \{\mathrm{lm}(f_1), \mathrm{lm}(f_2), \mathrm{lm}(f_3), \mathrm{lm}(f_4)\} = \{x_1, x_1x_2, x_1x_2x_3, x_1x_2x_3x_4\}.$$

- For $i = 1$, $\max_{j\in\{1,2,\ldots,4\}} \deg_1 \mathrm{lm}(f_j) = 1$ so x_1 is multiplicative for $f_1, \ldots, f_4$.
- For $i = 2$, $[d_1] = \{[1]\}$ where $[1] = \{x_1, x_1x_2, x_1x_2x_3, x_1x_2x_3x_4\}$ and
$$\max_{j\in\{1,2,3,4\}} \deg_2(\mathrm{lm}(f_j)) = 1;$$
so x_2 is multiplicative for $f_2, f_3, f_4 \in [1]$ and non-multiplicative for f_1.
- For $i = 3$, $[d_1, d_2] = \{[1,0], [1,1]\}$ where $[1,0] = \{x_1\}$,
$$[1,1] = \{x_1x_2, x_1x_2x_3, x_1x_2x_3x_4\},$$
and $\max_{j\in\{2,3,4\}} \deg_3(\mathrm{lm}(f_j)) = 1$; so x_3 is multiplicative for $f_1 \in [1,0]$, $f_3, f_4 \in [1,1]$ and non-multiplicative for f_2.
- For $i = 4$, $[d_1, d_2, d_3] = \{[1,0,0], [1,1,0], [1,1,1]\}$ where $[1,0,0] = \{x_1\}, [1,1,0] = \{x_1x_2\}, [1,1,1] = \{x_1x_2x_3, x_1x_2x_3x_4\}$ and $\max_{j\in\{3,4\}} \deg_4(\mathrm{lm}(f_j)) = 1$; so x_4 is multiplicative for $f_1 \in [1,0,0], f_2 \in [1,1,0], f_4 \in [1,1,1]$ and non-multiplicative for f_3.

We summarize the results above: x_2, x_3, x_4 are non-J-multiplicative to f_1, f_2 and f_3 respectively.

Definition 11. Let $G \subset \mathbb{F}[x_1, \ldots, x_n]$. *$G$ is L-autoreduced* if $\mathrm{lm}(g) \nmid_L \mathrm{lm}(g')$ for any $g, g' \in G$.

Example 12. Recall the Cyclic-4 system. Notice $\mathrm{lm}(f_1) \nmid_J \mathrm{lm}(f_2)$; $\mathrm{lm}(f_2) \nmid_J \mathrm{lm}(f_3)$; $\mathrm{lm}(f_3) \nmid_J \mathrm{lm}(f_4)$. In fact, $\mathrm{lm}(f_i) \nmid_J \mathrm{lm}(f_j)$ for $i, j = 1, 2, 3, 4$ and $i \neq j$. By Definition 11, the initial polynomial set of the Cyclic-4 is autoreduced.

We give a special name to multiples of a polynomial by a variable.

Definition 13. The *prolongation* of a polynomial g by a variable x is a product xg. If $x \in \mathrm{NM}(\mathrm{lm}(g))$ then the prolongation is called non-multiplicative, otherwise multiplicative.

We can now introduce a new kind of ideal basis.

Definition 14. $G \subset \mathbb{F}[x_1, \ldots, x_n]$ is an *Involutive Basis* if it is autoreduced and all non-multiplicative prolongations of its elements are linear combinations of multiplicative prolongations of its elements. That is, for $G = \{f_1, f_2, \ldots, f_m\}$,

$$\forall g \in G\ \forall x \in \mathrm{NM}(\mathrm{lm}(g))\ \exists u_1, u_2, \ldots, u_m \in \mathbb{M}: \quad g \cdot x = \sum_i^m u_i \times f_i.$$

Another way of saying this is that a polynomial set G is said to be an *involutive basis* if any non-multiplicative prolongation of the element in this set is L-reduced to zero by G.

Remark 15. The Buchberger's algorithm tries to compute the generators of a Gröbner Basis by constructing and reducing S-polynomials. In this paper we use non-multiplicative prolongations and reduce them by involutive division. But the reduction of a non-multiplicative prolongation is the same as the computation of an S-polynomial, since we can see the combination of the non-multiplicative prolongation and its first involutive divisor as an S-polynomial.

Using this definition, we can compute an involutive basis as follows [ZB96]. Let $G := \emptyset$ and F be the given set of polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. While $F \neq \emptyset$, repeat the following:

- Let $G := \mathrm{Autoreduce}(G \cup F)$ and set $F = \emptyset$.
- For each polynomial $g \in G$:
  - Find the non-multiplicative set of $\mathrm{lm}(g) = \{x_1, \ldots, x_i \mid 1 \leqslant i \leqslant n\}$.
  - For each non-multiplicative variable of $\mathrm{lm}(g)$:
    - Compute the non-multiplicative prolongation $x_i \cdot g$ and reduce it by G using L-division.
    - The result, p, is no longer L-divisible by $\mathrm{lm}(f)$ for any $f \in G$. If p is non-zero, add it to F and autoreduce F.

Remark 16. In fact, involutive basis algorithm does not terminates for all involutive divisions, but it does for Janet division.

3. F4-style involutive algorithm

In this section we describe another algorithm based on combining these two algorithms.

Definition 17. The degree of prolongation of xp is

$$\deg(xp) = \deg(x\mathrm{lm}(p)).$$

Using this definition, we compute an F4-style involutive basis as follows:

- As a modified F4 algorithm, we still pick several polynomials of minimal degree and process the reduction in a matrix. However, instead of picking critical pairs to generate S-polynomials, here we apply involutive division to choose non-multiplicative prolongations.
- As a modified involutive basis algorithm, this new approach inherits from the old approach of reducing a non-multiplicative prolongation in each step. However, instead of picking one prolongation, we choose several and process the reduction by multiplicative prolongations using the matrix.

See Figure 3.1 for pseudocode.

Example 18. Recall the Cyclic-4 system F from Example 10. We compute an Involutive Basis of F using F4-style involutive method in Janet division. Recall that we have summarized all the non-J-multiplicative variables for $f_1, f_2, \ldots, f_4$. So we have $P = \{(x_2, f_1), (x_3, f_2), (x_4, f_3)\}$ and $G = F$. Here we use X_{intL} as the intermediate list of X_L and $M(P_d)$ as the matrix of monomials of degree d.

Loop 1: Set $d = 2$, then $P_2 = \{(x_2, f_1)\}$ and $P = \{(x_3, f_2), (x_4, f_3)\}$. Before we reduce P_2 by G we first find the set X_L using Symbolic Preprocessing: Set $F_M = \emptyset$ and $F_{NM} = P_2$

$X_{intL} = \{\mathbf{x_1x_2}, x_2^2, x_2x_3, x_2x_4\}$ where x_1x_2 is J-reducible by $\mathrm{lm}(f_2)$. So add $(1, f_2)$ to F_M and add all the monomials of f_2 to X_{intL};

$X_{intL} = \{x_1x_2, x_2^2, x_2x_3, x_2x_4, \mathbf{x_1x_4}, x_3x_4\}$ where x_1x_4 is J-reducible by $\mathrm{lm}(x_4 \cdot f_1)$ then update X_{intL} and add (x_4, f_1) to F_M ;

$X_{intL} = \{x_1x_2, x_2^2, x_2x_3, x_2x_4, x_1x_4, x_3x_4, x_4^2\}$, we can check that no element in X_{intL} is J-reducible by $\mathrm{lm}(f_i)$ for $i = 1, 2, \ldots, 4$. Now we have the ordered list

$$X_L = \{x_1x_2, x_2^2, x_2x_3, x_2x_4, x_1x_4, x_3x_4, x_4^2\}$$

and the matrix $M_{3\times 7}(P_2)$ with $F_{NM} = \{(x_2, f_1)\}$ and $F_M = \{(1, f_2), (x_4, f_1)\}$.

$$M(P_2) = \begin{pmatrix} & x_1x_2 & x_1x_4 & x_2^2 & x_2x_3 & x_2x_4 & x_3x_4 & x_4^2 \\ f_2 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ x_4f_1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ x_2f_1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Triangularizing $M(P_2)$ gives us:

$$M(P_2) = \begin{pmatrix} & x_1x_2 & x_1x_4 & x_2^2 & x_2x_3 & x_2x_4 & x_3x_4 & x_4^2 \\ f_2 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ x_4f_1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ x_2f_1 & 0 & 0 & 1 & 0 & 2 & 0 & 1 \end{pmatrix}.$$

The third row is reduced into a new polynomial, we say it as $f_5 = x_2^2 + 2x_2x_4 + x_4^2$ where $\mathrm{lm}(f_5) \notin \langle \mathrm{lm}(G) \rangle$. So now we add f_5 to G and update P into $P = \{(x_3, f_2), (x_4, f_3), (x_1, f_5)\}$.

Loop 2: Set $d = 3$, now we have $P_3 = \{(x_3, f_2), (x_1, f_5)\}$ and $P = \{(x_4, f_3)\}$. Let $F_{NM} = P_3$ and $F_M = \emptyset$. Symbolic Preprocessing gives us:

$$X_L = \{x_1x_2x_3, x_1x_3x_4, x_2x_3^2, x_2x_3x_4, x_3^2x_4, x_1x_2^2, x_1x_2x_4, x_1x_4^2, x_2^2x_3, x_2x_4^2, x_3x_4^2, x_4^3\};$$

Now we have obtained all the rows needed for the matrix $M_{8\times 12}(P_3)$.

$$M(P_3) = \begin{pmatrix} f_3 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ x_2f_2 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ x_2f_4 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ x_3x_4f_1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ x_4^2f_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ x_3f_5 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 \\ x_3f_2 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ x_1f_5 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

FIGURE 3.1.

algorithm *F4-style algorithm of Involutive Bases*
inputs
F, a finite subset of $\mathbb{F}[x_1, \ldots, x_n]$
outputs
G, a finite subset of $\mathbb{F}[x_1, \ldots, x_n]$
do
$G := F$
$P := \{x_i \cdot f \mid f \in G \text{ with } x_i \in \mathrm{NM}_L(\mathrm{lm}(f))\} \cup \{u \times f \mid u\mathrm{lm}(f) = \mathrm{lm}(g) \;\; f \neq g \in G\}$
$Done := \{\}$
while $P \neq Done$ **do**
Let d be the minimal degree of the elements in $P \backslash Done$
$P_d := \{x_i \cdot p \mid x_i \cdot p \in P \text{ and } \deg(x_i \cdot p) = d\}$
$F_{new} := Reduction(P_d, G)$
$Done := Done \cup P_d$
$G := G \cup F_{new}$
$P := (\{x_i \cdot f \mid f \in G \text{ with } x_i \in \mathrm{NM}_L(\mathrm{lm}(f))\} \cup \{u \times f \mid u\mathrm{lm}(f) = \mathrm{lm}(g) \;\; f \neq g \in G\}) \setminus Done$
return G

algorithm *Reduction*
inputs
P_d, a finite set of prolongations of degree d
G, a finite subset of $\mathbb{F}[x_1, \ldots, x_n]$
outputs
F_{new}, a finite subset of $\mathbb{F}[x_1, \ldots, x_n]$ (possible an empty set)
do
$F_M, F_{NM} := SymbolicPreprocessing(P_d, G)$
Let $M(P_d)$ be the matrix of coefficients of all polynomials in F_M and F_{NM}
Triangularize $M(P_d)$ and let $\tilde{F}$ be the set of polynomals resulting
$F_{new} := \left\{ f \in \tilde{F} \mid \mathrm{lm}(f) \notin \langle \mathrm{lm}(F) \rangle \right\}$
return F_{new}

algorithm *SymbolicPreprocessing*
inputs
P_d, a finite set of prolongations of degree d
G, a finite subset of $\mathbb{F}[x_1, \ldots, x_n]$
outputs
F_M, F_{NM}, finite sets of prolongations of degree d
do
$F := P_d$
$F_{NM} := F$
$Done := \emptyset$
Let X_L be the set of monomials of all polynomials in F.
while $X_L \neq Done$ **do**
Let $m \in X_L \setminus Done$
$Done := Done \cup \{m\}$
if m L-top reducible modulo G **then**
Let $f \in G$ such that $\mathrm{lm}(f) \mid_L m$
Let $m' = \frac{m}{\mathrm{lm}(f)}$
$F := F \cup \{m' \times f\}$
add the monomials of $m' \times f$ to X_L
return $F \setminus F_{NM}, F_{NM}$

Triangularizing $M(P_3)$, one row has been reduced to zero and one row is reduced into a new polynomial, we say it as $f_6 = x_2x_3^2 - x_1x_2x_4 - x_2x_3x_4 + x_3^2x_4$ where $\mathrm{lm}(f_6) \notin \langle \mathrm{lm}(G) \rangle$. So now we add f_6 to G and add (x_1, f_6) and (x_2, f_6) to P.

Following the previous steps, in **loop 3** computing F_M for $P_4 = \{(x_4, f_3), (x_1, f_6), (x_2, f_6)\}$ will give us a 15×19 matrix $M(P_4)$ whose columns represent monomials of degree 4 and triangularizing the matrix will give us a new polynomial $f_7 = x_2x_3x_4^2 + x_3^2x_4^2 + x_1x_4^3 + 2x_3x_4^3 - 1$. Then we have the updated basis $G = \{f_1, f_2, \ldots, f_7\}$ and the set of non-J-multiple pairs $P = P_5 = \{(f_1, f_7), (f_2, f_7), (f_3, f_7)\}$; In **loop 4**, symbolic preprocessing will give us a 13×18 matrix $M(P_5)$ and triangularizing the matrix will give us two new polynomials:

$$f_8 = -x_3^3x_4^2 - x_3^2x_4^3 - x_2x_4^4 - x_4^5 + x_2 + x_3 + 2x_4;$$
$$f_9 = x_2x_4^4 + x_4^5 - x_2 - x_4.$$

The updated $G = \{f_1, f_2, \ldots, f_9\}$ and $P = P_6 = \{(x_1, f_8), (x_2, f_8), (x_1, f_9), (x_2, f_9), (x_3, f_9)\}$ gives us a 21×26 matrix $M(P_6)$, then triangularizing the matrix results in a new polynomial of degree 6:

$$f_{10} = x_3^2x_4^4 + x_2x_3 - x_2x_4 + x_3x_4 - 2x_4^2.$$

Update $G = \{f_1, f_2, \ldots, f_{10}\}$ and $P = P_7 = \{(x_1, f_{10}), (x_2, f_{10}), (x_3, f_{10})\}$.

In the **last loop**, symbolic preprocessing and matrix triangularization will give us three zero rows in the bottom, which means no new polynomial is resulted. Now we have check all non-J-multiplicative prolongations. So G is an Involutive Basis of the cyclic-4 system.

Theorem 19. *If involutive basis algorithm terminates correctly for a given input, then so does F4-style involutive basis algorithm.*

Proof. In the symbolic preprocessing, it terminates when $X_L = Done$. Initially X_L is finite set and it has a maximal monomial t. We add monomials of $m' \times f$ to X_L such that $m'\mathrm{lm}(f) \in X_L$ so $m'\mathrm{lm}(f) \leqslant t$. Admissible ordering is a well ordering so that there are finitely many monomials less than or equal to t. So we add finitely many monomials to X_L. When $X_L \neq Done$, we keep adding to $Done$ the monomials in X_L that are not in $Done$. So symbolic preprocessing terminates. As long as symbolic preprocessing terminates, reduction terminates as well.

The F4-style involutive algorithm generates the same polynomials as involutive basis algorithm, but uses a matrix to reduce more than one polynomial in each step. For the contrapositive, assume F4-style involutive algorithm does not terminates. Then it keep adding prolongations to P that involutive algorithm would also compute. So involutive algorithm will not terminates either. □

References

[AH05] Joachim Apel and Ralf Hemmecke, *Detecting unnecessary reductions in an involutive basis computation*, Journal of Symbolic Computation **40** (2005), 1131–1149.

[Buc65] Bruno Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalem Polynomideal (an algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal)*, Ph.D. thesis, Mathematical Insitute, University of Innsbruck, Austria, 1965, English translation published in the Journal of Symbolic Computation (2006) 475–511.

[CLO97] David Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms*, second ed., Springer, 1997.

[Fau99] Jean-Charles Faugère, *A new efficient algorithm for computing Gröbner bases (F4)*, Journal of Pure and Applied Algebra **139** (1999), 61–88.

[GB98] Vladimir P. Gerdt and Yuri A. Blinkov, *Involutive bases of polynomial ideals*, Mathematics and Computers in Simulation **45** (1998), 519–541.

[GM88] Rudiger Gebauer and Hans Möller, *On an installation of Buchberger's algorithm*, Journal of Symbolic Computation **6** (1988), 275–286.

[ZB96] A. Yu. Zharkov and Yuri A. Blinkov, *Involution approach to investigating polynomial systems*, Mathematics and Computers in Simulation **42** (1996), no. 4–6, 323–332.

Current address: University of Southern Mississippi

E-mail address: miaoyu08@gmail.com