Summer 8-2010

An F4-Style Involutive Basis Algorithm

Miao Yu
University of Southern Mississippi

The University of Southern Mississippi

AN F4-STYLE INVOLUTIVE BASIS ALGORITHM

by

Miao Yu

A Thesis
Submitted to the Graduate School
of The University of Southern Mississippi
in Partial Fulfillment of the Requirements
for the Degree of Master of Science

Approved:

____
Director

____

____

____

Dean of the Graduate School

August 2010

ABSTRACT

AN F4-STYLE INVOLUTIVE BASIS ALGORITHM

by Miao Yu
August 2010

How to solve a linear equation system? The echelon form of this system will be obtained by Gaussian elimination then give us the solution. Similarly, Gröbner Basis is the “nice form” of nonlinear equation systems that can span all the polynomials in the given ideal [4]. So we can use Gröbner Basis to analyze the solution of a nonlinear equation system.

But how to compute a Gröbner Basis? There exist several ways to do it. Buchberger’s algorithm is the original method [2]. Gebauer-Möller algorithm [6] is a refined Buchberger’s algorithm. The F4 algorithm [5] uses matrix reduction to compute efficiently. Involutive Basis algorithm [8, 1, 12] is an effective method avoiding much ambiguity in the other algorithms.

In Chapters 1 and 2 we describe two well-known methods of computing Gröbner Basis called Buchberger’s and F4 algorithm. In Chapter 3 after presenting the definition of involutive division we give a detailed formulation of basic and improved Involutive Basis algorithm. We will see that there exists ambiguity both in Buchberger’s and F4 algorithm. But in the method of Involutive Basis Algorithm, the ambiguity for the choice of prolonagation has been avoided. So in Chapter 4 we combine the F4 algorithm and Involutive Basis algorithm in order to obtain a new approach that can reduce polynomials faster as well as avoid ambiguity. The combined algorithm called F4-involutive is a partial result due to its efficiency. More work such as implementing Buchberger’s criteria would be done in the future.

ACKNOWLEDGMENTS

Thanks to Dr. Vladimir Gerdt for his kind response to my email on Involutive Bases.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

Figure

LIST OF TABLES

Table

Chapter 1

WHAT IS A GRÖBNER BASIS?

Recall that in linear algebra, we use Gaussian elimination to obtain the *echelon form* of a linear equation system, which will help us analyze the solutions. As a key to the solutions, echelon form spans all the solutions to the given system. Similarly, **Gröbner Basis** can be said as the “nice form” of nonlinear equation systems that is a basis that span all the polynomials in the ideal. We now define these notations precisely.

1.1 Notation

Let $\mathbb{F}[x_1,\ldots,x_n]$ be a **polynomial ring** over a field $\mathbb{F}$. (A **ring** R is a nonempty set with at least two operations + and $\times$, such that $(R,+)$ is an abelian group and $(R,+,\times)$ is closed and associative under multiplication and satisfies distributivity of addition over multiplication. For other definitions of ring theory see [11].) Given a subset of R, denoted by S; if S is a ring under the same operations as R, then S is a **subring** of R.

Let I be a subring of R ($\emptyset \neq I \subseteq R$); we call I an **ideal** of R if it satisfies the absorption property: $ar \in I$ for all $a \in I$ and $r \in R$. An ideal I can be generated by some fixed elements $a_1, a_2, ..., a_n \in R$ by setting $I = \{a_1r_1 + a_2r_2 + ... + a_nr_n \mid r_1, ..., r_n \in R\}$. In this case we write $I = \langle a_1, a_2, ..., a_n\rangle$ and we call the list $(a_1, a_2, ..., a_n)$ a basis of I. In abstract algebra, ideals have many important applications in mathematics [4].

Example 1.1.1. Consider in $\mathbb{F}[x_1,\ldots,x_4]$ the system of polynomial equations

$$\begin{aligned} x_1+x_2+x_3+x_4 &= 0 \\ x_1x_2+x_2x_3+x_3x_4+x_4x_1 &= 0 \\ x_1x_2x_3+x_2x_3x_4+x_3x_4x_1+x_4x_1x_2 &= 0 \\ x_1x_2x_3x_4 &= 1. \end{aligned}$$

This corresponds to the ideal

$$\langle f_1, f_2, f_3, f_4\rangle \in \mathbb{F}[x_1,\ldots,x_4]$$

where

$$\begin{aligned} f_1 &= x_1+x_2+x_3+x_4 \\ f_2 &= x_1x_2+x_2x_3+x_3x_4+x_4x_1 \\ f_3 &= x_1x_2x_3+x_2x_3x_4+x_3x_4x_1+x_4x_1x_2 \\ f_4 &= x_1x_2x_3x_4-1. \end{aligned}$$

We call this system **Cyclic-4** and we will return to it several times.

We say that a **monomial** is any product of the polynomial ring's indeterminates. A **term** is a product of a monomial and an element of the base field. For example, x^2 is a monomial but $2x^2$ is a term.

For univariate polynomials, we can easily order terms by the degree of the variable in each term; however for multivariate polynomials, e.g. $x^2yz+xy^3+z^4$, it's not easy to determine the terms' order, so we need a method of ordering of terms (monomials).

Definition 1.1.1. [4] A **monomial ordering** on $\mathbb{F}[x_1,\ldots,x_n]$ is any relation $\succ$ on the set of monomials $\mathbf{x}^\alpha,\ \alpha\in\mathbb{Z}^n_{\geqslant 0}$ ($\mathbf{x}^\alpha = x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ and $\mathbb{Z}^n_{\geqslant 0}$ is the set of vectors of nonnegative integers), satisfying:

i) $\succ$ is a total ordering. This means any two items can be compared (for $\forall t_1 \neq t_2,\ t_1 \prec t_2$ or $t_1 \succ t_2$)

ii) If $\mathbf{x}^\alpha \succ \mathbf{x}^\beta$ and $\gamma \in \mathbb{Z}^n_{\geqslant 0}$, then $\mathbf{x}^{\alpha+\gamma} \succ \mathbf{x}^{\beta+\gamma}$.

iii) $\succ$ is a well-ordering on $\mathbb{Z}^n_{\geqslant 0}$ .This means that every nonempty subset of $\mathbb{Z}^n_{\geqslant 0}$ has a smallest element under $\succ$.

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 $\alpha,\beta\in\mathbb{Z}^n_{\geqslant 0}$ 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.

In the thesis we use grevlex ordering; other ordering exist [4] but we will not consider them.

Example 1.1.2. Consider a multivariate polynomial $f(x,y,z) = x^2yz+xy^3+z^4$; by graded reverse lex ordering we can rewrite it into descending order $f(x,y,z) = xy^3+x^2yz+z^4$.

Definition 1.1.2. 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 $\mathrm{lm}(f)$ and denote the **leading coefficient** of f by $\mathrm{lc}(f)$.

Example 1.1.3. Let us come back to Cyclic-4,

$$\begin{aligned}
f_1 &= x_1 + x_2 + x_3 + x_4 \\
f_2 &= x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1 \\
f_3 &= x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2 \\
f_4 &= x_1x_2x_3x_4 - 1.
\end{aligned}$$

By definition of monomial ordering :

$$\begin{aligned}
\mathrm{lm}\,(f_1) &= x_1 \\
\mathrm{lm}\,(f_2) &= x_1x_2 \\
\mathrm{lm}\,(f_3) &= x_1x_2x_3 \\
\mathrm{lm}\,(f_4) &= x_1x_2x_3x_4.
\end{aligned}$$

1.2 Definition of Gröbner Basis

Let $I = \langle f_1, f_2, \ldots, f_m \rangle$; let $p \in \mathbb{F}[x_1, \ldots, x_n]$; is $p \in I$? If it is, then by definition $p = \sum r_i f_i$ where $r_i \in \mathbb{F}[x_1, \ldots, x_n]$. It would seem that we could easily determine that $p \in I$ if there exists f_k such that $\mathrm{lm}(f_k) \mid \mathrm{lm}(p)$; but there may some cancellation that happened in $\sum r_i f_i$ which means $\mathrm{lm}(f_i) \nmid lm(p)$ for some $i \in \{1, 2, \ldots, m\}$; that will give you a false decision telling you $p \notin I$.

Example 1.2.1. Let $f_1 = x_1^2 + x_2^2$, $f_2 = x_1x_2 - 1$, $p = x_2^3 + x_1$. Is $p \in \langle f_1, f_2 \rangle$? It looks like it's not because $\mathrm{lm}(f_i) \nmid \mathrm{lm}(p)$ for $i = \{1, 2\}$. However, $p = h_1 f_1 + h_2 f_2$ where $h_1 = x_2$ and $h_2 = -x_1$, so $p \in \langle f_1, f_2 \rangle$.

How to fix this problem? We can modify $\langle f_1, f_2 \rangle$ by adding p to the list of generators of the ideal and call it f_3 ; now we have the same ideal $\langle f_1, f_2, f_3 \rangle$ with a different basis, where $\mathrm{lm}(f_3) \mid \mathrm{lm}(p)$. In fact f_1, f_2, f_3 have a special form that allows us to decide $\forall p \in \mathbb{F}[x_1, \ldots, x_n]$ whether $p \in I$. This basis of ideal I which has a special property is called Gröbner Basis.

Definition 1.2.1. Let $I = \langle g_1, g_2, \ldots, g_m \rangle$. If for every $p \in I$, $\mathrm{lm}\,(g_k) \mid \mathrm{lm}\,(p)$ for some $k \in \{1, 2, \ldots, m\}$, we say that $G = (g_1, g_2, \ldots g_m)$ is a **Gröbner Basis.** Furthermore, Gröbner Basis exists for every ideal of a polynomial ring [2, 4].

1.3 How Do We Compute a Gröbner Basis?

Let $G \subseteq \mathbb{F}[x_1,\ldots,x_n]$, we want a Gröbner basis of $\langle G \rangle$. We will look for polynomials in the ideal that do not satisfy the Gröbner basis property and add new polynomials to repair this defect. In Example 4, f_3 is a polynomial in $\mathbb{F}[x_1,x_2]$ which can't be detected in the ideal I if the generators of a basis of ideal I are only f_1, f_2, however, after adding f_3 to the list of generators of the ideal I we get a Gröbner basis which can generate all the polynomials in the ideal.

But how can we find the polynomials that we need to add ? First of all, we need to define a special polynomial called an S-polynomial: a minimal construction that cancels leading monomials of two selected polynomials.

Definition 1.3.1. Let $p,q \in \mathbb{F}[x_1,\ldots,x_n]$. We define the S**-polynomial** of p and q with respect to a monomial ordering to be

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

Buchberger's characterization suggests we compute the S-polynomials and top-reduce them. If they all top-reduce to zero, then Gröbner basis is done already; if not, add the reduced forms to the current basis and test the new S-polynomials as well. This suggests **Buchberger's algorithm** to compute a Gröbner basis [2]:

set $G = F$, then iterate the following three steps.

- Choose a critical pair $p,q \in G$ that has not yet been considered, and construct its S-polynomial.
- Top-reduce this S-polynomial with respect to G. That is, while $\mathrm{lm}(S)$ remains divisible by $\mathrm{lm}(g_i)$ for any $g_i \in G$, put $S := S - \frac{\mathrm{lm}(S)}{\mathrm{lm}(g_i)} \cdot g_i$.
- Once no more top-reductions of S are possible, either $S = 0$ or $\mathrm{lm}(S)$ is no longer divisible by $\mathrm{lm}(g_i)$ for any $g_i \in G$.
  −In the first case, we say that $S(p,q)$ reduces to zero with respect to G.
  −In the second case, append S to G. The new entry in G means that $S(p,q)$ now reduces to zero with respect to G.

The algorithm terminates once the S-polynomials of all pairs in G top reduce to zero. The pseudocode of Buchberger's algorithm 1 is given as follows:

Buchberger's algorithm allows us to compute Gröbner bases, but the algorithm is quite inefficient without any optimizations. To make it more efficient, Buchberger's criteria give

Algorithm 1 .

```
algorithm Buchberger's algorithm

  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
    Let $G := F$
    Let $P := \{(i,j) : 1 \leqslant i \leqslant j \leqslant m\}$
    while P$\neq \emptyset$ do
      Choose $(i,j) \in P$
      Remove $(i,j)$ from P
      Let $S$ be the $S-$polynomial of $g_i, g_j \in G$
      Let $r$ be the top-reduction of $S$ modulo $G$
      if $r \neq 0$ then
        $G = G \cup \{r\}$
        $P = P \cup \{(r,g) \mid \forall g \in G \textit{ and } r \neq g\}$
      return $G$
```

us a great way to detect useless computations and skip these S-polynomials in order to improve the efficiency.

- **Buchberger's gcd criterion**: Let p and q be two polynomials whose *leading monomials* u and v have no common variables. Then the S-polynomial of p and q reduces to zero with respect to the "current" G [2].

- **Buchberger's lcm criterion**: Let p and q be two polynomials whose *leading monomials* are u and v, respectively. Let f be a polynomial whose leading monomial is t. If t divides $\operatorname{lcm}(u,v)$, then the S-polynomial of p and q top-reduces to zero with respect to G [3].

Now we can detect many S-polynomials that should be skipped during the process of computation. But how can we detect which pair of the list of generators be selected to apply the criteria and computed? The selection of elements from the critical pair list during executions of the iteration is governed by certain *strategy*. There are two traditional strategies for this.

- The **normal strategy** for selecting critical pairs chooses a pair such that the least common multiple of the leading monomials $\operatorname{lm}(f_1)$ and $\operatorname{lm}(f_2)$ is minimal in the current monomial ordering [3].

- However, in the **sugar strategy**, critical pairs are ordered with respect to a phantom degree called sugar and the pair with minimal sugar will be selected [10].

In this thesis, we use only the normal strategy.

The Gebauer-Möller algorithm is a sophisticated implementation of Buchberger's algorithm that exploits Buchberger's criteria independent of strategy, which efficiently makes the computation of Gröbner basis faster [6]. First set $F := G$ then iterate the following steps:

- Choose a critical pair $p, q \in G$ that has not yet been considered, and construct its S-polynomial.
- Top-reduce the S-polynomial with respect to G, and find the remainder r: if $r \neq 0$ append r to G, compute critical pairs for r and each $g \in G$, then
    - Eliminate new pairs that safely satisfy Buchberger's lcm criterion.
    - Eliminate new pairs that satisfy Buchberger's gcd criterion from the critical pair list survived.
    - Eliminate old pairs that safely satisfy Buchberger's lcm criterion.
    - Remove elements of the basis made redundant by the new polynomial.

Finally we will get a Gröbner basis of $\langle F \rangle$. See the Gebauer-Möller main algorithm 2 and algorithm 3 for pseudocode.

Example 1.3.1. We compute a Gröbner basis of Cyclic-4 by the Gebauer-Möller algorithm. Recall the Cyclic-4 system,

$$\begin{aligned} f_1 &= \mathbf{x_1} + x_2 + x_3 + x_4 \\ f_2 &= \mathbf{x_1 x_2} + x_2 x_3 + x_3 x_4 + x_4 x_1 \\ f_3 &= \mathbf{x_1 x_2 x_3} + x_2 x_3 x_4 + x_3 x_4 x_1 + x_4 x_1 x_2 \\ f_4 &= \mathbf{x_1 x_2 x_3 x_4} - 1. \end{aligned}$$

(We have leading monomials in bold.) Let $F = \langle f_1, f_2, f_3, f_4 \rangle$, $G = \{\}$, add each polynomial $g \in \langle F \rangle$ to G and update the set of critical pairs P:

- For f_1, updated $G = \{f_1\}$, updated $P = \{\}$.
- For f_2, updated $G = \{f_1, f_2\}$, updated $P = \{(f_1, f_2)\}$.

Algorithm 2 .

```
algorithm Gebauer-Möller algorithm

  inputs
    $F$, a finite subset of $\mathbb{F}[x_1, \dots, x_n]$
  outputs
    $G$, a finite subset of $\mathbb{F}[x_1, \dots, x_n]$
  do
    Let $G := \{\}$
    Let $P := \{\}$
    while $F \neq \emptyset$ do
      Let $f \in F$
      Remove $f$ from $F$
      $G, P := Update(G, P, f)$
      while $P \neq \emptyset$ do
        Pick any $(f, g) \in P$ and remove it
        Let $h$ be the top-reduction of $S(f, g)$ modulo $G$
        if $h \neq 0$ then
          $G, P := Update(G, P, h)$
    return $G$
```

- For f_3, updated $G = \{f_1, f_2, f_3\}$, updated $P = \{(f_1, f_2), (f_1, f_3), (f_2, f_3)\}$. Since
$$\operatorname{lcm}(\operatorname{lm}(f_1), \operatorname{lm}(f_3)) = \operatorname{lcm}(\operatorname{lm}(f_2), \operatorname{lm}(f_3)) = x_1x_2x_3,$$
Buchberger's lcm criterion implies that we can safely eliminate critical pair (f_1, f_3), then updated $P = \{(f_1, f_2), (f_2, f_3)\}$.

- For f_4, updated $G = \{f_{1,}f_2, f_3, f_4\}$, updated
$$P = \{(f_1, f_2), (f_2, f_3), (f_1, f_4), (f_2, f_4), (f_3, f_4)\}.$$
By Buchberger's lcm criterion, we can safely eliminate critical pairs (f_1, f_4) and (f_2, f_4), then updated $P = \{(f_1, f_2), (f_{2,}f_3), (f_3, f_4)\}$.

Now use the normal strategy to select a critical pair, construct the S-polynomial for that pair, reduce it, and if it's non-zero add it to current G, then update the pairs P. (See Table 1.1). Here we show the details for the third row of Table 1.1.

By the Normal Strategy, we select pair (f_3, f_4) to compute for this step. The S-polynomial is

$$\begin{aligned} S(f_3, f_4) &= x_4 f_3 - f_4 \\ &= \left(\cancel{x_1x_2x_3x_4} + x_2x_3x_4^2 + x_3x_4^2x_1 + x_4^2x_1x_2\right) - \left(\cancel{x_1x_2x_3x_4} - 1\right) \\ &= x_2x_3x_4^2 + x_3x_4^2x_1 + \mathbf{x_4^2x_1x_2} + 1. \end{aligned}$$

Algorithm 3 .

```
algorithm Update the Gebauer-Möller pairs

  inputs
    $G_{old}$, a finite subset of $\mathbb{F}[x_1,\dots,x_n]$
    $F_{old}$, a finite set of critical pairs of elements of $G_{old}$
    $p$, a non-zero polynomial in $\langle G_{old} \rangle$
  outputs
    $G_{new}$, a finite subset of $\mathbb{F}[x_1,\dots,x_n]$, possibly different from $G_{old}$
    $P_{new}$, a finite set of critical pairs of $G_{new}$
  do
    Let $C := \{(p,g) : g \in G_{old}\}$
    Let $D := \{\}$
    while $C \neq \emptyset$ do
      Pick any $(p,g) \in C$ and remove it
      if $\mathrm{lm}(p)$ and $\mathrm{lm}(g)$ share no variables or no $(p,h) \in C \cup D$ satisfies
      $\mathrm{lcm}(\mathrm{lm}(p), \mathrm{lm}(h)) \mid \mathrm{lcm}(\mathrm{lm}(p), \mathrm{lm}(g))$ then
        Add $(p,g)$ to $D$
        Let $E := \emptyset$
        while $D \neq \emptyset$ do
          Pick any $(p,g) \in D$ and remove it
          if $\mathrm{lm}(p)$ and $\mathrm{lm}(g)$ share at least one variable then
            $E := E \cup (p,g)$
            Let $P_{int} := \{\}$
          while $P_{old} \neq \emptyset$ do
            Pick $(f,g) \in P_{old}$ and remove it
            if $\mathrm{lm}(p) \nmid \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$ or $\mathrm{lcm}(\mathrm{lm}(p), \mathrm{lm}(h)) = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$
            for $h \in \{f,g\}$ then
              Add $(f,g)$ to $P_{int}$
              $P_{new} := P_{int} \cup E$
              Let $G_{new} := \{\}$
              while $G_{old} \neq \emptyset$ do
                Pick any $g \in G_{old}$ and remove it
                if $\mathrm{lm}(p) \nmid \mathrm{lm}(g)$ then
                  Add $g$ to $G_{new}$
                  Add $p$ to $G_{new}$
    return $G_{new}, P_{new}$
```

Notice that the leading monomial of $S(f_3, f_4)$ is divisible by the leading monomial of f_2, so we can reduce:

$$
\begin{aligned}
S(f_3,f_4) - x_4^2 f_2 &= \left(\cancel{x_2x_3x_4^2} + x_3x_4^2x_1 + \cancel{x_4^2x_1x_2} + 1\right) - \left(\cancel{x_1x_2x_4^2} + \cancel{x_2x_3x_4^2} + x_3x_4^3 + x_4^3x_1\right) \\
&= \mathbf{x_3x_4^2x_1} + 1 - x_3x_4^3 - x_4^3x_1.
\end{aligned}
$$

Table 1.1: *Iteration of Gebauer-Möller algorithm on Cyclic-4 (See Example 1.3.1).*

CP	RR	LCM1	GCD	LCM2	updated P
(f_1,f_2)	x_2^2	$(f_2,f_5),(f_3,f_5),(f_4,f_5)$	(f_1,f_5)		$\{(f_2,f_3),(f_3,f_4)\}$
(f_2,f_3)	$x_2x_3^2$	$(f_2,f_6),(f_3,f_6),(f_4,f_6)$	(f_1,f_6)		$\{(f_3,f_4),(f_5,f_6)\}$
(f_3,f_4)	$x_2x_3x_4^2$	$(f_2,f_7),(f_3,f_7),(f_4,f_7)$	(f_1,f_7)		$\{(f_5,f_6),(f_5,f_7),(f_6,f_7)\}$
(f_5,f_6)	0				$\{(f_5,f_7),(f_6,f_7)\}$
(f_6,f_7)	$x_3^3x_4^2$	$(f_2,f_8),(f_3,f_8),(f_4,f_8),(f_7,f_8)$	$(f_1,f_8),(f_5,f_8)$		$\{(f_5,f_7),(f_6,f_8)\}$
(f_5,f_7)	$x_2x_3^2x_4^2$	$(f_2,f_9),(f_3,f_9),(f_4,f_9),(f_6,f_9),(f_8,f_9)$	(f_1,f_9)		$\{(f_6,f_8),(f_5,f_9),(f_7,f_9)\}$
(f_7,f_9)	$x_3^2x_4^4$	$(f_2,f_{10}),(f_3,f_{10}),(f_4,f_{10}),(f_7,f_{10}),(f_9,f_{10})$	$(f_1,f_{10}),(f_5,f_{10})$		$\{(f_6,f_8),(f_5,f_9),(f_6,f_{10}),(f_8,f_{10})\}$
(f_6,f_{10})	0				$\{(f_6,f_8),(f_5,f_9),(f_8,f_{10})\}$
(f_5,f_9)	0				$\{(f_6,f_8),(f_8,f_{10})\}$
(f_6,f_8)	0				$P=\{(f_8,f_{10})\}$
(f_8,f_{10})	0				$P=\{\}$

CP: critical pair selected by the Normal Strategy
RR: result of reduction, 0 or the leading monomial of a new non-zero polynomial
LCM1: new pairs eliminated by Buchberger's lcm criterion
GCD: new pairs eliminated by Buchberger's gcd criterion
LCM2: old pairs eliminated by Buchberger's lcm criterion

The leading monomial of this reduced form is divisible by the leading monomial of f_1, so we can reduce further:

$$\begin{aligned} S(f_3,f_4)-x_4^2f_2-x_3x_4^2f_1 &= \left(\cancel{x_3x_4^2x_1}+1-x_3x_4^3-x_4^3x_1\right) \\ &\quad -\left(\cancel{x_1x_3x_4^2}+x_2x_3x_4^2+x_3^2x_4^2+x_3x_4^3\right) \\ &= 1-2x_3x_4^3-x_4^3x_1-\mathbf{x_2x_3x_4^2}-x_3^2x_4^2. \end{aligned}$$

The leading monomial of this reduced form is *not* divisible by the leading monomial of f_i

for $i = 1,2,\ldots,6$, so we can reduce no further. We must add a new polynomial to the basis,

$$f_7 = -\mathbf{x_2 x_3 x_4^2} - x_3^2x_4^2 - x_1x_4^3 - 2x_3x_4^3 + 1,$$

and update P.

We start with new critical pairs $\{(f_1,f_7),(f_2,f_7,)(f_3,f_7),(f_4,f_7),(f_5,f_7),(f_6,f_7)\}$. Observe that $\mathrm{lcm}(\mathrm{lm}(f_1),\mathrm{lm}(f_7)) \mid \mathrm{lcm}(\mathrm{lm}(f_i),\mathrm{lm}(f_7))$ for $i = 2,\ldots 4$, so by Buchberger's lcm criterion, eliminate $(f_2,f_7,),(f_3,f_7),(f_4,f_7)$ [LCM1]. Also, $\mathrm{lm}(f_1)$ and $\mathrm{lm}(f_7)$ share no common variables, so by Buchberger's gcd criterion, eliminate (f_1,f_7) [GCD]. Now $P = \{(f_5,f_6),(f_5,f_7),(f_6,f_7)\}$ where (f_5,f_6) is an old pair from the previous iteration, and $\mathrm{lcm}(\mathrm{lm}(f_5),\mathrm{lm}(f_6)) = x_2^2x_3^2$. Since $\mathrm{lm}(f_7) = x_2x_3x_4^2$, we have $\mathrm{lm}(f_7) \nmid \mathrm{lcm}(\mathrm{lm}(f_5),\mathrm{lm}(f_6))$, so no old pairs are eliminated by using Buchberger's lcm criterion [LCM2]. Therefore this iteration concludes with $P = \{(f_5,f_6),(f_5,f_7),(f_6,f_7)\}$ and $G = \{f_1,f_2,f_3,f_4,f_5,f_6,f_7\}$.

Once no critical pairs are left, we have found a Gröbner Basis G such that for all $p \in \langle F\rangle$, p is top-reducible by G. Thus, $G = \{f_1,f_2,f_3,f_4,f_5,f_6,f_7,f_8,f_9,f_{10}\}$ where

$$\begin{aligned}
f_5 &= x_2^2 - x_1x_4 + x_2x_4 - x_3x_4\\
f_6 &= x_2x_3^2 - x_1x_2x_4 - x_2x_3x_4 + x_3^2x_4\\
f_7 &= -x_2x_3x_4^2 - x_3^2x_4^2 - x_1x_4^3 - 2x_3x_4^3 + 1\\
f_8 &= -x_3^3x_4^2 - x_1x_2x_4^3 - x_1x_3x_4^3 - x_2x_3x_4^3 - x_3^2x_4^3 + x_3\\
f_9 &= -x_2x_4^4 - x_4^5 + x_2 + x_4\\
f_{10} &= -x_3^2x_4^4 - x_1x_4^5 - x_3x_4^5 - x_2x_3 - x_3x_4 + x_4^2.
\end{aligned}$$

Chapter 2

THE F4 ALGORITHM AND STRATEGY FOR SELECTING CRITICAL PAIRS

Now we introduce a new algorithm for computing Gröbner Basis called F4. This algorithm was first described by Faugére in [5]. F4 replaces the traditional polynomial reduction found in Buchberger's algorithm by the simultaneous reduction of several polynomials. It uses the same mathematical principles as Buchberger's algorithm, but computes many S-polynomials in one go by forming a matrix and using linear algebra to do the reduction in parallel.

Definition 2.0.2. Let $L = [f_1, f_2, \ldots, f_s]$ be a list of polynomials. Let $\mathbf{X_L}$ be the ordered list of monomials of elements of L and n is the number of elements in X_L. Define $\mathbf{M(L)}$ as the $s \times n$ matrix where the entry in row i, column j is the coefficient of the jth element of X_L in f_i.

Example 2.0.2. Given $G = \{g_1 = \mathbf{x^2} + y,\ g_2 = \mathbf{xy^2} - xy,\ g_3 = \mathbf{y^3} - 1\}$, for the critical pair (g_1, g_2) we get a new polynomial by computing $S(g_1, g_2)$, which is $g_4 = \mathbf{x^2y} + y^3$. Recall that by Buchberger's algorithm, we do reduction as follows:

$$g_4 - yg_1 = y^3 - y^2;$$

$$y^3 - y^2 - g_3 = -y^2 + 1.$$

We also can use a matrix trangularization to do the reduction. Let $L = [g_4, yg_1, g_3]$. Then $X_L = [x^2y, y^3, y^2, 1]$. Then

$$M(L) = \left(\begin{array}{ccccc} & x^2y & y^3 & y^2 & 1 \\ S_{12} & 1 & 1 & 0 & 0 \\ yg_1 & 1 & 0 & 1 & 0 \\ g_3 & 0 & 1 & 0 & -1 \end{array}\right).$$

Triangularizing $M(L)$ gives us

$$M(L) = \left(\begin{array}{ccccc} & x^2y & y^3 & y^2 & 1 \\ S_{12} & 1 & 1 & 0 & 0 \\ yg_1 & 0 & -1 & 1 & 0 \\ g_3 & 0 & 0 & 1 & -1 \end{array}\right).$$

The first two rows correspond to polynomials whose leading monomials are already accounted for in G by g_2 and g_3. The third row $(0,0,1,-1)$ corresponds to the polynomial y^2-1 (check the labels on the columns) which is equivalent to the result above.

Faugère argues that instead of using the Normal Strategy (or any other strategy) to pick *one* critical pair at a time, we should pick *all* S-polynomials of minimal degree and process the reduction in a matrix using techniques for sparse linear algebra. That will be much more efficient than the traditional, one polynomial at a time reduction of Buchberger's algorithm. In fact Faugère used F4 to compute a Gröbner basis for Cyclic-9, which had previously been intractable. See the basic F4 algorithm 4 for pseudocode.

Algorithm 4 .

```
algorithm F4 algorithm

  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
    $G := F, F_{new} := F$ and $d := 0$
    $P := \{(f,g) \mid f,g \in G \; with \; f \neq g\}$
    $Done := \{\}$
    while $P \neq \emptyset$ do
      $d := d+1$
      $P_d := \{(f,g) \mid (f,g) \in P$ and $\deg(S(f,g)) = d\}$
      $P := P \setminus P_d$
      $L_d := Left(P_d) \cup Right(P_d)$
      $F_{new} := Reduction(L_d, G)$
      for $h \in F_{new}$ do
        $P := P \cup \{(h,g) \mid g \in G\}$
        $G := G \cup \{h\}$
    return $G$
```

Now we apply F4 algorithm to solve Cyclic-4 problem as well as using Buchberger's Criteria 1.3.

Example 2.0.3. Solve Cyclic-4 problem by F4 algorithm,

$$\begin{aligned}
f_1 &= \mathbf{x_1} + x_2 + x_3 + x_4, \\
f_2 &= \mathbf{x_1 x_2} + x_2 x_3 + x_3 x_4 + x_4 x_1, \\
f_3 &= \mathbf{x_1 x_2 x_3} + x_2 x_3 x_4 + x_3 x_4 x_1 + x_4 x_1 x_2 \\
f_4 &= \mathbf{x_1 x_2 x_3 x_4} - 1.
\end{aligned}$$

Algorithm 5 .

```
algorithm Reduction

  inputs
    $L$, a finite subset of $\mathbb{M} \times \mathbb{F}[x_1, \ldots, x_n]$
    $G$, a finite subset of $\mathbb{F}[x_1, \ldots, x_n]$
  outputs
    $F$, a finite subset of $\mathbb{F}[x_1, \ldots, x_n]$ (possible an empty set)
  do
    $F := SymbolicPreprocessing\,(L, G)$
    $F_{int:=}$ Reduction to Row Echelon Form of $F$ w.r.t $\prec$
    $F_{new} := \left\{ f \in \tilde{F} \mid \operatorname{lm}(f) \notin \langle \operatorname{lm}(F) \rangle \right\}$
  return $F_{new}$
```

Algorithm 6 .

```
algorithm SymbolicPreprocessing

  inputs
    $L$, a finite set of $\mathbb{M} \times \mathbb{F}[x_1, \ldots, x_n]$
    $G$, a finite subset of $\mathbb{F}[x_1, \ldots, x_n]$
  outputs
    $F$, a finite subset of $\mathbb{F}[x_1, \ldots, x_n]$
  do
    $F := \{t \cdot f \mid (t, f) \in L\}$ where $t \in \mathbb{M}$
    $Done := \operatorname{lm}(F)$
    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 $m$ top reducible modulo $G$ then
        Let $f \in G$ such that $\operatorname{lm}(f) \mid_L m$
        Let $m' = \frac{m}{\operatorname{lm}(f)}$
        $F := F \cup \{m' \cdot f\}$
        add the monomials of $m' \cdot f$ to $X_L$
    return $F$
```

Let $F = \langle f_1, f_2, f_3, f_4 \rangle$, $G = \{\}$, add each polynomial $g \in \langle F \rangle$ to G and update the set of critical pairs P using Buchberger's criteria 1.3. Then we have $G = \{f_1, f_2, f_3, f_4\}$, $P = \{(f_1, f_2), (f_2, f_3), (f_3, f_4)\}$. To make it easier to see which pair to choose, we will list each pair with the lcm of its leading monomials; that is,

$$P = \{(x_1x_2, f_1, f_2), (x_1x_2x_3, f_2, f_3), (x_1x_2x_3x_4, f_3, f_4)\}.$$

We pick all pairs of smallest degree; here that gives us $\{(x_1x_2, f_1, f_2)\}$. The S-polynomial of

f_1 and f_2 is $S_{12} = x_2 f_1 - f_2$. To determine L and X_L we will think about what terms might be used while reducing S_{12}. Start with $L = \{x_2 f_1, f_2\}$ and $X_L = \{\mathbf{x_1 x_2}, x_2^2, x_2x_3, x_2x_4, x_3x_4, x_1x_4\}$. Since $\mathrm{lm}(x_2 f_1) = x_1x_2$ is already accounted for in L, the only monomial that might be reduced is x_1x_4, which is divisible by f_1, so we add $x_4 f_1$ to L and its monomials to X_L. The remaining elements of X_L (including new ones) are not reducible by G, so use $L = \{f_2, x_2 f_1, x_4 f_1\}$. This gives us

$$M(L) = \left(\begin{array}{cccccccc} & x_1x_2 & x_2^2 & x_2x_3 & x_1x_4 & x_2x_4 & x_3x_4 & x_4^2 \\ x_2 f_1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ x_4 f_1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ f_2 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{array} \right).$$

Notice that triangularizing the first and third rows of $M(L)$ is equivalent to computing the S-polynomial of f_1 and f_2. Triangularizing the matrix gives

$$M(L) = \left(\begin{array}{cccccccc} & x_1x_2 & x_2^2 & x_2x_3 & x_1x_4 & x_2x_4 & x_3x_4 & x_4^2 \\ x_2 f_1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ x_4 f_1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ f_2 & 0 & -1 & 0 & 1 & -1 & 1 & 0 \end{array} \right).$$

The third row gives us the polynomial

$$f_5 = -x_2^2 + x_1x_4 - x_2x_4 + x_3x_4,$$

which matches the result of Example 1.3.1. Now $G = \{f_1, f_2, \ldots, f_5\}$. Updating the pairs gives us $P = \{(x_1x_2x_3, f_2, f_3), (x_1x_2x_3x_4, f_3, f_4)\}$.

In the next step we need to study (f_2, f_3). The S-polynomial is $S_{23} = x_3 f_2 - f_3$, so $X_L = \{x_1x_2x_3, x_2x_3^2, x_3^2x_4, x_2x_3x_4, x_3x_4x_1, x_4x_1x_2\}$. Since $x_1x_3x_4$ is reducible by $x_3x_4 f_1$, and $x_1x_2x_4$ is reducible by $x_2x_4 f_1$, add $x_3x_4 f_1$, $x_2x_4 f_1$ to L and their monomials to X_L. Update L and X_L, then we have:

$$L = \{x_2x_4 f_1, x_3x_4 f_1, x_3 f_2, f_3\}$$

$$X_L = \{x_1x_2x_3, x_2x_3^2, x_1x_2x_4, \mathbf{x_2^2 x_4}, x_1x_3x_4, x_2x_3x_4, x_3^2x_4, \mathbf{x_2 x_4^2}, \mathbf{x_3 x_4^2}\}.$$

The new monomials are highlighted. Of the new monomials only one of them is divisible by a leading monomial of other polynomials in the basis, that is, $x_2^2x_4$ is divisible by $\mathrm{lm}(f_5)$. Update L and X_L, then we have:

$$L = \{x_2x_4 f_1, x_3x_4 f_1, x_3 f_2, f_3, x_4 f_5\}$$

$$X_L = \{x_1x_2x_3, x_2x_3^2, x_1x_2x_4, x_2^2x_4, x_1x_3x_4, x_2x_3x_4, x_3^2x_4, \mathbf{x_1 x_4^2}, x_2x_4^2, x_3x_4^2\}.$$

The new monomial are highlighted, that is $x_1x_4^2$, which is divisible by $x_4^2f_1$. Update L and X_L, then we have:

$$L=\{x_2x_4f_1,x_3x_4f_1,x_4^2f_1,x_3f_2,f_{3,}x_4f_5\}$$

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

This gives us:

$$M(L)=\left(\begin{array}{ccccccccccc} & & 1 & 1 & & 1 & & & 1 & & \\ & & & & 1 & 1 & 1 & & & 1 & \\ & & & & & & & 1 & 1 & 1 & 1 \\ 1 & 1 & & & 1 & & 1 & & & & \\ 1 & & 1 & & 1 & 1 & & & & & \\ & & & -1 & & & & 1 & -1 & -1 & \end{array}\right).$$

And triangularizing this matrix gives us:

$$M(L)=\left(\begin{array}{ccccccccccc} & & 1 & 1 & & 1 & & & 1 & & \\ & & & & 1 & 1 & 1 & & & 1 & \\ & & & & & & & 1 & 1 & 1 & 1 \\ 1 & 1 & & & 1 & & 1 & & & & \\ & -1 & 1 & & & 1 & -1 & & & & \\ & & & -1 & & & & 1 & -1 & -1 & \end{array}\right)$$

The fifth row gives us the polynomial $f_6=-x_2x_3^2+x_1x_2x_4+x_2x_3x_4-x_3^2x_4$ which matches the result of Example1.3.1. Now $G=\{f_1,f_2,\ldots,f_6\}$ then updating the pairs gives us: $P=\{(x_1x_2x_3x_4,f_3,f_4),(x_2^2x_3^2,f_5,f_6)\}$. By the lowest degree strategy, we compute S-polynomial $S_{34}=x_4f_3-f_4$ and $S_{56}=x_3^2f_5-x_2f_6$. Now $L=\{x_4f_3,f_4,x_3^2f_5,x_2f_6\}$ and

$$X_L=\{x_2^2x_3^2,x_1x_2x_3x_4,\mathbf{x_1x_2^2x_4},\mathbf{x_2^2x_3x_4},\mathbf{x_1x_3^2x_4},\mathbf{x_2x_3^2x_4},$$
$$x_3^3x_4,\mathbf{x_1x_2x_4^2},\mathbf{x_1x_3x_4^2},x_2x_3x_4^2,1\}$$

Notice that $x_1x_2^2x_4$is divisible by $\operatorname{lm}(x_1x_4f_5)$, $x_2^2x_3x_4$ is divisible by $\operatorname{lm}(x_3x_4f_5)$, $x_1x_3^2x_4$ is divisible by $\operatorname{lm}\left(x_3^2x_4f_1\right)$, $x_2x_3^2x_4$ is divisible by $\operatorname{lm}(x_4f_6)$, $x_1x_2x_4^2$ is divisible by $\operatorname{lm}\left(x_4^2f_2\right)$ and $x_1x_3x_4^2$ is divisible by $\operatorname{lm}\left(x_3x_4^2f_1\right)$; update L and X_L then we have:

$$L=\{x_3^2x_4f_1,x_3x_4^2f_1,x_4^2f_2,x_4f_3,f_4,x_3^2f_5,x_1x_4f_5,x_3x_4f_5,x_2f_6,x_4f_6\}$$
$$X_L=\{x_2^2x_3^2,x_1x_2x_3x_4,x_1x_2^2x_4,x_2^2x_3x_4,x_1x_3^2x_4,x_2x_3^2x_4,x_3^3x_4,\mathbf{x_1^2x_4^2},$$
$$x_1x_2x_4^2,x_1x_3x_4^2,x_2x_3x_4^2,\mathbf{x_3^2x_4^2},\mathbf{x_3x_4^3},\mathbf{x_1x_4^3},1\}$$

Of the new monomials highlighted, $x_1^2x_4^2$ is divisible by $\operatorname{lm}\left(x_1x_4^2f_1\right)$ and $x_1x_4^3$ is divisible by $\operatorname{lm}\left(x_4^3f_1\right)$, updating L and X_L gives us :

$$L=\{x_3^2x_4f_1,\mathbf{x_1x_4^2f_1},x_3x_4^2f_1,\mathbf{x_4^3f_1},x_4^2f_2,x_4f_3,f_4,x_3^2f_5,x_1x_4f_5,x_3x_4f_5,x_2f_6,x_4f_6\}$$

$$X_L = \{x_2^2x_3^2, x_1x_2x_3x_4, x_1x_2^2x_4, x_2^2x_3x_4, x_1x_3^2x_4, x_2x_3^2x_4, x_3^3x_4, x_1^2x_4^2, x_1x_2x_4^2, x_1x_3x_4^2,$$
$$x_2x_3x_4^2, x_3^2x_4^2, x_1x_4^3, \mathbf{x_2x_4^3}, x_3x_4^3, \mathbf{x_4^4}, 1\}$$

Notice that no new monomials are divisible by a leading monomial of the polynomial in the basis in this step. So we get the 12×17 matrix:

$$M(L) = \begin{pmatrix}
 & & & & 1 & 1 & 1 & & & & & 1 & & & & & \\
 & & & & & & & 1 & 1 & 1 & & & 1 & & & & \\
 & & & & & & & & & 1 & 1 & 1 & & & 1 & & \\
 & & & & & & & & & & & & 1 & 1 & 1 & 1 & \\
 & & & & & & & & 1 & & 1 & & 1 & & 1 & & \\
 & 1 & & & & & & & 1 & 1 & 1 & & & & & & \\
 & 1 & & & & & & & & & & & & & & & -1 \\
-1 & & & & 1 & -1 & 1 & & & & & & & & & & \\
 & & -1 & & & & & 1 & -1 & 1 & & & & & & & \\
 & & & -1 & & & & & & 1 & -1 & 1 & & & & & \\
-1 & & 1 & 1 & & -1 & & & & & & & & & & & \\
 & & & & & -1 & & & 1 & & 1 & -1 & & & & &
\end{pmatrix}$$

Triangularizing this matrix gives us:

$$M(L) = \begin{pmatrix}
 & & & & 1 & 1 & 1 & & & & & 1 & & & & & \\
 & & & & & & & 1 & 1 & 1 & & & 1 & & & & \\
 & & & & & & & & & 1 & 1 & 1 & & & 1 & & \\
 & & & & & & & & & & & & 1 & 1 & 1 & 1 & \\
 & & & & & & & & 1 & & 1 & & 1 & & 1 & & \\
 & & & & & & & & & & -1 & -1 & -1 & & -2 & & 1 \\
 & 1 & & & & & & & & & & & & & & & -1 \\
-1 & & & & 1 & -1 & 1 & & & & & & & & & & \\
 & & -1 & & & & & 1 & -1 & 1 & & & & & & & \\
 & & & -1 & & & & & & 1 & -1 & 1 & & & & & \\
 & & & & & & & & & & & & & & & & \\
 & & & & & -1 & & & 1 & & 1 & -1 & & & & &
\end{pmatrix}$$

The sixth row gives us a new polynomial $f_7 = -x_2x_3x_4^2 - x_3^2x_4^2 - x_1x_4^3 - 2x_3x_4^3 + 1$ which matches the result of example 1.3.1 and note that the rank of $M(L)$ is 11 now, which means that there is one S-polynomial reduction to zero, it is S_{56}. Now $G = \{f_1, f_2, \ldots, f_7\}$ then updating the pairs gives us: $P = \{\left(x_2^2x_3x_4^2, f_5, f_7\right), \left(x_2x_3^2x_4^2, f_6, f_7\right)\}$. By the lowest degree strategy, we compute S-polynomial $S_{57} = x_3x_4^2f_5 - x_2f_7$ and $S_{67} = x_4^2f_6 - x_3f_7$. Now $L = \{x_3x_4^2f_5, x_4^2f_6, x_2f_7, x_3f_7\}$ and

$$X_L = \{x_2, x_3, x_2^2x_3x_4^2, x_2x_3^2x_4^2, x_3^3x_4^2, \mathbf{x_1x_2x_4^3}, \mathbf{x_1x_3x_4^3}, \mathbf{x_2x_3x_4^3}, x_3^2x_4^3\}$$

Note that $x_1x_3x_4^3$ is divisible by $\mathrm{lm}\left(x_3x_4^3f_1\right)$, $x_1x_2x_4^3$ is divisible by $\mathrm{lm}\left(x_4^3f_2\right)$and $x_2x_3x_4^3$ is divisible by $\mathrm{lm}\left(x_4f_7\right)$. Update L and X_L, then we have:

$$L = \{\mathbf{x_3x_4^3f_1}, \mathbf{x_4^3f_2} x_3x_4^2f_5, x_4^2f_6, x_2f_7, x_3f_7, \mathbf{x_4f_7}\}$$

$$X_L = \{x_2, x_3, \mathbf{x_4}, x_2^2x_3x_4^2, x_2x_3^2x_4^3, x_3^3x_4^2, x_1x_2x_4^3, x_1x_3x_4^3, x_2x_3x_4^3, x_3^2x_4^3, \mathbf{x_1x_4^4}, \mathbf{x_3x_4^4}\}$$

Since only one of the new monomials $x_1x_4^4$ is divisible by $\mathrm{lm}\left(x_4^4f_1\right)$. Updating L and X_L gives us:

$$L = \{x_3x_4^3f_1, \mathbf{x_4^4f_1}, x_4^3f_2, x_3x_4^2f_5, x_4^2f_6, x_2f_7, x_3f_7, x_4f_7\}$$

$$X_L = \{x_2^2x_3x_4^2, x_2x_3^2x_4^2, x_3^3x_4^2, x_1x_2x_4^3, x_1x_3x_4^3, x_2x_3x_4^3, x_3^2x_4^3, x_1x_4^4, \mathbf{x_2x_4^4}, x_3x_4^4, \mathbf{x_4^5}, x_2, x_3, x_4\}$$

We notice that no new monomials are divisible, now we have the 8×14 matrix:

$$M(L) = \left(\begin{array}{cccccccccccccc}
 & & & & 1 & 1 & 1 & & & 1 & & & & \\
 & & & & & & & 1 & 1 & 1 & 1 & & & \\
 & & & 1 & & 1 & & 1 & & 1 & & & & \\
-1 & & & & 1 & -1 & 1 & & & & & & & \\
 & -1 & & 1 & & 1 & -1 & & & & & & & \\
-1 & -1 & & -1 & & -2 & & & & & & 1 & & \\
 & -1 & -1 & & -1 & & -2 & & & & & & 1 & \\
 & & & & & -1 & -1 & -1 & & -2 & & & & 1
\end{array}\right)$$

Triangularizing this matrix gives us:

$$M(L) = \left(\begin{array}{cccccccccccccc}
 & & & & 1 & 1 & 1 & & & 1 & & & & \\
 & & & & & & & 1 & 1 & 1 & 1 & & & \\
 & & & 1 & & 1 & & 1 & & 1 & & & & \\
-1 & & & & 1 & -1 & 1 & & & & & & & \\
 & -1 & & 1 & & 1 & -1 & & & & & & & \\
 & & & & & & & & -1 & & -1 & 1 & & 1 \\
 & & -1 & -1 & -1 & -1 & -1 & & & & & & 1 & \\
 & & & & & -1 & -1 & -1 & & -2 & & & & 1
\end{array}\right)$$

We note that the seventh row is the reduction of S-polynomial S_{67}: $f_8 = -x_3^3x_4^2 - x_1x_2x_4^3 - x_1x_3x_4^3 - x_2x_3x_4^3 - x_3^2x_4^3 + x_3$ and the sixth row give us a new polynomial which is the reduction of S_{57}: $f_9 = -x_2x_4^4 - x_4^5 + x_2 + x_4$, both match the results of example 1.3.1. Now we have updated $G = \{f_1, f_2, \ldots, f_9\}$ and using Buchberger's criteria we have $P = \{\left(x_2x_3^3x_4^2, f_6, f_8\right), \left(x_2^2x_4^4, f_5, f_9\right), \left(x_2x_3x_4^4, f_7, f_9\right)\}$.

Following the previous steps will give us a new 17×23 matrix $M(L)$ whose columns represent monomials of degree six and triangularizing the matrix will give us a new polynomial f_{10}. Then we have the updated basis $G = \{f_1, f_2, \ldots, f_{10}\}$ and the set of critical pairs $P = \{(f_6, f_8), (f_5, f_9), (f_6, f_{10}), (f_8, f_{10})\}$; by constructing and triangularizing the matrix from the new L and X_L , a zero matrix will be found, which means G is a Gröbner Basis of the cyclic-4 system. At this point, we've show the main idea of the F4 algorithm for computing the Gröbner Basis.

Chapter 3

INVOLUTIVE BASES

In this chapter we describe another algorithmic approach to computing a special kind of Gröbner basis, called an *involutive basis* [9, 1]. This algorithm is based on a special concept of monomial multiplication that originates in work done on partial differential equations early in the 20th century. For each monomial, we separate the set of variables into two disjoint subsets: multiplicative and non-multiplicative. Using this criterion, some divisions are forbidden. Modifying Buchberger's algorithm to accommodate this division will allow us to compute an involutive basis.

3.1 Involutive Division

In this section we describe involutive division. We will see that there is a general concept and three specifications in general use.

Definition 3.1.1. Let $\mathbb{M}$ be the set of monomials of $\mathbb{F}[x_1,\dots,x_n]$. 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 $u, u_1 \in U$ and any $v, w \in \mathbb{M}$ the following holds:

i) $u \,|_L\, w$ implies $u \mid w$.

ii) $u \,|_L\, u$ for any $u \in U$.

iii) $u \,|_L\, (uv)$ and $u \,|_L\, (uw)$ if and only if $u \,|_L\, (uvw)$.

iv) If $u \,|_L\, w$ and $v \,|_L\, w$, then $u \,|_L\, v$ or $v \,|_L\, u$.

v) If $u \,|_L\, v$ and $v \,|_L\, w$, then $u \,|_L\, w$.

vi) If $U \subseteq V$ and $u \in U$, then $u \,|_L\, w$ with respect to V implies $u \,|_L\, w$ with respect to U.

In other words, L-division holds the following properties for any $u, v, w \in \mathbb{M}$ and any $U \subset \mathbb{M}$:

i) compatibility with ordinary division;

ii) any u is L-divisible by itself;

$$\begin{tikzcd}
 & x_1x_2^2x_4 \arrow[dl] \arrow[dr] & \\
\operatorname{lm}(f_2) = x_1x_2 \arrow[d] & & \operatorname{lm}(f_5) = x_2^2 \\
\operatorname{lm}(f_1) = x_1 & &
\end{tikzcd}$$

Two choices of paths for non-involutive division

$$\begin{tikzcd}
 & x_1x_2^2x_4 \arrow[dr] & \\
\operatorname{lm}(f_2) = x_1x_2 \arrow[d] & & \operatorname{lm}(f_5) = x_2^2 \\
\operatorname{lm}(f_1) = x_1 & &
\end{tikzcd}$$

Only one choice of path for one involutive division

$$\begin{tikzcd}
 & x_1x_2^2x_4 \arrow[dl] & \\
\operatorname{lm}(f_2) = x_1x_2 \arrow[d] & & \operatorname{lm}(f_5) = x_2^2 \\
\operatorname{lm}(f_1) = x_1 & &
\end{tikzcd}$$

Only one choice of path for a different involutive division

Figure 3.1: *Choices of paths for non-involutive division and involutive division.*

iii) v and w are L-multiplicative for u if and only if vw is L-multiplicative for u;

iv) any w has a unique chain of divisibility;

v) transitivity of L-division;

vi) when adding elements to U, any $u \in U$ can only lose L-multiples, and will never gain any.

Remark 3.1.1. The significance for property (iv) is we only have one way to do reduction by involutive division. Contrast to this Example 2.0.3 on page 15. The monomial $x_1x_2^2x_4$ can be reduced by two paths: f_1 and f_2, or f_5. According to the different rule of involutive division, we only have one choice of path. See Figure 3.1.

Definition 3.1.2. 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 3.1.2. In mathematics, × and · have the same meaning. But for involutive division, we use × instead of ordinary · to mean the involutive multiple of monomials, which differs from the conventional multiple.

In addition, let $t \in \mathbb{M}$. We denote $\deg_i(t)$ as the degree of the ith variable of t. By convention x, y, and z are interpreted as x_1, x_2, x_3.

Now we describe three different examples of involutive division introduced by Janet, Thomas, and Pommaret.

Definition 3.1.3. Given a finite set U, let

$$h_i(U) = \max\{\deg_i(u) \mid u \in U\}.$$

A variable x_i is **multiplicative in Thomas Division** (or T-multiplicative) for $u \in U$ if $\deg_i(u) = h_i(U)$ and non-multiplicative, otherwise.

Example 3.1.1. Let $U = \left\{xyz, y^2, z^3\right\}$ $(x \succ y \succ z)$. We have $h_1 = 1$; $h_2 = 2$; $h_3 = 3$.

- Since $\deg_1(xyz) = h_1$, x_1 is T-multiplicative for xyz and non-T-multiplicative for y^2 and z^3.
- Since $\deg_2\left(y^2\right) = h_2$, y is T-multiplicative for y^2 and non-T-multiplicative for xyz and z^3.
- Since $\deg_3\left(z^3\right) = h_3$, z is T-multiplicative for z^3 and non-T-multiplicative for xyz and y^2.

Definition 3.1.4. Let U be a finite set. For each $1 \le i \le n$ 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 $\deg_i(u) = \max\{\deg_i(v) \mid v \in [d_1, \ldots, d_{i-1}]\}$.

Example 3.1.2. Let $U = \left\{xyz, y^2, z^3\right\}$ $(x \succ y \succ z)$.

Table 3.1: *Three different kinds of involutive division.*

Monomial	Thomas		Janet		Pommaret	
	multiplicative (M)	non-multiplicative (NM)	M	NM	M	NM
xyz	x	y,z	x,y,z	–	z	x,y
y^2	y	x,z	y,z	x	y,z	x
z^3	z	x,y	z	x,y	z	x,y

- For $i=1$ we have $\deg_1(xyz)=\max\left\{\deg_1(xyz),\deg_1\left(y^2\right),\deg_1\left(z^3\right)\right\}$. So x is J-multiplicative for xyz.

- For $i=2$ we have $[d_1]=\{[0],[1]\}$, where

$$[0]=\left\{y^2,z^3\right\};\ [1]=\{xyz\}.$$

  So y is J-multiplicative for y^2 and xyz.

- For $i=3$ we have $[d_1,d_2]=\{[1,1],[0,2],[0,0]\}$ where

$$[1,1]=\{xyz\};[0,2]=y^2;[0,0]=z^3.$$

  So z is J-multiplicative for xyz, y^2, and z^3.

Definition 3.1.5. For a monomial $x_1^{d_1}\cdots x_k^{d_k}$ with $d_k>0$ the variables x_j with $j\geq k$ are considered to be **multiplicative in Pommaret division** (or P-multiplicative) and x_j with $j<k$ as non-multiplicative. For the monomial $u=1$, all the variables are P-multiplicative.

Example 3.1.3. Let $U=\left\{xyz,y^2,z^3\right\}$ $(x\succ y\succ z)$. By definition of Pommaret division, we can say that x is non-P-multiplicative for $xyz,y^2$and z^3; y is P-multiplicative for y^2 ; z is multiplicative for xyz, y^2, and z^3.

We summarize the different kinds of division for $U=\left\{xyz,y^2,z^3\right\}$ $(x\succ y\succ z)$ in Table 3.1.

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 3.1.4. Recall the Cyclic-4 system,

Table 3.2: Cyclic-4 Janet division.

t	M	NM
$\mathrm{lm}(f_1) = x_1$	x_1, x_3, x_4	x_2
$\mathrm{lm}(f_2) = x_1x_2$	x_1, x_2, x_4	x_3
$\mathrm{lm}(f_3) = x_1x_2x_3$	x_1, x_2, x_3	x_4
$\mathrm{lm}(f_4) = x_1x_2x_3x_4$	x_1, x_2, x_3, x_4	$-$

$$\begin{aligned} f_1 &= x_1 + x_2 + x_3 + x_4 \\ f_2 &= x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1 \\ f_3 &= x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2 \\ f_4 &= x_1x_2x_3x_4 - 1. \end{aligned}$$

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 $i = 1$, $\max_{j\in\{1,2,\ldots,4\}} \deg_1 \mathrm{lm}\left(f_j\right) = 1$ 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

  $$\max_{j\in\{1,2,3,4\}} \deg_2 \left(\mathrm{lm}\left(f_j\right)\right) = 1;$$

  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 $\max_{j\in\{2,3,4\}} \deg_3 \left(\mathrm{lm}\left(f_j\right)\right) = 1$; 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 $\max_{j\in\{3,4\}} \deg_4 \left(\mathrm{lm}\left(f_j\right)\right) = 1$; 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.

Now we summarize the results above into Table 3.2 for Janet division.

3.2 Involutive Bases of Polynomial Ideals

In this section we describe an algorithm that uses involutive division to compute a special Gröbner basis of a polynomial ideal. We first need to describe an important concept called *autoreduction.*

Definition 3.2.1. Let $G \subset \mathbb{F}[x_1,\dots,x_n]$. *G is L-autoreduced* if $\operatorname{lm}(g) \nmid_L \operatorname{lm}(g')$ for any $g, g' \in G$.

Example 3.2.1. Recall the Cyclic-4 system. Notice $\operatorname{lm}(f_1) \nmid_J \operatorname{lm}(f_2)$; $\operatorname{lm}(f_2) \nmid_J \operatorname{lm}(f_3)$; $\operatorname{lm}(f_3) \nmid_J \operatorname{lm}(f_4)$. In fact, $\operatorname{lm}(f_i) \nmid_J \operatorname{lm}\left(f_j\right)$ for $i, j = 1,2,3,4$ and $i \neq j$. By Definition 3.2.1, the initial polynomial set of the Cyclic-4 is autoreduced.

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

Definition 3.2.2. The *prolongation* of a polynomial g by a variable x is a product xg. If $x \in \mathrm{NM}(\operatorname{lm}(g))$ then the prolongation is called non-multiplicative, otherwise multiplicative.

We can now introduce a new kind of ideal basis.

Definition 3.2.3. $G \subset \mathbb{F}[x_1,\dots,x_n]$ 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 $G = \{f_1, f_2, \dots, f_m\}$,

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

Another way of saying this is that a autoreduced 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 3.2.1. Recall that in Chapter 1, the Gebauer-Möller algorithm [6] tries to compute the generators of a Gröbner Basis by constructing and reducing S-polynomials. In this chapter we use non-multiplicative prolongations and reduce them in terms of involutive division instead of S-polynomials. 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 [12]. Let $G := \emptyset$ and F be the given set of polynomial in $\mathbb{F}[x_1,\dots,x_n]$. While $F \neq \emptyset$, repeat the following:

- Let $G := \operatorname{Autoreduce}(G \cup F)$ 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.

See algorithm 7 for pseudocode.

Algorithm 7 .

algorithm *Basic algorithm of Involutive Bases*

```
  inputs
    $F$, a finite polynomial set.
  outputs
    $G$, an involutive basis of ideal $\langle F \rangle$.
  do
    $G := \emptyset$
    while $F \neq \emptyset$ do
      $G :=$ Autoreduce$(G \cup F)$
      $F := \emptyset$
      for each $g \in G$ do
        for $x_i \in \mathrm{NM}_L(\mathrm{lm}(g))$ do
          $f := \mathrm{NF}_L(g \cdot x_i, G)$
          if $f \neq 0$ then
            $F := F \cup \{f\}$
    return $G$
```

Example 3.2.2. Let F be the Cyclic-4 system. We compute an Involutive Basis of F using Janet division.

The leading monomial of f_1 has a non-multiplicative variable because $\mathrm{NM}_J = \{x_2\}$. Observe that $x_2 \cdot f_1$ is Janet-divisible by f_2, so we reduce:

$$x_2 \cdot f_1 - f_2 = x_2^2 - x_1 x_4 + x_2 x_4 - x_3 x_4.$$

We let f_5 be this new polynomial, and update the $[d_1, \ldots, d_{i-1}]$:

- For $i = 1$, $\deg_1 \mathrm{lm}(f_5) = 0 < \max_{i \in \{1,2,\ldots,5\}} \deg_1 \mathrm{lm}(f_j)$ so x_1 is not multiplicative for f_5.

- For $i=2$, $[d_1]=\{[0],[1]\}$ where $[0]=\left\{x_2^2\right\}$ and $[1]$ is the same as Example 3.1.4. So x_2 is multiplicative for f_5.
- For $i=3$, $[d_1,d_2]=\{[0,2],[1,0],[1,1]\}$ where $[0,2]=\left\{x_2^2\right\}$ and $[1,0]$ and $[1,1]$ are the same as Example 3.1.4. So x_3 is multiplicative for f_5.
- For $i=4$, $[d_1,d_2,d_3]=\{[0,2,0],[1,0,0],[1,1,0],[1,1,1]\}$ where $[0,2,0]=\left\{x_2^2\right\}$ and the remaining elements are as Example 3.1.4. So x_4 is multiplicative for f_5.

By Janet division, the only non-multiplicative variable for $\operatorname{lm}(f_5)$ is $\mathrm{NM}_J(\operatorname{lm}(f_5))=\{x_1\}$.

Update $G_{int}=G\cup\{f_5\}$; let $G=\text{Autoreduce}(G_{int})=\{f_1,f_2,f_3,f_4,f_5\}$, and pick $f_2\in G$ with $\mathrm{NM}_J(\operatorname{lm}(f_2))=\{x_3\}$. The first prolongation is reducible:

$$x_3\cdot f_2-f_3=x_2x_3^2-x_1x_2x_4-x_2x_3x_4+x_3^2x_4.$$

Let f_6 be this new polynomial. We have $\operatorname{lm}(f_6)=x_2x_3^2$, and update the $[d_1,\ldots,d_{i-1}]$:

- For $i=1$, $\deg_1\operatorname{lm}(f_6)=0<\max_{i\in\{1,2,\ldots,6\}}\deg_1\operatorname{lm}\left(f_j\right)$ so x_1 is not multiplicative for f_6.
- For $i=2$, $[d_1]=\{[0],[1]\}$ where $[0]=\left\{x_2^2,x_2x_3^2\right\}$ and $[1]$ is the same as before. So x_2 is not multiplicative for f_6.
- For $i=3$, $[d_1,d_2]=\{[0,1],[0,2],[1,0],[1,1]\}$ where $[0,1]=\left\{x_2x_3^2\right\}$ and the remaining elements are as before. So x_3 is multiplicative for f_6.
- For $i=4$, $[d_1,d_2,d_3]=\{[0,1,2],[0,2,0],[1,0,0],[1,1,0],[1,1,1]\}$ where $[0,1,2]=\left\{x_2x_3^2\right\}$ and the remaining elements are as before. So x_4 is multiplicative for f_6.

So $\mathrm{NM}_J(\operatorname{lm}(f_6))=\{x_1,x_2\}$.

Update $G_{int}=\{f_1,f_2,f_3,f_4,f_5,f_6\}$ and autoreduce G_{int}; now $G=\{f_1,f_2,f_3,f_4,f_5,f_6\}$. We study f_3 in the next step. Since $\mathrm{NM}_J(\operatorname{lm}(f_3))=\{x_4\}$, compute

$$x_4\cdot f_3-f_4=x_1x_2x_4^2+x_1x_3x_4^2+x_2x_3x_4^2\rightarrow p.$$

Now $\operatorname{lm}(p)=x_1x_2x_4^2$, since $\operatorname{lm}(f_2)\mid_J\operatorname{lm}(p)$ then reduce p into f_7 as follows:

$$p-x_4^2\times f_2=x_1x_3x_4^2-x_1x_4^3-x_3x_4^3+1$$
$$p-x_4^2\times f_2-x_3x_4^2\times f_1=-x_2x_3x_4^2-x_3^2x_4^2-x_1x_4^3-2x_3x_4^3+1\rightarrow f_7.$$

We have $\operatorname{lm}(f_7)=x_2x_3x_4^2$. We skip the details of the remaining $[d_1,\ldots,d_{i-1}]$ but now we have $\mathrm{NM}_J(\operatorname{lm}(f_7))=\{x_1,x_2,x_3\}$.

Update G and we get the autoreduced $G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7\}$; now choose f_4. For $\operatorname{lm}(f_4)$ we have $\mathrm{NM}_J(\operatorname{lm}(f_4)) = \emptyset$, so no prolongations of f_4 need be computed. Now we choose f_5 and $\mathrm{NM}_J(\operatorname{lm}(f_5)) = \{x_1\}$:

$$\begin{aligned} x_1 \cdot f_5 - x_2 \times f_2 &= -x_2^2 x_3 + x_1 x_2 x_4 - x_2 x_3 x_4 + x_1 x_4^2 \\ (x_1 \cdot f_5 - x_2 \times f_2) + x_3 \times f_5 &= x_1 x_2 x_4 + x_2 x_3 x_4 + x_1 x_4^2 + x_3 x_4^2 \\ (x_1 \cdot f_5 - x_2 \times f_2 + x_3 \times f_5) - x_4 \times f_2 &= 0. \end{aligned}$$

So $x_1 \cdot f_5$ J-reduces to 0. We turn to f_6, which has two non-multiplicative prolongations. First choose f_6 with $\mathrm{NM}_J(\operatorname{lm}(f_6)) = \{x_1, x_2\}$:

$$\begin{aligned} x_1 \cdot f_6 - x_3 \times f_3 &= -x_1 x_2 x_3 x_4 - x_2 x_3^2 x_4 - x_1 x_2 x_4^2 - x_1 x_4^3 \\ (x_1 \cdot f_6 - x_3 \times f_3) + f_4 &= -x_2 x_3^2 x_4 - x_1 x_2 x_4^2 - x_1 x_4^3 - 1 \\ (x_1 \cdot f_6 - x_3 \times f_3 + f_4) + x_4 \times f_6 &= -x_1 x_2 x_4^2 + x_3^2 x_4^2 - x_1 x_4^3 - x_2 x_4^2 - x_4^4 - 1 \\ (x_1 \cdot f_6 - x_3 \times f_3 + f_4 + x_4 \times f_6) + x_4^2 \times f_2 - f_7 &= 0. \end{aligned}$$

So $x_1 \cdot f_6$ J-reduces to 0. The next prolongation gives us,

$$x_2 \cdot f_6 - x_3^2 \times f_5 + x_4 \times f_6 + x_4^2 \times f_5 = 0.$$

So all the non-multiplicative prolongations of f_6 reduces to 0 by the current basis G.

In the following step, we compute the prolongation of $f_7 \in G$. Recall $\mathrm{NM}_J(\operatorname{lm}(f_7)) = \{x_1, x_2, x_3\}$:

$$\begin{aligned} x_1 \cdot f_7 + x_4 \times f_4 &= -x_1 x_3^2 x_4^2 - x_1^2 x_4^2 - 2 x_1 x_3 x_4^3 + x_1 - x_4 \\ (x_1 \cdot f_7 + x_4 \times f_4) + x_3^2 x_4^2 \times f_1 - x_4^2 \times f_6 &= x_3^3 x_4^2 - x_1^2 x_4^3 + x_1 x_2 x_4^3 - 2 x_1 x_3 x_4^3 \\ &\quad + x_2 x_3 x_4^3 + x_1 - x_4 \\ &\to f_8. \end{aligned}$$

Now we have $\operatorname{lm}(f_8) = x_3^3 x_4^2$ and $\mathrm{NM}_J(\operatorname{lm}(f_8)) = \{x_1, x_2\}$. Update $G_{int} = \{f_1, f_2, \ldots, f_8\}$ and $\operatorname{Autoreduce}(G_{int}) = \{f_1, f_2, \ldots, f_8\} = G$. The next prolongation $x_2 \cdot f_7$ gives us:

$$\begin{aligned} & x_2 \cdot f_7 + x_3 x_4^2 \times f_5 + x_4^2 \times f_6 + 2 x_4^3 \times f_2 \\ & \qquad + x_3 x_4^3 \times f_1 + x_4 \times f_7 - x_4^4 \times f_1 = -x_2 x_4^4 - x_4^5 + x_2 + x_4 \to f_9. \end{aligned}$$

For the new polynomial f_9 with $\operatorname{lm}(f_9) = x_2 x_4^4$, $\mathrm{NM}_J(\operatorname{lm}(f_9)) = \{x_1, x_2, x_3\}$. We have updated $G_{int} = \{f_1, f_2, \ldots, f_9\}$ and $\operatorname{Autoreduce}(G_{int}) = \{f_1, f_2, \ldots, f_9\} = G$. The final prolongation of f_7 gives us:

$$x_3 \cdot f_7 + x_4^2 \times f_6 + f_8 + x_1 x_4^3 \times f_1 - x_4^3 \times f_2 + 2 x_3 x_4^3 \times f_1 + x_4 \times f_7 + x_4^4 \times f_1 + f_9 - f_1 = 0.$$

So $x_3 \cdot f_7$ J-reduces to 0.

Now we compute the non-multiplicative prolongations of f_8. Since $\mathrm{NM}_J(\mathrm{lm}(f_8)) = \{x_1, x_2\}$, we consider $x_1 \cdot f_8$ and $x_2 \cdot f_8$. The first gives us a new polynomial, f_{10}:

$$\begin{aligned} x_1 \cdot f_8 - x_3^3 x_4^2 \times f_1 + x_3 x_4^2 \times f_6 + x_3 \times f_8 + x_1^2 x_4^3 \times f_1 & \\ -2x_1 x_4^2 \times f_2 + 2x_1 x_3 x_4^3 \times f_1 - x_4^2 \times f_4 & \\ +x_1 x_4^4 \times f_1 - x_3 x_4^4 \times f_1 - 2x_4^2 \times f_7 &= x_3^2 x_4^4 + 2x_1 x_4^5 + 2x_3 x_4^5 + x_1^2 \\ &\quad + x_1 x_3 - x_1 x_4 - x_3 x_4 - x_4^2 \\ &\to f_{10}. \end{aligned}$$

Update $G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9, f_{10}\}$ and $\mathrm{lm}(f_{10}) = x_3^2 x_4^4$. Computing $x_2 \cdot f_8$ gives us:

$$\begin{aligned} x_2 \cdot f_8 + x_3^2 \times f_7 + x_3 \times f_8 + x_4^3 \times f_2 - x_2 x_4^3 \times f_2 & \\ +x_1 x_3 x_4^3 \times f_1 - x_4^2 \times f_4 + 2x_3^2 x_4^3 \times f_1 & \\ -3x_4^3 \times f_6 - x_1 x_4^4 \times f_1 - x_4^4 \times f_2 - x_3 x_4^4 \times f_1 & \\ +2f_{10} - 2x_4^5 \times f_1 - 2x_4 \times f_9 - 2x_1 \times f_1 & \\ +f_2 - x_3 \times f_1 + 3x_4 \times f_1 &= 0. \end{aligned}$$

So $x_2 \cdot f_8$ $J-$reduces to 0.

Now we choose f_9. We know $\mathrm{lm}(f_9) = x_2 x_4^4$ with $\mathrm{NM}_J(\mathrm{lm}(f_9)) = \{x_1, x_2, x_3\}$. All non-multiplicative prolongations of f_9 J- reduce to 0, so no new polynomials result. Likewise, all the non-multiplicative prolongations of f_{10}, $x_1 \cdot f_{10}, x_2 \cdot f_{10}$ and $x_3 \cdot f_{10}$ J- reduce to 0, so no new polynomial results in these two loops.

We have verified that all the non-multiplicative prolongations of elements in G reduce to zero with respect to the Janet division, which means that $G = \{f_1, f_2, \ldots, f_{10}\}$ is an Janet Basis for the Cyclic-4 system.

Remark 3.2.2. In the step reducing $x_4 \cdot f_3$ of the previous example, in both Buchberger's algorithm and F4, we could choose either f_1 or f_2 to reduce p. However, $\mathrm{lm}(p)$ is not a Janet multiple of f_1 because x_2 is non-multiplicative for Janet division. Thus we *have* to use f_2 to reduce p.

In the previous example, f_8 has the same leading monomial as the f_8 generated by Buchberger's algorithm (see Example 1.3.1 on page 6) but using a different S-polynomial pair: $(4,7)$ instead of $(6,7)$. We get a different polynomial and thus a different basis of the ideal, but it is still an involutive basis, and thus a Gröbner basis. This illustrates how one ideal can have more than one Gröbner basis.

3.3 Computing an Involutive Basis with Buchberger's Criteria

The algorithm of Section 3.2 above is a basic method for computing an involutive basis. We can see that 10 out of 15 non-multiplicative prolongations reduce to zero, and thus make no contribution to our work. So now we describe an improved algorithm that avoids unnecessary reductions in Example 3.2.2 by applying *Buchberger's lcm criterion.*

Definition 3.3.1. Let $\mathbb{T} = \{au \mid u \in \mathbb{M}, a \in \mathbb{R}\}$ be the set of terms in $\mathbb{F}[x_1, \ldots, x_n]$. Let L be an involutive division L on $\mathbb{M}$ and let F be a finite set of polynomials. We say:

- p is *L-reducible modulo* $f \in F$ if p has a term $t = au \in \mathbb{T}\,(a \neq 0)$ such that $u = \mathrm{lm}(f) \times v$, for some $v \in \mathrm{M}_L(\mathrm{lm}(f))$ in F. It yields the L-reduction $p \to g = p - (a/\mathrm{lc}(f))\, f \times v$.

- p is *L- reducible modulo F* if there exists $f \in F$ such that p is L-reducible modulo f.

- p is in L-Normal Form *modulo F* if p is not L-reducible modulo F and we denote p as $p = \mathrm{NF}_L(f, F)$.

Now we describe a new version of Buchberger's lcm criterion regarding involutive division.

Definition 3.3.2. Let $u \in \mathbb{M}$, $\deg(u) = \sum_{i=1}^{n} \deg_i(u)$ be the total degree of all the variables of u. An *ancestor* of a polynomial $f \in F \subset \mathbb{R} \setminus \{0\}$ is a polynomial $g \in F$ of the smallest $\deg(\mathrm{lm}(g))$ among those satisfying $f = g \cdot u$ modulo $\langle F \setminus \{f\} \rangle$ with $u \in \mathbb{M}$. If $\deg(\mathrm{lm}(g)) < \deg(\mathrm{lm}(f))$ $(u \neq 1)$ the ancestor g of f is called proper.

Recall that in Chapter 1 we state Buchberger's lcm criterion in normal sense; here we give a different statement of Buchberger's lcm criterion in involutive version.

Theorem 3.3.1 (*[7]*)**.** Let F be a finite L-autoreduced polynomial set, and let $p = x \cdot g$ be a non-multiplicative prolongation of $g \in F$. Then $\mathrm{NF}_L(x \cdot g, F) = 0$ if there exists a different polynomial $f \in F$ and

- $\mathrm{lm}(\mathrm{anc}(p)) \cdot \mathrm{lm}(\mathrm{anc}(f)) = \mathrm{lm}(\mathrm{pol}(p))$*; or*

- $\mathrm{lcm}(\mathrm{lm}(\mathrm{anc}(p)), \mathrm{lm}(\mathrm{anc}(f)))$ *properly divides* $\mathrm{lm}(\mathrm{pol}(p))$.

Now we can use Buchberger's lcm criterion to compute an involutive basis. Before the computation, we create for each element f in the intermediate set of polynomials the triplet structure

$$p = (f, g, vars)$$

where $\operatorname{pol}(p) = f$; $\operatorname{anc}(p) = g$ is a polynomial ancestor of f in F; $vars = \operatorname{nmp}(p)$ is a (possibly empty) set of variables. The set $\operatorname{nmp}(p)$ associated with polynomial f accumulates those non-multiplicative variables that have already been used to construct non-multiplicative prolongations.

We compute an involutive basis by repeating the following:

- Divide all elements in F into two sets, T and Q: choose $f \in F$ without proper divisor of $\operatorname{lm}(f)$ in the rest of the elements' leading monomials in F and add triplet of f to T. Let Q be the set of all other triplets of $q \in F \setminus \{f\}$.
- Top-reduce Q by T in an involutive division, then let Q be the set of top-normal forms from Q.
- Choose $p \in Q$ without proper divisors of $\operatorname{lm}(\operatorname{pol}(q))$ in $\operatorname{lm}(\operatorname{pol}(Q)) \setminus \{\operatorname{lm}(\operatorname{pol}(q))\}$ and remove q from Q.
- Apply Buchberger's lcm criterion (Theorem 3.3.1) to add triplets of elements in T to Q.
- Tail-reduce p by T in an involutive division then let h be the tail-normal form of h, add triplet $(h, \operatorname{anc}(p), \operatorname{nmp}(p))$ to T.
- For all $q \in T$ compute the non-multiplicative prolongation $x \cdot \operatorname{pol}(q)$ where $x \in \operatorname{NM}_L(q,T) \setminus \{\operatorname{nmp}(q)\}$ and add the triplet of this prolongation to Q and add x to the set $\operatorname{nmp}(q)$.
- Top-reduce Q by T in an involutive division.
- Return all first entries in the triplets of T.

Definition 3.3.3. A *minimal involutive basis* is an involutive basis such that $\operatorname{lc}(p) = 1$ for all $p \in G$ and for all $p \in G$, $\operatorname{lm}(p)$ is not L-divisible by any $q \in G \setminus \{p\}$.

See Algorithm 8 for pseudocode.

Example 3.3.2. Let F be the Cyclic-4 system. Now we compute an involutive basis using Janet division of G.

Recall that $F = \{f_1, f_2, f_3, f_4\}$, choose $f_1 \in F$. Then $T = \{(f_1, f_1, \emptyset)\}$ and

$$Q = \{(f_2, f_2, \emptyset), (f_3, f_3, \emptyset), (f_4, f_4, \emptyset)\}.$$

Since x_2 is non-multiplicative for f_1, J-top-reduction of Q is

$$Q = \{(f_2, f_2, \emptyset), (f_3, f_3, \emptyset), (f_4, f_4, \emptyset)\}.$$

Algorithm 8 .

```
algorithm Involutive Basis with Buchberger's criteria

  inputs
    $F$, a finite polynomial set
  outputs
    $G$, an minimal involutive basis of the ideal $\langle F\rangle$
  do
    Choose $f \in F$ without proper divisors of $\mathrm{lm}(f)$ in $\mathrm{lm}(F)\setminus\{\mathrm{lm}(f)\}$
    $T := \{(f,f,\emptyset)\}$
    $Q := \{(q,q,\emptyset) \mid q \in F\setminus\{f\}\}$
    $L$-Top reduce $Q$ by $T$, checking Buchberger's criteria and changing ancestors of reduced
    polynomials to themselves.
    while $Q \neq \emptyset$ do
      choose $p \in Q$ without proper divisors of $\mathrm{lm}(\mathrm{pol}(p))$ in $\mathrm{lm}(\mathrm{pol}(Q))\setminus\{\mathrm{lm}(\mathrm{pol}(p))\}$
      $Q := Q\setminus\{p\}$
      if $\mathrm{pol}(p) = \mathrm{anc}(p)$ then
        for all $q \in T$ such that $\mathrm{lm}(\mathrm{pol}(p))$ properly divides $\mathrm{lm}(\mathrm{pol}(q))$ do
          $Q := Q \cup \{q\}$
          $T := T\setminus\{q\}$
      Let $h$ be the $L$-tail reduction of $p$ by $T$
      $T := T \cup \{(h, \mathrm{anc}(p), \mathrm{nmp}(p))\}$
      for all $q \in T$ and $x \in \mathrm{NM}_L(q,T)\setminus\mathrm{nmp}(q)$ do
        $Q := Q \cup \{(\mathrm{pol}(q)\cdot x, \mathrm{anc}(q), \emptyset)\}$
        $\mathrm{nmp}(q) := \mathrm{nmp}(q) \cap \mathrm{NM}_L(q,T) \cup \{x\}$
      $L$-top reduce $Q$ by $T$ and checking Buchberger's criteria.
    return  $\{\mathrm{pol}(f) \mid f \in T\}$ or $\{\mathrm{pol}(f) \mid f \in T \mid f = \mathrm{anc}(f)\}$
```

- Loop 1: choose $(f_2, f_2, \emptyset) \in Q$ and update $Q = \{(f_3, f_3, \emptyset), (f_4, f_4, \emptyset)\}$; there does not exist $q \in T$ such that $\mathrm{lm}(\mathrm{pol}(f_2))$ properly divides $\mathrm{lm}(\mathrm{pol}(q))$.

  - Now J- tail-reduce f_2 by T:

    $$f_2 - x_4 \times f_1 = x_1x_2 + x_2x_3 - x_2x_4 - x_4^2.$$

    Let f_5 be the new polynomial, so $f_5 = x_1x_2 + x_2x_3 - x_2x_4 - x_4^2$ and update $T = \{(f_1, f_1, \emptyset), (f_5, f_2, \emptyset)\}$.

  - Now we compute the non-multiplicative prolongations of $f_1, f_5 \in T$. Since $\mathrm{NM}_J(f_1, T) = \{x_2\}, \mathrm{NM}_J(f_5, T) = \emptyset$, we only compute $x_2 \cdot f_1$ in this loop, which gives us:

    $$x_2 \cdot f_1 = x_1x_2 + x_2^2 + x_2x_3 + x_2x_4.$$

Update Q into $Q = \{(f_3, f_3, \emptyset), (f_4, f_4, \emptyset), (x_2 \cdot f_1, f_1, \emptyset)\}$ and update $\mathrm{nmp}(f_1) = \{x_2\}$.

- Now J-top-reduce Q by T:

$$x_2 \cdot f_1 - f_5 = x_2^2 + 2x_2x_4 + x_4^2 \rightarrow f_6.$$

Checking Buchberger's criteria gives us: $\mathrm{lm}(f_2) \cdot \mathrm{lm}(f_1) \neq \mathrm{lm}(x_2 \cdot f_1)$ and $\mathrm{lcm}(\mathrm{lm}(f_1), \mathrm{lm}(f_2))$ does not divides $\mathrm{lm}(x_2 \cdot f_1)$, since $\mathrm{NF}_J(x_2 \cdot f_1) = f_6 \neq 0$ and $\mathrm{lm}(\mathrm{pol}(x_2 \cdot f_1)) \neq \mathrm{lm}(f_6)$, remove $(x_2 \cdot f_1, f_1, \emptyset)$ from Q and add $(f_6, f_6, \emptyset)$ to Q. Note that f_6 has the same leading monomial as f_5 we computed in Example 3.2.2 and it passes through the main loop then is added to T.

- Loop 2: now we have $T = \{(f_1, f_1, \{x_2\}), (f_5, f_2, \emptyset)\}$; choose $(f_3, f_3, \emptyset) \in Q$ and update $Q = \{(f_4, f_4, \emptyset), (f_6, f_6, \emptyset)\}$; there does not exist $q \in T$ such that $\mathrm{lm}(\mathrm{pol}(f_3))$ properly divides $\mathrm{lm}(\mathrm{pol}(q))$.

  - Now J- tail-reduce f_3 by T:

$$f_2 - x_3 \times f_5 - x_3x_4 \times f_1 = -x_2x_3^2 + x_2x_3x_4 - x_3^2x_4 \rightarrow f_7.$$

  where $f_7 = \mathrm{NF}_J(f_3, T)$. Update $T = \{(f_1, f_1, \{x_2\}), (f_5, f_2, \emptyset), (f_7, f_3, \emptyset)\}$.

  - Now we compute the non-multiplicative prolongations of $f_1, f_5, f_7 \in T$. Since $\mathrm{NM}_J(f_1, T) \setminus \{x_2\} = \emptyset, \mathrm{NM}_J(f_5, T) = \emptyset, \mathrm{NM}_J(f_7, T) = \{x_1\}$, so update Q into $Q = \{(f_4, f_4, \emptyset), (f_6, f_6, \emptyset), (x_1 \cdot f_7, f_3, \emptyset)\}$ and update $\mathrm{nmp}(f_7) = \{x_1\}$.

  - Now J-top-reduce Q by T:

$$f_4 - x_3x_4 \times f_5 = -x_2x_3^2x_4 + x_2x_3x_4^2 + x_3x_4^3 - 1 \rightarrow f_8.$$

  add $(f_8, f_8, \emptyset)$ to Q; $f_6 \in Q$ is irreducible by T, so return f_6 ; top-reduce $x_1 \cdot f_7$ by T, which gives us $\mathrm{NF}_J(x_1 \cdot f_7, T) = 0$, so update $Q = \{(f_8, f_8, \emptyset), (f_6, f_6, \emptyset)\}$ and $T = \{(f_1, f_1, \{x_2\}), (f_5, f_2, \emptyset), (f_7, f_3, \{x_1\})\}$.

- Loop 3: choose $(f_8, f_8, \emptyset) \in Q$ and update $Q = \{(f_6, f_6, \emptyset)\}$. Similarly, there does not exist $q \in T$ such that $\mathrm{lm}(\mathrm{pol}(f_8))$ properly divides $\mathrm{lm}(\mathrm{pol}(q))$.

  - Now J- tail-reduce f_8 by T:

$$f_8 - x_4 \times f_7 = x_3^2x_4^2 + x_3x_4^3 - 1 \rightarrow f_9$$

  Update $T = \{(f_1, f_1, \{x_2\}), (f_5, f_2, \emptyset), (f_7, f_3, \{x_1\}), (f_9, f_8, \emptyset)\}$.

- Now we compute the non-multiplicative prolongations of all elements in T. Since $\mathrm{NM}_J(f_9,T)=\{x_1,x_2\}$ and the non-multiplicative variables for f_1,f_5,f_7 are the same as before; add triplet of $x_1\cdot f_9$ and $x_2\cdot f_9$ to Q, then update $Q=\{(f_6,f_6,\emptyset),(x_1\cdot f_9,f_8,\emptyset),(x_2\cdot f_9,f_8,\emptyset)\}$ and $\mathrm{nmp}(f_9)=\{x_1,x_2\}$.
- Now J-top-reduce Q by T : f_6 is irreducible, return f_6;

  $$x_1\cdot f_9 = x_1x_3^2x_4^2+x_1x_3x_4^3-x_1 \longrightarrow f_{10}.$$

  This new polynomial f_{10} is J-irreducible modulo G, so return f_{10};

  $$x_2\cdot f_9 = x_2x_3^2x_4^2+x_2x_3x_4^3-x_2.$$

  We see that $\mathrm{lm}(f_7)\mid_J \mathrm{lm}(x_2\cdot f_9)$ and $\mathrm{lm}(x_2\cdot f_9)\neq \mathrm{lm}(\mathrm{anc}(x_2\cdot f_9))$. Checking Buchberger's criteria gives us:

  $$\mathrm{lm}(\mathrm{anc}(x_2\cdot f_9))\cdot\mathrm{lm}(\mathrm{anc}(f_7))\neq \mathrm{lm}(\mathrm{pol}(x_2\cdot f_9))$$

  and as $\mathrm{lcm}(\mathrm{lm}(\mathrm{anc}(x_2\cdot f_9),\mathrm{lm}(\mathrm{anc}(f_7))))$ does not J-divide $\mathrm{lm}(\mathrm{pol}(x_2\cdot f_9))$ properly, return $x_2\cdot f_9$. Update Q into:

  $$Q=\{(f_6,f_6,\emptyset),(x_1\cdot f_9,f_8,\emptyset),(x_2\cdot f_9,f_8,\emptyset)\}$$

  and $T=\{(f_1,f_1,\{x_2\}),(f_5,f_2,\emptyset),(f_7,f_3,\{x_1\}),(f_9,f_8,\{x_1,x_2\})\}$.

- Following previous steps until $Q=\emptyset$, we will have five more triplets of new polynomials added to T, return the set $\{\mathrm{pol}(f)\mid f\in T\}$, it results in a minimal involutive basis of Cyclic-4, that is $G=\{g_1,g_2,\ldots,g_7\}$ where

$$\begin{aligned}
g_1 &= x_1+x_2+x_3+x_4;\\
g_2 &= x_2^2+2x_2x_4+x_4^2;\\
g_3 &= -x_2x_3^2-x_3^2x_4+x_2x_4^2+x_4^3;\\
g_4 &= x_2x_3x_4^2+x_3^2x_4^2-x_2x_4^3+x_3x_4^3-x_4^4-1;\\
g_5 &= x_2x_4^4+x_4^5-x_2-x_4;\\
g_6 &= x_3^3x_4^2+x_3^2x_4^3-x_3-x_4;\\
g_7 &= x_3^2x_4^4+x_2x_3-x_2x_4+x_3x_4-2x_4^2.
\end{aligned}$$

Chapter 4

AN F4-STYLE INVOLUTIVE BASIS ALGORITHM

Recall that in chapter 3 we used F4 algorithm to compute Gröbner Basis for Cyclic-4 problem in Example 2.0.3 and in the previous chapter we introduced involutive division which can improve the efficiency of computing the Involutive Basis. In this chapter we describe another algorithm based on combining these two algorithms in order to obtain a faster approach.

4.1 Algorithm

Recall the definition of *prolongation* Definition 3.2.2 on page 24.

Definition 4.1.1. The degree of prolongation $x \cdot p$ is

$$\deg\left(x \cdot p\right) = \deg\left(x \cdot \mathrm{lm}\left(p\right)\right).$$

Using this definition, we compute an F4-style involutive basis by combining F4 algorithm and basic Involutive Basis algorithm 7 as follows:

- As a modified algorithm from F4, 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 of minimal degree for the sparse matrix.

- As a modified algorithm from Involutive Basis I, this new approach inherits from the old approach of reducing a non-multiplicative prolongation in each step and autoreducing. However, instead of picking one prolongation in each step, we choose several prolongations and process the reduction by multiplicative prolongations using the matrix.

See Algorithms 9, 10, and 11 for pseudocode.

We see that algorithm 9 is a modified standard F4 algorithm [5] in which the use of critical pairs is replaced by non-L-multiplicative prolongations, that is, instead of finding the set of critical pairs in the traditional way, we select the similar set of fewer pairs by

Algorithm 9 .

```
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
    $G := F$
    $P := \{x_i \cdot f \mid f \in G$ 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 $P \backslash Done$
      $P_d := \{x_i \cdot p \mid x_i \cdot p \in P$ and $\deg(x_i \cdot p) = d\}$
      $F_{new} := Reduction(P_d, G)$
      $Done := Done \cup P_d$
      $G := G \cup F_{new}$
      $P := (\{x_i \cdot f \mid f \in G$ with $x_i \in \mathrm{NM}_L(\mathrm{lm}(f))\}$
               $\cup \{u \times f \mid u\mathrm{lm}(f) = \mathrm{lm}(g)\ \ f \neq g \in G\}) \backslash Done$
    return $G$
```

Algorithm 10 .

```
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 polynomials resulting
    $F_{new} := \left\{f \in \tilde{F} \mid \mathrm{lm}(f) \notin \langle \mathrm{lm}(F) \rangle\right\}$
    return $F_{new}$
```

involutive division, since some pairs are forbidden. For the sub-algorithm of *Reduction* and *SymbolicPreprocessing*, see the pseudocode of algorithm 10 and algorithm 11.

We know that each row of the constructed matrix in algorithm 10 is an element of P_d, a polynomial. But we have to take care that which rows should be reduced and which rows should not be. In order to reduce the existing non-L-multiplicative pairs of p, (x_i, p) for $i \in \{1,2,\ldots,n\}$ and $p \in G$, so we denote P_d as the set of all these pairs of minimal degree and put their products in the last rows of the matrix $M(P_d)$. We call these F_{NM}. Let the set of the J-multiplicative products which can reduce be F_M, then reduce F_{NM} by F_M using row elimination. Remark that here column swaps are not allowed since only row eliminations reduce the polynomials.

Algorithm 11 .

```
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 $\operatorname{lm}(f) \mid_L m$
        Let $m' = \frac{m}{\operatorname{lm}(f)}$
        $F := F \cup \{m' \times f\}$
        add the monomials of $m' \times f$ to $X_L$
    return  $F \setminus F_{NM}, F_{NM}$
```

4.2 Example

Example 4.2.1. Let $F = \{f_1, f_2, f_3, f_4\}$ be the Cyclic-4 system. We compute an Involutive Basis of F using F4-style involutive method in Janet division. Recall that in Chapter 2 X_L denotes an ordered list of all the monomials required for the construction of matrix $M(L)$, here we use X_{intL} as the intermediate list of X_L and $M(P_d)$ as the matrix of monomials of degree d.

$$f_1 = x_1 + x_2 + x_3 + x_4$$

$$f_2 = x_1x_2 + x_2x_3 + x_3x_4 + x_1x_4$$

$$f_3 = x_1x_2x_3 + x_2x_3x_4 + x_1x_3x_4 + x_1x_2x_4$$

$$f_4 = x_1x_2x_3x_4 - 1.$$

Recall that Table 3.2 has 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 $G = F$.

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 $F_{NM} = P_2$

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

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

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

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

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

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

Triangularizing $M(P_2)$ gives us:

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

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 $\operatorname{lm}(f_5) \notin \langle \operatorname{lm}(G) \rangle$. 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:

$$X_{intL} = \left\{\mathbf{x_1x_2x_3}, \mathbf{x_1x_3x_4}, x_2x_3^2, x_3^2x_4, \mathbf{x_1x_2^2}, \mathbf{x_1x_2x_4}, \mathbf{x_1x_4^2}\right\}$$

We can see that there are five monomials in bold that are J-reducible by $\{\operatorname{lm}(G)\}$. So add all the monomials of $f_3, x_3x_4f_1, x_2f_2, x_4f_2, x_4^2f_1$ to X_{intL} and update F_M into:

$$F_M = \left\{(1, f_3), (x_3x_4, f_1), (x_2, f_2), (x_4, f_2), \left(x_4^2, f_2\right)\right\};$$

$X_{intL} = \left\{x_1x_2x_3, x_1x_3x_4, x_2x_3^2, x_2x_3x_4, x_3^2x_4, x_1x_2^2, x_1x_2x_4, x_1x_4^2, \mathbf{x_2^2x_3}, x_2x_4^2, x_3x_4^2, x_4^3\right\}$ where x_1x_4 is J-reducible by $\operatorname{lm}(x_3 \cdot f_5)$ then update X_{intL} and add $Pair(x_3, f_5)$ to F_M. We have the updated X_{intL} :

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

Now all the elements in X_{intL} have been checked and no more monomials are necessary to add to X_{intL}. So we have obtained all the rows needed for the matrix $M_{8\times 12}(P_3)$.

$$M(P_3) = \left(\begin{array}{cccccccccccc c} f_3 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ x_2f_2 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ x_4f_2 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ x_3x_4f_1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ x_4^2f_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ x_3f_5 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 \\ x_3f_2 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ x_1f_5 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right).$$

Triangularizing $M(P_3)$ gives us:

$$M(P_3) = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We see that the eighth row has been reduced to zero and the seventh row is reduced into a new polynomial, we say it as $f_6 = x_2x_3^2 + x_3^2x_4 - x_2x_4^2 - x_4^3$ where $\text{lm}(f_6) \notin \langle \text{lm}(G) \rangle$. 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, **loop 3** computes F_M for $P_4 = \{(x_4, f_3), (x_1, f_6), (x_2, f_6)\}$ which gives us a 12×16 matrix $M(P_4)$ whose columns represent monomials of degree four and trangularizing the matrix will give us a new polynomial $f_7 = x_2x_3x_4^2 + x_3^2x_4^2 - x_2x_4^3 + x_3x_4^3 - x_4^4 - 1$. Then we have the updated basis $G = \{f_1, f_2, \ldots, f_7\}$ and the set of non-J-multiple pairs $P = P_5 = \{(x_1, f_7), (x_2, f_7), (x_3, f_7)\}$. In **loop 4**, symbolic preprocessing will give us a 13×18 matrix $M(P_5)$ and trangularizing the matrix will give us two new polynomials: f_8 and f_9.

$$\begin{aligned} f_8 &= x_3^3x_4^2 - x_3^2x_4^3 + 2x_3 + 2x_4; \\ f_9 &= x_2x_4^4 + x_4^5 - x_2 - x_4. \end{aligned}$$

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 20×23 matrix $M(P_6)$, then trangularizing the matrix results in a new polynomial of degree 6. We say it as f_{10}:

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

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 $G = \{f_1, f_2, \ldots, f_{10}\}$ is an involutive basis of the Cyclic-4 system. At this point, we have shown the main idea of the algorithm of F4-style involutive basis.

4.3 Termination and Correctness

Theorem 4.3.1. *If Involutive Basis I algorithm 7 on page 25 terminates correctly, then so does F4-style involutive basis algorithm.*

Proof. Assume that Involutive Basis I algorithm terminates on $\mathbb{F}[x_1, \ldots, x_n]$.

Since the F4-style involutive algorithm generates the same polynomials as the involutive basis I algorithm, but uses a matrix to reduce more than one polynomial in any step, eventually there will be no new polynomials resulted from the triangularized matrix. This proves the termination of the algorithm.

For correctness, recall from the definition of Gröbner Basis (Definition 1.2.1) that if all the S-polynomials in G can be top-reduced to zero by G then G is a Gröbner Basis. In this algorithm, we do reduction for each prolongation. If one does not reduce to zero, we add it to the basis. And we can see that every S-polynomial is the first reduction of a non-multiplicative prolongation or an autoreduction.

Let $1 \leqslant i < j \leqslant \#G$, where $\#G$ means the size of the set G. Let $S = S\left(g_i, g_j\right)$ for $g_i, g_j \in G$. Since S is a first reduction of a non-multiplicative prolongation and every prolongation reduces to zero then S reduces to zero. Therefore, output of this algorithm is a Gröbner Basis of input G. □

Remark 4.3.1. Not all involutive divisions lead the algorithm terminates but Janet division does[8, 7]. So Janet division is an involutive division which can make this algorithm terminate.

Chapter 5

SOURCE CODE

```
def monomial_cmp(t,u):
  if (t+u).lm()==t:
    result = int(-1)
  elif t==u:
    result = int(0)
  else:
    result = int(1)
  return result

def determine_non_multiplicatives(xi,S):
  # expects S to be a set of leading monomials such that
  #   for all j < i, for all t in S, deg(t,xj) is constant
  # modifies rules so that if deg(t,xi) is not maximal,
  #   xi is non-multiplicative for t
  # first find maximal degree of xi in S
  di = 0
  for t in S:
    if t.degree(xi) > di:
      di = t.degree(xi)
  # now assign xi non-mult for each t such that
  #   deg(t,xi) < di
  for t in S:
    if not (xi in rules[t]):
      if t.degree(xi) < di and t != 0:
        rules[t].add(xi)
      elif t == 0:
        rules[t] = set()
  return
```

```
def setup_rules_Janet(T):
  global rules
  # initialize rules to no non-mult vars
  #rules = {}
  for p in T:
    if not rules.has_key(p):
      rules[p.lm()] = set([])
  # get variables of poly ring
  vars = T[0].parent().gens()
  # get lms of T
  lms = [each.lm() for each in T]
  # determine for which terms x1 is non-multiplicative
  determine_non_multiplicatives(vars[0], lms)
  # determine for which terms
  # the rest of the vars are non-multiplicative
  for i in range(len(vars)-1):
    lms_tmp = copy(lms)
    vars_i = vars[0:i+1]
    while len(lms_tmp) != 0:
      t = lms_tmp.pop()
      S = [t]
      j = 0
      while j < len(lms_tmp):
        u = lms_tmp[j]
        if all(u.degree(xk) == t.degree(xk) for xk in vars_i):
          S.append(u)
          lms_tmp.pop(j)
        else:
          j += 1
      determine_non_multiplicatives(vars[i+1], S)
  return

def J_NM(f):
  return rules[f.lm()]

L_NM = J_NM
```

```
setup_rules = setup_rules_Janet

def L_divisible(u,f):
  t = f.lm()
  if (t.divides(u)):
    q = (u/f.lm()).numerator().variables()
    if len(set(q).intersection(L_NM(f))) != 0:
      return False
    else:
      return True
  else:
    return False

def Prolongation(F):
    P = set()
    for f in F:
        if L_NM(f) != set():
            for xi in L_NM(f):
              P.add((xi,f))
    #add autoreduction to P
    for f in F:
       for g in F:
         if (f != g) and (L_divisible(g.lm(), f)):
            u=(g.lm()/f.lm()).numerator()
            P.add((u,f))
    return P

def minimum_deg(P):
   di = infinity
   for (u,f) in P:
      if f.lm().degree()+1 < di:
         di = f.lm().degree()+1
   return di

def F4_matrix(polys):
  # modify this so that it recognizes pairs (u,f)
  # instead of polynomials: polys = { (u1,f1), (u2,f2),   .}
  L=[]
  mons=set()
  for (u,f) in polys:
    p = u*f
    mons.update(p.monomials())
    L.append(p)
  mons = list(mons)
  mons.sort(lambda t,w: monomial_cmp(t,w))
  mons_dict={}
  for each in range(len(mons)):
    mons_dict.update({mons[each]:each})
  M = matrix(mons[0].parent(),len(L),len(mons))
  for i in range(len(L)):
    p=L[i]
    pmons=p.monomials()
    pcoeffs=p.coefficients()
    for j in range(len(pmons)):
      M[i,mons_dict[pmons[j]]]=pcoeffs[j]
  return M,mons

def triangularize_matrix(M):
  # M is a matrix
  # triangularization does not swap columns
  N=M.copy()
  m=N.nrows()
  n=N.ncols()
  print "triangularizing", m, "x", n, "matrix"
  for j in range(n):
    pivot=0
    while pivot < m and (N[pivot,j] == 0 or\
        any(N[pivot,k] != 0 for k in range(j))):
      pivot = pivot+1
    if pivot < m:
      a = N[pivot,j]
      for i in range(m):
        if i != pivot:
          if N[i,j] != 0:
            b = N[i,j]
            for k in range(j):
              N[i,k] *= a
            for k in range(j,n):
              N[i,k] = a*N[i,k] - b*N[pivot,k]
  return N

def extract_polys(M,mons,F):
  # M is a matrix
  # mons is a list of monomials corresponding to the columns
  # F is an old basis of the ideal
  # returns polynomials of M * mons whose leading terms
  #   are not in <lt(F)>
  L=[]
  for i in range(M.nrows()):
    if not M.row(i).is_zero():
      j=0
      while(M[i,j]==0):
        j=j+1
      if(not any(f.lm().divides(mons[j]) for f in F)):
        p=0
        for j in range(M.ncols()):
          if M[i,j]!=0:
            p=p+M[i,j]*mons[j]
        L.append(p)
  return L

def Triangularize(Fnm,Fm,G):
    FF = Fm.union(Fnm)
    M, mons = F4_matrix(FF)
    N = triangularize_matrix(M)
    new_polys = extract_polys(N,mons,G)
    return new_polys
```

```
def Symbolic_Preprocessing(Pd,G):
    F = copy(Pd)
    Fnm = F
    Done = set()
    XL = set()
    for (u,f) in F:
      for t in f.monomials():
        XL.add(t*u)
    while XL != Done:
       for m in XL.difference(Done):
          Done.add(m)
          for g in G:
             if L_divisible(m,g):
                 mm = (m/g.lm()).numerator()
                 F.add((mm,g))
                 for t in g.monomials():
                   XL.add(t*mm)
    Fm = F.difference(Fnm)
    print "XL =", XL
    return Fm,Fnm

def Reduction(Pd,G):
    Fm,Fnm = Symbolic_Preprocessing(Pd,G)
    Fnew = Triangularize(Fnm,Fm,G)
    return Fnew

def F4_involutive_basis (F):
    # call update rules
    global rules
    rules = {}
    setup_rules_Janet(F)
    G = copy(F)
    P = Prolongation(G)
    Done = set()
    while len(P)!=0:
        Pd = set()
        di= minimum_deg(P)
        print "degree", di
        for (u,f) in P:
          if f.lm().degree()+1 == di and f.lm() != 0:
             Pd.add((u,f))
        P.difference_update(Pd)
        Fnew = Reduction(Pd,G)
        Done.update(Pd)
        G.extend(Fnew)
        # call update rules
        setup_rules_Janet(G)
        P = Prolongation(G).difference(Done)
    return G
```

Chapter 6

FUTURE DIRECTION

As a new presented algorithm for computing Gröbner Bases, F4-involutive algorithm provides a new approach to generate matrices for reduction as inheriting the idea of F4; on the other hand, it also avoids lots of useless computations by involutive division. However, we still need to testify the efficiency of F4-involutive algorithm. By comparing the computations in Example 2.0.3 and Example 4.2.1, we can see that in F4-involutive algorithm the matrix used to reduce prolongations of degree 3 is a 8×12 matrix which is larger than the 6×11 matrix used in F4 algorithm. Furthermore we can observe that the size of matrices generated in F4-involutive algorithm are all larger than the matrices in F4 algorithm except the one generated in the first loop as Table 6.1 shows below.

Table 6.1: *Comparison of Matrices.*

degree	F4-involutive algorithm	F4 algorithm
2	3×7	3×7
3	8×12	6×11
4	15×19	12×17
5	13×18	8×14
6	21×26	17×23

The reason is F4-involutive algorithm does not implement Buchberger's criteria when it chooses the prolongation pairs in each step. So our future work would be to reformulate the Involutive Basis II algorithm in an F4-style, but that is beyond the scope of the current work.

BIBLIOGRAPHY

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

[2] 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)*. PhD thesis, Mathematical Insitute, University of Innsbruck, Austria, 1965. English translation published in the Journal of Symbolic Computation (2006) 475–511.

[3] Bruno Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner bases. In E. W. Ng, editor, *Proceedings of the EUROSAM 79 Symposium on Symbolic and Algebraic Manipulation, Marseille, June 26-28, 1979*, volume 72 of *Lecture Notes in Computer Science*, pages 3–21, Berlin - Heidelberg - New York, 1979. Springer.

[4] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer, second edition, 1997.

[5] Jean-Charles Faugére. A new efficient algorithm for computing gröbner bases (f4). *Journal of Pure and Applied Algebra*, 139:61–88, 1999.

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

[7] Vladimir P. Gerdt. Involutive algorithms for computing gröbner bases. In *Proceeding of the NATO Advanced Research Workshop "Computational Commutative and Noncommutative Algebraic Geometry"*, Amsterdam, 2004. IOS Press. preprint downloaded from arXiv.

[8] Vladimir P. Gerdt and Yuri A. Blinkov. Involutive bases of polynomial ideals. *Mathematics and Computers in Simulation*, 45(519–541):323–332, 1998.

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

[10] Alessandro Giovini, Teo Mora, Gianfranco Niesi, Lorenzo Robbiano, and Carlo Traverso. "One sugar cube, please" or selection strategies in the Buchberger algorithm. In *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation*, pages 49–54. ACM Press, 1991.

[11] Nathan Jacobson. *Algebra*. W. H. Freeman and Company, second edition, 1985.

[12] A. Yu. Zharkov and Yuri A. Blinkov. Involution approach to investigating polynomial systems. *Mathematics and Computers in Simulation*, 42(4–6):323–332, November 1996.