Algorithmic techniques in algebraic cryptanalysis and their applications

Makarim, R.H.

3 Theory of Gröbner Bases

Contents

This chapter is an overview of mathematical theory on Gröbner bases. The notion of Gröbner basis for a polynomial ideal was introduced in 1965 by Bruno Buchberger in his PhD thesis [Buc65, Buc06].* Buchberger also proposed an algorithm that computes a Gröbner basis given a basis or a set of generators for an ideal. In this chapter, we limit ourselves to describing Gröbner bases as mathematical objects and their applications. The explanation on algorithms that compute Gröbner bases shall be given in Chapter 4

This chapter is divided into five sections. We first introduce the notations, definitions, and necessary preliminaries in Section 3.1. This will be followed by the definition of monomial orderings and their examples in Section 3.2. Section 3.3 introduces the division algorithm in a multivariate polynomial ring, generalizing the existing algorithm in the univariate case. A natural characterization of the remainder together with the dedicated algorithm that computes it are also given in the same section. The definition of Gröbner bases and some of its properties will be presented in Section 3.4. Two relevant applications of Gröbner bases in this thesis are going to be described in Section 3.5. This chapter is a collection of topics from various existing literature on Gröbner bases, such as Chapter 1-3 of [CLO15] and [BW93, KR00].

3.1 Notations and Preliminaries

Definition 3.1 (Group)**.** *A group is a set G together with a binary operation $* : G \times G \mapsto G$ such that*

1. *The binary operation $*$ is associative, that is $a * (b * c) = (a * b) * c$ for any $a, b, c \in G$.*
2. *There exists an element $0 \in G$, called the identity, such that $0 * a = a * 0 = a$ for all $a \in G$.*
3. *For every $a \in G$, there exists an element $b \in G$ such that $a * b = b * a = 0$.*

If the group G also satisfies $a * b = b * a$ for all $a, b \in G$, then G is said to be Abelian.

Definition 3.2 (Subgroup)**.** *A subset H of a group G is a subgroup of G if H is itself a group w.r.t. the operation of G.*

* The name "Gröbner bases" is originated from Buchberger's PhD advisor, Wolfgang Gröbner.

Definition 3.3 (Ring)**.** *A ring is a set R together with two binary operations $+, \cdot : R \times R \mapsto R$, called addition and multiplication respectively, such that*

1. *R is an Abelian group under $+$.*
2. *The binary operation $\cdot$ is associative, that is $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for any $a, b, c \in R$.*
3. *The distributive laws hold, that is, for all $a, b, c \in R$ we have $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.*

A ring R is called a ring with identity if there exists an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$. A ring R is called a commutative ring if $a \cdot b = b \cdot a$ for all $a, b \in R$.

Definition 3.4 (Characteristic of a ring)**.** *Let R be a ring. If there exists a positive integer n such that $nr = 0$ for all $r \in R$, then the least such positive integer is called the characteristic of R. If no such positive integer exists, then R is of characteristic 0.*

Definition 3.5 (Field)**.** *A ring $\{0\} \neq R$ is called a field if R is a commutative ring with identity and for all $0 \neq a \in R$ there exists an element $b \in R$ such that $a \cdot b = 1$. In other words, the nonzero elements of R form a group w.r.t. the multiplication.*

Definition 3.6 (Ideal)**.** *A subset $I \subseteq R$ of a commutative ring R is an ideal of R if it satisfies:*

1. *$0 \in I$,*
2. *If $f, g \in I$ then $f + g \in I$,*
3. *If $f \in I$ and $h \in R$ then $hf = fh \in I$.*

Remark. *The notion of ideal also exists for noncommutative ring. That is, a left (resp. right) ideal is a subset I of a ring R which is an additive subgroup of R and such that for all $f \in I$ and all $h \in R$ we have $hf \in I$ (resp. $fh \in I$).*

We use $\mathbb{Z}$ to denote the ring of integers and $\mathbb{Z}_{\geq 0}$ as the set of nonnegative integers. The symbols $\mathbb{F}$ and $\mathbb{F}_q$ are used to denote an arbitrary field and the finite field of order q, respectively.

The central subject of this thesis deals with polynomials in finitely many variables. We start by introducing monomials, being the basic building blocks of a polynomial, together with some of its related definitions below.

Definition 3.7. *A **monomial** in variables $x_1, \ldots, x_n$ is a product of the form*

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

where $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_{\geq 0}$. The notation for monomial above can be simplified as x^α where $x = (x_1, \ldots, x_n)$ and $\alpha = (\alpha_1, \ldots, \alpha_n)$. For the case $\alpha = (0, \ldots, 0)$ we simply write x^α as 1.

Definition 3.8. *Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ with $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$. We say that the monomial x^α **divides** x^β, denoted by $x^\alpha \mid x^\beta$, if $\alpha_i \leq \beta_i$ for all $i \in \{1, \ldots, n\}$.*

Definition 3.9. *A **polynomial** in n variables $x_1, \ldots, x_n$ with coefficients in a field $\mathbb{F}$ is a finite linear combination (with coefficients in $\mathbb{F}$) of monomials. We shall write a polynomial f in the form*

$$f = \sum_{\alpha \in \mathcal{A}} \mathfrak{c}_\alpha x^\alpha, \quad \mathfrak{c}_\alpha \in \mathbb{F}$$

where $\mathcal{A}$ is a finite subset of $\mathbb{Z}^n_{\geq 0}$. If $\mathcal{A}$ is empty or $\mathfrak{c}_\alpha = 0$ for all $\alpha \in \mathcal{A}$, we shall write $f = 0$ and f is said to be the zero polynomial.

Definition 3.10. *The set of all polynomials in variables $x_1, \ldots, x_n$ with coefficients in the field $\mathbb{F}$ is denoted by*

$$\mathbb{F}[x_1, \ldots, x_n].$$

The set $\mathbb{F}[x_1, \ldots, x_n]$ is a commutative ring with identity with respect to polynomial addition and multiplication.

Notation. *Throughout this thesis, the polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$ will be denoted by $\mathcal{R}$ unless explicitly stated otherwise.*

Remark 3.11. *The ring $\mathcal{R}$ can also be viewed as an infinite-dimensional vector space over $\mathbb{F}$ and the set of all monomials in $\mathcal{R}$ serves as a basis of $\mathcal{R}$.*

Definition 3.12. *Let $f = \sum_\alpha \mathfrak{c}_\alpha x^\alpha$ be a nonzero polynomial in $\mathcal{R}$.*

1. *If $\mathfrak{c}_\alpha \neq 0$ then we call $\mathfrak{c}_\alpha x^\alpha$ a **term** of f.* We say that a term $\mathfrak{t}$ divides another term $\mathfrak{t}'$, denoted by $\mathfrak{t} \mid \mathfrak{t}'$, if the monomial of $\mathfrak{t}$ divides the monomial of $\mathfrak{t}'$.*

2. *For a term $\mathfrak{c}_\alpha x^\alpha$ of f, we call $\mathfrak{c}_\alpha$ the **coefficient** of the monomial x^α.*

3. *The set of all terms of f and the set of all monomials of f are respectively denoted by*

$$\mathsf{T}(f) = \{\mathfrak{c}_\alpha x^\alpha : \mathfrak{c}_\alpha \neq 0\},$$
$$\mathsf{M}(f) = \{x^\alpha : \mathfrak{c}_\alpha \neq 0\}.$$

4. *The definition of $\mathsf{T}(f), \mathsf{M}(f)$ are naturally extended for a subset of polynomials $F \subseteq \mathcal{R}$, that is*

$$\mathsf{T}(F) = \bigcup_{f \in F} \mathsf{T}(f),$$
$$\mathsf{M}(F) = \bigcup_{f \in F} \mathsf{M}(f).$$

   The set of all terms in $\mathcal{R}$ and all monomials in $\mathcal{R}$ are then denoted by $\mathsf{T}(\mathcal{R}), \mathsf{M}(\mathcal{R})$ respectively.

* In other existing literature, some authors interchange our definition of term and monomial such as in [Fau99, BW93].

5. *The degree of a nonzero $f \in \mathcal{R}$ is defined as*

$$\deg(f) = \max_{\alpha} \left\{ \sum_{i=1}^{n} \alpha_i : \mathfrak{c}_\alpha \neq 0 \right\}.$$

The degree of the zero polynomial is equal to $-\infty$ by convention.

Definition 3.13. *Let $F = \{f_1, \ldots, f_m\} \subseteq \mathcal{R}$. We define the following set*

$$\langle F \rangle = \langle f_1, \ldots, f_m \rangle = \left\{ \sum_{i=1}^{m} h_i f_i : h_1, \ldots, h_m \in \mathcal{R} \right\}.$$

*The set $\langle F \rangle = \langle f_1, \ldots, f_m \rangle$ is an ideal of $\mathcal{R}$. We call $\langle f_1, \ldots, f_m \rangle$ the **ideal generated by** $f_1, \ldots, f_m$.*

3.2 Monomial Orderings

The first question that arises when dealing with multivariate polynomials is how the monomials are supposed to be ordered. While it is trivial for the case of univariate polynomials, the situation is no longer obvious when more variables involved. For this purpose one needs to define the notion of *monomial ordering*, that allows unambiguous arrangement of terms in a polynomial and at the same time preserves the compatibility with the algebraic structure of multivariate polynomial rings.

Definition 3.14 (Monomial Ordering [CLO15])**.** *A monomial ordering $\geq$ is a relation on $\mathsf{M}(\mathcal{R})$ satisfying:*

1. *$\geq$ is a total ordering on $\mathsf{M}(\mathcal{R})$, i.e., it satisfies the following*
   (a) *$x^\alpha \geq x^\alpha$ for all $x^\alpha \in \mathsf{M}(\mathcal{R})$.*
   (b) *$x^\alpha \geq x^\beta$ and $x^\beta \geq x^\alpha$ implies $x^\alpha = x^\beta$.*
   (c) *$x^\alpha \geq x^\beta$ and $x^\beta \geq x^\gamma$ implies $x^\alpha \geq x^\gamma$.*
   (d) *For any $x^\alpha, x^\beta \in \mathsf{M}(\mathcal{R})$, either $x^\alpha \geq x^\beta$ or $x^\beta \geq x^\alpha$*
2. *If $x^\alpha \geq x^\beta$ and $x^\gamma \in \mathsf{M}(\mathcal{R})$, then $x^\alpha x^\gamma \geq x^\beta x^\gamma$.*
3. *$\geq$ is a well-ordering on $\mathsf{M}(\mathcal{R})$, that is every nonempty subset of $\mathsf{M}(\mathcal{R})$ has a smallest element under $\geq$.*

Remark 3.15. *Since any monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ can be associated with the n-tuple of exponents $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ and vice versa, it follows that a monomial ordering is also an ordering on the set $\mathbb{Z}^n_{\geq 0}$.*

Proposition 3.16. *An ordering on $\mathsf{M}(\mathcal{R})$ is a well-ordering if and only if every strictly decreasing sequence in $\mathsf{M}(\mathcal{R})$*

$$\mathfrak{m}_1 > \mathfrak{m}_2 > \mathfrak{m}_3 > \cdots$$

eventually terminates

Proof. See the proof of Lemma 2 in [CLO15, pg. 56]. ■

We mention three examples of monomial ordering below: lexicographic (*lex*), degree lexicographic (*deglex*), and degree-reverse lexicographic ordering (*degrevlex*). Other monomial orderings do exist, however these are the most relevant orderings within the scope of this thesis.

Definition 3.17 (Lexicographic Order)**.** *Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ be elements of $\mathbb{Z}^n_{\geq 0}$. We say that $x^\alpha >_{\text{lex}} x^\beta$ if and only if the leftmost nonzero entry of $\alpha - \beta \in \mathbb{Z}^n$ is positive.*

Definition 3.18 (Degree Lexicographic Ordering)**.** *Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say that $x^\alpha >_{\text{deglex}} x^\beta$ if and only if:*

- $\deg(x^\alpha) > \deg(x^\beta)$ *or*
- $\deg(x^\alpha) = \deg(x^\beta)$ *and* $x^\alpha >_{\text{lex}} x^\beta$.

Definition 3.19 (Degree-Reverse Lexicographic Ordering)**.** *Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say that $x^\alpha >_{\text{degrevlex}} x^\beta$ if and only if:*

- $\deg(x^\alpha) > \deg(x^\beta)$ *or*
- $\deg(x^\alpha) = \deg(x^\beta)$ *and the rightmost nonzero entry of $\alpha - \beta \in \mathbb{Z}^n$ is negative.*

In addition to *lex* and *degrevlex*, we also mention a generic ordering below called *block ordering*, which allows the incorporation of multiple monomial orderings for disjoint subsets of the variables.

Definition 3.20 (Block Ordering)**.** *Let $(x_1, \ldots, x_i)$ and $(y_1, \ldots, y_j)$ be two ordered sets of variables. Let $>_1, >_2$ be monomial orderings on $\mathbb{F}[x_1, \ldots, x_i]$ and $\mathbb{F}[y_1, \ldots, y_j]$, respectively. We say that $x^\alpha y^\beta > x^A y^B$ with respect to the block ordering $(>_1, >_2)$ on $\mathbb{F}[x_1, \ldots, x_i, y_1, \ldots, y_j]$ if and only if:*

- $x^\alpha >_1 x^A$ *or*
- $x^\alpha = x^A$ *and* $y^\beta >_2 y^B$.

Remark. *From now on whenever a polynomial ring $\mathcal{R}$ is defined, we adopt a monomial ordering $\geq$ on $\mathsf{M}(\mathcal{R})$.*

Definition 3.21 (Monomial Ideal [CLO15])**.** *An ideal $I \subseteq \mathcal{R}$ is a **monomial ideal** if there exists a (possibly infinite) subset $A \subseteq \mathsf{M}(\mathcal{R})$ such that $I = \langle A \rangle$.*

Proposition 3.22. *Let $A \subseteq \mathsf{M}(\mathcal{R})$ and let $I = \langle A \rangle$ be a monomial ideal. A monomial $\mathfrak{m} \in \mathsf{M}(\mathcal{R})$ is an element of I if and only if $\mathfrak{m}$ is divisible by a monomial $\mathfrak{m}'$ for some $\mathfrak{m}' \in A$.*

Proof. See the proof of Lemma 2 in [CLO15, pg. 70]. ■

Theorem 3.23 (Dickson's Lemma)**.** *Let $A \subseteq \mathsf{M}(\mathcal{R})$ and let $I = \langle A \rangle$ be a monomial ideal. Then I can be written in the form $I = \langle \mathfrak{m}_1, \ldots, \mathfrak{m}_s \rangle$ for some $\mathfrak{m}_1, \ldots, \mathfrak{m}_s \in A$. Thus, being finitely generated by monomials, we say that the ideal I has a finite basis.*

Proof. See the proof of Theorem 5 in [CLO15, pg. 72]. ■

Once the notion of monomial ordering is established, we define the following terminologies related to the largest monomial of nonzero polynomials in $\mathcal{R}$.

Definition 3.24. *Let $f = \sum_\alpha \mathfrak{c}_\alpha x^\alpha$ be a nonzero polynomial in $\mathcal{R}$ and let $\geq$ be a monomial ordering.*

1. *The **multidegree** of f is*

$$\text{multdeg}(f) = \max\{\alpha \in \mathbb{Z}^n_{\geq 0} : \mathfrak{c}_\alpha \neq 0\}$$

   where the maximum is taken with respect to $\geq$.

2. *The **leading coefficient** of f is $\mathsf{LC}(f) = \mathfrak{c}_{\text{multdeg}(f)} \in \mathbb{F}$.*

3. *The **leading monomial** of f is $\mathsf{LM}(f) = x^{\text{multdeg}(f)}$.*

4. *The **leading term** of f is $\mathsf{LT}(f) = \mathsf{LC}(f) \cdot \mathsf{LM}(f)$.*

5. *The **tail*** of f is $\mathsf{Tail}(f) = f - \mathsf{LT}(f)$.*

3.3 Polynomial Reduction

One of the important algorithms to work with multivariate polynomials is the computation of the remainder of $f \in \mathcal{R}$ after division by a finite nonempty ordered subset $G \subseteq \mathcal{R}$. The central idea of the algorithm relies on the existence of division algorithms in $\mathcal{R}$.

Theorem 3.25 ([CLO15, KR00])**.** *Let $G = \{g_1, \ldots, g_s\}$ be a nonempty finite subset of $\mathcal{R}$. Then every polynomial $f \in \mathcal{R}$ can be written as*

$$f = \sum_{i=1}^{s} q_i g_i + r, \tag{3.1}$$

where $q_1, \ldots, q_s, r \in \mathcal{R}$ such that

1. *either $r = 0$ or no monomials of r is divisible by any of $\mathsf{LM}(g_1), \ldots, \mathsf{LM}(g_s)$,*

2. *if $q_i g_i \neq 0$ then $\mathsf{LM}(q_i g_i) \leq \mathsf{LM}(f)$.*

Proof. The pseudo-code of the division algorithm is given in Algorithm 3.1 for the computation of r and $q_1, \ldots, q_s$. Starting with $p = f$, in every step of the iteration, the algorithm tries to eliminate the leading term of p, using polynomials in G whenever possible. During the execution of the algorithm, either one of the two events below happens :

1. When some $\mathsf{LT}(g_i)$ divides $\mathsf{LT}(p)$, we call this step the *division step*. This is seen in the line 6-9.

2. If there exists no $\mathsf{LT}(g_i)$ that divides $\mathsf{LT}(p)$, we call this step the *remainder step*. This is seen in the line 11-12.

* Also called reductum in [BW93].

Termination : Let p_j denote the value of p after the j-th iteration where $p_0 = f$. Suppose that at the j-th iteration, the division step occurred. We have $p_j = p_{j-1} - \mathsf{LT}(p_{j-1})/\mathsf{LT}(g_i) \cdot g_i$ and

$$\begin{aligned}\mathsf{LT}(\mathsf{LT}(p_{j-1})/\mathsf{LT}(g_i) \cdot g_i) &= \mathsf{LT}(p_{j-1})/\mathsf{LT}(g_i) \cdot \mathsf{LT}(g_i) \quad \text{(by 2 of Definition 3.14)} \\ &= \mathsf{LT}(p_{j-1}).\end{aligned}$$

so that p_{j-1} and $\mathsf{LT}(p_{j-1})/\mathsf{LT}(g_i) \cdot g_i$ have the same leading term. This implies that $\mathsf{LM}(p_j) < \mathsf{LM}(p_{j-1})$ when $p_j \neq 0$. Next, suppose that at the j-th iteration, the remainder step occurred. We have $p_j = \mathsf{Tail}(p_{j-1}) = p_{j-1} - \mathsf{LT}(p_{j-1})$. Here, it is obvious that $\mathsf{LM}(p_j) < \mathsf{LM}(p_{j-1})$ when $p_j \neq 0$. Thus, in either case we have

$$\mathsf{LM}(p_0) > \mathsf{LM}(p_1) > \mathsf{LM}(p_2) > \cdots .$$

If the algorithm never terminated, then we would get an infinite decreasing sequence of leading monomials. However, this contradicts the well-ordering property of $>$ in Proposition 3.16. Eventually, $p = 0$ must happen so that the algorithm terminates after finitely many iterations.

Correctness : To prove the correctness, we will show that

$$f = \sum_{i=1}^{s} q_i g_i + p + r \tag{3.2}$$

holds at every iteration. This is clearly true during the initialization since $q_1 = \ldots = q_s = r = 0$ and $p = f$. Suppose that (3.2) holds at one step of the while-loop. If the algorithm executed the division step, then there exists $g_i \in G$ such that $\mathsf{LT}(g_i) \mid \mathsf{LT}(p)$ and the following equality

$$q_i g_i + p = (q_i + \mathsf{LT}(p)/\mathsf{LT}(g_i))g_i + (p - \mathsf{LT}(p)/\mathsf{LT}(g_i) \cdot g_i)$$

shows that $q_i g_i + p$ remains unaffected. Since other variables are also unchanged, then (3.2) remains true in this case. Now if, instead of the division step, the algorithm executed the remainder step then it affects both p and r. However, the sum $p + r$ is unchanged since

$$p + r = \mathsf{Tail}(p) + (r + \mathsf{LT}(p))$$

and therefore (3.2) remains true.

Note that the algorithm is terminated when $p = 0$ which (3.2) eventually becomes

$$f = \sum_{i=1}^{s} q_i g_i + r.$$

Since the leading term of p in each iteration is added to r whenever it is not divisible by any of $\mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_s)$ it follows that r has the desired property when the algorithm terminates.

It remains to show the relation between $\mathsf{LM}(f)$ and $\mathsf{LM}(q_i g_i)$ when $q_i g_i \neq 0$. Every term of q_i is of the form $\mathsf{LT}(p)/\mathsf{LT}(g_i)$ for some polynomial $0 \neq p$. Initially $p = f$ and in the proof of termination we showed that the leading monomial of p decreases in every iteration. This implies that that $\mathsf{LM}(p) \leq \mathsf{LM}(f)$. Using 2 of Definition 3.14, it follows that $\mathsf{LM}(q_i g_i) \leq \mathsf{LM}(f)$ when $q_i g_i \neq 0$.

■

Input: $G = \{g_1, \ldots, g_s\} \subseteq \mathcal{R}, f \in \mathcal{R}$
Output: $q_1, \ldots, q_s, r \in \mathcal{R}$ such that $f = \sum_{i=1}^{s} q_i g_i + r$ and either $r = 0$ or no monomial of r is divisible by any of $\mathsf{LM}(g_1), \ldots, \mathsf{LM}(g_s)$

```
1  (q_1, ..., q_s) ← (0, ..., 0)
2  r ← 0
3  p ← f
4  while p ≠ 0 do
5      if ∃ g_i ∈ G : LT(g_i) | LT(p) then
6          Select g_i ∈ G such that LT(g_i) | LT(p)
7          t ← LT(p)/LT(g_i)
8          q_i ← q_i + t
9          p ← p − t · g_i
10     else
11         r ← r + LT(p)
12         p ← Tail(p)
13 return q_1, ..., q_s, r
```

Algorithm 3.1: The division algorithm in $\mathcal{R}$.

Remark 3.26. *The description of Algorithm 3.1 leaves some degrees of freedom in the selection of g_i in line 6. One way is to treat G as an ordered set $(g_1, \ldots, g_s)$ and choose the smallest $i \in \{1, \ldots, s\}$ such that $\mathsf{LT}(g_i) \mid \mathsf{LT}(p)$. This strategy is used in the description of the division algorithm in [CLO15, pg. 64]. In that respect we denote by $\overline{f}^G$ the remainder after division of f by an ordered set $G \subseteq \mathcal{R}$.*

Definition 3.27. *Let $f \in \mathcal{R}$ be a nonzero polynomial. A polynomial $0 \neq g \in \mathcal{R}$ is a **reductor** of f if $\mathsf{LM}(g) \in \mathsf{M}(f)$.*

Definition 3.28. *An algorithm that computes the remainder r (by omitting the quotients q_i) in Theorem 3.25 is called a **reduction algorithm**.*

In this work we consider a family of reduction algorithms, instead of one dedicated algorithm, such that each of the algorithms eliminates terms appearing in a specific part of a polynomial. Before describing them, we first introduce the notion of "reducibility".

Definition 3.29. *Let $0 \neq f \in \mathcal{R}$ and $G = \{g_1, \ldots, g_t\}$ be a subset of $\mathcal{R}$.*

1. *The polynomial f is **reducible** by G if there exists a monomial $\mathfrak{m} \in \mathsf{M}(f)$ such that $\mathfrak{m} \in \langle \mathsf{LM}(g_1), \ldots, \mathsf{LM}(g_t) \rangle$.*
2. *The polynomial f is **lead-reducible** by G if $\mathsf{LM}(f) \in \langle \mathsf{LM}(g_1), \ldots, \mathsf{LM}(g_t) \rangle$.*
3. *The polynomial f is **tail-reducible** by G if $\mathsf{Tail}(f) \neq 0$ and $\mathsf{Tail}(f)$ is reducible by G.*

Definition 3.29 suggests formulation of reduction algorithms that are applied on terms appearing in the leading term of a polynomial, the polynomial itself, and its tail. We describe three reduction algorithms below.

1. LeadReduce: This reduction algorithm plays the role of iteratively cancelling the leading term of a polynomial $f \in \mathcal{R}$ by an ordered set $G \subset \mathcal{R}$ until f is no longer lead-reducible by G. The description is given in Algorithm 3.2.

2. FullReduce: The FullReduce algorithm returns either a zero polynomial or a polynomial that is not reducible by G. One can verify this is equal to computing the remainder of f after division by G. The iterative reduction on f is done by calling the LeadReduce algorithm. This is formally described in Algorithm 3.3.

3. TailReduce: The TailReduce algorithm returns a nonzero polynomial that is not tail-reducible by G. It applies FullReduce algorithm on the tail of f. The pseudo-code is given in Algorithm 3.4.

Input: A polynomial $f \in \mathcal{R}$
Input: An ordered subset $G = (g_1, \ldots, g_t) \subset \mathcal{R}$
Result: A polynomial f such that $f = 0$ or $\mathsf{LM}(f) \notin \langle \mathsf{LM}(g_1), \ldots, \mathsf{LM}(g_t) \rangle$.

```
if f = 0 then
    return f
for i = 1 to t do
    if LT(g_i) | LT(f) then
        t ← LT(f)/LT(g_i)
        return LeadReduce(f − t · g_i, G)
return f
```

Algorithm 3.2: LeadReduce Algorithm.

Input: A polynomial $f \in \mathcal{R}$.
Input: An ordered subset $G = (g_1, \ldots, g_t) \subset \mathcal{R}$.
Result: A polynomial r such that $r = 0$ or for all $\mathfrak{m} \in \mathsf{M}(r)$: $\mathfrak{m} \notin \langle \mathsf{LM}(g_1), \ldots, \mathsf{LM}(g_t) \rangle$.

```
r ← 0
f ← LeadReduce(f, G)
while f ≠ 0 do
    r ← r + LT(f)
    f ← LeadReduce(f − LT(f), G)
return r
```

Algorithm 3.3: FullReduce Algorithm.

3.4 Gröbner Bases

This section presents the definition of Gröbner bases as the central subject of this thesis. Gröbner bases are considered as the "nice" basis for polynomial ideals. Its properties, that will be explained later, help in solving various problems in computational commutative algebra. Before defining Gröbner bases in

Input: A polynomial $f \in \mathcal{R}$.
Input: An ordered subset $G \subseteq \mathcal{R}$.
Result: A polynomial f such that $\mathsf{Tail}(f) = 0$ or
$\mathfrak{m} \notin \langle \mathsf{LM}(g_1), \ldots, \mathsf{LM}(g_t) \rangle$ for all $\mathfrak{m} \in \mathsf{M}(\mathsf{Tail}(f))$.
1 **return** $\mathsf{LT}(f) + \text{FullReduce}(\mathsf{Tail}(f), G)$

Algorithm 3.4: TailReduce Algorithm.

Definition 3.31, we want to recall the Hilbert basis theorem, that describes a fundamental property of polynomial ideals.

Theorem 3.30 (Hilbert Basis Theorem)**.** *Every ideal $I \subset \mathcal{R}$ has a finite generating set, i.e. $I = \langle g_1, \ldots, g_t \rangle$ for some $g_1, \ldots, g_t \in I$.*

Proof. See the proof of Theorem 4 in [CLO15, pg. 77]. ■

Definition 3.31 (Gröbner basis)**.** *Fix a monomial order on $\mathsf{M}(\mathcal{R})$. A finite subset G of an ideal $\{0\} \neq I \subseteq \mathcal{R}$ is said to be a **Gröbner basis** of I if for all $0 \neq f \in I$, there exists a polynomial $g \in G$ such that $\mathsf{LT}(g) \mid \mathsf{LT}(f)$.*

Theorem 3.32. *Every ideal $\{0\} \neq I \subseteq \mathcal{R}$ has a Gröbner basis. Moreover, any Gröbner basis for I is a basis of I.*

Proof. See Corollary 6 in Section §2.5 of [CLO15]. ■

Theorem 3.33 (The Ascending Chain Condition)**.** *Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be ascending chain of ideals in $\mathbb{F}[x_1, \ldots, x_n]$. Then there exists a positive integer N such that $I_N = I_{N+1} = I_{N+2} = \ldots$.*

Proof. See the proof of Theorem 7 in Section §2.5 of [CLO15, pg. 80]. ■

Remark 3.34. *A commutative ring that satisfies the property in Theorem 3.33 is also called a Noetherian ring.*

We remark that Definition 3.31 allows inclusion of some unnecessary elements in a Gröbner basis. Let G be a Gröbner basis of an ideal I and let $p \in G$. If there exists a polynomial $g \in G \setminus \{p\}$ such that $\mathsf{LT}(g) \mid \mathsf{LT}(p)$, we can remove p from G as $G \setminus \{p\}$ remains a Gröbner basis of I. This observation, together with adjustment of coefficients to normalize the leading coefficient of elements in G leads to the definition of minimal Gröbner bases.

Definition 3.35. *A Gröbner basis G of an ideal I is a **minimal Gröbner basis** if for all $g \in G$*

1. $\mathsf{LC}(g) = 1$ *and*
2. $\mathsf{LM}(g) \notin \langle \mathsf{LM}(G \setminus \{g\}) \rangle$.

In addition to Definition 3.35, there exists a stronger type of minimal Gröbner bases that adds the condition that every polynomial $g \in G$ is not reducible by $G \setminus \{g\}$.

Definition 3.36. *A Gröbner basis G of an ideal I is a **reduced Gröbner basis** if for all $g \in G$*

1. $\mathsf{LC}(g) = 1$ *and*
2. *For all $\mathfrak{m} \in \mathsf{M}(g)$, the monomial $\mathfrak{m} \notin \langle \mathsf{LM}(G \setminus \{g\}) \rangle$.*

3.5 Applications

One of the main reasons behind the extensive study of Gröbner bases for the past decades is its diverse application across numerous disciplines in mathematics. The wide-spectrum of its applications makes it impossible to exhaustively mention all of it. Some of them are already discussed, for example, in Chapter 3 of [KR00] and Chapter 2 of [AL94]. We refer to [SSM+09] for readers who are interested in applications related to coding theory and cryptography.

Within the scope of this thesis, we only describe two well-known applications of Gröbner bases in this section.

3.5.1 Ideal Membership Problem

Problem (Ideal Membership). *Given an ideal $I = \langle f_1, \ldots, f_m \rangle \subseteq \mathcal{R}$, determine whether a given polynomial $f \in \mathcal{R}$ lies in I.*

Although the division algorithm seems to be an obvious solution for this problem, i.e., if the remainder after division of f by the ordered set $G = (f_1, \ldots, f_m)$ is zero then $f \in I$, we want to recall that uniqueness of the remainder and the quotients in the division algorithm relies on the ordering of elements in G. Thus, we may encounter a situation where $f \in I$ and yet the remainder on the division of f by G is nonzero.

Gröbner bases then plays the role of remedies in such situation. The following property of Gröbner bases, together with the division algorithm, solves the ideal membership problem in multivariate polynomial rings.

Proposition 3.37 ([CLO15]). *Let $I \subseteq \mathcal{R}$ be an ideal and let G be a Gröbner basis of I. Given $f \in \mathcal{R}$, there exists a unique $r \in \mathcal{R}$ with the following properties*

1. *For any $g \in G$, no term of r is divisible by $\mathsf{LT}(g)$.*
2. *There exists a $q \in I$ such that $f = q + r$.*

More specifically, r is the remainder after division of f by G, no matter how the elements of G are ordered when using the division algorithm.

Proof. See Proposition 1 in Section §2.6 of [CLO15]. ■

Corollary 3.38 ([CLO15]). *Let $I \subseteq \mathcal{R}$ be an ideal and let $G \subseteq I$ be a Gröbner basis of I. The polynomial $f \in \mathcal{R}$ is an element of I if and only if the remainder after division of f by G is zero.*

Proof. First, it is obvious that if the remainder is zero, it immediately follows that $f \in I$. To prove the converse for any $f \in I$, we can write $f = f + 0$. Since G is a Gröbner basis, $f = f + 0$ satisfies both conditions in Proposition 3.37. Thus, 0 is the remainder after division of f by G. ■

Assume that a Gröbner basis G of a polynomial ideal I is known. We already have an algorithm that determines whether a polynomial $f \in \mathcal{R}$ is an element of I by computing the remainder after division of f by G with the division or FullReduce algorithm. The complete solution for the ideal membership problem requires an algorithm that obtains a Gröbner basis from an arbitrary basis of a polynomial ideal. This will be further described in Chapter 4.

3.5.2 Solving Systems of Polynomial Equations

Another well-known application of Grobner bases, in addition to solving the ideal membership problem, is its ability to solve systems of polynomial equations.

Problem. *Let $f_1, \ldots, f_m \in \mathcal{R}$. Find all solutions $(x_1, \ldots, x_n) \in \mathbb{F}^n$ of the following system of polynomial equations*

$$f_1(x_1, \ldots, x_n) = \ldots = f_m(x_1, \ldots, x_n) = 0.$$

The analogous concept in algebraic geometry for a set that consists of solutions of polynomial equations is known as an affine variety.

Definition 3.39. *Let $f_1, \ldots, f_m$ be polynomials in $\mathcal{R}$. We define the set*

$$\mathbf{V}(f_1, \ldots, f_m) = \{(a_1, \ldots, a_n) \in \mathbb{F}^n : f_i(a_1, \ldots, a_n) = 0,\ \forall i \in \{1, \ldots, m\}\}$$

*and we call $\mathbf{V}(f_1, \ldots, f_m)$ the **affine variety** defined by $f_1, \ldots, f_m$.*

Both propositions below are crucial in order to understand the relation between the affine variety defined by a finite set of polynomials and the corresponding ideal generated by the same polynomials.

Proposition 3.40. *If $f_1, \ldots, f_m \in \mathcal{R}$ and $g_1, \ldots, g_t \in \mathcal{R}$ are bases of the same ideal, i.e. $\langle f_1, \ldots, f_m \rangle = \langle g_1, \ldots, g_t \rangle$, then we have*

$$\mathbf{V}(f_1, \ldots, f_m) = \mathbf{V}(g_1, \ldots, g_t).$$

Proof. Let $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots f_m)$. Since $\langle f_1, \ldots, f_m \rangle = \langle g_1, \ldots, g_t \rangle$ then $g_1, \ldots, g_t \in \langle f_1, \ldots, f_m \rangle$. This implies that, every g_j can be written as

$$g_j = \sum_{i=i}^{m} h_i f_i, \quad h_i \in \mathcal{R}.$$

This shows that for all $j = 1, \ldots, t$, we have

$$\begin{aligned} g_j(a_1, \ldots, a_n) &= \sum_{i=1}^{m} h_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) \\ &= 0. \end{aligned}$$

Thus $(a_1, \ldots, a_n) \in \mathbf{V}(g_1, \ldots, g_t)$ and hence $\mathbf{V}(f_1, \ldots, f_m) \subseteq \mathbf{V}(g_1, \ldots, g_t)$. The other direction of the proof can be done in a similar manner by interchanging the role of $\langle f_1, \ldots, f_m \rangle$ and $\langle g_1, \ldots, g_t \rangle$, i.e., expressing each f_i as element of $\langle g_1, \ldots, g_t \rangle$. ■

Proposition 3.41. *Let I be an ideal of $\mathcal{R}$ and let $\mathbf{V}(I)$ be the following set*

$$\mathbf{V}(I) = \{(a_1, \ldots, a_n) \in \mathbb{F}^n : f(a_1, \ldots, a_n) = 0,\ \forall f \in I\}.$$

The set $\mathbf{V}(I)$ is an affine variety. In particular, if $I = \langle f_1, \ldots, f_m \rangle$, then $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_m)$.

Proof. By the Hilbert Basis Theorem, there exists a finite generating set of polynomials $\{f_1, \ldots, f_m\}$ for I, i.e. $I = \langle f_1, \ldots, f_m \rangle$. Let $(a_1, \ldots, a_n) \in \mathbf{V}(I)$. Since $f_1, \ldots, f_m \in I$, then $f_i(a_1, \ldots, a_n) = 0$ for all $i = 1, \ldots, m$ by definition and this shows that $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_m)$. Hence $\mathbf{V}(I) \subseteq \mathbf{V}(f_1, \ldots, f_m)$. On the other hand, let $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_m)$. Every polynomial $f \in I$ can be expressed as $f = \sum_{i=1}^{m} h_i f_i$, for some $h_1, \ldots, h_m \in \mathcal{R}$. It follows that

$$\begin{aligned} f(a_1, \ldots, a_n) &= \sum_{i=1}^{m} h_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) \\ &= \sum_{i=1}^{m} h_i(a_1, \ldots, a_n) \cdot 0 = 0. \end{aligned}$$

Thus, $(a_1, \ldots, a_n) \in \mathbf{V}(I)$ and $\mathbf{V}(f_1, \ldots, f_m) \subseteq \mathbf{V}(I)$. Therefore, we have $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_m)$. ■

Proposition 3.42. *Let $V \subseteq \mathbb{F}^n$ be an affine variety. We define*

$$\mathbf{I}(V) = \{f \in \mathcal{R} : f(a_1, \ldots, a_n) = 0, \forall (a_1, \ldots, a_n) \in V\}.$$

*The set $\mathbf{I}(V)$ is an ideal of $\mathcal{R}$ called the **ideal of** V.*

Remark 3.43. *Let $f_1, \ldots, f_m \in \mathcal{R}$ and let $\langle f_1, \ldots, f_m \rangle$ be an ideal of $\mathcal{R}$. Since $f_1, \ldots, f_m$ vanish on $\mathbf{V}(f_1, \ldots, f_m)$ so does $f = \sum_{i=1}^{m} h_i f_i \in I$ where $h_i \in \mathcal{R}$. This shows that $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots f_m))$ and implies that*

$$\langle f_1, \ldots, f_m \rangle \subset \mathbf{I}(\mathbf{V}(f_1, \ldots f_m)).$$

An important remark following Proposition 3.41 is the fact that affine varieties are determined by ideals. An implication of this together with Proposition 3.40 shows that in order to compute an affine variety defined by $f_1, \ldots, f_m$, one needs to obtain the right generating set for the ideal $\langle f_1, \ldots, f_m \rangle$ that gives a better description for the set of solutions. We will see that Gröbner bases with respect to lexicographic monomial ordering is the desired generating set that helps in solving a system of polynomial equations.

Definition 3.44 (ℓ-th Elimination Ideal)**.** *Let I be an ideal in $\mathbb{F}[x_1, \ldots, x_n]$. For $\ell = 0, \ldots, n-1$, the ℓ-**th elimination ideal** I_ℓ is the ideal of $\mathbb{F}[x_{\ell+1}, \ldots, x_n]$ defined by*

$$I_\ell = I \cap \mathbb{F}[x_{\ell+1}, \ldots, x_n].$$

Theorem 3.45 (The Elimination Theorem)**.** *Let $\mathbb{F}[x_1, \ldots, x_n]$ be a polynomial ring with lexicographic monomial ordering where $x_1 > x_2 > \cdots > x_n$. Let I be an ideal in $\mathbb{F}[x_1, \ldots, x_n]$ and G be a Gröbner basis of I. Then for every $\ell \in \{0, 1, \ldots, n-1\}$, the set*

$$G_\ell = G \cap \mathbb{F}[x_{\ell+1}, \ldots, x_n]$$

is a Gröbner basis of the ℓ-th elimination ideal I_ℓ.

Proof. See Theorem 2 in Section §3.1 of [CLO15, pg. 122]. ■

Polynomial systems that come from cryptographic primitives are typically defined over a finite field $\mathbb{F}_q$ and have a finite number of solutions. The ideal generated by such polynomials has several algebraic properties described in the following proposition.

Proposition 3.46 (Finiteness Criterion)**.** *Let $\overline{\mathbb{F}}$ be an algebraic closure of the field $\mathbb{F}$ and let $I = \langle f_1, \ldots, f_m \rangle$ be an ideal of $\mathcal{R} = \mathbb{F}[x_1, \ldots, x_n]$. The following conditions are equivalent.*

1. *The system of equations $\{f_1, \ldots, f_m\}$ has only finitely many solutions in $\overline{\mathbb{F}}$.*
2. *For $i = 1, \ldots, n$, we have $I \cap \mathbb{F}[x_i] \neq \{0\}$.*
3. *The $\mathbb{F}$-vector space $\mathbb{F}[x_1, \ldots, x_n]/I$ is finite-dimensional.*
4. *The set $\mathsf{M}(\mathcal{R}) \setminus \mathsf{LM}(I)$ is finite.*
5. *For every $i \in \{1, \ldots, n\}$, there exists a nonnegative integer α_i such that $x_i^{\alpha_i} \in \mathsf{LT}(I)$.*

*Any ideal of $\mathcal{R}$ that satisfies one of the conditions above is called a **zero-dimensional** ideal.*

Proof. See Proposition 3.7.1 in Section §3.7 of [KR00, pg.243]. ■

Theorem 3.47 (Hilbert Nullstellensatz [CLO15])**.** *Let $\overline{\mathbb{F}}$ be an algebraically closed field. If $f, f_1, \ldots, f_m \in \overline{\mathbb{F}}[x_1, \ldots, x_n]$ then $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_m))$ if and only if*

$$f^s \in \langle f_1, \ldots, f_m \rangle$$

for some positive integer s.

Proof. See the proof of Theorem 2 in [CLO15, pg. 179]. ■

Definition 3.48. *Let $I \subseteq \mathcal{R}$ be an ideal of $\mathcal{R}$. The radical of I, denoted by $\sqrt{I}$, is defined to be the following set*

$$\sqrt{I} = \{f : f^s \in I \text{ for some integer } s \geq 1\}.$$

Proposition 3.49. *Let $V \subseteq \mathbb{F}^n$ be a variety and let $f \in \mathcal{R}$. If $f^s \in \mathbf{I}(V)$ for some integer $s \in \mathbb{Z}_{\geq 1}$ then $f \in \mathbf{I}(V)$.*

Proof. Let $v \in V$. If $f^s \in \mathbf{I}(V)$ then $(f(v))^s = 0$. Since $f(v) \in \mathbb{F}$, the relation $(f(v))^s = 0$ is possible only if $f(v) = 0$. Since $v \in V$ is arbitrary, then $f \in \mathbf{I}(V)$. ■

The above proposition implies that an ideal that consists of all polynomials of $\mathcal{R}$ that vanish on a variety has a property that if some power of a polynomial in $\mathcal{R}$ belongs to the ideal, then the polynomial itself must belong to the ideal. This property motivates the following definition.

Definition 3.50 (Radical Ideal)**.** *An ideal I is **radical** if $f^s \in I$ for some positive integer s implies that $f \in I$. Equivalently, $I = \sqrt{I}$.*

Let $F = \{f_1, \ldots, f_m\} \subseteq \overline{\mathbb{F}}_q[x_1, \ldots, x_n]$ where $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$. Note that, in the context of cryptanalysis, we are not interested with solutions that exist in $\overline{\mathbb{F}}_q \setminus \mathbb{F}_q$. In order to remove these unnecessary solutions, the following set is appended to F

$$\{x_i^q - x_i : \forall i = 1, \ldots, n\}.$$

This also ensures that the ideal $\langle F \cup \{x_i^q - x_i : 1 \leq i \leq n\}\rangle$ is zero-dimensional by condition 5 of Proposition 3.46. In addition to being a zero-dimensional ideal, the following Proposition shows that $\langle F \cup \{x_i^q - x_i : 1 \leq i \leq n\}\rangle$ is a radical ideal.

Proposition 3.51 (Seidenberg's Lemma)**.** *Let I be a zero-dimensional ideal in $\mathbb{F}[x_1, \ldots, x_n]$. Suppose that for every $i \in \{1, \ldots, n\}$, there exists a nonzero univariate polynomial $g_i \in I \cap \mathbb{F}[x_i]$ such that the greatest common divisor of g_i and its formal derivative is equal to 1. Then I is a radical ideal.*

Proof. See Proposition 3.7.15 in Section §3.7 of [KR00, pg.250]. ■

Definition 3.52 (Perfect Field[KR00])**.** *A field $\mathbb{F}$ is called a **perfect field** if either*

- *its characteristic is equal to 0 or*
- *its characteristic is $p > 0$ and for every $\alpha \in \mathbb{F}$ there exists $\beta \in \mathbb{F}$ such that $\beta^p = \alpha$.*

Remark 3.53. *Every finite field $\mathbb{F}_q$, where $q = p^e$ with p a prime number and $e \in \mathbb{Z}_{>0}$, is a perfect field. By definition, the characteristic of $\mathbb{F}_q$ is equal to $p > 1$. Note that the map $x \mapsto x^{p^{e-1}}$ implies that $\left(x^{p^{e-1}}\right)^p = x^q = x$ for all $x \in \mathbb{F}_q$.*

The most important implication of the ideal $\langle F \cup \{x_i^q - x_i : 1 \leq i \leq n\}\rangle$ being zero-dimensional and radical is related to the shape of its reduced Gröbner basis w.r.t. lexicographic monomial ordering. This is formally described in the following Theorem (also known as the Shape Lemma).

Theorem 3.54 (The Shape Lemma)**.** *Let $\mathbb{F}$ be a perfect field and let $\mathbb{F}[x_1, \ldots, x_n]$ be a polynomial ring with lexicographic monomial ordering. Let $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be a zero-dimensional radical ideal such that for any two distinct elements in $\mathbf{V}(I)$ their n-th coordinates are distinct. Also let $g_n \in \mathbb{F}[x_n]$ be the monic generator of the $(n-1)$-th elimination ideal, i.e. $\langle g_n\rangle = I_{n-1} = I \cap \mathbb{F}[x_n]$.*

1. *The reduced Gröbner basis of I is of the form*

$$\{x_1 - g_1, \ldots, x_{n-1} - g_{n-1}, g_n\}$$

where $g_1, \ldots, g_{n-1} \in \mathbb{F}[x_n]$.

2. *The polynomial g_n has $d = \deg(g_n)$ distinct zeros $a_1, \ldots, a_d \in \overline{\mathbb{F}}$ in the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$. The set of zeros of I is*

$$\{(g_1(a_i), \ldots, g_{n-1}(a_i), a_i) : i = 1, \ldots, d\}.$$

Proof. See Theorem 3.7.25 in Section §3.7 of [KR00, pg.257]. ■

Following the Shape Lemma, if the reduced Gröbner basis G of an ideal I has a triangular form, then g_n is a univariate polynomial in $G \cap I_{n-1} \subseteq \mathbb{F}[x_n]$. The roots of g_n can be obtained by polynomial factorization. Once the possible solutions for x_n are found, we can substitute each value in the polynomials $x_i - g_i \in \mathbb{F}[x_i, x_n]$, for $i = 1, \ldots, n-1$, to obtain all solutions of the complete system of equations.

One particular case that is often encountered in algebraic cryptanalysis is that there exists an unique solution to the system of equations which lies in the base field. This has the following consequences on the corresponding ideal and its reduced Gröbner basis.

Proposition 3.55. *Let $F = \{f_1, \ldots, f_m\} \subset \mathcal{R} = \mathbb{F}_q[x_1, \ldots, x_n]$ and let $\tilde{I}$ be the ideal $\tilde{I} = \langle f_1, \ldots, f_m, x_1^q - x_1, \ldots, x_n^q - x_n \rangle \subset \mathcal{R}$. A solution $(a_1, \ldots, a_n) \in \mathbb{F}_q^n$ of F is the unique solution in $\mathbb{F}_q^n$ if and only if $\tilde{I} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$.*

Proof. If $(a_1, \ldots, a_n)$ is the unique solution of F in $\mathbb{F}_q^n$, then $\tilde{I} \subset \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Since the only roots of polynomials $x_i^q - x_i$ are elements of $\mathbb{F}_q$, the vector $(a_1, \ldots, a_n)$ is also the unique solution in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ for the system of equations $F \cup \{x_i^q - x_i : i = 1, \ldots, n\}$. Theorem 3.47 states that for all $i = 1, \ldots, n$ there exists a positive integer m_i such that $(x_i - a_i)^{m_i} \in \tilde{I}$. We have $x_i - a_i = \gcd(x_i^q - x_i, (x_i - a_i)^{m_i}) \in \tilde{I}$ and therefore $\tilde{I} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. The converse is obvious. ■

Corollary 3.56. *The reduced Gröbner basis G of $\tilde{I}$ with respect to degree-reverse lexicographic ordering is $G = \{x_1 - a_1, \ldots, x_n - a_n\}$.*

Given a Gröbner basis G of an ideal I w.r.t. a particular monomial ordering, there are algorithms that convert G to a Gröbner basis w.r.t. another monomial ordering. Two of the examples are the FGLM algorithm [FGLM93] and the Gröbner walk algorithm [CKM97]. Moreover, for a zero-dimensional ideal, the FGLM algorithm has a polynomial-time complexity in the number of solutions for the system of equations. A common strategy to solve a system of polynomial equations that corresponds to a zero-dimensional ideal I is then done in the following way: one starts by computing a Gröbner basis G of I using a monomial ordering that is considered to be efficient for computational purpose (e.g., degree-reverse lexicographic), then G is converted to another Gröbner basis G' w.r.t. lexicographic ordering using the FGLM algorithm. This, in practice, is considered to be a more efficient technique rather than computing G' directly using lexicographic ordering.