Gröbner bases and applications to multivariable cryptographic systems (MPK)

Marta Centellas Nadal

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Director del trabajo: José Ignacio Cogolludo
13 de septiembre de 2019

Prologue

What is Cryptography?

Cryptography is the art and science of secret writing. Cryptography enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient.

To carry out this process we need: Encrypt and decrypt. Data that can be read and understood without any special measures is called plaintext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption.

$$\text{Encrypting: ciphertext} = \text{cipher (key, plaintext)}$$

$$\text{Decrypting: plaintext} = \text{cipher (key, ciphertext)}$$

Cryptography has a sister discipline called Cryptanalysis, which is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck.

Why is Cryptography important?

If you reveal your secrets to the wind you should not blame the wind for revealing them to the trees.

- Kalil Gibran, Sand and Foam [2].

Cryptography is important because on the surface it is about making something secret, but it is also about controlling access, specifying who can get to information under what terms.

Cryptography seems closely linked to modern electronic communication. However, cryptography is not an invention of the last few years, in fact, its birth dates back 2000 B.C when non-standard "secret" hieroglyphics were used in ancient Egypt. Since Egyptian days cryptography has been used in one form or the other in many, if not most, cultures that developed written language.

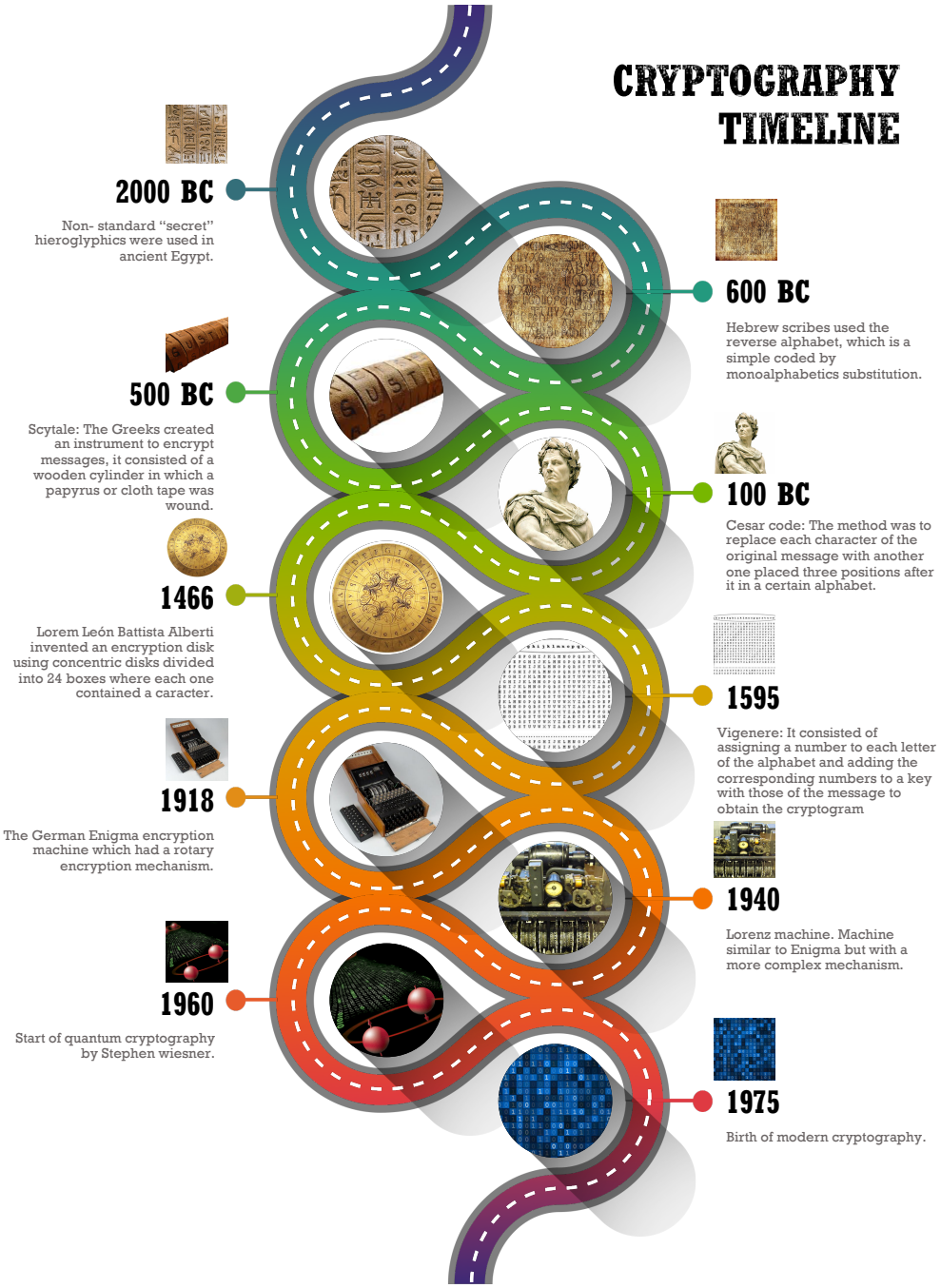

Figure 1: Timeline based in [5].

Until the onset of modern cryptography, conventional cryptography was used.

In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystem that is widely employed by the Federal Government.

Throughout the history of cryptography, there has been one problem that has made the practical use of cryptography difficult and unwieldy, the problem of key distribution. The best cipher is only as strong as its keys.

With Whitfield Diffie and Martin Hellman born the public key cryptography in 1975 and with it, the modern Cryptography.

Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption. It is computationally infeasible to deduce the private key from the public key.

Some examples of public-key cryptosystems are Elgamal, RSA, Diffie-Hellman and DSA, the Digital Signature Algorithm.
Public key encryption is the technological revolution that provides strong cryptography to the adult masses.

The most widely deployed public key cryptosystem nowadays is without any doubt the RSA cryptosystem.

The success of this method lies in the difficulty of factoring large integers, of the form $N = pq$ where p and q are prime numbers between 1024 and 2048 bits.
But, despite not being able to develop efficient algorithms that break the RSA encryption system, a new advance threatens to destroy it: It is quantum computers.

Under the assumption that quantum computers can be built, Shor in 1997,discovered an algorithm that could factor an integer in polynomial time in terms of its size in bits, thus rendering the RSA cryptosystem useless and this algorithm can also break essentially all number theoretic based public key cryptosystem. There have been great efforts dedicated to the construction of quantum computers and although nobody has built such computersable to attack the RSA or the discrete logarithm based cryptosystems, definitely there is a need for other efficient and secure cryptosystems.

There are currently a few families of cryptosystems that could potentially resist future quantum computers: these are the cryptosystems based on error-correcting codes, the public key cryptosystems based on lattices, and the multivariate public key cryptosystems. The class of multivariate cryptosystems is a special class of schemes whose security is related to the hardness of solving sets of multivariate equations. The way of solving them is to compute a Gröbner basis.

The multivariate polynomials that constitute the system are generally chosen to be quadratic polynomials defined over a small finite field which is ranging from $\mathbb{F}_2$ to $\mathbb{F}_{2^8}$.

The security of the scheme has to be assessed by mounting a specially crafted algebraic attack that exploits the underlying algebraic structure.

The current proposals for multivariate asymmetric cryptosystems might be classified into three main categories:

- Matsumoto-Imai like schemes
- Oil and Vinegar like schemes
- Tepwise triangular schemes

All of the schemes from the first three categories rely on the hardness of system solving, but some of them additionally rely on other hard problems such as finding rational mappings between polynomial maps or finding a linear combination of small rank of a given set of matrices.

Because of this, in this document we will focus on the study of the Matsumoto-Imai Scheme.

Resumen

Este trabajo está constituido por 3 capítulos distribuidos de la siguiente forma:

- Capítulo 1: Conceptos previos.
- Capítulo 2: Bases de Gröbner.
- Capítulo 3: Técnicas de criptoanálisis en criptografía de clave pública multivariable.

En el primero de ellos, comenzamos dando al lector los conceptos necesarios para la comprensión de los posteriores capítulos. Entre estos conceptos se incluyen definiciones como las de monomio, polinomio, máximo común divisor y mínimo común múltiplo de monomios, ideal y variedad entre otras.
También revisamos la existencia de un algoritmo de la división para polinomios en una variable, que posteriormente ampliaremos a varias variables. El contenido de este capítulo está basado en su totalidad en [4].

Una vez completada la parte anterior, abordamos la parte principal de este trabajo, pues en el segundo capítulo se desarrolla la construcción de las bases de Gröbner, a través del algoritmo de Buchberger. Para ello, definiremos orden monomial y estableceremos el algoritmo de la división en $k[x_1, \ldots, x_n]$.

Gracias a los conceptos anteriores concluiremos que el resto de la división de un polinomio entre una base de Gröbner es único independientemente del orden monomial establecido.
Sin abandonar este capítulo enunciamos y demostramos resultados de gran importancia como son el **Lema de Dickson**, el **Teorema de las bases de Hilbert** y el **Teorema de unicidad de las bases de Gröbner reducidas**.

Para finalizar esta segunda parte, daremos solución a cuatro problemas que somos capaces de resolver gracias a las bases de Gröbner:

1. Problema de descripción de un ideal, es decir, saber sí un ideal está generado por un conjunto finito.
2. Problema de pertenencia a un ideal.
3. Problema referente a la resolución de sistemas de ecuaciones de polinomios.
4. Problema de Implicitación, de obtención de un sistema de ecuaciones a partir de sus soluciones.

Con ayuda de la herramienta SageMath [6] implementamos los algoritmos incluidos en los anexos para poder calcular de manera eficaz los ejemplos propuestos a lo largo de la extensión del capítulo. La teoría de dicho capítulo se halla en los textos referentes a [1] y [4].

En el último capítulo nos centramos en los sistemas criptográficos multivariables, más conocidos como MPK. En él establecemos el esquema general para la construcción de la clave pública en este tipo de criptosistemas.

Seguidamente desarrollamos el primer MPK propuesto en la historia de la griptografía: **El esquema A de Matsumoto-Imai**, también conocido como **esquema en C***. El cual está basado en **la representación oscura de polinomios** y fue presentado por primera vez en 1985.

Para finalizar este capítulo, y con él, este trabajo; planteamos un ataque a este criptosistema mediante bases de Gröbner.

En los ejemplos de ataque al criptosistema de Matsumoto-Imai estudiados comprobamos que la dificultad de éxito crece rápidamente al aumentar el número de variables involucradas.

Para este último capítulo nos basamos en el árticulo que da comienzo en [3, pag. 263].

Contents

Chapter 1

Previous concepts

In this chapter we will introduce the necessary concepts and definitions to tackle for later, the rest of the chapters.

1.1 Polynomials and Affine Space

Definition 1. A **monomial** in $x_1, ..., x_n$ is a product of the form

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot ... \cdot x_n^{\alpha_n}$$

where all of the exponents $\alpha_1, ..., \alpha_n$ are non-negative integers. The **total degree** of this monomial is the sum of its exponents.
We can simplify the notation for monomials as follows: let $\alpha = (\alpha_1, ..., \alpha_n)$ be an n-tuple of non-negative integers. When $\alpha = (0, ..., 0)$, note that $x^\alpha = 1$. We also let $|\alpha| = \alpha_1 + ... + \alpha_n$ denote the total degree of the monomial x^α.

Definition 2. A polynomial f in $x_1, ..., x_n$ with coefficients in k is a finite linear combination of monomials. We will write a polynomial f in the form

$$f = \sum_\alpha a_\alpha x^\alpha, \ a_\alpha \in k$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, ..., \alpha_n)$. The set of all polynomials in $x_1, ..., x_n$ with coefficients in k is denoted $k[x_1, ..., x_n]$.

Definition 3. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial in $k[x_1, ..., x_n]$.

i) We call a_α the coefficient of the monomial x^α.

ii) If $a_\alpha \neq 0$, then we call $a_\alpha x^\alpha$ a term of f.

iii) The total degree of f, denoted $deg(f)$, is the maximun $|\ \alpha\ |$ such that the coefficient a_α is nonzero.

Example 1. Let's see an example, a polynomial

$$f = \tfrac{2}{3}x^2y^3z^2 + \tfrac{3}{2}x^4z^3 - 3xyz + y^2 \in \mathbb{Q}[x, y, z].$$

The polynomial has four terms and total degree is seven. In this case, there are two terms of maximal total degree, which is something that can't happen for polynomials of one variable.

Definition 4. Given a field k and a positive integer n, we define the n-dimensional affine space over k to be the set

$$k^n = \{(a_1, ..., a_n) | a_1, ..., a_n \in k\}.$$

Proposition 1.1. *Let k be an infinite field, and let $f \in k[x_1, ..., x_n]$. Then $f = 0$ in $k[x_1, ..., x_n]$ if and only if $f : k^n \longrightarrow k$ is the zero function.*

1.2 Affine Varieties

Definition 5. Let k be a field, and let $f_1,...,f_s$ be the polynomials in $k[x_1,...x_n]$.
Then we set

$$V(f_1,...,f_s) = \{(a_1,...,a_n) \in k^n | f_i(a_1,...,a_n) = 0 \text{ for all } 1 \leq i \leq s\}.$$

We call $V(f_1,...,f_s)$ the affine variety defined by $f_1,...,f_s$.

Thus, an affine variety $V(f_1,...,f_s) \subset k^n$ is the sest of all solutions of the system of equations $f_1(x_1,...x_n) = ... = f_s(x_1,...x_n) = 0$

Lemma 1.2. *If $V,W \subset k^n$ are varieties, then so are $V \cap W$ and $V \cup W$.*

1.3 Ideals

The goal of this section is to introduce the reader to some naturally ocurring ideals and to see how iedals relate to affine varieties.

Definition 6. A subset $I \subset k[x_1,...,x_n]$ is an ideal if it satisfies:

i) $0 \in I$.

ii) If $f,g \in I$, then $f+g \in I$.

iii) If $f \in I$ and $h \in K[x_1,...,x_n]$, then $hf \in I$.

Definition 7. Let $f_1,...,f_s$ be polynomials in $k[x_1,...x_n]$, the set generated by

$$\langle f_1,...,f_s\rangle = \left\{ \sum_{i=1}^{s} h_i f_i : h_1,...,h_s \in k[x_1,...,x_n] \right\} \text{ is an ideal.}$$

Lemma 1.3. *If $f_1,...,f_s \in K[x_1,...,x_n]$, then $\langle f_1,...,f_s\rangle$ is an ideal of $K[x_1,...,x_n]$.*

Definition 8. We will call $\langle f_1,...,f_s\rangle$ the ideal generated by $f_1,...,f_s$.

Also, given $f_1,...,f_s \in K[x_1,...,x_n]$, we set the system of equations

$$\begin{aligned} f_1 &= 0 \\ &\vdots \\ f_s &= 0. \end{aligned}$$

If we multiply the first equation by $h_1 \in K[x_1,...,x_n]$, the second by $h_2 \in k[x_1,...,x_n]$ and so on; then add the resulting equations, we obtain:

$$h_1 f_1 + h_2 f_2 + ... + h_s f_s = 0,$$

wich is a consequence of our original system. Notice that the left-hand side of this equation is an element of the ideal $\langle f_1,...,f_s\rangle$. Thus, we can think of $\langle f_1,...,f_s\rangle$ as consisting of all "polynomial consequences" of the equations $f_1 = f_2 = ... = f_s = 0$.

Proposition 1.4. *If $f_1,...,f_s$ and $g_1,...g_r$ are bases of the same ideal in $K[x_1,...,x_n]$, so that $\langle f_1,...,f_s\rangle = \langle g_1,...,g_r\rangle$, then $V(f_1,...,f_s) = V(g_1,...,g_t)$.*

Definition 9. Let $V \subset k^n$ be an affine variety. Then we set

$$I(V) = \{f \in K[x_1,...,x_n] : f(a_1,...,a_n) = 0 \quad \forall \quad (a_1,...,a_n) \in V\}.$$

Where $I(V)$ is an ideal.

1.4 Polynomials of One Variable

Definition 10. Given a non zero polynomial $f \in k[x]$, let

$$f = a_0x^m + a_1x^{m-1} + ... + a_m$$

where a_0 is not null and all $a_i \in k$.
Then we say that a_0x^m is the **leading term** of f, written $LT(f) = a_0x^m$.

Example 2. If $f = 2x^3 + x^2 - 3x + 1$, then $LT(f) = 2x^3$.

Proposition 1.5. $deg(f) \leq deg(g) \Longleftrightarrow LT(f)$ *divides* $LT(g)$.

Proposition 1.6. ***The Division Algorithm***

Let k be a field and let g be a non zero polynomial in $k[x]$. Then every $f \in k[x]$ can be written as

$$f = q \cdot g + r,$$

where $q, r \in k[x]$, and either $r = 0$ or $deg(r) < deg(g)$. Furthermore, q and r are unique, and there is an algorithm for finding q and r.

Here is the algorithm for finding q and r, presented in pseudocode:

Input: g, f
Output : q, r
$q := 0; r := f$
WHILE $r \neq 0$ *AND* $LT(g)$ *divides* $LT(r)$ *DO*
$q := q + LT(r)/LT(g)$
$r - (LT(r)/LT(g))g$

Corollary 1. If k is a field and $f \in k[x]$ is a nonzero polynomial, then f has a most $\deg(f)$ roots in k.

Corollary 2. If k is a field, then every ideal of $k[x]$ can be written in the form $\langle f \rangle$ for some $f \in k[x]$. Furthermore, f is unique up to multiplication by a nonzero constant in k.

Definition 11. A **greatest common divisor** of polynomials f,$g \in k[x]$ is a polynomial h such that:

- h divides f and g.
- If p is another polynomial which divides f and g, then p divides h.

When h has these propierties, we write $h = GCD(f, g)$.

Proposition 1.7. *These are the main properties of GCDs. Let f, $g \in k[x]$. Then:*

- $GCD(f, g)$ *exists and is unique up to multiplication by a nonzero constant in k.*
- $GCD(f, g)$ *is a generator of the ideal* $\langle f, g \rangle$.
- *There is an algorithm for finding* $GCD(f, g)$.

Example 3. Let's see an example of how the Euclidean algorithm works, for x^8-1 and $x^{12}-1$.

- We use de division algorithm:

$$x^8-1 = 0(x^{12}-1)+(x^8-1)$$
$$x^{12}-1 = x^4(x^8-1)+(x^4-1)$$
$$x^8-1 = (x^4+1)(x^4-1)+0.$$

Then, by the last equation, we have:

$$GCD(x^8-1,x^{12}-1) = GCD(x^{12}-1,x^8-1) \text{ and}$$
$$GCD(x^8-1,x^{12}-1) = GCD(x^8-1,x^4-1) = GCD(x^4-1,0) = x^4-1.$$

- This GCD computation answers our earlier question of findin a generator for the ideal $\langle x^8-1,x^{12}-1\rangle$ and for the proposition 1.7 we have:

$$GCD(x^8-1,x^{12}-1) = x^4-1.$$

Definition 12. A **greatest common divisor** of polynomial $f_1,...,f_s \in k[x]$ is a polynomial h such that:

- h divides $f_1,...,f_s$.
- If p is another polynomial which divides $f_1,...,f_s$, then p divides h.

When h has these propierties, we write $h = GCD(f_1,...,f_s)$.

Proposition 1.8. *Let $f_1,...,f_s \in k[x]$, where $s \geq 2$. Then:*

- *$GCD(f_1,...,f_s)$ exists and is unique up to multiplication by a nonzero constant in k.*
- *$GCD(f_1,...,f_s)$ is a generator of the ideal $\langle f_1,...,f_s\rangle$.*
- *If $s \geq 3$, then $GCD(f_1,...,f_s) = GCD(f_1,GCD(f_2,...,f_s))$.*
- *There is an algorithm for finding $GCD(f_1,...,f_s)$.*

Example 4. Consider the ideal

$$\langle x^3-3x+2,x^4-1,x^6-1\rangle \subset k[x].$$

We know that $GCD(x^3-3x+2,x^4-1,x^6-1)$ is a generator. But also we can check that

$$GCD(x^3-3x+2,x^4-1,x^6-1) = GCD(x^3-3x+2,GCD(x^4-1,x^6-1)) = GCD(x^3-3x+2,x^2-1) = x-1.$$

It follows that $\langle x^3-3x+2,x^4-1,x^6-1\rangle = \langle x-1\rangle$.

Proposition 1.9. *Given $f_1,..,f_s \in k[x]$, is there an algorithm for deciding whether a given polynomial $f \in k[x]$ lies in the ideal $\langle f_1,...,f_s\rangle$*
To answer this question we will describe the following algorithm: The first step is use GCDs to find a generator h of $\langle f_1,..,f_s\rangle$ is equivalent to $f \in \langle h\rangle$, we need only use the division algorithm to write $f = qh+r$, where $deg(r) < deg(h)$. It follows that is in the ideal if an olnly if $r = 0$.

Example 5. Suppose we wanted to know whether $x^3+4x^2+3x-7 \in \langle x^3-3x+2,x^4-1,x^6-1\rangle$.
We saw above that $x-1$ is a generator of this ideal so that our question can be rephrased as whether $x^3+4x^2+3x-7 \in \langle x-1\rangle$
Dividing, we find that

$$x^3+4x^2+3x-7 = (x^2+5x+8)(x-1)+1$$

and it follows that x^3+4x^2+3x-7 is not in the ideal $\langle x^3-3x+2,x^4-1,x^6-1\rangle$.

Chapter 2

Gröbner Bases

2.1 Problems

Through Gröbner bases we will solve the following problems:

a. The IDEAL DESCRIPTION PROBLEM:
Does every ideal $I \subseteq k[x_1,...,x_n]$ have a finite basis? In other words, can we write $I = \langle f_1,...,f_s \rangle$ for $f_i \in k[x_1,...,x_n]$?.

b. The IDEAL MEMBERSHIP PROBLEM:
Given $f \in k[x_1,...,x_n]$ and an ideal $I = \langle f_1,...,f_s \rangle$, determine if $f \in I$. Geometrically, this is closely related to the problem of determining whether $V(f_1,...,f_s)$ lies on the variety $V(f)$.

c. The PROBLEM OF SOLVING POLYNOMIAL EQUATIONS:
Find all common solutions in k^n of a system of polynomial equations

$$f_1(x_1,...,x_n) = \cdots = f_s(x_1,...,x_n) = 0.$$

This is the same as asking for the points in the affine variety $V(f_1,...,f_s)$.

d. The IMPLICITIZATION PROBLEM:
Let $V \subseteq k^n$ be given parametrically as

$$\begin{aligned} x_1 &= g_1(t_1,...,t_m), \\ &\vdots \\ x_n &= g_n(t_1,...,t_m). \end{aligned}$$

If the g_i are polynomials (or rational functions) in the variables t_j, then V will be an affine variety or part of one. Find a system of polynomial equations (in the x_i) that defines the variety.

2.2 Finite Fields

Definition 13. A field $\mathbb{F}$ is finite if there is a finite number of elements.

Definition 14. Let $\mathbb{F}_q$ be a finite field of characteristic p-prime, $q = p^n$.

Definition 15. The field $\mathbb{F}_2 = \{0,1\}$ is given by the following operation tables.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Figure 2.1: Addition and multiplication tables in $\mathbb{F}_2$.

$\mathbb{F}_2$ is also denoted by $\mathbb{GF}(2)$, the Galois field of two elements, and it is the smallest field.

Properties of $\mathbb{F}_2$:

- Every element x of $\mathbb{F}_2$ satisfies $x+x=0$ and therefore $-x=x$, this means that the characteristic of $\mathbb{F}_2$ is 2.
- Since $1\cdot 1 = 1$ and $0\cdot 0 = 0$, then $x^2 = x$ for all elements of $\mathbb{F}_2$. Likewise, $x^k = x$ for all $k > 0 \Longrightarrow x$ is idempotent with respect to multiplication.

From now on, all the examples will be done on $\mathbb{F}_2$.

2.3 Ordering on the Monomials

Definition 16. A **monomial ordering** on $k[x_1,...,x_n]$ is any relation $>$ on $\mathbb{Z}^n_{\geq 0}$, or equivalently, any relation on the set of monomials x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, satisfying:

- $>$ is a total (or linear) ordering on $\mathbb{Z}^n_{\geq 0}$.
- If $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha+\gamma > \beta+\gamma$.
- $>$ is a well ordering on $\mathbb{Z}^n_{\geq 0}$. This means that every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $>$.

Lemma 2.1. *An order relation $>$ on $\mathbb{Z}^n_{\geq 0}$ is a well ordering if and only if every strictly decreasing sequence in $\mathbb{Z}^n_{\geq 0}$*

$$\alpha(1) > \alpha(2) > \alpha(3) > ...$$

must be finite. That is, there are no strictly decreasing infinite chains.

Definition 17. Lexicographic Order
Let $\alpha = (\alpha_1,...,\alpha_n)$ and $\beta = (\beta_1,...,\beta_n) \in \mathbb{Z}^n_{\geq 0}$.
We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the left-most nonzero entry is positive. We will write $x^\alpha >_{lex} \beta$.

Proposition 2.2. *The lex ordering on $\mathbb{Z}^n_{\geq 0}$ is a monomial ordering.*

Definition 18. Graded Lex Order
Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i, \quad or \quad |\alpha| = |\beta| \quad and \quad \alpha >_{lex} \beta.$$

Definition 19. Graded Reverse Lex Order
Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grvlex} \beta$ if

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \quad or \quad |\alpha| = |\beta|$$

and, in $\alpha - \beta \in \mathbb{Z}^n$, the right-most nonzero entry is negative.

Example 6. Let a polynomial $f(x,y,z) = x+y+x^2+z^2+x^3$ in $\mathbb{F}_2[x,y,z]$. We rewrite f, ordering the terms with $x > y > z$ using lex order, grlex order and grevlex order.

We write each of the terms of the polynomial f as a vector with three componentes:

$$\begin{array}{lll} x \to (1,0,0), & y \to (0,1,0), & x^2 \to (2,0,0), \\ z^2 \to (0,0,2), & x^3 \to (3,0,0). & \end{array}$$

- **Lexicographic Order:** We must subtract the vectors and will be the greater, it will be greater that in this subtraction the term has more to the left is not null and positive.

$$f = x^3 + x^2 + x + y + z^2.$$

- **Graded Lex Order:** The greater term is the term that when add the components of the vector is greater and if two are equal we take the lexicographic order.

  In this case, we add the components of each vector:

$$\begin{array}{ll} x \to 1+0+0 = 1, & y \to 0+1+0 = 1, \\ x^2 \to 2+0+0 = 2, & z^2 \to 0+0+2 = 2, \\ x^3 \to 3+0+0 = 3. & \end{array}$$

  In cases where the value of the sum is the same, we will apply lexicographic order, and then we have the polynomial rewrite:

$$f = x^3 + x^2 + z^2 + x + y.$$

- **Graded Reverse Lex Order:** The greater term is the term that when add the components of the vector is greater and if two are equal the one that when we doing the subtraction has the term more to the right not null negative.
  The solution is:

$$f = x^3 + x^2 + z^2 + x + y.$$

Definition 20. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, ..., x_n]$ and let $>$ be a monomial order.

i) The **multidegree** of f is

$$multideg(f) = max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0).$$

ii) The **leading coefficient** of f is

$$LC(f) = a_{multideg(f)} \in k.$$

iii) The **leading monomial** of f is

$$LM(f) = x^{multideg(f)}.$$

iv) The **leading term** of f is

$$LT(f) = LC(f) \cdot LM(f).$$

Example 7. To illustrate, let $f = x^4y^5z + x^3y^2z - xy^2z^4 \in \mathbb{F}_2[x,y,z]$ as before and let $>$ denote the lex order. Then:

$$\begin{gathered} multideg(f) = (4,5,1), \\ LC(f) = 1, \\ LM(f) = x^4y^5z, \\ LT(f) = x^4y^5z. \end{gathered}$$

Lemma 2.3. *Let $f, g \in k[x_1,...,x_n]$ be nonzero polynomials. Then:*

i) $multideg(fg) = multideg(f) + multideg(g)$.

ii) If $f+g \neq 0$, then $multideg(f+g) \leq max(multideg(f), multideg(g))$.

If, in addition, $multideg(f) \neq multideg(g)$, then equality occurs.

2.4 Division Algorithm in $K[x_1,\ldots,x_n]$

We saw how the division algorithm could be used to solve the ideal membership problem for polynomials of one variable. To study this problem when there are more variables, we will formulate a division algorithm for polynomials in $k[x_1,...,x_n]$ that extends the algorithm for $k[x]$. In the general case, the goal is to divide $f \in k[x_1,...,x_n]$ by $f_1,...,f_s \in k[x_1,...,x_n]$. As we will see, this means expressing f in the form

$$f = q_1f_1 + ... + q_sf_s + r,$$

where the quotients $q_1,...,q_s$ and remainder r lie in $k[x_1,...,x_n]$.

Theorem 2.4. ***Division Algorithm in*** $k[x_1,...,x_n]$

Fix a monomial order $>$ on $\mathbb{Z}^n_{\geq 0}$, and let $F = (f_1,...,f_s)$ be an ordered s-tuple of polynomials in $k[x_1,...,x_n]$. Then every $f \in k[x_1,...,x_n]$ can be written as

$$f = q_1f_1 + ... + q_sf_s + r,$$

where $q_i, r \in k[x_1,...,x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in k, of monomials, none of which is divisible by any of $LT(f_1),...,LT(f_s)$.
We will call r a ***remainder*** *off on division by F. Furthermore, if $q_if_i \neq 0$, then we have*

$$multideg(f) \geq multideg(q_if_i).$$

The structure of the algorithm would be:

Input : $f_1,...,f_s,f$
Output: $q_1,...,q_s,r$
$q_1 := 0;...;q_s := 0; r := 0$
$p := f$
WHILE $p \neq 0$ *DO*
    $i := 1$
    $divisionoccurred := false$
    WHILE $i \leq s$ *AND* $divisionoccurred = false$ *DO*
        IF $LT(f_i)$ *divides* $LT(p)$ *THEN*
            $q_i := q_i + LT(p)/LT(f_i)$
            $p := p - (LT(p)/LT(f_i))f_i$
            $divisionoccurred := true$
        ELSE
            $i := i + 1$

IF $divisionoccurred = false$ *THEN*
$r := r + LT(p)$
$p := p - LT(p)$
RETURN $q_1, ..., q_s, r$

There are two possiblities:

- *DIVISION STEP: If some* $LT(f_i)$ *divides* $LT(p)$*, then the algorithm proceeds as in the one-variable case.*
- *REMAINDER STEP: If no* $LT(f_i)$ *divides* $LT(p)$*, then the algorithm adds* $LT(p)$ *to the remainder.*

Example 8. We will first divide $f = xy^3 + xy + y^2 + x + 1$ by $f_1 = xy + 1$ and $f_2 = x + 1$, using lex order in $\mathbb{F}_2[x,y]$.
We want to employ the same scheme as for division of one variable polynomials, the difference being that there are now several divisors and quotients.

Look at the leading terms $LT(f_1) = xy$ and $LT(f_2) = x$, in this case both divide the leading term of f wich is $LT(f) = xy^3$. Since f_1 is listed first, we will use it.
Thus, we divide xy^3 into xy, leaving y^2, so that when you divide f by f_1 the leaving $y^2 + 1$ and the remainder x.
Now, we repeat the same process on x. This time we must use f_2 because $LT(f_1) = xy$ does not divide $LT(x) = x$, and then we obtain a new quotient,which is 1 and new rest, which is 1.

Since $LT(f_1)$ and $LT(f_2)$ do not divide 1, the remainder is $r = 1$ and we are done.
Finally, we obtain:

$$xy^3 + xy + y^2 + x + 1 = (y^2 + 1)(xy + 1) + 1(x + 1) + 1.$$

For other more complex examples we will use the alghorithm A that we have programmed in SageMath [6].

Example 9. In this example, we will see that order matters. So we will make the same division in differents orders.
Let $f = xy^2z + xz + y + z$, $f_1 = xy + 1$, $f_2 = y^2 + 1$ and $f_3 = y + z$ in $\mathbb{F}_2[x,y,z]$ with lex order.

- Dividing f by $F = (f_1, f_2, f_3)$, the result is:

$$xy^2z - 2xz + y = yz(xy + 1) + 0(y^2 + 1) + (z + 1)(y + z) + (xz + z^2)$$

$$f = yz \cdot f_1 + 0 \cdot f_2 + (z + 1) \cdot f_3 + (xz + z^2).$$

- Dividing f by $F = (f_2, f_1, f_3)$, the result is:

$$xy^2z - 2xz + y = xz(y^2 + 1) + 0(xy + 1) + 1(y + z) + 0$$

$$f = xz \cdot f_2 + 0 \cdot f_1 + 1 \cdot f_3 + 0.$$

- Dividing f by $F = (f_3, f_2, f_1)$, the result is:

$$xy^2z - 2xz + y = (xyz + xz^2 + 1)(y + z) + 0(y^2 + 1 + 0(xy + 1) + (xz^3 + xz)$$

$$f = (xyz + xz^2 + 1) \cdot f_3 + 0 \cdot f_2 + 0 \cdot f_1 + (xz^3 + xz).$$

Thus, we have verified that the remainder is not unique, since it varies depending on the order in which the dividers are taken.

As in the previous example, we can do the operations with an algorithm A.

2.5 Monomial Ideals and Dickson's Lemma

Definition 21. An ideal $I \subset k[x_1,...,x_n]$ is a **monomial ideal** if there a subset $A \subset \mathbb{Z}^n_{\geq 0}$ (possibly infinite) such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in k[x_1,...,x_n]$. In this case, we write $I = \langle x^\alpha : \alpha \in A \rangle$.

Lemma 2.5. *Let $I = \langle x^\alpha : \alpha \in A \rangle$ be a monomial ideal. Then a monomial x^β lies in I and only if x^β is divisible by x^α for some $\alpha \in a$.*

Lemma 2.6. *Let I be a monomial ideal, and let $f \in k[x_1,...,x_n]$. Then the following are equivalent:*

i) $f \in I$.

ii) Every term of f lies in I.

iii) f is a k-linear combination of the monomials in I.

Corollary 3. Two monomial ideals are the same if and only if they contain the same monomials.

Theorem 2.7. ***Dickson's Lemma***
A monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle \subset k[x_1,...,x_n]$ can be written down in the form $I = \langle x^{\alpha(1),...,\alpha(s)} \rangle$, where $\alpha(1),...,\alpha(s) \in A$. In particular, I has a finite basis.

Proof. We proceed by induction on n.

- Let $n = 1 \Rightarrow I$ is generated by the monomials x_1^α, where $\alpha \in A \subset \mathbb{Z}_{\geq 0}$. Let β be the smallest element of $A \subset \mathbb{Z}_{\geq 0}$.

- Now assume $n > 1$ and that the theorem is true for $n-1$. We will write the variables as $x_1,...,x_{n-1},y$, so that monomials in $k[x_1,...,x_{n-1},y]$ can be written as $x^\alpha y^m$, where $\alpha = (\alpha_1,...,\alpha_{n-1}) \in \mathbb{Z}^{n-1}_{\geq 0}$ and $m \in \mathbb{Z}_{\geq 0}$.

  Suppose that $I \subset k[x_1,...,x_{n-1},y]$ is a monomial ideal. To find generators for I, let J be the ideal in $k[x_1,...,x_{n-1}]$ generated by the monomials x^α for which $x^\alpha y^m \in I$ for some $m \geq 0$.
  Since J is a monomial ideal in $k[x_1,...,x_{n-1}]$, our inductive hypothesis implies that finitely many of the x^α generate J , say $J =< x^{\alpha(1)},...,x^{\alpha(s)} >$.

  For each i between 1 and s, the definition of J tells us that $x^{\alpha(i)} y^{m_i} \in I$ for some $m_i \geq 0$. Let m be the largest of the m_i and then, for each k between 0 and $m-1$, consider the ideal $J_k \subset k[x_1,...,x_{n-1}]$ generated by the monomials x^β such that $x^\beta y^k \in I$.

  Using our inductive hypothesis again, J_k has a finite generating set of monomials, say $J_k =< x^{\alpha_k(1)},...,x^{\alpha_k(sk)} >$.

  We claim that I is generated by the monomials in the following list:

$$J : x^{\alpha(1)} y^m,...,x^{\alpha(s)} y^m,$$
$$J_0 : x^{\alpha_0(1)},...,x^{\alpha_0(s_0)},$$
$$J_1 : x^{\alpha_1(1)},...,x^{\alpha_1(s_1)} y,$$
$$\vdots$$
$$J_{m-1} : x^{\alpha_{m-1}(1)} y^{m-1},...,x^{\alpha_{m-1}(s_{m-1})} y^{m-1}.$$

  First note that every monomial in I is divisible by one on the list. To see why, let $x^\alpha y^p \in I$:

- If $p \geq m$, then$x^{\alpha}y^{p}$ is divisible by some $x^{\alpha}(i)y^{m}$ by the construction of J.
- If $p \leq m-1$, then $x^{\alpha}yp$ is divisible by some $x_p^{\alpha}(j)y^{p}$ by the construction of J_p.

So by the lemma 2.5 we have that the above monomials generate an ideal having the same monomials as I and by corollary 3 we appreciate that they must be the same.

To complete the proof of the theorem, we need to showthat the finite set of generators can be chosen from a given set of generators for the ideal. If we switch back to writing the variables as $x_1,...,x_n$, then our monomial ideal is $I =< x^{\alpha} : \alpha \in A >\subset k[x_1,...,x_n]$.
We need to show that I is generated by finitely many of the x^{α}'s, where $\alpha \in A$.

But previously , we have seen that $I =< x^{\beta(1)},...,x^{\beta}(s)$ for some monomials $x^{\beta(i)}$ in I, as $x^{\beta}(i) \in I =< x^{\alpha} : \alpha \in A >$ that implies that each $x^{\beta(i)}$ is divisible by $x^{\beta(i)}$ for some $\alpha(i) \in A$. And for this reason we have $I =< x^{\alpha(1)},...,x^{\alpha(s)} >$. □

2.6 The Hilbert Basis Theorem and Gröbner Bases

Definition 22. Let $I \subset k[x_1,...,x_n]$ be an ideal other than $\{0\}$.

i) We denote by $LT(I)$ the set of leading terms of elements of I. Thus,

$$LT(I) = \{cx^{\alpha} : \text{ there exists } f \in \text{ with } LT(f) = cx^{\alpha}\}.$$

ii) We denote by $\langle LT(I)\rangle$ the ideal generated by the elements of $LT(I)$.

Proposition 2.8. *Let $I \subset k[x_1,...,x_n]$ be an ideal.*

i) $\langle LT(I)\rangle$ is a monomial ideal.

ii) There are $g_1,...,g_s \in I$ such that $\langle LT(I)\rangle = \langle LT(g_1),...,LT(g_t)\rangle$.

Theorem 2.9. ***Hilbert Basis Theorem***
Every ideal $I \subset k[x_1,...,x_n]$ has a finite generating set. That is, $I = \langle g_1,...,g_s\rangle$ for some $g_1,...,g_s \in I$

Proof. We separate in two cases:

- In the first case, let $I = 0$, we take our generating set to be 0, which is certainly finite.
- If $I \neq \{0\}$, that is, contains some nonzero polynomial, then a generating set $g_1,...,g_s$ for I can be constructed as follows. By Proposition 2.8 , there are $g_1,...,g_s \in I$ such that $< LT(I) >=< LT(g_1),...,LT(g_t) >$, which it invovles $I =< g_1,...,g_s >$. Let's see it for double content:

  - It is clear that $< g_1,...,g_s >\subset I$ since each $g_t \in I$.
  - Conversely, let $f \in I$ be any polynomial. If we apply the division algorithm to divide f by $< g_1,...,g_s >$, then we get an expression of the form

  $$f = a_1g_1 + ... + a_tg_t + r$$

  where no term of r is divisible by any of $LT(g_1),...,LT(g_t)$. We claim that $r = 0$. To see this, note that

  $$r = f - a_1g_1 - ... - a_tg_t \in I.$$

If $r \neq 0$, then $LT(r) \in < LT(I) > = < LT(g_1), ..., LT(g_t) >$, and by Lemma 2.5, it follows that $LT(r)$ must be divisible by some $LT(g_i)$. This contradicts what it means to be a remainder, and, consequently, r must be zero. Thus,

$$f = a_1 g_1 + ... + a_t g_t + 0 \in < g_1, ..., g_s >,$$

which shows that $I \subset < g_1, ..., g_s >$.

This completes the proof.

□

Definition 23. Fix a monomial order. A finite subset $G = \{g_1, ..., g_s\}$ of an ideal I is said to be a **Gröbner basis** if

$$\langle LT(g_1), ..., LT(g_t) \rangle = \langle LT(I) \rangle.$$

Corollary 4. Fix a monomial order. Then every ideal $I \subset k[x_1, .., x_n]$ other than $\{0\}$ has a Gröbner basis. Furthermore, any Gröbner basis for an ideal I is a basis of I.

Theorem 2.10. ***The Ascending Chain Condition***
Let

$$I_1 \subset I_2 \subset I_3 \subset ...$$

be an ascending chain of ideals in $k[x_1, ..., x_n]$. Then where exists an $N \geq 1$ such that

$$I_N = I_{N+1} = I_{N+2} = ... \quad .$$

Definition 24. Let $I \subset k[x_1, ..., x_n]$ be an ideal. We will denote by $V(I)$ the set

$$V(I) = \{(a_1, ..., a_n) \in k^n : f(a_1, ..., a_n) = 0 \text{ for all } f \in I\}.$$

Proposition 2.11. *$V(I)$ is an affine variety. In particular, if $I = \langle f_1, ..., f_s \rangle$, then $V(I) = V(f_1, ..., f_s)$.*

2.7 Propierties of Gröbner Bases

Proposition 2.12. *Let $G = \{g_1, ..., g_s\}$ be a Gröbner basis for an ideal $I \subset k[x_1, ..., x_n]$ and let $f \in k[x_1, ..., x_n]$. Then there is a unique $r \in k[x_1, ..., x_n]$ with the following two propierties:*

i) No term of r is divisible by any of $LT(g_1), ..., LT(g_t)$.

ii) There is $g \in I$ such that $f = g + r$.

In particular, r is the remainder on division of f by G no matter how the elements of G are listed when using the division algorithm.

Example 10. Let $f = xy$ and $G = \{f_1, f_2\}$ a Gröbner basis with $f_1 = x + z$ and $f_2 = y - z$ in $\mathbb{F}_2[x, y, z]$. We use G to study the uniquess of the division algorithm. We should get the same remainder, but the quotients should be different for the two divisions (lex order).

- Divide xy by $\{f_1, f_2\}$ with a lex order.

$$f = y \cdot f_1 + z \cdot f_2 + z^2 \Rightarrow \text{ The remainder is } + z^2.$$

- Divide xy by $\{f_2, f_1\}$ with a lex order.

$$f = x \cdot f_2 + z \cdot f_1 + z^2 \Rightarrow \text{ The remainder is } + z^2.$$

Corollary 5. Let $G = \{g_1, ..., g_s\}$ be a Gröbner basis for an ideal $I \subset k[x_1, ..., x_n]$ and let $f \in k[x_1, ..., x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.

Definition 25. We will write $\overline{f}^F$ for the remainder on division of f by the ordered s-tuple $F = (f_1, ..., f_s)$. If F is a Gröbner basis for $\langle f_1, ..., f_s \rangle$, then we can regard F as a set.

Example 11. For instance, we take the same function, and the same basis of the example 10.

$$\overline{xy}^G = z^2$$

Definition 26. Let $f, g \in k[x_1, ..., x_n]$ be nonzero polynomials.

i) If $multideg(f) = \alpha$ and $multideg(g) = \beta$, then let $\gamma = (\gamma_1, ..., \gamma_n)$, where $\gamma_i = max(\alpha_i, \beta_i)$ for each i. We call x^γ the **least common multiple** of $LM(f)$ and $LM(g)$, written $x^\gamma = LCM(LM(f), LM(g))$.

ii) The S**-polynomial** of f and g is the combination

$$S(f,g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g \quad .$$

Example 12. Let $f = x^3y^2 - x^2y^3 + x$ and $g = 3x^4y + y^2$ in $\mathbb{F}_2[x, y]$ with the grlex order.
Then $\gamma = (4,2) \Rightarrow x^\gamma = x^4y^2$ and

$$S(f,g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{x^4y} \cdot g = x \cdot f + y \cdot g = x^3y^3 + x^2 + y^3.$$

An S-polynomial $S(f,g)$ is "designed " to produce cancellation of leading terms.

Proposition 2.13. *Let $I \subset k[x_1, ..., x_n]$ be an ideal, and let G be a Gröbner basis of I. Then:*

i) $\overline{f}^G = \overline{g}^G$ *if and only if* $f - g \in I$.

ii) $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$.

iii) $\overline{fg}^G = \overline{\overline{f}^G \overline{g}^G}$.

Proposition 2.14. *Let $f, g \in k[x_1, ..., x_n]$ and x^α, x^β be monomials. Verify that*

$$S(x^\alpha f, x^\beta g) = x^\gamma S(f,g)$$

where

$$x^\gamma = \frac{LCM(x^\alpha LM(f), x^\beta LM(g))}{LCM(LM(f)LM(g))}.$$

Lemma 2.15. *Suppose we have a $\sum_{i=1}^s c_i f_i$, where $c_i \in k$ and $multideg(f_i) = \gamma \in \mathbb{Z}^n_{\geq 0}$ for all i. If $multideg(\sum_{i=1}^s c_i f_i) < \delta$, then $\sum_{i=1}^s c_i f_i$ is a lineal combination , with coefficientes in k, of the S-polynomials $S(f_j, f_k)$ for $1 \leq j, k \leq s$. Furthermore, each $S(f_i, f_k)$ has multidegree $< \delta$.*

Theorem 2.16. ***Buchberger's S-pair criterion***
Let I be a polynomial ideal. Then a basis $G = \{g_1, ..., g_s\}$ for I is a Gröbner basis for I if and only if for all pairs $i \neq j$, the remainder of the division of $S(g_i, g_j)$ by G is zero.

2.8 Buchberger's Algorithm

Example 13. Consider the ring $\mathbb{F}_2[x,y]$ with grlex order, and let

$$I =< f_1, f_2 >=< x^2y+1, xy^2+x > .$$

We see that $\{f_1, f_2\}$ is not a Gröbner basis for I because $LT(S(f_1,f_2)) = x^2 \notin < LT(f_1), LT(f_2) >$. To produce a Gröbner basis, one easy idea is to try first to extend tge ordiginal generating set to a Gröbner basis by adding more polynomials in I. What generators should we add?
We have $S(f_1,f_2) = x^2+y$ and the remainder on division by $F =< f_1, f_2 >=< x^2y+1, xy^2+x >$ is x^2+y, which is non zero. Hence, we should to add that remainer in oir generating set, as a new generator $f_3 = x^2+y$. But,

$$S(f_1,f_2) = f_3 \Rightarrow \overline{S(f_1,f_2)}^F = 0$$

$$S(f_1,f_3) = y^2-1 \Rightarrow \overline{S(f_1,f_3)}^F = y^2+1$$

After that, we can see F is not a Gröbner basis yet. Hence, we will add $f_4 = y^2+1$ to our generating set,

$$F =< f_1, f_2, f_3, f_4 >=< x^2y+1, xy^2+x, x^2+y, y^2+1 > .$$

And we obtain:

$$\overline{S(f_i,f_j)}^F = 0 \quad for \quad all \quad 1 \le i \le j \le 4.$$

It follows that a grlex Gröbner basis for I is:

$$< f_1, f_2, f_3, f_4 >=< x^2y+1, xy^2+x, x^2+y, y^2+1 > .$$

The above example suggests than in general, one should try to extend a basis F to a Gröbner basis by successively adding nonzero remainders $\overline{S(f_1,...,f_j)}^F$ to F.

Theorem 2.17. *Let $I = \langle f_1,...,f_s\rangle \neq 0$ be a polynomial ideal. Then a Gröbner basis for I can be constructed in a finite number of steps by the following algorithm:*

Input: $F = (f_1,...,f_s)$
Output: a Gröbner basis $G = (g_1,...,g_t)$ for I, with $F \subset G$
$G := F$
REPEAT
  $G' := G$
  FOR each pair $\{p,q\}, p \neq q$ *in G' DO*
    $S := \overline{S(p,q)}^{G'}$
    IF $S \neq 0$ *THEN* $G := G \cup \{S\}$
UNTIL $G = G'$.

Lemma 2.18. *Let G be a Gröbner basis for the polynomial ideal I. Let $p \in G$ be a polynomial such that $LT(p) \in \langle LT(G-\{p\})\rangle$. Then $G-\{p\}$ is also a Gröbner basis for I.*

Definition 27. A **minimal Gröbner basis** for a polynomial ideal I is a Gröbner basis G for I such that:

i) $LC(p) = 1$ for all $p \in G$.

ii) For all $p \in G$, $LT(p) \notin \langle LT(G-\{p\})\rangle$.

Example 14. In this example, we going to construct a minimal Gröbner basis. We return once again to the ideal I studied in the example 13.

- In this case, any of the leading coefficients are different from 1, so we already have the first condition of the previous definition.

- Now, we going to eliminate any unneeded generators that might have been including.

$$LT(f_1) = x^2y = y \cdot x^2 = y \cdot LT(f_3).$$

So, we can dispense with f_1 in the minimal Gröbner basis.

$$LT(f_2) = xy^2 = x \cdot y^2 = x \cdot LT(f_4).$$

We can also eliminate f_2.

For this reason, the minimal Gröbner basis is: $G =< f_3, f_4 >=< x^2 + y, y^2 + 1 >$.

Proposition 2.19. *Given a monomial order, if G and $\tilde{G}$ be minimal Gröbner bases for the ideal I,then:*

i) $LT(G) = LT(\tilde{G})$.

ii) G and $\tilde{G}$ have the same number of elements.

Definition 28. A **reduced Gröbner basis** for a polynomial ideal I is a Gröbner basis G for I such that:

i) $LC(p) = 1$ for all $p \in G$.

ii) For all $p \in G$, no monomial of p lies in $\langle LT(G - \{p\})\rangle$.

Proposition 2.20. *Let $I \neq \{0\}$ be a polynomial ideal. Then, for a given monomial ordering, I has unique reduced Gröbner basis.*

Proof. Let G be a minimal Gröbner basis for I . We say that $g \in G$ is reduced for G provided that no monomial of g is in $< LT(G - \{g\}) >$.
Our goal is to modify G until all of its elements are reduced.
A first observation is that if g is reduced for G, then g is also reduced for any other minimal Gröbner basis of I that contains g and has the same set of leading terms. This follows because the definition of reduced only involves the leading terms.
Next, given $g \in G$, let $g' = \overline{g}^{G-\{g\}}$ and set $G' = (G - \{g\}) \cup \{g'\}$. We claim that G' is a minimal Gröbner basis for I . To see this, first note that $LT(g') = LT(g)$, for when we divide g by $G - \{g\}$,$LT(g)$ goes to the remainder since it is not divisible by any element of $LT(G - \{g\})$.
This shows that $< LT(G') >=< LT(G) >$. Since G' is clearly contained in I , we see that G' is a Gröbner basis, and minimality follows.
Finally, note that g' is reduced for G'.
Now, take the elements of G and apply the above process until they are all reduced.
The Gröbner basis may change each time we do the process, but our earlier observation shows that once an element is reduced, it stays reduced since we never change the leading terms. Thus, we end up with a reduced Gröbner basis.

Finally, to prove uniquenes, suppose that G and $\tilde{G}$ are reduced Gröbner bases for I . Then in particular, G and $\tilde{G}$ are minimal Gröbner bases, we will show that this implies they have the same leading terms, i.e., $LT(G) = LT(\tilde{G})$. Thus, given $g \in G$, there is $\tilde{g} \in \tilde{G}$ such that $LT(g) = LT(\tilde{g})$. If we can show that $g = \tilde{g}$, it will follow that $G = \tilde{G}$, and uniqueness will be proved.

Fix a monomial order, and let G and $\tilde{G}$ be minimal Gröbner bases for the ideal I. Prove that $LT(G) = LT(\tilde{G})$. Conclude that G and $\tilde{G}$ have the same number of elements.

To show $g = \tilde{g}$, consider $g - \tilde{g}$. This is in I , and since G is a Gröbner basis, it follows that $\overline{g - \tilde{g}}^G = 0$. But we also know $LT(g) = LT(\tilde{g})$. Hence, these terms cancel in $g - \tilde{g}$, and the remaining terms are divisible by none of $LT(G) = LT(\tilde{G})$ since G and $\tilde{G}$ are reduced. This shows that $\overline{g - \tilde{g}}^G = g - \tilde{g}$, and then $g - \tilde{g} = 0$ follows. This completes the proof. □

2.9 First Applications of Gröbner Bases

In this section, we going to solve the last three problems about ideals and varieties using Gröbner bases.

2.9.1 The Ideal Membership Problem

Theorem 2.21. *$f \in I$ if and only if $\overline{f}^G = 0$*

Example 15. Now, we can decide whether a given polynomial f lies in I as folows:

- Determine whether $f = xy^3 + z^2 + y^5 + z^3$ is in the ideal $I =< x^3 + y, x^2y - z > \in \mathbb{Q}[x,y,z]$. Use the grlex.

  First, we check if I is a Gröbner basis. In this case it isn't. So, we begin by computing a Gröbner basis for I and we find:

  $$G = (f_1, f_2, f_3, f_4, f_5) = \left(y^5 + z^3, xy^3 + z^2, x^3 + y, x^2y + z, xz + y^2\right).$$

  Also, that is a reduced Gröbner basis.

  Dividing, f above by G, we find:

  $$f = 1 \cdot f_1 + 1 \cdot f_2 + 0 \cdot f_3 + 0 \cdot f_4 + 0 \cdot f_5 + 0.$$

  Where, we can see the remiander is zero, because of we have $f \in I$.

- Let $I =< xz - y, xy + z^2, y - z > \in \mathbb{F}_2[x,y,z]$, and use the grlex. Let $f = x^3z$. We want to know if $f \in I$.

  Following the above method, we get:

  $$G = (f_1, f_2, f_3) = \left(xz + z, z^2 + z, y + z\right).$$

  And then,

  $$f = (x^2 + z \cdot f_1 + x \cdot f_2 + z \cdot f_3 + z^2.$$

  The remainder not is zero, for this reason: $f \notin I$.

2.9.2 The Problem of Solving Polynomial Equations

We will study how the Gröbner basis technique can be applied to solve systems of polynomial equations in several variables.

Example 16.

- Find the points in $\mathbb{F}_2[x,y,z]$ on the variety $V(I) = (xz + yz + 1, xy + z + 1, y + 1)$.

  We will a compute a Gröbner basis on I respect to the lex order.

  $$G = (g_1, g_2, g_3) = \left(x + z + 1, y + 1, z^2 + 1\right)$$

If we examine these polynomials, we find somethig remarkable. The polynomial g_2 depends on y alone, we can solve it:

$$y = 1$$

And the polynomial g_3 depends on z alone. Equalizing to zero, we get:

$$z = 1$$

So, we obtains the following solution:

$$y = 1, z = 1 \Rightarrow x + z + 1 = 0 \Rightarrow x + 1 + 1 = 0 \Rightarrow x = 0$$

- Repeat the above exercise for $V(x^2y - z^3, xy - z - 1, z - y^2, x^3 - zy)$.
  In this case, we get:

$$G = (g_1, g_2, g_3) = 1$$

These examples indicate that finding a Gröbner basis for an ideal with respect to the lex order simplifies the form of the equations considerably. A system of equations in this form is easy to solve, especially when the last equation contains only one variable.

2.9.3 The Implicitization Problem

Example 17. Consider the parametric curve V

$$x = t^4$$
$$y = t^3$$
$$z = t^2$$

in $\mathbb{F}_2$. We compute a Gröbner basis G of $I = < t^4 + x, t^3 + y, t^2 + z >$ with respect to the lex order in $\mathbb{F}_2[t, x, y, z]$ and we find

$$G = \{g_1, g_2, g_3, g_4, g_5\} = \{t^2 + z, ty + z^2, tz + y, x + z^2, y^2 + z^3\}.$$

The last two polynomials depends only on x, y, z so they define an affine variety of $\mathbb{C}^3$ containing our curve V

$$x + z^2 = 0$$
$$y^2 + z^3 = 0.$$

Example 18. Now, consider the superface parametrized by

$$x = t + u - x$$
$$y = t^2 + tu - y$$
$$z = t^3 + t^2u - z.$$

We compute a Gröbner basis G for this ideal relative to the lex order, and we obtain:

$$G = (t + u + x, ux + x^2 + y, uy + xy + z, xz + y^2)$$

The last polynomial depends only on x, y, z:

$$xz + y^2 = 0$$

So this polynomial defined a variety.

Chapter 3

Cryptanalysis Techniques in Multivariate Public Key Cryptography

Aulthought we know that there are several multivariate authentication schemes, in this chapter we hereafter focus on **multivatiate asymmetric encryption schemes** and **multivariate signature schemes**.

The **multivariate public key cryptosystems (MPK)** is a special class of schemes whose security is based on the difficulty of solving a set of multivariate polynomial equations. MPK cryptosystem's public keys are a set of multivariate polynomials.

The standard way of building these systems is the next:

1. Fix a finite field $\mathbb{F}_q$ (usually a field of characteristic 2).
2. Fix a quadratic polynomial map Q.
3. Two invertible linear maps S and T are chosen.
4. With the previous steps, we produce the public key $P = T \circ Q \circ S$.

$$\left.\begin{array}{rl} & \text{input } x \\ \text{Private Key } S & \downarrow \\ & x' \\ \text{Private Key } Q & \downarrow \\ & y' \\ \text{Private Key } T & \downarrow \\ & \text{output } y \end{array}\right\} P \text{ Public Key}$$

Definition 29. Let $\mathbb{F}_q$ be the finite field and $\mathbb{F}_{q^n}$ an extension field of size q^n. Let $f(x)$ be an irreducible polynomial of degree n in $\mathbb{F}_q[x]$ and let a represent one of its roots. The field $\mathbb{F}_q(a)$ is isomorphic to

$$\frac{\mathbb{F}_q[x]}{(f)}.$$

Lemma 3.1. *Let the finite field*

$$\mathbb{F}_{q^n} = \frac{\mathbb{F}_q[x]}{(f)}$$

where f is an irreducible polyomial of degree n in $\mathbb{F}_q[x]$.
Then, if a is a root of f we can choose as a basis of $\mathbb{F}_p^n$ over $\mathbb{F}_p$ the set $\{1, a, ..., a^{n-1}\}$.

With this kind of bases the products between elements of the field are very fast it their coordinates are known with respect to that basis.

Definition 30. We denote a multivariable public key by a polynomial mapping from the vector space $\mathbb{K}^n$ to the vector space $\mathbb{K}^m$:

$$\begin{array}{rccc} f: & \mathbb{K}^n & \longrightarrow & \mathbb{K}^m \\ & x=(x_0,...,x_{n-1}) & \longmapsto & y=(p_0(x),...,p_{m-1}(x)) \end{array}$$

where p_i with $1 \leq i \leq m$ are multivariate polynomials defined over $\mathbb{K}[x_0,...,x_{n-1}]$.

Notation.

- *We denote the base field by* $\mathbb{K}$.
- *We use x and y to respectively denote the input and the output of a public key function. In other words, x and y respectively denote the plain text and the cipher text.*

3.1 Matsumoto - Imai Scheme A

The first MPK was proposed in 1985 by Matsumoto and Imai, who presented a scheme "based on obscure representation of polynomials", often called C* and hereafter called Matsumoto-Imai scheme A.

This Scheme uses exponentiation over an extension $\mathbb{E}$ of degree n of a base finite field $\mathbb{K}$ of size q, that is, $\mathbb{K}=\mathbb{F}_q$ and it is defined as follows:

$$\mathbb{K}^n \xrightarrow{S} \mathbb{K}^n \xrightarrow{\varphi} \mathbb{E} \xrightarrow{\wedge^{(1+q^\theta)}} \mathbb{E} \xrightarrow{\varphi^{-1}} \mathbb{K}^n \xrightarrow{T} \mathbb{K}^n \tag{3.1}$$

where:

i) $S:\mathbb{K}^n \longrightarrow \mathbb{K}^n$ and $T:\mathbb{K}^n \longrightarrow \mathbb{K}^n$ are linear transformations, that is, aplications which are fixed and easy to invert whose function is to conceal the exponentiation.

ii) $\varphi:\mathbb{K}^n \longrightarrow \mathbb{E}$ is the canonical embedding of $\mathbb{K}^n$ into $\mathbb{E}$ and $x=\varphi(x)$.
In this case, this map transforms a n-tuple in a polynomial, as follows:

$$\begin{array}{rccc} \varphi: & \mathbb{K}^n & \longrightarrow & \mathbb{E} \\ & x=(x_0,...,x_{n-1}) & \longmapsto & \varphi(x)=\sum_{i=0}^{n} x_i a^i = x_0+x_1 a+...+x_{n-1}a^{n-1}. \end{array}$$

iii) $\varphi^{-1}:\mathbb{E} \longrightarrow \mathbb{K}^n$ transform one plynomial in a n-tuple.

iv) $\wedge^{(1+q^\theta)}:\mathbb{E} \longrightarrow \mathbb{E}$ it is a internal transformation, being $\mathbb{E}$ an extension of fields. The exponent is chosen of the form $1+q^\theta$ and prime to q^n-1 so as to allow efficient inversion.

In other words, the public key is therefore given by the n-tuple $(p_0,...,p_{n-1})$ of polynomials in n unknowns $x_0,...,x_{n-1}$ defined over $\mathbb{K}$ via:

$$\begin{array}{rccc} p: & \mathbb{K}^n & \longrightarrow & \mathbb{K}^n \\ & x=(x_0,...,x_{n-1}) & \longmapsto & p_0(x),...,p_{n-1}(x))=T\circ\ \varphi^{-1}((\varphi\circ\ S(x))^{1+q^\theta}) \end{array}$$

Proposition 3.2. *Given the map*

$$\begin{array}{rccc} \wedge^{(1+q^\theta)}: & \mathbb{E} & \longrightarrow & \mathbb{E} \\ & x & \longmapsto & x^{1+q^\theta} \end{array}$$

we define its inverse as:

$$\begin{array}{rccc} \left(\wedge^{(1+q^\theta)}\right)^{-1}: & \mathbb{E} & \longrightarrow & \mathbb{E} \\ & y & \longmapsto & y^e \end{array}$$

Proof. We are going to see that the reverse map is well defined:

$$(1+q^\theta)e \equiv 1 \mod (q^n-1) \Rightarrow (1+q^\theta)e = k(q^n-1)+1$$

Then,

$$x^{(1+q^\theta)e} = x^{k(q^n-1)+1} = x^{k(q^n-1)}x \tag{3.2}$$

We know $\#\mathbb{E} = q^n$, because of Fermat's little theorem A.1 we have:

$$x^{k(q^n-1)} = (x^{q^n-1})^k = 1^k = 1$$

Thus replacing this in equation (3.2), we have:

$$x^{(1+q^\theta)e} = x^{k(q^n-1)+1} = x^{k(q^n-1)}x = 1 \cdot x = x.$$

□

One key fact allowing an eficient representation of the public key as the n-tuple of polynomials $(p_0,...,p_{n-1})$ is that the mapping $x \mapsto x^q$ is a $\mathbb{K}$-linear mapping, which brings us to the next result.

Proposition 3.3. *The exponential map $x \mapsto x^{(1+q^\theta)}$ is $\mathbb{K}$-quadratic.*

Proof. For the Frobenius Endomorphism A.3 we have :

$$x \mapsto x^q \Longrightarrow x+y \mapsto (x+y)^q = x^q + y^q \Rightarrow \text{It is a linear map.} \tag{3.3}$$

Now, in this case:

$$x \mapsto x^{1+q^\theta} = x(x^q)^\theta = (x^{q^0})(x^{q^\theta}) = \phi_0(x) \cdot \phi_\theta(x)$$

where $\phi_i(x) = x^{q^i}$ and for (3.3) ϕ_i is linear since $\phi_i(x+y) = (x+y)^{q^\theta}$. Thus $\phi_0(x)$ and $\phi_\theta(x)$ are linear, and for this reason $x \mapsto x^{1+q^\theta}$ is quadratic.
Let's see the addition:

$$(x+y) \mapsto (x+y)^{1+q^\theta} = (x+y)\underbrace{(x+y)^{q^\theta}}_{x^{q^\theta}+y^{q^\theta}} = (x+y)(x^{q^\theta}+y^{q^\theta}) =$$

$$= x \cdot x^{q^\theta} + x \cdot y^{q^\theta} + y \cdot x^{q^\theta} + y \cdot y^{q^\theta} = x \cdot \overline{x} + x \cdot \overline{y} + y \cdot \overline{x} + y \cdot \overline{y} \Rightarrow (x+y) \mapsto (x+y)^{1+q^\theta} \text{ is quadratic.}$$

This completes the proof. □

The end result of the map (3.1) is a non-linear system of equations in several variables:

$$\begin{cases} p_0(x_0,...,x_{n-1}) = y_0 \\ \vdots \\ p_{n-1}(x_0,...,x_{n-1}) = y_{n-1} \end{cases} \tag{3.4}$$

for every n-tuple $y = (y_0,...,y_{n-1})$. To recover the plaintext, the given system must be resolved.
To do this, the owner of the secret key uses their knowledge of S and T and an exponent e such that

$$e(1+q^\theta) \equiv 1 \pmod{q^n-1}$$

to invert each component of the public map in turn, which is equivalent to the following calculation:

$$x = S^{-1} \circ \varphi^{-1}((\varphi \circ T^{-1}(y))^e).$$

The name *obscure representation* comes from the assumption that the input and output coordinate systems are unknown to anyone but the secret key owner. Hence, the security of the cryptosystem not only relies on the hardness of solving (3.4), but also on the hardness of recovering any pair of mappings S_0 and T_0 such that:

$\forall x \in \mathbb{K}^n$,

$$T_0 \circ \varphi^{-1}((\varphi \circ S_0(x))^{1+q^\theta}) = T \circ \varphi^{-1}((\varphi \circ S(x))^{1+q^\theta}).$$

Example 19. Fix the field $\mathbb{F}_2^3$ and its extension $\mathbb{E} = \mathbb{F}_{2^3}$ with $\theta = 7$ and S and T invertible, that is regular, matrices, say:

$$S = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \Longrightarrow S(x_0,x_1,x_2) = (x_0+x_1+x_2, x_1, x_0+x_1),$$

$$T = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \Longrightarrow T(x_0,x_1,x_2) = (x_2, x_1+x_2, x_0+x_2).$$

Thus, we have:

$$\mathbb{F}_2^3 \xrightarrow{S} \mathbb{F}_2^3 \xrightarrow{\varphi} \mathbb{F}_{2^3} \xrightarrow{\wedge^{(1+2^7)}} \mathbb{F}_{2^3} \xrightarrow{\varphi^{-1}} \mathbb{F}_2^3 \xrightarrow{T} \mathbb{F}_2^3 .$$

If we take as plain text the vector (1,0,0) and we apply the public key we, obtain:

$$\begin{array}{lccccccccccc} p: & \mathbb{F}_2^3 & \xrightarrow{S} & \mathbb{F}_2^3 & \xrightarrow{\varphi} & \mathbb{F}_{2^3} & \xrightarrow{\wedge^{1+q^\theta}} & \mathbb{F}_{2^3} & \xrightarrow{\varphi^{-1}} & \mathbb{F}_2^3 & \xrightarrow{T} & \mathbb{F}_2^3 \\ & (1,0,0) & \longrightarrow & (1,0,1) & \longrightarrow & 1+a^2 & \longrightarrow & (1+a^2)^{(1+2^7)} = a^2+a & \longrightarrow & (0,1,1) & \longrightarrow & (1,0,1). \end{array}$$

In the same way, from the encrypted text we obtain the plaintext. We take the vector $(0,1,1)$. But, this time we use the exponent e, S^{-1} and T^{-1}. For this reason, the first step is calculate them:

$$(1+q^\theta)e \equiv 1 \; mod(q^n-1) \Rightarrow (1+2^7)e \equiv 1 \; mod(2^3-1) \Rightarrow e = 5$$

$$S^{-1} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \Longrightarrow S^{-1}(x_0,x_1,x_2) = (x_1+x_2, x_1, x_0+x_2),$$

$$T^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \Longrightarrow T^{-1}(x_0,x_1,x_2) = (x_0+x_2, x_0+x_1, x_0).$$

And then, we calculate the inverse map, with help of the secret key:

$$\begin{array}{ccccccccccc} \mathbb{F}_2^3 & \xrightarrow{S} & \mathbb{F}_2^3 & \xrightarrow{\varphi} & \mathbb{F}_{2^3} & \xrightarrow{\wedge^{1+q^\theta}} & \mathbb{F}_{2^3} & \xrightarrow{\varphi^{-1}} & \mathbb{F}_2^3 & \xrightarrow{T} & \mathbb{F}_2^3 \\ (1,0,0) & \longleftarrow & (1,0,1) & \longleftarrow & a^2+1 = (a+a^2)^5 & \longleftarrow & a+a^2 & \longleftarrow & (0,1,1) & \longleftarrow & (1,0,1). \end{array}$$

Finally, we have obtained the plaintext $(1,0,0)$.

Example 20. With the same data from the previous example, we calculate the following:

- The plaintext is $(1,0,0)$ and the ciphertext is $(1,0,1)$.
- The plaintext is $(0,1,0)$ and the ciphertext is $(0,1,0)$.

We going to see that the proposition 3.3 is true:
If we add both plaintexts, we obtain $(1,1,0)$ whereas the ciphertext is $(0,1,1) \neq (1,0,1)+(0,1,0)$. This shows that the map is *not linear.*

3.2 Direct Inversion Attacks

Our goal in this section is to propose a method to decrypt a ciphertext whithout using the private key.

The mapping p constitutes the public key and an attacker can directly search for a value x verifying $p(x) = y$ in order to decrypt y or to forge a signature x.
Such attacks consist in solving the proposed system of quadratic equations of low degree (3.4) and there have been several algorithms designed to solve this task. The most famous is **Buchberger's algorithm**.

This is a system that depends on the variables $(x_0,...,x_{n-1})$, since the $y = (y_0,...,y_{n-1})$ is known, where y is an ciphertext that has been intercepted.
We are going to see that it can be solved by computing **Gröbner bases.**

To optimize the search for the solution, we will include in the original system the polynomial equations satisfied by all polynomial maps coming from the coefficient field, that is,

$$x_i^q - x_i = 0 \quad i = 0,...,n-1.$$

This only works when the size of the field is small, because this way you can limit the exponents of the monomials during the search for a Gröbner Basis. If the field size is large the limitation of the exponents will not affect and, therefore, we will be adding equations that hinder in the intermediate calculations. Thus, we have to solve:

$$\begin{cases} p_0(x_0,...,x_{n-1}) = y_0 \\ \vdots \\ p_{n-1}(x_0,...,x_{n-1}) = y_{n-1} \\ x_0^q - x_0 = 0 \\ \vdots \\ x_{n-1}^q - x_{n-1} = 0 \end{cases} \tag{3.5}$$

So solving this system is equivalent to calculating a Gröbner basis G for the following ideal

$$I = \langle p_0(x_0,...,x_{n-1}) + y_0, \ldots, p_{n-1}(x_0,...,x_{n-1}) + y_{n-1}, x_0^q - x_0, \ldots, x_{n-1}^q - x_{n-1} \rangle$$

and then we solve the new system generated by G as explained in 2.9.2.

3.2.1 Examples

Example 21. In this example, first we going to do de public key in general step by step with the following values:

$$p : \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2^3$$

$$\theta = 7$$

$$S(x_0,x_1,x_2) = (x_0 + x_2, x_0, x_0 + x_1 + x_2)$$

$$T(x_0,x_1,x_2) = (x_1, x_1 + x_2, x_0 + x_2)$$

And then, we will attack the cryptosystem assuming that the intercepted message is $(0,1,1)$.

Let $(x_0,x_1,x_2) \in \mathbb{F}_2^3$:

$$S(x) = (x_0 + x_2, x_0, x_0 + x_1 + x_2) \longmapsto x_0 + x_2 + x_0 a + (x_0 + x_1 + x_2)a^2 \longmapsto$$

$$ax_0^{129} + \left(a^2+a+1\right)x_0^{128}x_1 + a^2x_0x_1^{128} + \left(a^2+1\right)x_1^{129} + a^2x_0^{128}x_2 + \\ + (a+1)x_1^{128}x_2 + (a+1)x_0x_2^{128} + x_1x_2^{128} + \left(a^2+a\right)x_2^{129}.$$

Applying the equations of the field $x_i^2 - x_i = 0 \quad i = 0,\ldots,n-1$, we have:

$$(a+1)x_0x_1 + (a^2+1)x_1^2 + (a^2+a+1)x_0x_2 + ax_1x_2 + (a^2+a)x_2^2 + ax_0 \longmapsto \\ \left(x_0x_1 + x_1^2 + x_0x_2, x_0x_1 + x_0x_2 + x_1x_2 + x_2^2 + x_0, x_1^2 + x_0x_2 + x_2^2\right)$$

Finally, we apply T to the previous result:

$$\left(x_0x_1 + x_0x_2 + x_1x_2 + x_2^2 + x_0, x_0x_1 + x_1^2 + x_1x_2 + x_0, x_0x_1 + x_2^2\right)$$

Thus the public key is given by the following system:

$$\begin{cases} x_0x_1 + x_0x_2 + x_1x_2 + x_2^2 + x_0 = y_0 \\ x_0x_1 + x_1^2 + x_1x_2 + x_0 = y_1 \\ x_0x_1 + x_2^2 = y_2 \end{cases}$$

Now, we begin the attack on the cryptosystem. For this reason, we substitute y and we add the equations of the field:

$$\begin{cases} x_0x_1 + x_0x_2 + x_1x_2 + x_2^2 + x_0 = 0 \\ x_0x_1 + x_1^2 + x_1x_2 + x_0 = 1 \\ x_0x_1 + x_2^2 = 1 \\ x_0^2 - x_0 = 0 \\ x_1^2 - x_1 = 0 \\ x_2^2 - x_2 = 0 \end{cases}$$

To solve the system, we calculate a Gröbner basis G for the ideal that generates its equations, and we obtain $G = \{x_0+1, x_1+1, x_2\}$. Now solving the next system is very easy:

$$\begin{cases} x_0 + 1 = 0 \\ x_1 + 1 = 0 \\ x_2 = 0 \end{cases}$$

And so, we can say that the plaintext was $(1,1,0)$.

Example 22. We attack other cryptosistem with $p : \mathbb{F}_2^8 \longrightarrow \mathbb{F}_2^8$, $\theta = 8$ and S, T the following matrices:

$$S = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

The public key is:

$$\begin{cases} x_0 + x_4 + x_6 = y_0 \\ x_0 + x_2 + x_3 + x_5 + x_6 = y_1 \\ x_0 + x_3 = y_2 \\ x_0 + x_1 + x_7 = y_3 \\ x_2 + x_3 + x_4 + x_5 + x_7 = y_4 \\ x_2 + x_4 + x_5 + x_6 = y_5 \\ x_0 + x_1 + x_2 + x_3 + x_4 + x_6 + x_7 = y_6 \\ x_0 + x_2 + x_4 + x_5 + x_6 = y_7 \end{cases}$$

Now, we begin the attack on the cryptosystem again for the ciphertext $(0,0,1,1,0,0,1)$ and the Gröbner basis obtained is: $\{x_0+1, x_1+1, x_2, x_3, x_4+1, x_5+1, x_6, x_7+1\}$.

Thus, the plaintext was:

$$(1,1,0,0,1,1,0,1).$$

3.2.2 Computational cost

The rationale behind the design of multivariate asymmetric cryptosystems is that the complexity of solving systems of randomly generated quadratic multivariate equations defined over a finite field is exponential in the number of unknowns on the average.

Thanks to the software package SageMath [6] we have been able to create a code that allows the attack to this cryptosystem, thus studying the computational cost in each case as shown in Table 3.1.

q	n	t	time (s)
2	2	2	0.004393
2	3	7	0.004138
2	4	8	0.003899
2	5	28	0.031937
2	6	20	0.214858
2	7	64	10.543728
2	7	93	15.183119
2	7	102	16.04270
2	8	176	0.003543
2	8	224	0.0046949
2	16	32640	0.0041968

q	n	t	time (s)
2^2	2	10	0.0021162
2^2	2	14	0.0035309
2^3	2	22	0.00455713
2^3	2	50	0.00455808
2^3	3	246	0.0053930
2^3	3	370	0.0529861
2^4	2	224	0.002377
2^4	3	2773	1.63645
2^5	2	732	0.0050449
2^5	3	3799	91.092567
2^5	3	17390	738.2297

Figure 3.1: Computational cost in seconds.

The used code can be found in Appendix.

Performing the above calculations we have found that we are not able to crack the cryptosystem through Gröbner bases for the following fields among others:

$$\mathbb{F}_2^9, \mathbb{F}_2^{10}, \mathbb{F}_2^{11}, \mathbb{F}_2^{12}, \mathbb{F}_2^{13}, \mathbb{F}_2^{14}, \mathbb{F}_2^{15}.$$

In addition, there are cases in which we are not able to generate the public key due to the large size of the field.

For this reason in this type of systems the choice of the field is important. It is not interesting that the size of the field is very large so that the size of the key does not shoot, but on the other hand, it is interesting that the size of the field is not very small so that the attacker cannot use the simplifying equations mentioned above coming from the field in an effective way.

Bibliography

[1] GREGORY V.BARD, *Algebraic Cryptanalysis*, Colection Springer, 2009.

[2] JON CALLAS, *An Introduction to Cryptography*, `http://cisweb.bristolcc.edu/ ik/Download/CIT18/IntroToCrypto.pdf`

[3] MASSIMILIANO SALA, TEO MORA, LUDOVIC PERRET, SHOJIRO SAKATA, CARLO TRAVERSO, *Gröbner Bases, Coding, and Cryptography*, Colection Springer, 2009.

[4] DAVID COX, JOHN LITTLE AND DONAL 0'SHEA, *Ideals, Varieties, and Algoritms*, Colection Springer, Second Edition.

[5] CHRISTOF PAAR, JAN PELZL, *Understanding Cryptography*, Colection Springer, 2010.

[6] SAGEMATH, *the Sage Mathematics Software System (Version 8.6)*, *The Sage Developers, 2019,* `https://www.sagemath.org`.

Appendix A

In this chapter we have written some theorems that have been known throughout the text. We also include their respective demonstrations too.

Theorem A.1. *Fermat's Little Therorem*
Let p be a prime. Then for any integer n with $p \nmid n$ we have $n^{p-1} \equiv 1$ modulo p.

Proof. Let G be the group of units of $\mathbb{Z}_p$. As $\mathbb{Z}_p$ is a field, $G = \mathbb{Z}_p - \{0\}$ thus G is a finite group of order $p-1$. For any n with $p \nmid n$, the coset $\overline{n}$ is an element of G thus

$$\overline{n}^{p-1} = 1.$$

□

Proposition A.2. *Let $p \in \mathbb{N}$ prime and $q \in \mathbb{N}$ with $q < p$. Then, $\binom{p}{q}$ is multiple of p.*

Proof.

$$\binom{p}{q} = \frac{p!}{q!(p-q)!} = \frac{(p-1)!}{q!(p-q)!} \cdot p$$

p prime and $\begin{cases} p > q \\ p > p-q \end{cases} \Rightarrow \begin{cases} p \nmid q! \\ p \nmid (p-q)! \end{cases} \Rightarrow \binom{p}{q}$ is multiple of p. □

Theorem A.3. *Frobenius Endomorphism*

Let F be a commutative ring with prime characteristic p,then the application $\phi : F \longrightarrow F$ given by $\alpha \longmapsto \phi(\alpha) = \alpha^p \quad \forall \alpha \in F$ is called Frobenius Endomorphism.

Proof. For all α and $\beta \in F$, developing for Newton's binomial we have:

$$(\alpha+\beta)^p = \alpha^p + \binom{p}{1}\alpha^{p-1}\beta + ... + \binom{p}{i}\alpha^{p-i}\beta^i + ... + \binom{p}{p-1}\alpha\beta^{p-1} + \beta^p$$

We know:

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+2)(p-i+1)}{i(i-1)\cdots 2\cdot 1} \in \mathbb{N}.$$

But, p is prime and by A.2 each factor of denominator is less than p, then p divides $\binom{p}{i}$ for all $i = 1,2,...,p-1$ and also F has characteristic p, $\binom{p}{i}\alpha^{p-i}\beta^i = 0$. Then:

$$\phi(\alpha+\beta) = (\alpha+\beta)^p = \alpha^p + \beta^p = \phi(\alpha) + \phi(\beta).$$

Now,

$$\phi(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \phi(\alpha)\phi(\beta).$$

Thus, we have seen that ϕ is a homomorphism of ring, and with this the proof is ends.

□

ALGORITHMS

Below are the algorithms which are used in the chapter on rings and Gröbner bases.

- **Division Algorithm in $k[x_1, \ldots, x_n]$**
  - Input (f, g, R): Where R is a polinomial Ring, f a polynomial and g a polynomial list.
  - Output (a, r): Where a is a tuple with the quotients and r is the remainder of f on division by g.

```
def div(f,g,R):
    n = len(g)
    p, r, a = R(f),R(0),n*[R(0)]
    while p != 0:
        i, divisionoccured = 0, False

        while i < n and divisionoccured == False:
            if g[i].lt().divides(p.lt()):
                a[i] = a[i] + p.lt()//g[i].lt()
                p = p - (p.lt()//g[i].lt())*g[i]
                divisionoccured = True
            else:
                i = i + 1
        if divisionoccured == False:
            r = r + p.lt()
            p = p - p.lt()
    return   a, r
```

- **S-Polynomial**
  - Input (f, g, R): Where R is a polynomial ring and f and g two polynomials.
  - Output (S): Where S is the sought polynomial.

```
def mcm(f,g,R):
    return (f*g).quo_rem(gcd(f,g))[0]
```

```
def Spol(f,g,R):
    p=mcm(f.lt(),g.lt(),R)
    S=(p.quo_rem(f.lt())[0])*f-(p.quo_rem(g.lt())[0])*g
    return S
```

- **Buchberger's Algorithm**
  - Input (g, R): Where R is a polynomial ring ang g a polynomial list.
  - Output (g): That is, a Gröbner basis.

```
def buch(g,R):
    n=len(g)
    i=0
    j=0
    for i in [0..n-2]:
        for j in [i+1..n-1]:
            S=Spol(g[i],g[j], R)
            #print S
            r=div(S,g,R)
            #print r
            if r!=0:
                return buch(g+[r],R)
    return g
```

PLAINTEXT AND CIPHERTEXT

In this paper, we found the code for encrypting and decrypting a known tuple in a finite field.

We define:

- $\mathbb{K} = \mathbb{F}_q$ a finite field with $q = 2^m$ elements.
- $\mathbb{E}$ as the extension $\mathbb{F}_{q^n}$.
- Kn the vector space $\mathbb{K}^n$.
- $\mathbb{E}$ as the extension $\mathbb{F}_{q^n}$.

The function φ is given by `from_Kn()` and its inverse is given by `to_Kn()`.

We select the following dates, for this example:

- $n = 3$
- $q = 2$
- $t = 2$
- plaintext $= (1, 1, 0)$

```
n=3
q=2
K=GF(q)
E=FiniteField(q^n)
listax=[var('x%d'%i) for i in range(n)]
E2=PolynomialRing(E,listax)
Kn, from_Kn, to_Kn = E.vector_space(K, map=True)
```

We choose t like θ in the paper, which must be that $1 + q^t$ is prime with $q^n - 1$.

And then, from the previous data we calculate $t1$ which is the inverse of t, in the document it corresponds to e.

```
t=2
gcd(1+q^t,q^n-1)
t1=ZZ(mod(1/(1+q^t),(q^n-1)))
show(t)
show(t1)
```

2

3

```
follow=True
while follow:
    T=random_matrix(K,n)
    if det(T)<>0:
        follow=False
follow=True
while follow:
    S=random_matrix(K,n)
    if det(S)<>0:
        follow=False
T,S
```

$$\left(\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}\right)$$

The function $x^{(1+q^\theta)}$ is defined as a polynomial.

```
R.<x>=PolynomialRing(E2)
```

Let **encrypt**:

- Input $(v, M1, M2, q, t)$: Where v is a plaintext (vector), $M1$ and $M2$ the matrix associated with the S and T linear morphisms respectively and, q, t previously defined.
- Output : Vector corresponding to the ciphertext.

Let **decrypt**:

- Input $(v, M1, M2, q, t, t1)$: Where v is a ciphertext (vector), $M1$ and $M2$ the matrix associated with the S and T linear morphisms respectively and, $q, t, t1$ previously defined.
- Output : Vector corresponding to the plaintext.

```
def encrypt(v,M1,M2,q,t):
    f=x^(1+q^t)
    return M2*to_Kn(f(x=from_Kn(M1*v)))
def decrypt(v,M1,M2,q,t,t1):
    f=x^t1
    return M1^(-1)*to_Kn(f(x=from_Kn(M2^(-1)*v)))
```

```
v=vector([1,1,0])
w=encrypt(v,S,T,q,t)
w,decrypt(w,S,T,q,t,t1)
```

$$((0, 1, 1), (1, 1, 0))$$

MATSUMOTO - IMAI ATTACK

We define the necessary fields and extensions for then, attack the cryptosystem.

- $\mathbb{K} = \mathbb{F}_q$ a finite field with $q = 2^m$ elements.
- $\mathbb{E}$ as the extension $\mathbb{F}_{q^n}$.
- Kn the vector space $\mathbb{K}^n$.
- $\mathbb{E}$ as the extension $\mathbb{F}_{q^n}$.
- $E2aux$ is a polynomial ring with variables $x_0, \ldots, x_{n-1}$ and coefficientes over $\mathbb{E}$.
- $E2$ is a quotient ring $\frac{E2aux}{< x_0^q - x_0, \ldots, x_{n-1}^q - x_{n-1} >}$.
- $E22$ is a polynomial ring with variables as $E2$ and coefficients in E, that say $\mathbb{F}_{q^n}[X_0, \ldots, X_{n-1}]$.
- Ka is a polynomial ring with a variable over E and coefficientes in K, $\mathbb{F}_2^n$.
- $E3$ is a polynomial ring with a variables of $E2aux$ and Ka, and coefficients in ka, thus $E3 = K[a][x_0, \ldots, x_{n-1}]$.
- $E4$ is a polynomial ring with a variables of $E2aux$ and Ka, and coefficients in ka, thus $E4 = K[a, x_0, \ldots, x_{n-1}]$.
- $E5$ is a polynomial ring of the form $\mathbb{F}_{2^n}[x_1, .., x_{n-1}]$.
- $E6$ is the last polynomial ring, and it a field that contains the variables corresponding to the ciphertext and plaintext.

```
import time
n=3
q=2^5
K=GF(q)
E=FiniteField(q^n)
listax=[var('x%d'%i) for i in range(n)]
listay=[var('y%d'%i) for i in range(n)]
E2aux=PolynomialRing(E,listax)
eqs0=[E2aux(_^q-_) for _ in listax]
E2=E2aux.quotient_ring(eqs0)
E22=PolynomialRing(E,E2.gens())
Ka=PolynomialRing(K,E.variable_name())
E3=PolynomialRing(Ka,listax)
varsx=list(E3.variable_names())
vars=[Ka.variable_name()]+varsx
E4=PolynomialRing(K,vars)
E5=PolynomialRing(K,varsx)
E6=PolynomialRing(K,varsx+listay,order='lex')
z3=E4.variable_names()[0]
aes=[Ka(Ka.variable_name())^i for i in range(n)]
Kn = E.vector_space(K, map=True)
```

We choose t like θ in the paper, which must be that $1 + q^t$ is prime with $q^n - 1$.

```
follow=True
while follow:
    taux=randint(0,q^n-1)
    if gcd(1+q^taux,q^n-1)==1:
        t=taux
        follow=False
t
```

```
11479
```

```
j=sum([E2(listax[i])*E2(aes[i]) for i in range(n)])
j2=j^(1+q^t)
```

```
eqs1aux=[E5(_) for _ in
(E4(E3(E22(j2))).polynomial(E4(z3))).coefficients()[::-1]]
eqs1=[E6(eqs1aux[i])+E6(listay[i]) for i in range(n)]
eqs2=[E5(_^q-_) for _ in listax]
eqs=eqs1+eqs2
I=E6.ideal(eqs)
```

Now, we already have the system of equations that make up our cryptosystem(in our paper (3.5)).

And, now we are going to attack it with Gröbner bases.

```
w1=walltime()
gb=I.groebner_basis()
w2=walltime()
w2-w1
```

```
91.24908399581909
```