Criptografía con bases de Gröbner

Gröbner basis and Cryptography

Pablo de la Torre Fernández

Trabajo de Fin de Grado

Álgebra

Sección de Matemáticas

Universidad de La Laguna

La Laguna, 16 de junio de 2016

Dra. Dña. **Evelia R. García Barroso**, con N.I.F. 42.851.422-F Profesora Titular de Universidad adscrita al Departamento de Matemáticas, Estadística e Investigación Operativa de la Universidad de La Laguna

C E R T I F I C A

Que la presente memoria titulada:

"*Criptografía con bases de Gröbner*"

ha sido realizada bajo su dirección por D. **Pablo de la Torre Fernández**, con N.I.F. 78.854.078-G.

Y para que así conste, en cumplimiento de la legislación vigente y a los efectos oportunos firman la presente en La Laguna a 16 de junio de 2016

Agradecimientos

A todas esas personas que han hecho que mi etapa en la carrera haya sido increíble. En especial a mis amigos y novia, por hacer que de puertas hacia fuera de la Universidad, haya tenido siempre alguien con quien contar y sobre todo alguien con quien disfrutar.

A mi familia por brindarme la oportunidad de acceder a la Universidad y por su apoyo en todo momento.

A mi tutora, Evelia García Barroso, por su inmensa ayuda durante estos 2 años de trabajo. Por haberme dedicado su tiempo y compartido su conocimiento.

A la ULL por hacer posible este camino que llega a su final.

Resumen

La Criptografía es la ciencia que se encarga de codificar información para ser protegida frente a observadores no autorizados, mediante el uso de procedimientos cuya seguridad se sustenta en la dificultad de resolver determinados problemas matemáticos. En esta memoria tratamos los procedimientos definidos a partir de un sistema de ecuaciones polinomiales en varias variables, representados mediante el ideal generado por los polinomios que definen el sistema. Buchberger introdujo las denominadas bases de Gröbner, que son un conjunto de generadores de un ideal de polinomios en varias variables, con ciertas características óptimas para su aplicación en la Criptografía.

Mostramos aquí la aplicación de las bases de Gröbner a la Criptografía en una doble vertiente: por un lado su utilización en el diseño de los criptosistemas denominados Polly Cracker, y por otro su uso para definir estrategias de ataques algebraicos en función de la información interceptada.

Palabras clave: Criptografía, bases de Gröbner, criptosistemas Polly Cracker, ataques algebraicos.

Abstract

Cryptography is the science based on the process for encoding information to be secure against a non authorizated observer. The security of this process lies on the hardness of solving some mathematical problems. In this memory we had focus our attention on polynomial equations system in several variables, that can be represented by the ideal generated by the polynomials on the system. The representation of this ideal was studied by Buchberger, who introduced the Gröbner basis, which are a generating set of a polynomial ideal with some proper characteristic to be applied on Cryptography.

We show the applications of the Gröbner basis on Cryptography in two different ways, one to design the denominated Polly Cracker cryptosystems, and the other to define different algebraic attack strategies depending on the intercepted information.

Keywords: *Cryptography, Gröbner basis, cryptosystem, Polly Cracker, algebraic attack.*

Índice general

Introducción

Durante siglos los *códigos secretos* fueron usados para proteger los mensajes de los lectores no autorizados. La falta de un modelo riguroso para la comunicación impedía que dicha comunicación fuera segura. La Criptografía era considerada como un arte más que una ciencia y un cifrado era considerado seguro hasta que un atacante podía romperlo. A finales de los años cuarenta del siglo XX, Shannon (ver [S1],[S2]) presenta un modelo matemático riguroso basado en un conjunto de funciones desde el espacio de texto sin formato al espacio de texto cifrado. El problema con los sistemas de cifrado tal como fue diseñado por Shannon es que los interesados en compartir información tienen que intercambiar la clave antes de la transmisión de datos. Esto puede ser difícil ya que requiere la presencia de un canal seguro. En 1976, Diffie y Hellman resolvieron este problema con un protocolo de intercambio de claves y sus ideas fueron adaptadas para diseñar un sistema de cifrado basado en dos claves, una pública y una secreta. Nace así la denominada *Criptografía de clave pública o asimétrica*, en contraposición a la *Criptografía tradicional o simétrica*. Aunque los criptosistemas asimétricos no pueden proporcionar el mismo nivel de seguridad que los simétricos sin un coste computacional más grande, son los únicos viables para garantizar protocolos seguros de intercambio de información imprescindibles para el modo de vida actual en el que internet está cada vez más presente.

Shannon afirma en su trabajo que *The problem of good cipher design is essentially one of finding difficult problems ...How can we ever be sure that a system which is not ideal . . . will require a large amount of work to break with every method of analysis? ...We may construct our cipher in such a way that breaking it is equivalent to..the solution of some problem known to be laborious.*

Entre los problemas matemáticos *laboriosos* hay uno de gran interés: ¿Cómo *resolver* un sistema de ecuaciones polinomiales? Esto conlleva a un problema más general: representar de una manera *estándar* un ideal del anillo de polinomios en varias variables y con coeficientes en un cuerpo. En esta memoria estudiaremos una familia de criptosistemas asimétricos basada en este problema.

En 1965 Buchberger, en su tesis doctoral, presentó un marco adecuado para el estudio de los ideales de polinomios, con la introducción de las *bases de Gröbner*. Sus trabajos dieron lugar a nuevos resultados de investigación en el Álgebra computacional, con innumerables aplicaciones en Matemáticas, Ingeniería, Física e incluso en Biología y otras ciencias. En esta memoria mostraremos aplicaciones de las bases de Gröbner a la Criptografía.

Un cuerpo finito K puede no parecer particularmente interesante para los matemáticos

acostumbrados a cuerpos infinitos, pues únicamente contiene un número finito de elementos y todos los elementos no nulos son exactamente las potencias de un elemento primitivo, proporcionando una estructura de grupo a las unidades de K. Sin embargo, su estructura de cuerpo es importante desde el punto de vista de los anillos de polinomios y de las *variedades algebraicas*. Por otra parte, K tiene la interesante propiedad de que todas las aplicaciones de K^n a K pueden ser representadas como polinomios en $K[x_1, ..., x_n]$. Ello determina la interacción entre las bases de Gröbner y la Criptografía.

En Criptografía de clave pública el sistema de cifrado más ampliamente desplegado hoy es sin ninguna duda el sistema RSA. Su seguridad está relacionada con el hecho de que, hasta ahora, no se conoce ningún algoritmo razonablemente rápido para la factorización de números enteros grandes en máquinas convencionales. Sin embargo una nueva amenaza ha aparecido recientemente que podría romper el criptosistema RSA: los ordenadores cuánticos. Bajo el supuesto de que los ordenadores cuánticos pueden ser construidos, en 1997 Shor propuso un algoritmo que puede factorizar un número entero en tiempo polinómico en función de su tamaño en bits, haciendo así el criptosistema RSA vulnerable. En la actualidad se destina gran cantidad de recursos a la construcción de ordenadores cuánticos y aunque aún no existen ordenadores de este tipo capaces de atacar el RSA, cada vez es más acuciante la necesidad de otros sistemas criptográficos eficientes y seguros, que puedan resistir futuros ordenadores cuánticos. En este sentido se tienen los sistemas criptográficos basados en códigos correctores de errores, como el dado por McEliece en 1978 - para el cual ya se conocen ataques [Cou-MC-P] - y aquellos basados en sistemas de ecuaciones polinomiales en varias variables, en los que nos centraremos en esta memoria. La seguridad de estos últimos reside en la dificultad de resolver dichos sistemas. Presentaremos los criptosistemas llamados *Polly cracker*, introducidos en [Fe-Ko] y estudiados en [Levy et al.] y [Bau et al.]. Estos criptosistemas intentaron dar respuesta a la pregunta *¿Por qué no se puede tener la esperanza de utilizar bases de Gröbner en criptografía de clave pública? : una carta abierta a un científico que falló y un desafío para aquellos que aún no han fallado* planteada en [Bar]. El desafío de Boo Barkee et al. sigue en pie con respecto al punto de vista del diseño de criptosistemas seguros y eficientes basados en bases de Gröbner, pues ninguna de las propuestas realizadas hasta ahora ha tenido éxito. Sin embargo las bases de Gröbner sí se han mostrado útiles como herramienta para el criptoanálisis, es decir, para el diseño de ataques a criptosistemas establecidos, tal y como mostraremos en este trabajo.

Esta memoria consta de tres capítulos: en el primero estudiamos las bases de Gröbner de un ideal del anillo de polinomios y la variedad algebraica asociada al mismo. En el segundo capítulo presentamos los criptosistemas Polly Cracker, que se definen usando bases de Gröbner y en el tercero, exponemos ataques a criptosistemas de clave pública, donde las bases de Gröbner juegan un papel fundamental.

Capítulo 1

Ingredientes algebraicos y geométricos

En este capítulo empezamos abordando los principales conceptos necesarios para introducir la *Teoría de bases de Gröbner* y en los posteriores capítulos presentaremos los criptosistemas denominados *Polly Cracker* y posibles ataques a los mismos haciendo uso de dicha teoría.

Trabajaremos en un cuerpo K, que usualmente será el cuerpo $\mathbb{F}_q$ de característica p y de q elementos y consideramos el anillo de polinomios en n variables con coeficientes en K:

$$P := K[x_1, \ldots, x_n] = \left\{ \sum_{i=1}^{m} a_i x_1^{v_{i_1}} \cdots x_n^{v_{i_n}} \ : \ m \in \mathbb{N},\ a_i \in K,\ (v_{i_1}, \ldots, v_{i_n}) \in \mathbb{N}^n \right\}.$$

Para simplificar la notación, si $v_i = (v_{i_1}, \ldots, v_{i_n}) \in \mathbb{N}^n$ denotaremos $x^{v_i} := x_1^{v_{i_1}} \cdots x_n^{v_{i_n}}$. En toda esta memoria el conjunto $\mathbb{N}$ denota el conjunto de los números enteros no negativos.

1.1. Ingredientes algebraicos

Las bases de Gröbner serán sistemas generadores de un ideal contenido en un anillo de polinomios en varias variables. Estamos acostumbrados a operar con polinomios en una variable para los que el grado de los monomios están ordenados gracias al orden total de los números naturales. Para ordenar los monomios de un polinomio en varias variables debemos definir una ordenación de términos:

Definición 1.1.1. *Un orden parcial $\leq$ en $\mathbb{N}^n$ se denomina ordenación de términos si*

(i) $\leq$ *es un orden total,*

(ii) $0 \leq v_i$ *para todo* v_i *perteneciente a* $\mathbb{N}^n$*,*

(iii) $v_1 \leq v_2$ *entonces* $v_1 + v \leq v_2 + v$ *para cualesquiera* v_1, v_2*, y pertenecientes a* $\mathbb{N}^n$*.*

Recordemos que un orden total en $\mathbb{N}^n$ *es aquel en el que* $v_1 \leq v_2$ *o* $v_2 \leq v_1$ *para cualesquiera* v_1 *y* v_2 *pertenecientes a* $\mathbb{N}^n$.

Durante este trabajo usaremos el *orden lexicográfico* $\leq_{lex}$ en $\mathbb{N}^n$ que se define como sigue: si $(v_1, ..., v_n), (w_1, ..., w_n) \in \mathbb{N}^n$ diremos que $(v_1, ..., v_n) \leq_{lex} (w_1, ..., w_n)$ si se verifica alguna de las siguientes condiciones:

- $v_1 < w_1$,
- $v_1 = w_1$ y $v_2 < w_2$,

  $\vdots$
- $v_1 = w_1$, $v_2 = w_2, \cdots, v_{n-1} = w_{n-1}$ y $v_n \leq w_n$.

Definición 1.1.2. *Sean* $f = \sum_{v \in \mathbb{N}^n} a_v \cdot x^v$ *un polinomio no nulo en el anillo de polinomios* P *y* $\leq$ *una ordenación de términos. El término inicial de* f *respecto de* $\leq$ *se define como* $in_{\leq}(f) = a_w x^w$ *donde* $w = max_{\leq}\{v \in \mathbb{N}^n : a_v \neq 0\}$. *Sea* $F = \{f_1, ..., f_n\}$ *un conjunto de polinomios del anillo de polinomios* P. *Se define el conjunto de términos iniciales de* F *respecto a una ordenación de términos* $\leq$ *como:*

$$IN_{\leq}(F) = \{in_{\leq}(f_i) \, : \, f_i \in F\}.$$

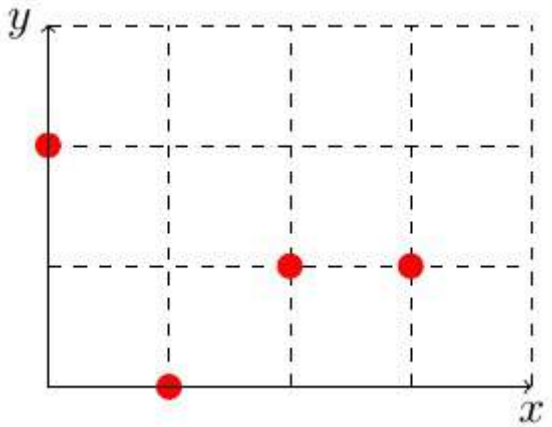
Propiedades 1.1.3. *Sean* f *y* g *polinomios no nulos en* P. *Entonces:*

1. $in_{\leq}(f \cdot g) = in_{\leq}(f) \cdot in_{\leq}(g)$.
2. $in_{\leq}(f + g) \leq max\{in_{\leq}(f), in_{\leq}(g)\}$.

Demostración. Análogas a las propiedades del grado de los polinomios en una variable. □

Definición 1.1.4. *Llamamos soporte de un polinomio* $f = \sum_{i=1}^{m} a_i \cdot x^{v_i} \in P$ *al conjunto de vectores* $v_i \in \mathbb{N}^n$ *tal que* $a_i \neq 0$. *Lo representamos como* $Sop(f)$.

Ejemplo 1.1.5. *Sea* $f(x, y) = x^3y + x^2y + x + y^2$, *entonces su soporte es* $Sop(f) = \{(3, 1), (2, 1), (1, 0), (0, 2)\}$.



Definición 1.1.6. *Dados un subconjunto F del anillo de polinomios P, un polinomio f de P y una ordenación de términos $\leq$, denominamos forma normal de f respecto de F y $\leq$, a un polinomio mónico $\overline{f}$ que verifique que:*

1. *La intersección de $Sop(\overline{f})$ con $(IN_{\leq}(F) + \mathbb{N}^n)$ es vacía.*
2. *Existe un elemento h del ideal generado por F tal que $\overline{f} = f + h$.*

Proposición 1.1.7 (Algoritmo de la división). *Sean $f, f_1, ..., f_m \in P\backslash\{0\}$. Fijamos una ordenación de términos $\leq$ en $\mathbb{N}^n$. Entonces existen $a_1, ..., a_m, r \in P$ tales que $f = a_1 \cdot f_1 + ... + a_m \cdot f_m + r$, donde r=0 o ninguno de los términos en r es divisible por $in_{\leq}(f_1), ..., in_{\leq}(f_m)$. Además $in_{\leq}(a_i \cdot f_i) \leq in_{\leq}(f)$ para $a_i \cdot f_i \neq 0$.*

Demostración. Empezamos tomando $a_1 := 0, ..., a_m := 0, r := 0$ y $s := f$. Se verifica la siguiente expresión:

$$f = a_1 \cdot f_1 + ... + a_m \cdot f_m + r + s \tag{1.1}$$

que se mantendrá cierta en cada paso a lo largo del algoritmo. Procedemos de la siguiente manera:

Paso 1: Si $s = 0$ hemos terminado, de lo contrario continuamos al siguiente paso.

Paso 2: Observamos si $in_{\leq}(s)$ es divisible por algún $in_{\leq}(a_i \cdot f_i)$, si es divisible continuamos al paso 3, en caso contrario pasamos al paso 4.

Paso 3: Tomamos el menor i que verifique que $in_{\leq}(s)$ es divisible por $in_{\leq}(a_i \cdot f_i)$ y ponemos: $s := s - \frac{in_{\leq}(s)}{in_{\leq}(f_i)} \cdot f_i$ y $a_i = a_i + \frac{in_{\leq}(s)}{in_{\leq}(f_i)}$.
Observamos que (1.1) continua verificándose y nuestro término s ha disminuido su grado. Volvemos al paso 1.

Paso 4: Ponemos $r := r + in_{\leq}(s)$ y $s := s - in_{\leq}(s)$. Nuevamente (1.1) continúa verificándose, además el término s ha disminuido su grado. Volvemos al paso 1.

De esta forma obtendremos una secuencia de términos s a lo largo del algoritmo y el grado de s va disminuyendo estrictamente. Por lo que eventualmente después de un número finito de pasos, obtendremos $s := 0$ y el algoritmo nos proporcionará la expresión (1.1) con los a_i y r correspondientes y con $s := 0$.
Ahora debemos demostrar que $in_{\leq}(a_i \cdot f_i) \leq in_{\leq}(f)$. Después del paso 3 tenemos que $a_i = a_i + \frac{in_{\leq}(s)}{in_{\leq}(f_i)}$, es en el único paso donde se actualice el valor de los a_i; por lo tanto todos los términos de a_i serán de la forma $\frac{in_{\leq}(s)}{in_{\leq}(f_i)}$, por lo que el término inicial de a_i será $\frac{in_{\leq}(s)}{in_{\leq}(f_i)}$ para cierto s de un paso intermedio del algoritmo. Por otro lado tenemos que $in_{\leq}(s) \leq in_{\leq}(f)$, ya que s en un principio es igual f pero a lo largo del algoritmo va disminuyendo su grado, por lo que podemos escribir:
$in_{\leq}(a_i f_i) = in_{\leq}((\frac{in_{\leq}(s)}{in_{\leq}(f_i)})f_i) = \frac{in_{\leq}(s)}{in_{\leq}(f_i)} in_{\leq}(f_i) = in_{\leq}(s) \leq in_{\leq}(f)$. Como queríamos ver. □

Veamos con un ejemplo como funciona el algoritmo de la división:

Ejemplo 1.1.8. *Sean* $f = x^3y + x^2y + x + y^2$, $f_1 = x^2 + y$ *y* $f_2 = x^2y + 1$ *polinomios del anillo* $\mathbb{R}[x, y]$, *trabajaremos con el orden lexicográfico, siendo* $x \geq y$. *La división de* f *entre* $\{f_1, f_2\}$ *por lo que el algoritmo comienza con la siguiente expresión:*
$f = a_1f_1 + a_2f_2 + (r + s)$, *donde* $a_1 := a_2 := r := 0$ *y* $s := f$.

Paso 1: $in_{\leq}(s) = x^3y$ *es divisible por* $in_{\leq}(f_1) = x^2$, *por lo que actualizamos los valores de* s *y* a_1*:*
$s := s - \frac{in_{\leq}(s)}{in_{\leq}(f_1)}f_1 = x^2y - xy^2 + x + y^2$
$a_1 := a_1 + \frac{in_{\leq}(s)}{in_{\leq}(f_1)} = xy.$

Paso 2: $in_{\leq}(s) = x^2y$ *será divisible por* $in_{\leq}(f_1) = x^2$, *y los valores actualizados:*
$s := -xy^2 + x$
$a_1 := xy + y.$

Paso 3: $in_{\leq}(s) = -xy^2$ *que en este caso no es divisible ni por* $in_{\leq}(f_1)$ *ni* $in_{\leq}(f_2)$, *ahora actualizamos los valores de* s *y* r*:*
$s := s - in_{\leq}(s) = x$
$r := r + in_{\leq}(s) = -xy^2.$

Paso 4: Por último tenemos que $in_{\leq}(s) = x$ *que tampoco es divisible por* $in_{\leq}(f_1)$ *ni* $in_{\leq}(f_2)$, *y acabamos con:*
$s := 0$
$r := -xy^2 + x.$

Por lo que finalizamos con la expresión: $f = (xy + y)(x^2 + y) + 0(x^2 + 1) + (-xy^2 + x)$.

Definición 1.1.9. *Suponemos que* f *es un polinomio de* P *y sea* $F = \{f_1, ...f_m\}$ *una secuencia de polinomios no nulos en* P. *Denotamos* f^F *como el resto* r *que nos da el algoritmo de la división de* f *entre* F.

Ejemplo 1.1.10. *El resto de dividir* $f = x^3y+x^2y+x+y^2$ *entre* $f_1 = x^2+y$ *y* $f_2 = x^2y+1$ *es* $r := -xy^2+x$. *Mientras que si cambiamos el orden y ponemos* $f_1 = x^2y+1$ *y* $f_2 = x^2+y$ *el resto será* $r := y^2 - 1$.

1.1.1. Bases de Gröbner

Nos interesa un conjunto generador con la propiedad de que el resto del algoritmo de la división es independiente del orden de los elementos dentro de la base. Un sistema generador con esta propiedad lo denominaremos *base de Gröbner*.

Definición 1.1.11. *Un conjunto de polinomios no nulos* $F = \{f_1, ..., f_m\}$ *contenido en* P *se llama* base de Gröbner para un ideal I de P *respecto una ordenación de términos* $\leq$ *si* F *está contenido en* I *y para todo polinomio no nulo del ideal* I *se verifica que existe algún polinomio* f_i *tal que el término inicial de* f_i *divide al término inicial de* f. *El conjunto* F

se llama base de Gröbner respecto de $\leq$ *si es base de Gröbner para el ideal generado por* $f_1, ..., f_m$ *respecto de* $\leq$.

Proposición 1.1.12. *Sea* $G = \{f_1, ..., f_m\}$ *una base de Gröbner respecto de* $\leq$. *Un polinomio* f *de* P *pertenece al ideal* $I =< f_1, ..., f_m >$ *si sólo si el resto de dividir* f *entre* G *es cero* ($f^G = 0$).

Demostración. Por el algoritmo de la división obtenemos la expresión $f = a_1 \cdot f_1 + ... + a_m \cdot f_m + f^G$, y despejando el resto de esta expresión tenemos: $f^G = f - a_1 \cdot f_1 - ... - a_m \cdot f_m$, por lo que el resto pertenece al ideal I.
Por reducción al absurdo suponemos que el resto es no nulo. Como $\{f_1, ..., f_m\}$ es base de Gröbner del ideal I y el resto pertenece a este ideal, tendremos que $in_{\leq}(f^G)$ será divisible por algún $in_{\leq}(f_i)$, contradiciendo que f^G pueda ser el resto del algoritmo de la división. Concluimos que $f^G = 0$.
Para demostrar la otra implicación, aplicamos el algoritmo de la división y obtenemos la siguiente expresión: $f = a_1 \cdot f_1 + ... + a_m \cdot f_m$, con resto nulo, por lo que podemos concluir que f pertenece al ideal $I =< f_1, ..., f_m >$. □

Ejemplo 1.1.13. *Sea* I *el ideal del anillo de polinomios* $\mathbb{R}[x, y]$ *generado por* $F = \{x^2 + y, x^2y+1\}$, *y consideramos el orden lexicográfico dado por* $x > y$. *Tenemos que el polinomio* $x^2y + x^2y + x + y^2$ *pertenece al ideal* I, $x^2y + +x^2y + x + y^2 = y(x^2 + y) + x(x^2y + 1)$, *pero sin embargo el resto del algoritmo de la división será* $-xy^2 + x$ *por el Ejemplo 1.1.8. Por lo que podemos concluir que* F *no es una base de Gröbner del ideal generado por* f_1 *y* f_2.

Corolario 1.1.14. *Sea* $G = \{f_1, ..., f_m\}$ *una base de Gröbner para un ideal* I *del anillo de polinomios* P, *respecto de una ordenación de términos* $\leq$. *Entonces* G *es un sistema generador del ideal* I,*es decir,* $I =< f_1, ..., f_m >$.

Demostración. El ideal generado por $f_1, ..., f_m$ está contenido en I, ya que G es base del ideal I. Ahora debemos demostrar que el ideal I está contenido en el ideal generado por $f_1, ..., f_m$. Por la Proposición 1.1.12, se tiene que para todo polinomio de I el algoritmo de la división nos proporciona una expresión $f = a_1 \cdot f_1 + \cdots + a_m \cdot f_m$ siendo el resto nulo al ser G base de Gröbner. Por lo que concluimos que el ideal I está generado por $f_1, ..., f_m$. □

Proposición 1.1.15. *Sea* $G = \{f_1, ..., f_m\}$ *una base de Gröbner en el anillo de polinomios* P *respecto de una ordenación de términos* $\leq$. *El resto del algoritmo de la división es único para todo polinomio* f *del anillo* P. *Además el resto es independiente del orden de los elementos de* G.

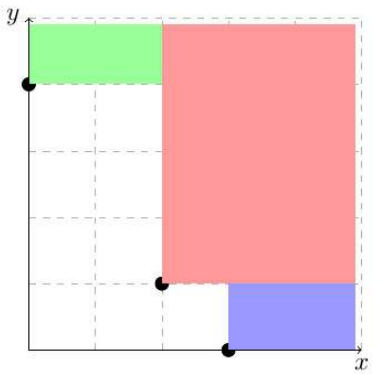
Demostración. Suponemos que el algoritmo de la división da dos restos diferente r_1 y r_2, obteniendo: $f = a_1f_1 + \cdots + a_mf_m + r_1 = b_1f_1 + \cdots + b_m + r_2$, por lo que la diferencia de $r_2 - r_1 = (a_1 - b_1)f_1 + \cdots + (a_m - b_m)f_m$ pertenecerá al ideal generado por los polinomios de G. Entonces existirá algún $in_{\leq}(f_i)$ que divida a $in_{\leq}(r_2 - r_1)$, por lo que $in_{\leq}(f_i)$ divide a algún término de r_1 o r_2, pero es una contradicción por la definición del resto. Podemos concluir entonces que $r_1 = r_2$. Una permutación G' del orden de los elementos en G, nos

dará las expresiones $f = a_1 \cdot f_1 + ... + a_m \cdot f_m + f^{G'}$, siendo $f^{G'} = f^G$, como queríamos demostrar. □

Lema 1.1.16 (Lema de Dickson). *Sea S un subconjunto del conjunto de n-uplas de $\mathbb{N}$. Existe un subconjunto finito de vectores en S, $v_1, ..., v_r$ tales que: S está contenido en la unión de los conjuntos $(v_i + \mathbb{N}^n)$, $i = 1, ..., r$.*

Demostración. Procedemos por inducción sobre n.
Si $n = 1$, entonces S será un subconjunto de $\mathbb{N}$, por lo que si tomamos $v_1 = \text{mín}\{s \in S\}$ tendremos que S está contenido en el conjunto $v_1 + \mathbb{N}$.
Lo suponemos cierto para m siendo $m < n$, es decir, si S es subconjunto de $\mathbb{N}^m$ tendremos r vectores en $\mathbb{N}^m$ que verifican que S está contenido en $(v_1 + N^m) \bigcup ... \bigcup (v_r + N^m)$.
Ahora lo demostramos para $m = n$. Definimos una aplicación ϕ de $\mathbb{N}^n$ al conjunto $\mathbb{N}^{n-1}$, tal que a los vectores $(x_1, ..., x_n)$ les sustraemos la primera coordenada, $(x_2, ..., x_n)$ perteneciente a $\mathbb{N}^{n-1}$. Usando la hipótesis de inducción en el subconjunto $\phi(S) = \{\phi(s) : s \in S\} \subset \mathbb{N}^{n-1}$, obtenemos la existencia de $s_1, ..., s_r$ de S que verifican que $\phi(S) \subset (\phi(s_1) + \mathbb{N}^{n-1}) \bigcup ... \bigcup (\phi(s_r) + \mathbb{N}^{n-1})$.
Ahora tomamos M como el máximo de las primeras coordenadas de $s_1, ..., s_r$ y definimos los conjuntos $S_{\geq M}$ y S_i, para $i = 0, ..., M-1$. En $S_{\geq M}$ tendremos los vectores en S cuya primera coordenada sea mayor o igual que M y en los S_i están los vectores de S tal que la primera coordenada de estos sea i, siendo $0 \leq i < M$. Tendremos que S es la unión de los $M + 1$ conjuntos definidos. Por la definición de $S_{\geq M}$, este estará contenido en $(s_1 + \mathbb{N}^n) \bigcup ... \bigcup (s_r + \mathbb{N}^n)$. Para los conjuntos S_i tendremos fija la primera coordenada por i. Por lo que aplicando la hipótesis de inducción a los conjuntos $\phi(S_0), ..., \phi(S_{M-1})$ obtenemos vectores $v_1^0, ..., v_{r_0}^0, ..., v_1^{M-1}, ..., v_{r_{M-1}}^{M-1}$, ahora aumentamos la dimensión de estos vectores añadiendoles como primera coordenada la i que estaba fija por el conjunto S_i, obetenemos así $w_1^0, ..., w_{r_0}^0, ..., w_1^{M-1}, ..., w_{r_{M-1}}^{M-1}$. De esta forma hemos obtenido un número finito de vectores que verifican la propiedad del Lema, quedando así demostrado. □

Ejemplo 1.1.17. *La idea del Lema 1.1.16 es bastante simple, si analizamos un caso concreto en $\mathbb{N}^2$, por ejemplo si tenemos $S = in_{\leq}(I)$, siendo I el ideal generado por $F = \{x^3 + y, x^2y + x, y^4 + 1\}$, $in_{\leq}(F) = \{(3,0), (2,1), (0,4)\}$, por el Lema 1.1.16 tenemos que $S \subseteq \big((3,0) + \mathbb{N}^2\big) \bigcup \big((2,1) + \mathbb{N}^2\big) \bigcup \big((0,4) + \mathbb{N}^2\big)$.*



Teorema 1.1.18 (Existencia de base de Gröbner). *Sean I un ideal de P, y $\leq$ una ordenación de términos. Entonces el ideal I tendrá una base de Gröbner respecto $\leq$.*

Demostración. Sea $S = \{v \in \mathbb{N}^n \ : \ x^v = in_{\leq}(f)$ para algún f del ideal $I\}$. El lema de Dickson nos proporciona un número finito de vectores $v_1, ..., v_m$ de $\mathbb{N}^n$, de forma que S estará contenido en $(v_1 + \mathbb{N}^n) \bigcup ... \bigcup (v_m + \mathbb{N}^n)$. Tomamos m polinomios $f_1, ..., f_m$ del ideal I que verifican que $in_{\leq}(f_i) = x^{v_i}$. Vamos a demostrar que $G = \{f_1, ..., f_m\}$ es una base de Gröbner de nuestro ideal I. Para ello tomamos un polinomio $f \in I$, y debemos probar que $in_{\leq}(f)$ es divisible por algún $in_{\leq}(f_i)$:
$in_{\leq}(f) = ax^w$, por el Lema 1.1.16 tenemos que $w = v_i + v$, para algún $i = 1, ..., m$ y v un vector de $\mathbb{N}^n$, entonces $x^w = x_i^v x^v$, lo que implica que $in_{\leq}(f_i)$ divide a $in_{\leq}(f)$, y por lo tanto G es base de Gröbner. □

Hemos probado la existencia de una base de Gröbner para un ideal de un anillo de polinomios. A continuación presentamos un criterio, conocido como el *S-criterio de Buchberger*, que nos permite comprobar si un conjunto $F = \{f_1, ..., f_m\}$ es una base de Gröbner.

Definición 1.1.19. *Decimos que un polinomio f del anillo de polinomios P reduce a cero módulo $F = \{f_1, ..., f_m\}$, si existen m polinomios $a_1, ..., a_m$ en P tales que:*
$f = a_1 f_1 + \cdots + a_m f_m$ *e* $in_{\leq}(a_i f_i) \leq in_{\leq}(f)$. *Lo denotamos por* $f \longrightarrow_F 0$.

Proposición 1.1.20. *Sean $F = \{f_1, ..., f_m\}$ y el ideal I generado por los polinomios en F, se tiene que:*

1. *Si todo polinomio del ideal I reduce a cero módulo F, entonces F es una base de Gröbner.*

2. *Si F es una base de Gröbner para el ideal I entonces $f^F = 0$, si sólo si, f reduce a cero módulo F para todo polinomio f del ideal I.*

Demostración.

1. Tomamos un polinomio f no nulo del ideal I. Tenemos que f reduce a cero modulo F por lo que $f = a_1 f_1 + ... + a_m f_m$, siendo a_i polinomios del anillo de polinomios P e $in_{\leq}(a_i f_i) \leq in_{\leq}(f)$. Para probar que F es base de Gröbner, veamos que el término inicial de f es dividido por algún $in_{\leq}(a_i \cdot f_i)$ con $i = 1, ..., m$. Para ello definimos $\delta = \text{máx}_{\leq}\{v_i + u_i, i = 1, ..., m\}$, donde $c_i x^{u_i} = in_{\leq}(a_i)$ y $d_i \cdot x^{v_i} = in_{\leq}(f_i)$. Siendo $in_{\leq}(f) = a \cdot x^v$ se tendrá que $\delta \geq v$. Suponemos ahora que $\delta > v$, por lo que para algún $i = 1, ..., m$ tendremos que $in_{\leq}(a_i f_i) > in_{\leq}(f)$, lo que es una contradicción por definición, entonces se da la igualdad de δ y v.
   Asumimos que existe $r \leq m$ tal que $\delta = v_1 + u_1 = ... = v_r + u_r$ y $a_i f_i$ no nulo para $i = 1, ..., r$. Entonces $in_{\leq}(f) = ax^v = (c_1 d_1 + ... + c_r d_r) x^{u_1 + v_1}$, luego $in_{\leq}(f_1) = d_1 x^{v_1}$ divide a $in_{\leq}(f) = ax^v$, lo que queríamos probar; así que concluímos que F es una base de Gröbner.

2. Si el resto del algoritmo de la división es cero para todo polinomio f del ideal I, entonces se tendrá la siguiente expresión por el Algoritmo de la división: $f = a_1f_1 + ... + a_mf_m$, $a_i \in P$ e $in_{\leq}(a_if_i) \leq in_{\leq}(f)$, por lo que f reduce a cero módulo F.
   Ahora f reduce a cero módulo F para todo polinomio f del ideal I, por lo que se tiene que $f = a_1f_1 + a_mf_m$ con a_i polinomios del anillo P e $in_{\leq}(a_if_i) \leq in_{\leq}(f)$, y como F es base de Gröbner el resto del algoritmo de la división es único, por lo que debe ser cero.

□

Veamos que si F no es base de Gröbner podemos tener que f reduzca a cero módulo F pero que el resto del algoritmo de la división sea no nulo.

Ejemplo 1.1.21. *Por el Ejemplo 1.1.8 se tiene que el resto de dividir $f = x^2y+x^2y+x+y^2$ entre $\{x^2+y, x^2y+1\}$ es $-xy^2+x$. Sin embargo $f = y(x^2+y)+x(x^2y+1)$ e $in_{\leq}(a_1f_1) = x^2y < in_{\leq}(f)$, $in_{\leq}(a_2f_2) = x^2y = in_{\leq}(f)$, por lo que f reduce a cero módulo F pero el resto del algoritmo de la división es no nulo.*

Si bien la Proposición 1.1.20 caracteriza las bases de Gröbner, la misma es poco práctica pues debemos verificar todos los polinomios del ideal que no siempre es finito. Veamos cómo podemos solventar esta dificultad. Observamos que el conjunto F será base de Gröbner siempre y cuando $\delta = v$, donde recordamos que $\delta = \text{máx}_{\leq}\{v_i + u_i, i = 1, ..., m\}$, $c_ix^{u_i} = in_{\leq}(a_i)$, $d_ix^{v_i} = in_{\leq}(f_i)$ y $ax^v = in_{\leq}(f)$. Tenemos que un polinomio f del ideal I, generado por F, es de la forma $f = a_1f_1+...+a_mf_m$, donde a_i son polinomios del anillo P. Escribimos f como:

$$f = C + (a_1 - in_{\leq}(a_1))f_1 + \cdots + (a_r - in_{\leq}(a_m))f_m + a_{m+1}f_{m+1} + \cdots + a_mf_m,$$

donde

$$\begin{aligned} C &= in_{\leq}(a_1)f_1 + \cdots + in_{\leq}(a_m)f_m = c_1x^{u_1}f_1 + \cdots + c_mx^{u_m}f_m \\ &= c_1 \cdot x^{u_1}d_1x^{v_1} + \cdots + c_mx^{u_m}d_mx^{v_m} + [c_1x^{u_1}(f_1 - in_{\leq}(f_1)) \\ &+ \cdots + c_mx^{u_m}(f_m - in_{\leq}(f_m))] = x^{u_1+v_1} \cdot (c_1 \cdot d_1 + \cdots + c_r \cdot d_m) + D, \end{aligned}$$

siendo $D = c_1x^{u_1}(f_1 - in_{\leq}(f_1)) + \cdots + c_rx^{u_m}(f_m - in_{\leq}(f_m))$.

Hemos escrito f como suma de polinomios de grado menor o igual a δ según nuestra ordenación de términos, y $x^{u_1+v_1}(c_1d_1 + \cdots + c_md_m)$, es el único término que puede ser de grado igual a δ. Por lo que si se cumple que $c_1d_1 + ... + c_md_m \neq 0$ se tendrá que F es base de Gröbner.

Ahora bien si $c_1 \cdot d_1 + ... + c_m \cdot d_m = 0$, debemos probar que F sigue siendo base de Gröbner, para ello definimos $g_i = x^{u_i} \cdot \frac{f_i}{d_i}$ e insertamos en la expresión de C:

$C = c_1d_1g_1+...+c_rd_rg_r = c_1d_1(g_1-g_2)+(c_1d_1+c_2d_2)(g_2-g_3)+\cdots+(c_1d_1+\cdots+c_md_m)(g_{m-1}-g_m)$.

Esto prueba que C es una combinación lineal de $(g_i - g_j) = x^{u_i} \cdot \frac{f_i}{d_i} - x^{u_j} \cdot \frac{f_j}{d_j}$. Tenemos que $u_i + v_i = u_j + v_j$ para $1 \leq i, j \leq r$, por lo que los términos iniciales de g_i y g_j se anularán. Introducimos $\omega_{i,j}$ como el mínimo común múltiplo de x^{v_i} y x^{v_j}, por lo que la diferencia de g_i y g_j nos queda como sigue: $g_i - g_j = x^{\xi_{i,j}}(\frac{x^{\omega_{i,j}}}{d_i \cdot x^{v_i}} \cdot f_i - \frac{x^{\omega_{i,j}}}{d_j \cdot x^{v_j}} \cdot f_j)$, donde $\xi_{i,j} + \omega_{i,j} = u_i + v_i = u_j + v_j$.

Definición 1.1.22. *El polinomio S de dos polinomios no nulos f y g del anillo P respecto una ordenación de términos $\leq$ se define como: $S(f,g) = \frac{x^\omega}{in_\leq(f)} \cdot f - \frac{x^\omega}{in_\leq(g)} \cdot g$, siendo x^ω el mínimo común múltiplo de $in_\leq(f)$ e $in_\leq(g)$.*

Ejemplo 1.1.23. *Sean $f_1 = x^3 - 2xy$ y $f_2 = x^2y - 2y^2 + x$. Tenemos que $S(f_1, f_2) = \frac{x^3y}{x^3}(x^3 - 2xy) - \frac{x^3y}{x^2y}(x^2y - 2y^2 + x) = -x^2$.*

Obsérvese que $g_i - g_j = x^{\xi_{i,j}} S(f_i, f_j)$. Hemos probado que $C = in_\leq(a_1)f_1 + ... + in_\leq(a_r)f_r = b_1 x^{\xi_1} S(f_1, f_2) + ... + b_{r-1} x^{\xi_{r-1}} S(f_{r-1}, f_r)$, con b_i perteneciente al cuerpo K y $\xi_i + v_{i,j} < \delta$, $in_\leq S(f_i, f_j) = b_{i,j} x^{v_{i,j}}$, para $1 \leq i < j \leq m$.

Lema 1.1.24. *Sean $F = \{f_1, ..., f_m\}$ y el ideal $I =< f_1, ..., f_m >$. Si $S(f_i, f_j)$ reduce a cero módulo F para todo $1 \leq i < j \leq m$, entonces todo polinomio f del ideal reduce a cero módulo F, por lo que F es base de Gröbner de I.*

Demostración. Sea el polinomio $f = a_1 f_1 + ... + a_m f_m$ del ideal I, con $a_i \in P$. Como $S(f_i, f_j)$ reduce a cero módulo F, tenemos que:
$S(f_i, f_j) = e_1 f_1 + ... + e_m f_m$, con $e_i \in P$ e $in_\leq(e_l f_l) \leq in_\leq(S(f_i, f_j))$, $l = 1, \cdots, m$, para todos los polinomios S, $1 \leq i < j \leq m$.
Si retomamos la expresión:

$$f = C + (a_1 - in_\leq(a_1))f_1 + \cdots + (a_r - in_\leq(a_r)))f_r + a_{r+1}f_{r+1} + \cdots + a_m f_m,$$

donde

$$\begin{aligned} C &= in_\leq(a_1)f_1 + ... + in_\leq(a_r)f_r = b_1 x^{\xi_1} S(f_1, f_2) + ... + b_{r-1} x^{\xi_{r-1}}\ S(f_{r-1}, f_r) \\ &= b_1 x^{\xi_1}(e_1^1 f_1 + ... + e_m^1 f_m) + ... + b_{r-1} x^{\xi_{r-1}}(e_1^{r-1} f_1 + ... + e_m^{r-1} f_m). \end{aligned}$$

Insertando está expresión de C en f, obtenemos:

$$\begin{aligned} f &= f_1((a_1 - in_\leq(a_1)) + b_1 x^{\xi_1} e_1^1 + ... + b_{r-1} x^{\xi_{r-1}} e_1^{r-1}) + ... + f_r((a_r - in_\leq(a_r)) \\ &+ b_1 x^{\xi_1} e_r^1 + ... + b_{r-1} x^{\xi_{r-1}} e_r^{r-1}) + f_{r+1}(a_{r+1} + b_1 x^{\xi_1} e_{r+1}^1 + \cdots + b_{r-1} x^{\xi_{r-1}} e_{r+1}^{r-1}) \\ &+ ... + f_m(a_m + b_1 x^{\xi_1} e_m^1 + ... + b_{r-1} x^{\xi_{r-1}} e_m^{r-1}) = f_1 h_1 + ... + f_m h_m, \end{aligned}$$

con $w' = \text{máx}\left\{w'_{i,j}, a_{w'_{i,j}} x^{w'_{i,j}} = in_\leq(f_i h_i), i = 1, ..., m\right\} < \delta$.
Siempre que los polinomios $S(f_i, f_j)$ reduzcan a cero módulo F, para $1 \leq i < j \leq m$, y se tenga que alguno de los exponentes de los términos $in_\leq(f_i p_i), i = 1, ..., m$ sean mayor que

v, podremos encontrar una nueva expresión $f = f_1p_1 + ... + f_mp_m$ tal que los exponentes de $in_{\leq}(f_ip_i), i = 1, ..., m$ sean estrictamente menores que en la anterior expresión, por lo que podremos repetir este proceso hasta obtener una expresión con $in_{\leq}(f_ip_i') = b'x^{w_i''}$ tales que $w_i'' \leq v$ para todo $i = 1, ..., m$, obteniendo así que f reduce a cero módulo F. □

Teorema 1.1.25 (**Teorema de Buchberger**). *Un conjunto $F = \{f_1, ..., f_m\}$ de polinomios es una base de Gröbner si sólo si $S(f_i, f_j)$ reduce a cero módulo F para $1 \leq i < j \leq m$.*

Demostración. Es una consecuencia directa de la Proposición 1.1.20 y del Lema 1.1.24. □

Corolario 1.1.26. *Un conjunto $F = \{f_1, ..., f_m\}$ de polinomios es una base de Gröbner si sólo si el resto de dividir $S(f_i, f_j)$ entre F es cero para $1 \leq i < j \leq m$.*

Demostración. Si el resto de dividir $S(f_i, f_j)$ entre F es cero para $1 \leq i < j \leq m$, entonces $S(f_i, f_j)$ reduce a cero módulo F y por el Teorema de Buchberger obtenemos que F es base de Gröbner. Si F es base de Gröbner entonces el resto de dividir $S(f_i, f_j)$ entre F es cero por la Proposición 1.1.12, ya que $S(f_i, f_j)$ pertenece al ideal generado por $f_1, ..., f_m$. □

Con estas herramientas podemos presentar el algoritmo de Buchberber que nos proporcionará una base de Gröbner para un ideal I del anillo de polinomios P.

Teorema 1.1.27 (**Algoritmo de Buchberger**). *Sean $f_1, ..., f_m$ polinomios del anillo P, I el ideal generado por estos, $I =< f_1, ..., f_m >$, y $\leq$ una ordenación de términos de $\mathbb{N}^n$.*
Input: $F = \{f_1, ..., f_m\} \subseteq P$ con f_i no nulo para $i = 1, ..., m$.
Output: $G = \{g_1, ..., g_r\}$ una base de Gröbner para el ideal I.
Initialization: $G := F$, $G' := \{\{f_i, f_j\}, f_i \neq f_j \in G\}$
mientras: $G' \neq \emptyset$
do: Elegir cualquier $\{f_i, f_j\} \in G'$
$G' := G' \backslash \{f_i, f_j\}$ y $h := (S(f_i, f_j))^G$.
Si $h \neq 0$ entonces $G' := G' \bigcup \{u, h\}$, para todo $u \in G$ y $G := G \bigcup \{h\}$.

Demostración. Distinguimos dos casos:

1. Si todos los restos de dividir $S(f_i, f_j)$, $1 \leq i < j \leq m$ entre G es cero, entonces por el Corolario 1.1.26 se tendrá que G es base de Gröbner.

2. Ahora si existen i_0 y j_0, $1 \leq i_0 < j_0 \leq m$, para los que el resto de dividir $S(f_{i_0}, f_{j_0})$ entre G es no nulo, podremos escribir: $S(f_{i_0}, f_{j_0}) = h_1f_1 + ... + h_mf_m + (S(f_{i_0}, f_{j_0}))^G$, con $h_i \in P$. Además sabemos que $S(f_{i_0}, f_{j_0})$ pertenece al ideal generado por f_{i_0} y f_{j_0} que está contenido en I. Por lo tanto $(S(f_{i_0}, f_{j_0}))^G$ pertenece al ideal I, entonces el ideal I también está generado por $f_1, ..., f_m$ y $(S(f_{i_0}, f_{j_0}))^G$ e $in_{\leq}((S(f_{i_0}, f_{j_0})^G)$ no es divisible por ningún $in_{\leq}(f_i)$. Luego $< in_{\leq}(f_1), ..., in_{\leq}(f_m) >$ estará contenido en $< in_{\leq}(f_1), ..., in_{\leq}(f_m), in_{\leq}((S(f_{i_0}, f_{j_0})^G) >$. Ahora tenemos que $G := G \bigcup (S(f_i, f_j))^G$ y para todos los i, j que teníamos que $(S(f_i, f_j))^G = 0$, con el nuevo conjunto G seguirán siendo nulos y además $(S(f_{i_0}, f_{j_0}))^G$ será cero, ya que por el Algoritmo de la división tendremos $S(f_{i_0}, f_{j_0}) = h_1 \cdot f_1 + ... + h_m \cdot f_m + 1 \cdot (S(f_{i_0}, f_{j_0}))^G + 0$. E iniciamos nuevamente el proceso tomando $I =< f_1, ..., f_m, (S(f_i, f_j))^G >$.

Veamos que tras un número finito de iteraciones obtendremos $G = f_1, ..., f_m, f_{m+1}, ..., f_{m+N}$, verificándose que $(S(f_i, f_j))^G = 0$, para $1 \leq i < j \leq m + N$. Este proceso nos proporciona una cadena ascendentte de ideales del anillo de polinomios: $< in_{\leq}(f_1), ..., in_{\leq}(f_m) > \subset < in_{\leq}(f_1), ..., in_{\leq}(f_m), in_{\leq}(f_{m+1}) > \subset ... \subset < in_{\leq}(f_1), ..., in_{\leq}(f_m), in_{\leq}(f_{m+1}, ..., in_{\leq}(f_{m+N}) >$ Como consecuencia de la condición de la cadena ascendente de ideales en el anillo de polinomios (ver [Cox-Li-O, Theorem 7, Chapter 2, Section 5]), obtenemos que N es finito. □

Ejemplo 1.1.28. *Nuestro objetivo es encontrar una base de Gröbner del ideal I generado por $F = \{f_1, f_2\}$, siendo $f_1 = x^3 - 2xy$ y $f_2 = x^2y - 2y^2 + x$, estamos trabajando en el anillo $\mathbb{R}[x, y]$ con el orden lexicográfico $x \geq y$.*
Inicializamos con $G := F$ y $G' := \{f_1, f_2\}$.
Por el Ejemplo 1.1.23 $S(f_1, f_2) = -x^2$ y el resto al dividir entre G es $-x^2$, ya que no es divisible por $in_{\leq}(f_1)$ ni por $in_{\leq}(f_2)$. Renombramos $f_3 = -x^2$ y actualizamos los conjuntos tenemos: $G = \{f_1, f_2, f_3\}$ y en G' tendremos $\{\{f_1, f_3\}\{f_2, f_3\}\}$.
Ahora calculamos $S(f_1, f_3) = -(x^3 - 2xy) - x(-x^2) = 2xy$, y nuevamente al intentar dvidir entre G se tiene que el resto es $2xy$. Así que ponemos $f_4 = 2xy$ y se tendrá que $G = \{f_1, f_2, f_3, f_4\}$ y $G' = \{\{f_1, f_4\}, \{f_2, f_3\}, \{f_2, f_4\}, \{f_3, f_4\}\}$.
Computemos ahora $S(f_1, f_4) = 2y(x^3 - 2xy) - x^2(2xy) = -4xy$, ahora al dividir entre G, obtenemos que $-4xy = -2f_4$ con resto nulo. Actualizamos nuestra lista G' donde nos queda $\{\{f_2, f_3\}, \{f_2, f_4\}, \{f_3, f_4\}\}$.
El siguiente polinomio que debemos calcular es $S(f_2, f_3) = -(x^2y - 2y^2 + x) - y(-x^2) = -x + 2y^2$ y al dividir entre G se tiene que ningún término es divisible por $in_{\leq}(f_i)$, $i = 1, 2, 3, 4$, así que el resto será $-x + 2y^2$. Renombramos $f_5 = -x + 2y^2$ y actualizamos $G = \{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, 2xy, -x + 2y^2\}$. Se puede probar ahora que $(S(f_i, f_j))^G = 0$ para todo $0 \geq i < j \geq 5$. Concluimos por el Coroalrio 1.1.26 que G es una base de Gröbner para el ideal I.

Como hemos visto en la demostración del Algoritmo de Buchberger si añadimos un polinomio f del ideal I a una base de Gröbner, esta continuará siendo base de Gröbner. Por lo que existen numerosas bases de Gröbner para un ideal I. Introduciremos ahora un concepto con las propiedades de base de Gröbner y que además sea único. Observamos que si tenemos $G = \{f_1, ..., f_m\}$ una base de Gröbner del ideal I, generado por los polinomios $f_1, ..., f_m$, donde $in_{\leq}(f_1)$ es divisible por algún $in_{\leq}(f_2), ..., in_{\leq}(f_m)$, se tendrá que $G' = \{f_2, ..., f_m\}$ continuará siendo una base de Gröbner de I. Este procedimiento nos será útil para disminuir el tamaño de nuestra base de Gröbner, hasta obtener el número mínimo de elementos.

Definición 1.1.29. *Una base de Gröbner $G = \{f_1, .., f_m\}$ se le denomina base de Gröbner minimal si:*

1. *$in_{\leq}(f_i)$ no es divisible por $in_{\leq}(f_j)$ para todo $i \neq j$.*

2. *El coeficiente de $in_{\leq}(f_i)$ es igual a uno, para $i = 1, ..., m$.*

Obsérvese que la base de Gröbner minimal de un ideal no es única.

Ejemplo 1.1.30. *Sean el ideal* $I =< x^3 - 2xy, x^y - 2y^2 + x, -x^2, -2xy, -2y^2 + x > y \leq$ *el orden lexicográfico, entonces* $G_a = \{x^2 + axy, xy, y^2 - (1/2)x\}$, *donde* $a \in K$, *es una familia de bases de Gröbner minimales para el ideal* I *respecto de* $\leq$.

Sin embargo, demostramos a continuación que todas las bases de Gröbner minimales de un ideal tienen el mismo número de elementos:

Proposición 1.1.31. *Sean* I *un ideal del anillo de polinomios* P *y* $F = \{f_1, ..., f_m\}$ *y* $G = \{g_1, ..., g_s\}$ *dos bases de Gröbner minimales del ideal* I, *se tendrá que* $m = s$ *e* $in_{\leq}(f_1) = in_{\leq}(g_1), ..., in_{\leq}(f_m) = in_{\leq}(g_m)$, *reoordenando si fuese necesario.*

Demostración. Tenemos por definición de base de Gröbner que $in_{\leq}(f_j)$ dividirá a $in_{\leq}(g_1)$ para algún j. Suponemos sin pérdida de generalidad que $j = 1$. Como ambos tienen coeficiente igual a uno se tendrá que $in_{\leq}(f_1) = in_{\leq}(g_1)$. Aplicando el mismo argumento a los demás polinomios $f_2, ..., f_m$, obtenemos el resultado. □

Definición 1.1.32. *Una base de Gröbner minimal* $G = \{f_1, ..., f_m\}$ *se dirá reducida si ningún término de* f_i *es divisible por* $in_{\leq}(f_j)$ *para* $i \neq j$.

Ahora sí un ideal tiene una única base de Gröbner reducida.

Teorema 1.1.33 (Algoritmo para la obtención de la base de Gröbner reducida).
Sea I *un ideal del anillo de polinomios* P.
Input $G := g_1, ..., g_t$ *una base minimal de Gröbner de* I.
Output G' *base de Gröbner reducida de* I.

Paso 1: do $g_i' = \frac{1}{coef(g_i)} g_i$; $G'' = G'' \bigcup g_i'$, $i = 1, ..., t$.

Paso 2: do $g_i'' = (g_i')^{G''}$, $G' := G' \bigcup g_i''$, $i = 1, ..., t$.

Demostración. Sean I un ideal de P y $\leq$ una ordenación de términos. Siguiendo los siguientes pasos encontraremos una base de Gröbner reducida G' del ideal I.

Paso 1: Calculamos una base de Gröbner minimal de I. Primero reducimos el tamaño de una base de Gröbner $G = \{g_1, ..., g_t\}$ siguiendo el procedimiento que expusimos. Ahora normalizamos tomando $g_i'' = \frac{1}{coef(g_i)} g_i$ para todos los $i = 1, ..., t$. Obtenemos $G'' = \{g_1'', ..., g_t''\}$ base reducida de Gröbner.

Paso 2: Consideramos ahora $G' = \{g_1', ..., g_t'\}$ siendo $g_i' = (g_i'')^{G'' - \setminus \{g_i\}}$. Por el Algoritmo de la divisón obtenemos:

$$g_i'' = h_1 g_1'' + ... + h_{i-1} g_{i-1}'' + h_{i+1} g_{i+1}'' + ... + h_t g_t + g_i'.$$

Se tendrá que $in_{\leq}(g_i'')$ no es divisible por ningún $in_{\leq}(g_j'')$ para $i \neq j$, ya que G'' es una base de Gröbner minimal, por lo que $in_{\leq}(g_i') = in_{\leq}(g_i'')$, y G' continuará siendo

base de Gröbner minimal. Además por definición del resto ningún término de g_i' es divisible por $in_{\leq}(g_j')$ para $i \neq j$. Entonces tendremos que G' es base de Gröbner reducida.

□

Ejemplo 1.1.34. *Sea la base de Gröbner*

$$G = \{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, 2xy, -x + 2y^2\}$$

del ideal I generado por $F = \{f_1, f_2\}$, siendo $f_1 = x^3 - 2xy$ y $f_2 = x^2y - 2y^2 + x$. Para computar la base minimal tenemos que $in_{\leq}(f_1) = x^3$ e $in_{\leq}(f_2) = x^2y$ son divisibles por $in_{\leq}(f_3) = -x^2$, así que los podemos quitar de nuestra base G, normalizando f_3, f_4, f_5 obtenemos $G' = \{g_1 = x^2, g_2 = xy, g_3 = y^2 - \frac{1}{2}x\}$ que es la base de Gröbner minimal, además ningún término de g_i es divisible por $in_{\leq}(g_j)$, $i, j = 1, 2, 3$ $j \neq i$, por lo que también G' es una base de Gröbner reducida.

1.2. Ingredientes geométricos

Definición 1.2.1. *Sean K un cuerpo y $f_1, ..., f_s$ polinomios del anillo $K[x_1, ..., x_n]$. Entonces denominamos al conjunto:*

$$V(f_1, ..., f_s) = \{(a_1, ..., a_n) \in K^n \ : \ f_i(a_1, ..., a_n) = 0,$$

para todo $i = 1, ..., s\}$ variedad afín *definida por $f_1, ..., f_s$.*

Proposición 1.2.2. *El conjunto $I(V) = \{f \in K[x_1, .., x_n] : f(a_1, ..., a_n) = 0$, para todo $(a_1, ..., a_n) \in V\}$ es un ideal.*

Demostración. 1. *Tenemos que el polinomio nulo estará en $I(V)$.*
Si tenemos dos polinomios f y g del conjunto $I(V)$, la suma es cerrada, $(f+g)(a_1, ..., a_n) = f(a_1, ..., a_n) + g(a_1, ..., a_n) = 0$, para todo punto $(a_1, ..., a_n)$ de la variedad afín V.
Además si tomamos un polinomio h de $K[x_1, ..., x_n]$, el producto $(f \cdot h)$ pertenece a $I(V)$, $(f \cdot h)(a_1, ..., a_n) = f(a_1, ..., a_n) \cdot h(a_1, ..., a_n) = 0 \cdot h(a_1, ..., a_n) = 0$, para todo $(a_1, ..., a_n)$ de V.
Por lo que $I(V)$ es un ideal.

Proposición 1.2.3. *Sean V y W dos variedades afines en F^n. Entonces V está contenido en W si sólo si $I(W)$ está contenido en $I(V)$.*

Demostración. Si V está contenido en W se tiene que todo polinomio que se anule en W se debe anular en V, lo que prueba que $I(W)$ está contenido en $I(V)$. Ahora si $I(W)$ está contenido en $I(V)$, supongamos que W está definida por los polinomios $g_1, ..., g_t$ en el anillo $K[x_1, ..., x_n]$. Entonces $g_1, ..., g_t$ están en $I(W)$ y consecuentemente en $I(V)$, por lo que $g_1, ..., g_t$ se anulan en V. Como W consiste en el conjunto de ceros comunes de $g_1, ..., g_t$ tendremos que V está contenido en W. □

Definición 1.2.4. *Sea un ideal I del anillo de polinomios $K[x_1, ..., x_n]$. El radical de I, denotado por $\sqrt{I}$, es el conjunto* $\{f : f^m$ pertenece al ideal I para algún entero $m \geq 1\}$.

El radical de un ideal del anillo de polinomios $K[x_1, ..., x_n]$ es también un ideal que contiene a I.

El siguiente teorema es conocido como *Shape Lemma*, que bajo ciertas condiciones nos permite conocer la forma de la base reducida de Gröbner para un ideal radical. Ello será de gran ayuda en el Capítulo 3 de esta memoria.

Teorema 1.2.5. *Sean K un cuerpo algebraicamente cerrado e I un ideal radical finito en $K[x_1, .., x_n]$. Asumimos que $V(I)$ tiene m puntos que verifican que la n-ésima coordenada es distinta para los m puntos. Entonces la base reducida de Gröbner G' de I respecto al orden lexicógrafico dado por $x_1 \geq_{lex} \cdots \geq_{lex} x_n$, está compuesta por los n polinomios: $g_1 = x_1 + h_1(x_n)$, $g_2 = x_2 + h_2(x_n)$,..., $g_n = x_n^m + h_n(x_n)$, donde $h_1, ..., h_n$ son polinomios en $F_q[x_1]$ de grado menor o igual a $m - 1$.*

Demostración. Primero probamos que las clases de equivalencias $[1], [x_n], ..., [x_n^{m-1}]$ forman una base para el K-espacio vectorial $K[x_1, ..., x_n]/I$. Suponemos por reducción al absurdo que son linealmente dependientes, por lo que existirán $c_0, ..., c_{m-1}$ de K tal que $g(x_n) := c_0 + c_1 x_n + ... + c_{m-1} x_n^{m-1}$ pertenece al ideal I. Sean $\psi_{1,n}, ..., \psi_{m,n}$ m distintas n-ésimas coordenadas de puntos en $V(I)$. Como g pertenece al ideal, tenemos que $g(\psi_{i,n}) = 0$ para todo $i = 1, ..., m$, lo que nos da un sistema lineal homogéneo para $c_0, ..., c_{m-1}$ con su matriz de coeficientes Vandermonde, es decir, sus coeficientes presentan una progresión aritmétrica en cada fila. Esta matriz es no singular entonces implica que todos los $c_i = 0$, por lo que las clases de equivalencia son linealmente independientes. Para probar que las clases $[1], [x_n], ..., [x_n^{m-1}]$ generan $K[x_1, ..., x_n]/I$, será suficiente probar que la dimensión del espacio $K[x_1, ..., x_n]/I$ es menor o igual a m.
Consideramos la aplicación $\Phi : K[x_1, ..., x_n]/I \longrightarrow C^m$ tal que $(f(\psi_1), ..., f(\psi_m)), \psi_j \in V(I)$ es la imagen de la clase de un polinomio $[f]$. Si $[f_0]$ está en el núcleo de la aplicación Φ se tendrá que f_0 pertenece a $I(V(I))$ y por el teorema de los ceros de Hilbert (ver [Cox-Li-O, Theorem 6, Chapter 4, Section 2]) se tiene que $I(V(I)) = \sqrt{(I)}$ y como I es un ideal radical, y f_0 pertenece al ideal, la clase de equivalencia de f_0 será cero. Entonces $dim K[x_1, ..., x_n]/I \leq m$. Esto prueba que las clases de equivalencia $[1], [x_n], ..., [x_n^{m-1}]$ forman una base de $K[x_1, ..., x_n]/I$.
Ahora si expresamos $[x_1], [x_2], ..., [x_n^m]$ en funcion de esa base, obtenemos los polinomios $g_1, ..., g_n$ del ideal I. Entonces por la Proposición 1.2.3 se tendrá que $V(I) \subseteq V(g_1, ..., g_n)$. Como $g_1, ..., g_n$ tienen como mucho m raíces comunes tenemos que $V(I) = V(g_1, ..., g_n)$ lo que nos implica que $I =< g_1, ..., g_n >$. Hemos probado que $g_1, ..., g_n$ forman una base de Gröbner para nuestro ideal I. □

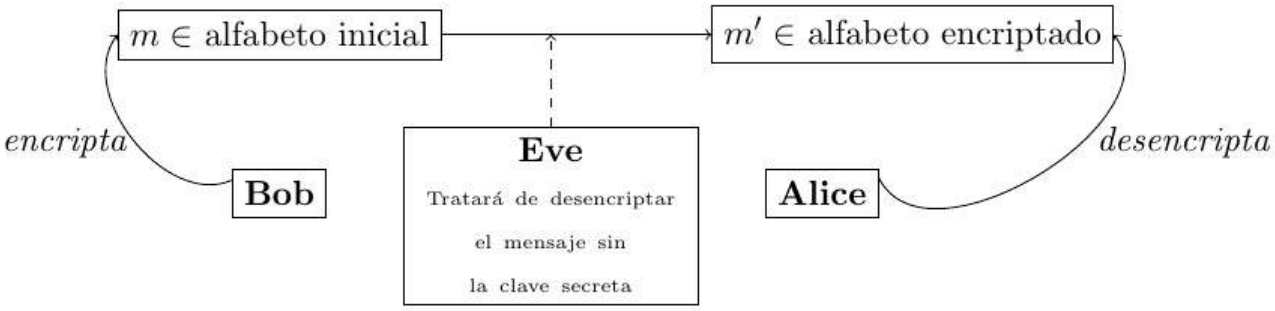
Capítulo 2

La criptografía y las bases de Gröbner

2.1. Introducción

Empezamos dando una breve introducción a la Criptografía.
La palabra Criptografía tiene su origen etimológico en los vocablos griegos, *kryptos* que significa oculto y *graphia* que significa escritura. Por lo que definimos la Criptografía como el conjunto de procedimientos y técnicas para escribir de un modo enigmático o con claves secretas, de tal forma que lo escrito solamente sea legible para quien sepa descifrarlo. A estos procedimientos se les denomina *criptosistemas*, que usan un algoritmo que se compone de dos fases, la primera encripta el mensaje con cierta clave, transformándolo de tal modo que sea ilegible, a menos que se tenga la clave de desencriptado. La segunda fase del algoritmo se encargará del uso de esta clave de desencriptado, que será secreta y nos posibilita la obtención del mensaje.

Podemos distinguir dos tipos de criptosistemas según sus claves: *simétrico o de clave privada* cuando se usa la misma clave para encriptar y desencriptar, y *asimétrico o de clave pública* cuando usa dos claves diferentes. En este caso la clave de encriptado se hace pública, mientras que la clave de desencriptado se mantiene privada. Estos criptosistemas de clave pública serán el objeto de estudio de este capítulo.
Matemáticamente hablando el encriptado consiste en una aplicación ϵ, donde el conjunto inicial lo llamaremos alfabeto inicial y al conjunto final alfabeto final. Por tanto un mensaje será un elemento del alfabeto inicial y su imagen por ϵ será el mensaje encriptado. Desencriptar un mensaje $\epsilon(m)$ consistirá en calcular su imagen por la aplicación inversa ϵ^{-1}. La seguridad de estos criptosistemas estará basada en la dificultad de determinar la aplicación ϵ^{-1}. Durante nuestro trabajo nos encontramos en la siguiente situación:



Ejemplo 2.1.1 (RSA). *El RSA es el criptosistema más conocido de clave pública. Fue propuesto por Rivest, Shamir y Adleman en 1977. Tendremos al emisor Bob y a Alice que es la receptora del mensaje, para esto ella se encarga de generar una clave pública para encriptar y una clave privada que usa para desencriptar el mensaje. Alice elige dos primos distintos p y q y calcula $n = p \cdot q$, que es parte de la clave pública. Ahora escoge un número e menor que la Phi de Euler de n, en nuestro caso $\varphi(n) = (p-1)(q-1)$, y que sea coprimo con $\varphi(n)$. La clave pública es el par (n, e). La clave privada es un número d que satisface la ecuación modular $e \cdot d \equiv 1 \,(mod\, \varphi(n))$.*
Bob, para encriptar un mensaje m, entero menor que n, calcula $c \equiv m^e \,(mod\, n)$. Y para desencriptarlo Alice debe calcular $c^d \equiv m^{ed} \equiv m \,(mod\, n)$.

2.2. Criptosistemas Polly Cracker

A continuación vamos a presentar los criptosistemas de clave pública llamados *Polly Cracker*. Esta familia de criptosistemas se caracteriza por estar apoyados en la Teoría de bases de Gröbner. Trabajaremos en el anillo de polinomios P de n variables con coeficientes en un cuerpo K:

$$P := K[x_1, \ldots, x_n] = \left\{ \sum_{i=1}^{m} a_i x_1^{v_{i1}} \cdots x_n^{v_{in}} \ : \ m \in \mathbb{N},\ a_i \in K,\ (v_{i1}, \ldots, v_{in}) \in \mathbb{N}^n \right\}.$$

Se denomina criptosistema Polly Cracker a aquellos que su clave pública es una base de Gröbner de un ideal de polinomios en varias variables, o un punto perteneciente a la variedad afín definida por un ideal. Los primeros que propusieron los criptosistemas Polly Cracker fueron Koblitz y Fellows en 1993 [Fe-Ko], describiendo el siguiente procedimiento:

2.2.1. Polly Cracker abstracto

Como mostramos en la figura, Bob mandará un mensaje a Alice. Para ello Alice toma un conjunto de polinomios F que generan un ideal I, del cual ella conoce un cero, $\psi \in K^n$, es decir, $\psi \in V(I)$ o equivalentemente $f(\psi) = 0$ para todo polinomio f del ideal I. Alice hace público el conjunto F que genera el ideal I y su clave secreta es el punto ψ. Entonces

Bob, para encriptar el mensaje m perteneciente al cuerpo K, toma un polinomio aleatorio h del ideal I y computa el mensaje encriptado, que es el polinomio $c := h + m$. Para desencriptar el mensaje, Alice evalúa este polinomio en el punto ψ, obteniendo así el mensaje m. El correcto funcionamiento de este criptosistema se fundamenta en el hecho de que independientemente del polinomio h que Bob elija, h se anula en ψ, y siendo m una constante, se tiene que $c(\psi) = h(\psi) + m = 0 + m = m$.
La seguridad de este criptosistema, siendo de clave pública, está basada en la dificultad de calcular un cero del ideal público I, es decir, resolver un sistema de ecuaciones algebraicas. Para asegurar que este sistema de ecuaciones no tenga una solución que sea relativamente fácil de calcular en tiempo polinomial, Alice selecciona el conjunto de polinomios F de tal modo que sean una transcripción de un problema NP-completo, por lo que resolver el sistema de ecuaciones equivale a encontrar una solución para este problema. Koblitz y Fellows se basaron en los problemas relacionados con la teoría de grafos, su idea fue codificar el problema de la 3-coloración de un grafo, que mostramos a continuación:

Ejemplo 2.2.1. *Sea un grafo* $\Gamma = (V, E)$*, donde* $V = \{1, \cdots, n\}$ *son los vértices y* $E \subset \{\{i, j\}, 1 \leq i < j \leq n\}$ *son las aristas. Alice conoce una 3-coloración de este grafo, que es una aplicación* $\Phi : V \longrightarrow \{1, 2, 3\}$ *tal que se verifica que si* $\{i, j\} \in E$ *entonces* $\Phi(i) \neq \Phi(j)$*. Para transcribir esta aplicación en lenguaje polinomial, Alice define los conjuntos de polinomios* F_0, F_1, F_2, F_3 *en las variables* $x_{i,k}$*, dadas por* $x_{i,k} = 1$ *si* $\Phi(i) = k$ *, o* $x_{i,k} = 0$ *en caso contrario:*

- $F_0 = \{x_{i,1}x_{i,2}, x_{i,1}x_{i,3}, x_{i,2}x_{i,3},\ 1 \leq i \leq n\}$*, cada vértice no puede estar pintado con dos colores.*

- $F_1 = \{x_{i,1} + x_{i,2} + x_{i,3} - 1,\ 1 \leq i \leq n\}$*, cada vértice está pintado con al menos un color.*

- $F_2 = \{x_{i,1}x_{j,1}, x_{i,2}x_{j,2}, x_{i,3}x_{j,3},\ \{i, j\} \in E\}$*, dos vértices conectados están pintados con colores distintos.*

- $F_3 = \left\{x_{i,k}^2 - x_{i,k},\ 1 \leq i \leq n,\ 1 \leq k \leq 3\right\}$*, las raíces* $x_{i,k}$ *que buscamos pertenecen al cuerpo* $\mathbb{Z}_2$*.*

La clave pública es $F := F_0 \bigcup F_1 \bigcup F_2 \bigcup F_3$*. Conocer una 3-coloración equivale a conocer un punto* α *de la variedad afín definida por el ideal generado por* F*, y dicho punto* α *es la clave privada de Alice.*

La seguridad no es el único inconveniente de un criptosistema, también la representación de las claves claves públicas y privadas. En nuestro caso la cantidad de datos con la que trabajamos es muy elevada para enviar un único elemento de K.

Se puede mejorar este criptosistema variando la clave privada y discutiendo la forma en la que representamos nuestro ideal, haciendo uso de las bases de Gröbner.

2.2.2. Criptosistema de Barkee

En 1994, Barkee [Bar] presentó un criptosistema Polly Cracker basado puramente en la teoría de las bases de Gröbner. Al igual que en el Polly Cracker abstracto trabajaremos en un cuerpo K, que usualmente será $\mathbb{F}_q$ de característica p, y en el anillo de polinomios P de n variables con coeficientes en K. Bob desea enviar un mensaje a Alice, para esto ella primero ha de crear su clave pública y privada del criptosistema. Para ello toma un ideal I del anillo de polinomios del cual ella conoce una base de Gröbner G, y esta base será su clave privada. La clave pública será el ideal I y un subconjunto de formas normales $N = \{g_1, ..., g_r\}$ en P respecto al ideal I. Bob enviará un mensaje, m, perteneciente en este caso a $K \cdot g_1 + ... + K \cdot g_r$. Para encriptarlo eligirá un polinomio aleatorio h del ideal I y calcula $c := h + m$, será este el polinomio que envíe a Alice. Ella, para desencriptarlo reducirá el polinomio c respecto a su base de Gröbner, lo que equivale a calcular el resto del algoritmo de la división. El correcto funcionamiento de este criptosistema se basa en la construcción del polinomio c, que es la suma de un polinomio h que pertenece al ideal I y el mensaje compuesto por términos que provienen de formas normales respecto al ideal I; esto implica que ningún término en m será divisible por algún término inicial de los elementos de G, y por la unicidad del resto del algoritmo de la división entre una base de Gröbner (ver Proposición 1.1.15) Alice obtiene que el resto de dividir c entre G es m ($c^G = m$).

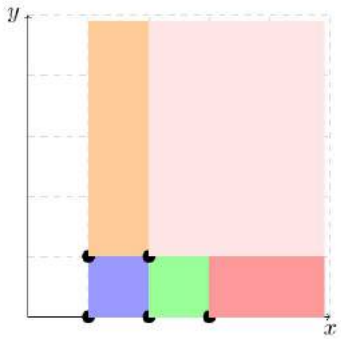
Ejemplo 2.2.2. *Bob desea mandar un mensaje a Alice, para esto ella define el siguiente criptosistema en* $\mathbb{Q}[x, y]$. *Alice toma el conjunto de polinomios*

$$F = \left\{ f_1 := x^3 - 2xy, f_2 := x^2y - 2y^2 + x \right\},$$

del cual conoce una base de Gröbner del ideal I *generado por* F *(ver Ejemplo 1.1.28),*

$$G := \left\{ x^3 - 2xy, x^2y - 2y^2 + x, -x^2, 2xy, -x + 2y^2 \right\}.$$

La clave pública es el conjunto F *y un subconjunto de formas normales en* P *respecto al ideal* I. *El soporte de las formas normales ha de tener intersección vacía con* $IN_{\leq}(G) + \mathbb{N}^2 = \{\left((3,0) + \mathbb{N}^2\right), \left((2,1) + \mathbb{N}^2\right), \left((2,0) + \mathbb{N}^2\right), \left((1,1) + \mathbb{N}^2\right), \left((1,0) + \mathbb{N}^2\right)\}$,



Alice toma $N = \{y^2, y\}$. *Bob encripta el mensaje* $m = 3y^2 + 4y$ *tomando el polinomio* $h := f_1 + f_2 - 2yf_4 = x^3 + x^2y - 4xy^2 - 2xy + x - 2y^2$, *y envía a Alice* $c := h + m =$

$x^3+x^2y-4xy^2-2xy+x+y^2+4y$. *Para desencriptar el mensaje, Alice aplica el Algoritmo de la división, y obtiene* $m = c^G$.

2.2.3. Criptosistema Polly Cracker concreto

En este criptosistema Alice toma como su clave privada un punto aleatorio ψ del cuerpo K^n. Para crear la clave pública ella elegirá tantos polinomios aleatorios como desee del anillo P. Supongamos que $f'_1, ..., f'_s$ sean los polinomios seleccionados por Alice. Ahora ella calcula $f_i = f'_i - f'_i(\psi)$, para $i = 1, ..., s$. Entonces el conjunto $\{f_1, ..., f_s\}$ será la clave pública de Alice, a la que Bob tendrá acceso. El, para encriptar un mensaje m del cuerpo K toma s polinomios aleatorios $h_1, ..., h_s$ del anillo P, y calcula $c = \sum_{i=1}^{s} h_i \cdot f_i + m$, que será el mensaje encriptado.
Alice para desencriptar el mensaje debe evaluar el polinomio c en su clave secreta ψ, $c(\psi) = \sum_{i=1}^{m} h_i(\psi) \cdot f_i(\psi) + m = \sum_{i=1}^{m} h_i(\psi) \cdot 0 + m = m$, obteniendo el mensaje m que Bob quería transmitir.

Ejemplo 2.2.3. *Supongamos que Alice y Bob trabajan en el anillo* $\mathbb{R}[x, y]$. *Alice toma el punto* $\psi = (3, 1)$, *que es su clave privada. También elige* $f'_1 = x^2y - x + 2y^2 + 3$ *y* $f'_2 = x^3-xy+2y+1$, *y computa su clave pública* $\{f_1 := f'_1-f'_1(3,1) = x^2-x+2y^2-8, f_2 := f'_1 - f'_1(3,1) = x^3 - xy + 2y - 22\}$. *Bob, para enviar el mensaje* $m = 7$, *lo encripta seleccionando* $h := xyf_1 + (-y)f_2 = -x^2y + 2xy^3 + xy^2 - 8xy + 2y^2 + 22y$, *y envía a Alice* $c := h + m = -x^2y + 2xy^3 + xy^2 - 8xy + 2y^2 + 22y + 7$. *Para desencriptar Alice evalúa* c *en* ψ *y obtiene* $c(3, 1) = 7$, *que es el mensaje enviado.*

Capítulo 3

Distintos ataques algebraicos a criptosistemas

En este capítulo suponemos que en el criptosistema hay un hacker, Eve, que intercepta el mensaje cifrado c y realiza algunos ataques para intentar descifrar el mensaje o tratar de romper el criptosistema, obteniendo una clave de descifrado.

Salvo que se diga lo contrario trabajaremos en este capítulo con el cuerpo base $\mathbb{Z}_2$.

Los procesos de encriptación de un criptosistema pueden ser representados por una aplicación que manda bit-uplas a bit-uplas. Matemáticamente lo representamos como la aplicación $\epsilon : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^s$, donde el alfabeto inicial estará contenido en $\mathbb{Z}_2^n$ y el alfabeto final en $\mathbb{Z}_2^s$. Esta aplicación siempre es polinomial, es decir, existen polinomios $f_1, \ldots, f_s$ en $\mathbb{Z}_2[x_1, \ldots, x_n]$ tales que

$$\epsilon(a_1, \ldots, a_n) = (f_1(a_1, \ldots, a_n), \ldots, f_s(a_1, \ldots, a_n)),$$

para los posibles mensajes $(a_1, \ldots, a_n) \in \mathbb{Z}_2^n$ que Bob podría enviar. Los polinomios $f_1, \ldots, f_s$ no son necesariamente únicos, por lo que podemos tener $g_1, \ldots, g_s$ en $\mathbb{Z}_2[x_1, \ldots, x_n]$ tales que $\epsilon(a_1, \ldots, a_n) = (g_1(a_1, \ldots, a_n), \ldots, g_s(a_1, \ldots, a_n))$, donde $(a_1, \ldots, a_n)$ es un elemento del alfabeto inicial. Si esto sucediese

$$\epsilon(a_1, \ldots, a_n) = (f_1(a_1, \ldots, a_n), \ldots, f_s(a_1, \ldots, a_n)) = (g_1(a_1, \ldots, a_n), \ldots, g_s(a_1, \ldots, a_n)),$$

y $f_i(a_1, \ldots, a_n) - g_i(a_1, \ldots, a_n) = 0$, para $1 \leq i \leq s$, por lo que los polinomios $f_i(x_1, \ldots, x_n) - g_i(x_1, \ldots, x_n)$ estarán contenidos en el ideal

$$I(\wp) = \{h \in \mathbb{Z}_2[x_1, \ldots, x_n] \ : \ h(a_1, \ldots, a_n) = 0, \text{para todo} (a_1, \ldots, a_n) \in \wp\},$$

donde $\wp \subseteq \mathbb{Z}_2^n$ es el alfabeto inicial. Recordemos que el ideal asociado a un subconjunto de puntos, como es el caso de $I(\wp)$, fue introducido en la Definición 1.2.1.

Existen diferentes métodos con los que Eve puede intentar obtener el mensaje m o una clave para romper el criptosistema. Empezamos presentando someramente algunos que se usan

en criptosistemas simétricos, pues aunque estos criptosistemas no son objeto de estudio de esta memoria, los ataques dirigidos a los mismos que mostramos a continuación, inspiran el ataque algebraico a criptosistemas de clave pública, sustentado en bases de Gröbner.

3.1. Ataque conociendo parte del mensaje

Supongamos que Alice y Bob usan un criptosistema simétrico y Eve conoce el valor de $\epsilon(x_1^i, \ldots, x_n^i)$, para ciertas bit-uplas del mensaje, siendo ϵ la aplicación de encriptación del sistema. Dado que ϵ debe ser una aplicación polinomial, pues está definida entre espacios afines sobre cuerpos finitos, y aunque ϵ no sea pública pues estamos en un criptosistema simétrico, Eve puede describirla como $\epsilon : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$, usando polinomios genéricos $f_1, ..., f_n$ de un anillo de polinomios, digamos $\mathbb{Z}_2[x_1, \ldots, x_n, y_{i,j}, k_1, \ldots, k_l]$, donde a las indeterminadas $x_1, \ldots, x_n$ que representan los bits del mensaje descifrado m, añadimos las indeterminadas $y_{i,j}$ que simbolizan ciertos bits de resultados intermedios y las indeterminadas $k_1, \ldots, k_l$ que representan los bits de la clave privada. Ahora Alice iguala

$$(\epsilon(x_1^i, \ldots, x_n^i)) = (f_1(x_1^i, \ldots, x_n^i, y_{i,j}, k_1, \ldots, k_l), \ldots, f_n(x_1^i, \ldots, x_n^i, y_{i,j}, k_1, \ldots, k_l)), \quad (3.1)$$

y obtiene un sistema de ecuaciones polinomiales en las indeterminadas $y_{i,j}, k_1, \ldots k_l$, con tantas ecuaciones como valores de $\epsilon(x_1^i, \ldots, x_n^i)$ ella conozca. Las indeterminadas $y_{i,j}$ juegan un papel auxiliar en este contexto pues se debe resolver un sistema de ecuaciones polinomiales cuyos polinomios no conocemos a priori pero cuyas soluciones serán, en principio, más fáciles de determinar mientras *más lineal* sea el sistema. Ello se puede conseguir por ejemplo reemplazando cada producto de la forma $x_i x_j$ por la variable auxiliar $y_{i,j}$.

En los casos para los cuales el sistema de ecuaciones definido a partir de (3.1) tenga una única solución $(a_{i,j}, b_1, \ldots, b_l)$ sobre $\mathbb{Z}_2$, que Eve pueda determinar, ella habrá obtenido la clave secreta $(b_1, \ldots, b_l)$ y habrá roto el criptosistema.

Observamos que en el lenguaje de las bases de Gröbner, decir que el sistema determinado por (3.1) tiene como única solución al punto $(a_{i,j}, b_1, ..., b_l)$ es equivalente a decir que el ideal generado por los polinomios que definen el sistema admite una base de Gröbner reducida de la forma $G = \{y_{i,j} - a_{i,j}\}_{i,j} \cup \{k_j - b_j\}_{j=1}^l$.

3.2. Ataque a un mensaje cifrado

Nuevamente Alice y Bob usan un criptosistema simétrico. Eve intercepta unas unidades del mensaje cifrado m. Como en el anterior ataque, ella representa la aplicación de encriptar como $\epsilon : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$ con polinomios $f_1^{(m)}, \ldots, f_n^{(m)}$ del anillo de polinomios $\mathbb{Z}_2[x_1^{(m)}, \ldots, x_n^{(m)}, y_{i,j}^{(m)}, k_1, \ldots, k_l]$, usando diferentes indeterminadas $x_1^{(m)}, \ldots, x_n^{(m)}$ para cada unidad del mensaje que ella haya interceptado; indeterminadas auxiliares $y_{i,j}^{(m)}$ e indeterminadas $k_1, \ldots, k_l$ que corresponden a los bits de la clave secreta de Alice. Eve

tratará de resolver el sistema de ecuaciones para $k_1, \ldots, k_l$ y así obtener la clave secreta y romper el criptosistema.

Usando un procedimiento similar vamos a describir cómo romper un criptosistema de clave pública, como lo son los criptosistemas Polly Cracker, que hemos presentado en el Capítulo 2.

3.3. Ataque a un criptosistema de clave pública

En esta situación Eve conocerá la clave pública, por lo que podrá describir la aplicación de encriptación: $\epsilon : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^s$, usando polinomios $f_1, \ldots, f_s$ en el anillo de polinomios $\mathbb{Z}_2[x_1, \ldots, x_n]$, correspondiendo las indeterminadas $x_1, \ldots, x_n$ a los bits del mensaje sin encriptar. Por lo que si Eve intercepta un mensaje cifrado compuesto por los bits c_i, donde $i = 1, \ldots, s$, y consigue resolver el sistema de ecuaciones $f_i(x_1, \ldots, x_n) = c_i$, $i = 1, \ldots, s$ tendrá los bits $x_1, \ldots, x_n$ correspondientes al mensaje sin encriptar.

Para poder hallar la clave privada, y romper el criptosistema, Eve describe la aplicación de desencriptar: $\delta : \mathbb{Z}_2^s \longrightarrow \mathbb{Z}_2^n$, con polinomios $g_1, \ldots, g_n$ en el anillo de polinomios $\mathbb{Z}_2[y_1, \ldots, y_s, k_1, \ldots, k_l]$ donde las indeterminadas $y_1, \ldots, y_s$ representan los bits del mensaje cifrado y las indeterminadas $k_1, \ldots, k_l$ simbolizan los bits de la clave secreta. Como Eve tiene descrita la aplicación de encriptar para las indeterminadas de un mensaje sin cifrar, y puede calcular tantas imágenes $\epsilon(x_1^i, \ldots, x_n^i)$ como necesite para resolver el sistema de ecuaciones determinado por la igualdad:

$$\delta(y_1^i, \ldots, y_s^i, k_1, \ldots, k_l) = (x_1^i, \ldots, x_n^i)$$

en las indeterminadas $k_1, \ldots, k_l$; obteniendo así la clave secreta.

Observamos que en los 3 ataques presentados hasta ahora el problema matemático se reduce a resolver un sistema de ecuaciones polinomiales. Las bases de Gröbner son de gran ayuda para ello. Veamos a continuación cómo podríamos romper el criptosistema RSA:

Ejemplo 3.3.1 (**Ataque al RSA**). *Bob y Alice eligen dos números primos distintos p y q, supongamos que Bob elige $p := 3$ y Alice $q := 5$, para simplificar los cálculos.*
Alice calcula $n = p \cdot q = 15$ que es el módulo de la clave pública y privada. Posteriormente escoge un número e menor que $\varphi(15) = 8$, y coprimo con él. Alice toma $e = 5$, y su clave pública es el par $(n, e) := (15, 8)$. Para la clave privada debe elegir d de tal modo que satisfaga la ecuación modular $5 \cdot d \equiv 1 \,(mod\, 8)$. Alice elige $d = 5$, por lo tanto su clave privada es $(15, 5)$.
Ahora Eve trata de romper este criptosistema, al tener acceso a la clave pública conoce el valor de n y por lo tanto sabe que tanto los cuerpos de los alfabetos de texto cifrado como descifrado, son las unidades del cociente $\mathbb{Z}/15\mathbb{Z}$, por lo que los mensajes cifrado y descifrado los podremos representar por $a_0 + 2a_1 + 4a_2 + 8a_3$, siendo $a_i \in \mathbb{Z}_2$. Eve

puede definir la aplicacion de encriptar $\epsilon : (\mathbb{Z}/15\mathbb{Z})^* \longrightarrow (\mathbb{Z}/15\mathbb{Z})^*$ *tal que un mensaje sin encriptar* (a_0, a_1, a_2, a_3) *es el mensaje encriptado* (c_0, c_1, c_2, c_3)*, determinado por* $c_0 + 2c_1 + 4c_2 + 8c_3 = (a_0 + 2a_1 + 4a_2 + 8a_3)^5$*, siendo* $a_i^2 = a_i$*, ya que* a_i *está en* $\mathbb{Z}_2$*. De esta manera Eve obtiene el siguiente sistema de ecuaciones:*

$$(S)\begin{cases} f_0 \equiv a_0a_1a_2a_3 + a_0a_1a_2 + a_0a_2 + a_0a_3 + a_2a_3 + a_0 + a_3 := c_0, \\ f_1 \equiv a_0a_1a_2a_3 + a_0a_1a_2 + a_0a_1a_3 + a_0a_2a_3 + a_0a_1 + a_1 + a_2 + a_3 := c_1, \\ f_2 \equiv a_1a_2a_3 + a_0a_1 + a_1a_2 + a_1a_3 + a_1 + a_2 := c_2, \\ f_3 \equiv a_0a_1a_2a_3 + a_0a_1a_2 + a_1a_2a_3 + a_0a_1 + a_0a_2 + a_0a_3 + a_2a_3 + a_3 := c_3. \end{cases}$$

El sistema (S) *representa la aplicación de encriptación del criptosistema establecido por Alice y Bob. Supongamos que Bob envía el mensaje cifrado* $3 = (c_0, c_1, c_2, c_3) = (1, 1, 0, 0)$*. Si Eve intercepta este mensaje, ella puede calcular una base de Gröbner del ideal generado por su sistema de ecuaciones,*

$$I =< f_0(a_0, a_1, a_2, a_3) - c_0, f_1(a_0, a_1, a_2, a_3) - c_1, f_2(a_0, a_1, a_2, a_3) - c_2, f_3(a_0, a_1, a_2, a_3) - c_3 >,$$

obteniendo $G = \{a_0 - 1, a_1 - 1, a_2, a_3\}$*, que corresponde al mensaje sin encriptar* $m = (1, 1, 0, 0) = 3$*.*

Observamos que una solución $(a_0, \ldots, a_3)$ del sistema (S) satisface:

$$f_0(x_0, x_1, x_2, x_3)g_1(x_0, x_1, x_2, x_3) + \ldots + f_3(x_0, x_1, x_2, x_3)g_3(x_0, x_1, x_2, x_3) = 3,$$

donde $g_i \in \mathbb{Z}_2[x_0, x_1, x_2, x_3]$.

En otras palabras, una solución del sistema (S) es un cero del ideal de polinomios I, generado por f_0, f_1, f_2, f_3. El conjunto de todas las soluciones del sistema (S) es la variedad definida por el ideal I.

3.4. Ataque algebraico con Bases de Gröbner

Como hemos visto, romper un criptosistema muchas veces se reduce a resolver un sistema de ecuaciones polinomiales sobre un cuerpo finito. Por tanto el problema que debemos resolver para romper un criptosistema lo traducimos como:

$$(S)\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_s(x_1, \ldots, x_n) = 0, \end{cases}$$

siendo los polinomios f_i del anillo $P := \mathbb{F}_q[x_1, \ldots, x_n]$, normalmente $\mathbb{F}_q = \mathbb{Z}_2$.

Nota 3.4.1. *Es este último apartado estamos trabajando en un cuerpo* $\mathbb{F}_q$*, por lo que debemos añadir las ecuaciones* $x_i^q - x_i = 0$*, para* $i = 1, ..., n$*.*

Tomamos el ideal I generado por $f_1, \ldots, f_s, x_1^q - x_1, \ldots, x_n^q - x_n$. Nuestro objetivo será encontrar su conjunto de ceros, o variedad algebraica asociada.

Para calcularlo Eve hallará una base de Gröbner del ideal I. Posteriormente ella deberá usar el algoritmo obteniendo la base de Gröbner reducida de I respecto al orden lexicográfico. Usando transformaciones lineales puede normalizar I respecto la última coordenada, y así asegurar que la última coordenada de los puntos de $V(I)$ sean distintas. Eve se encuentra ahora en las hipótesis del Lema 1.2.5, por lo tanto la base de Gröbner reducida de I respecto al orden lexicográfico tendrá la siguiente forma:

$$G' = \{x_1 - g_1(x_n), ..., x_{n-1} - g_{n-1}(x_n), g_n(x_n)\}.$$

Factorizando $g_n(x_n)$, obtendremos sus raíces, es decir, la última coordenada de los ceros de I, y ahora sustituyendo en los polinomios $g_i(x_n)$ para $i = 1, ...n-1$, Eve calculará las restantes coordenadas y obtendrá los ceros de I, pudiendo romper así los criptosistemas que podamos representar con un sistema de ecuaciones polinomiales.

Con estos ataques observamos que la seguridad de los criptosistemas Polly Cracker es cuestionable. Por lo tanto las bases de Gröbner no proporcionan seguridad a un criptosistema, sin embargo son de gran utilidad en el criptoanálisis.

Conclusiones

En este trabajo hemos expuesto los criptosistemas Polly Cracker, que fueron introducidos en 1993 por Fellows y Koblitz. Desde ese entonces las Matemáticas, y otras Ciencias han avanzado, figurando entre sus objetivos el desarrollo del sistema cuántico, con el que se abandona la dualidad del sistema binario, para pasar a un espacio vectorial unitario complejo y bidimensional. Los estados básicos - base ortonormal de tal espacio vectorial - se denotan como $|0>$ y $|1>$, y un qubit - vector de dicho espacio vectorial - es una combinación lineal $\alpha|0> + \beta|1>$, a diferencia de un bit *clásico* que solo toma los valores cero o uno.

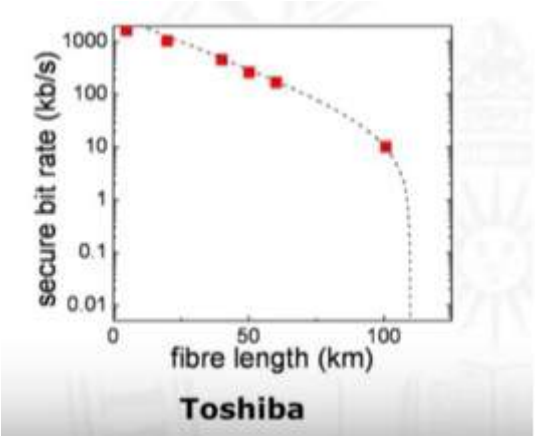
La velocidad de resolución de algunos problemas en un ordenador clásico crece exponencialmente respecto a la cantidad de información. Sin embargo, apoyados en la cuántica ya se ha probado la existencia de algoritmos con una velocidad de resolución para estos problemas considerablemente menor. Si tomamos como ejemplo el problema de factorización de un número N, en un canal clásico se realiza en un tiempo $O(exp[(\frac{64}{9}N)^{\frac{1}{3}}(\log N)^{\frac{2}{3}}])$, mientras que se ha demostrado que el *Algoritmo de Shor*, un algoritmo probabilístico apoyado en la teoría cuántica, calcula un factor de N en un tiempo $O((\log N)^3)$. Esto supone que con la ayuda de un ordenador cuántico todos los criptosistemas de clave pública son muy frágiles, por lo que debemos introducir criptosistemas apoyados en la cuántica para garantizar cierta seguridad.

La propiedad de la cuántica que nos invita a pensar en los grandes avances que puede suponer su uso en la criptografía, es que a la hora de medir un qubit, éste será $|0>$ o $|1>$, pero nunca sabremos si está en superposición, es decir en una combinación de ambos ($\alpha \neq 0 \neq \beta$). Supongamos que el qubit es $\alpha|0> + \beta|1>$, obtendremos la medida $|0>$ con una probabilidad de α^2 y la medida $|1>$ con una probabilidad de β^2, por lo que, para que esta suma de probabilidades sea uno, el vector del estado del qubit ha de ser unitario. Un receptor cuántico recibe correctamente solo dos estados de qubits que formen una base ortonormal del espacio vectorial, y a cada estado de esta base le asigna la medida 0 o 1; para otros estados le asigna en igual proporción la medida 0 o 1.

En la actualidad la Criptografía emplea criptosistemas de clave pública para la transmisión de las claves de un criptosistema simétrico, en el cual se mantendrá la conversación. La fragilidad de los criptosistemas de clave pública frente a los avances de la cuántica, supone la exposición de las claves de nuestro criptosistema simétrico. En los algoritmos de Criptografía apoyados en la cuántica, se transmiten las claves a través de un canal cuánti-

co, pero posteriormente la comunicación se hará a través de un canal clásico simétrico.

Este canal cuántico puede ser un transmisor de electrones o fotones en cierto estado y un receptor que realiza la medición de los mismos. Un inconveniente es la lentitud del proceso, ya que se ha de enviar partícula a partícula y esperar a que se estabilicen en el receptor. La velocidad también depende de las condiciones del medio, y la distancia a la que se encuentra el receptor del emisor: si por ejemplo usamos fibra óptica para unir un emisor y un receptor de la marca Toshiba, suponiendo una distancia de 120 kilómetros entre el emisor y el receptor, la velocidad de transmisión será menor a $1Kb/s$ (ver [Sem]).



En la actualidad esto nos proporciona una velocidad de transmisión del orden de $10mHZ$, mientras que un ordenador clásico es bastante más rápido, por ejemplo un procesador intel $i5$ llega a los $3GHz$. A pesar de este inconveniente, la gran ventaja será la completa seguridad de que se sabrá cuando alguien intenta interceptar la información transmitida por ese canal, esto se debe a que cuando alguien intenta leer un qubit lo perturbará, ya que no sabrá exactamente en el estado en el que se encuentra el qubit y al medirlo lo transformará.

Por ejemplo, si Alice desea mandar cierta clave a Bob, ella encripta los bits de una clave aleatoria binaria haciendo uso aleatorio del cambio de base definido por las aplicaciones f y g, siendo $f(1) = |1>$, $f(0) = |0>$, $g(0) = |0> + |1>$ y $g(1) = |0> - |1>$. Luego envía esta clave encriptada en qubits a Bob, que para descodificar usa la inversa de estas aplicaciones aleatoriamente, es decir Bob tiene dos tipos de receptores, uno que identifica los qubit en los estados $|0>$ y $|1>$ y otro identificará los qubit en los estados $|0> + |1>$ y $|0> - |1>$. Observamos que tendremos ciertos estados de qubits para los que las aplicaciones inversas de f o g no están definidas, es decir el receptor de Bob no es capaz de identificar el estado exacto y le asigna el valor 0 o el 1 en la misma proporción. De esta forma, Bob obtiene una clave en la que el 75 por ciento de los bits son correctos, aunque solo el 50 por ciento han sido desencriptados con la misma aplicación con la que se encriptó. A través de un canal clásico, Alice y Bob realizan un estudio muestral para eliminar estos bits que han sido desencriptados con distinta aplicación que la usada por Alice para encriptar. Este estudio muestral les proporcionará también la posible intrusión de Eve en

el sistema, pudiendo así desechar la clave y comenzar de nuevo el proceso. Una vez que obtienen una clave que consideran segura, harán uso de la teoría de códigos correctores para eliminar ciertos posibles errores generados por el mismo canal. Todos estos procesos de seguridad se engloban en el protocolo BB84, el protocolo de criptografía cuántica más común, propuesto por Charles Bennett y Gilles Brassard en 1984.

Sin duda, estamos ante un campo de la ciencia en pleno desarrollo. Si a principios del siglo XX tuvo lugar una revolución con la introducción de la teoría cuántica formulada por Planck, Heisenberg y otros físicos teóricos, ahora estamos en el camino de realizar la segunda revolución, impulsada por la gran inversión en este campo de investigación. En particular, Europa tiene en marcha un plan de inversión para el año 2018 de 1.000 millones de euros para diferentes proyectos relacionados con la cuántica, principalmente en el campo de la computación, donde se espera una mejor eficiencia de los ordenadores cuánticos. Por otra parte la empresa IBM ha creado la *Quatum Experience*, un simulador cuántico en la nube, de libre acceso, que trabaja con 5 qubits. Google y la Nasa adquirieron en 2013 un ordenador cuántico, de la marca D-wave, por 15 millones de euros que trabaja con 9 qubits y 1000 puertas lógicas, lo que le proporciona una gran potencia de procesador. En la sede de Google en Silicon Valley, donde está instalado el D-Wave 2X, colabora un grupo de la Universidad del País Vasco, dirigido por Enrique Solano, responsable del grupo de Tecnología Cuántica para Ciencias de la Información de la UPV, que comentó para El País (noticia del 13 de junio de 2016): *Para Google estas máquinas son estratégicas, su objetivo es que puedan resolver problemas de inteligencia artificial, sobre todo para el reconocimiento de imágenes, pues sus algoritmos actuales dan problemas que creen que pueden resolver con un ordenador cuántico. Estos ordenadores pueden usarse para problemas muy complejos en economía, demografía, simulación de pruebas nucleares sin necesidad de explosiones, estudios de aerodinámica que no podrían hacerse en ningún túnel de viento existente. . . . Casi todos estos problemas se basan en las mismas ecuaciones no lineales que los ordenadores comunes no pueden atacar y estos sí.* Dos grandes inconvenientes de los ordenadores cuánticos es su coste elevado y las condiciones físicas en las que los qubits han de ser procesados: para hacernos una idea, el ordenador de Google y la Nasa ha de estar a una temperatura de $-273^{o}C$. Es por ello que, aunque estemos en el camino de la revolución cuántica, la computación clásica aún tiene un papel que jugar y sigue siendo interesante el estudio de criptosistemas basados en la misma.

Bibliografía

[Bar] Barkee, B. et al., *Why you cannot even hope to use Gröbner bases in public key cryptography: an open letter to a scientist who failed and a challenge to those who have not yet failed.* J. Symbolic Comput. 18 (1994), no. 6, 497-501.

[Bau et al.] Baumslag, G., Fine, B. Kreuzer, M. and Rosenberger, G. *A course in Mathematical cryptography.* De Gruyter (2015).

[Be-Br] Bennett C. and Brassard G. *Quantum cryptography: public key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, IEEE press.* (1984) , 175-179.

[Bu1] Buchberger B. *Eim Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph.D. thesis, Innsbruck, 1965.

[Bu2] Buchberger B. *Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal.* J. Symb. Comput. 41 (2006), 3-4, 475-511.

[Cou-MC-P] Couvreur, A., Márquez Corbella, I., Pellikaan, R. *A polynomial time attack against Algebraic Geometry code based public key crypto systems.* IEEE International Symposium on Information Theory (ISIT). pp. 1446 - 1450. IEEE, 24/01/2014.

[Cox-Li-O] Cox, D., Little, A. and O'Shea, D. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra.* Fourth edition. Undergraduate Texts in Mathematics. Springer, Cham, 2015. xvi+646 pp.

[Fe-Ko] Fellows, M. and Koblitz, N. *Combinatorial cryptosystems galore!* Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993), 51-61, Contemp. Math., 168, Amer. Math. Soc., Providence, RI, 1994.

[La] Lauritzen, N. *Concrete Abstract Algebra. From Numbers to Gröbner Bases* (2005), 186-217

[Levy et al.] Levy-dit-Vehel, F. et al. *A Survey on Polly Cracker Systems*

[Sem] García, J. *Seminario de Introducción a la Computación y Criptografía cuántica*, ver: http://www.criptored.upm.es/crypt4you/temas/cuantica/leccion2/leccion02.html

[S1] Shannon, C. E. *A mathematical theory of communication* Bell System Tech. J. 27 (1948), 379-423, 623-656.

[S2] Shannon, C. E. *Communication theory of secrecy systems.* Bell System Tech. J. 28 (1949), 656-715.

[V] Van, L. *Polly Two-A Public Key Cryptosystem based on Polly Cracker.* Ruhr-Universität Bochum (2002), 1-11.

Gröbner basis and cryptography

Pablo de la Torre Fernández

Polynomials in several variable

Polynomials are natural objects to use in cryptography so let's define $P := K[x_1, \cdots, x_n]$ the ring of polynomials on n variables over the field K, usually $\mathbb{F}_q$:

$$P := K[x_1, \ldots, x_n] = \left\{ \sum_{v \in \mathbb{N}^n} a_v \cdot x^v,\ a_v \in K^n \right\}.$$

To order the monomials of a polynomials in several variables we define a term ordering as a partial ordering $\leq$ on $\mathbb{N}^n$ such that:

(i) $\leq$ is a total ordering.
(ii) $\mathbf{0} \leq v_i$ for every $v_i \in \mathbb{N}^n$,
(ii) $v_1 \leq v_2$ then $v_1 + v \leq v_2 + v$ for every $v_1, v_2, v \in \mathbb{N}^n$.

We use the lexicographic order, $x = (x_1, \cdots, x_n), y = (y_1, \cdots, y_n)$. Then $x \geq_{lex} y$ if and only if the left-most nonzero entry of $x - y$ is non negative.
The initial term of a polynomial $f = \sum_{v \in \mathbb{N}^n} a_v \cdot x^v$ is defined as $in_{\leq}(f_i) = a_w x^w$ and $w = max_{\leq}\{v \in \mathbb{N}^n : a_v \neq \mathbf{0}\}$.

- Division Algorithm:

Let $f, f_1, \cdots, f_m \in P \backslash \{\mathbf{0}\}$ and $\leq$ a term ordering on $\mathbb{N}^n$. Then there exists $a_1, ..., a_m, r \in P$ such that $f = a_1 \cdot f_1 + \cdots + a_m \cdot f_m + r$, where $r = \mathbf{0}$ or none of the terms in r is divisible by $in_{\leq}(f_1), ..., in_{\leq}(f_m)$. Futhermore $in_{\leq}(a_i \cdot f_i) \leq in_{\leq}(f)$ if $a_i \cdot f_i \neq \mathbf{0}$.
If $F = \{f_1, \cdots, f_m\}$ then we denote by f^F and we call it normal form.

Gröbner basis

- A set of non-zero polynomials $F = \{f_1, \cdots, f_m\} \subset P$ is called *Gröbner basis* for an ideal I of P respect to a term ordering $\leq$, if $F \subseteq I$ and for every $f \in I$ there exist some f_i such that $in_{\leq}(f)$ is divisible by $in_{\leq}(f_i)$.
- *Buchberger algorithm: Input:* $F = \{f_1, \cdots, f_m\} \subset P$, f_i *non-zero for* $i = \mathbf{1}, \cdots, m$.
Output: $G = \{g_1, \cdots, g_r\}$ *a Gröbner basis for* $I =< f_1, \cdots, f_m >$.
Inicialization: $G := F$, $G' = \{\{f_i, f_j\}, f_i \neq f_j \in G\}$ *while:* $G' \neq \emptyset$ *do Choose* $\{f_i, f_j\} \in G'$ $G' := G' \backslash \{f_i, f_j\}$ *and* $h := (s(f_i, f_j))^G$. *If* $h \neq \mathbf{0}$ *then* $G' := G' \bigcup \{u, h\}$, *for every* $u \in G$ *and* $G := G \bigcup \{h\}$.

Reduced Gröbner basis

- A Gröbner basis $G = \{f_1, \cdots, f_m\}$ is called *minimal Gröbner basis* if:
  1. $in_{\leq}(f_i) \mid in_{\leq}(f_j)$ for every $i \neq j$.
  2. The coefficient of $in_{\leq}(f_i)$ is one for $i = \mathbf{1}, \cdots, m$.

  This concept is still not unique.
- *A reduced Gröbner basis* $G = \{f_1, \cdots, f_m\}$ is a minimal Gröbner basis such that any term of f_i is divisible by some $in_{\leq}(f_j)$.
- *Reduced Gröbnerr basis algorithm* Let I be an ideal on P. *Input* $G := \{g_1, \cdots, g_t\}$ *a minimal Gröbner basis of* I.
Output G' *a reduced Gröbner basis of* I
do $g_i' = \frac{1}{coef(g_i)} g_i$; $G'' = G'' \bigcup g_i'$, $i = \mathbf{1}, ..., t$.
do $g_i'' = (g_i')^{G''}$, $G' := G' \bigcup g_i''$, $i = \mathbf{1}, ..., t$.

Geometric ingredients

- Let K be a field and $f_1, \cdots, f_m$ polynomials in the ring $K[x_1, \cdots, x_n]$. Then the set $V(f_1, ..., f_s) = \{(a_1, ..., a_n) \in K^n : f_i(a_1, ..., a_n) = \mathbf{0}$, for every $i = \mathbf{1}, ..., s\}$ is the *affine variety* defined by $f_1, ..., f_s$. And the set $I(V) = \{f \in K[x_1, .., x_n] : f(a_1, ..., a_n) = \mathbf{0}$, for every $(a_1, ..., a_n) \in V\}$ is the *ideal of V*.
Now we can define the radical of an ideal is $\{f : f^m \in I$ for some integer $m \geq \mathbf{1}\}$ and it is denoted by $\sqrt{(I)}$.

- *Shape Lemma:* Let K be an algebraic closed field and I an finite radical ideal on $K[x_1, \cdots, x_n]$. Suppose that $V(I)$ has m points with pairwise different x_n coordinate is not equal for every points. Then the reduced Gröbner basis of I with respect the lexycographic order, is the set:
$\{g_1 = x_1^m + h_1(x_n), g_2 = x_2 + h_2(x_n), \cdots, g_n = x_n + h_n(x_n)\}$, where $h_1, \cdots, h_n \in F_q[x_1]$ of degree less or equal to $m - \mathbf{1}$.

Polly Cracker Cryptosystems

The Polly Cracker Cryptosystems are based on the Gröbner basis theory, exactly its private key is a Gröbner basis, or a point of the variety defined by an ideal.

- *Abstract Polly Cracker*:
Public Key: A set of polynomial, $F = \{f_1, \cdots, f_m\}$, $f_i \in P$.
Private Key: A point $\psi \in K^n$, such that ψ is a zero of the ideal $I =< f_1, \cdots, f_m >$, $\psi \in V(I)$.
Encryption: Bob sends a message $m \in K$, he chooses an arbitrary polynomial $h \in I$ and he computes $c := m + h$.
Decryption: Alice evaluates the polynomial c on ψ and she gets the message m.

The security of this cryptosystem is based on the hardness of compute a zero of the ideal I, that it can be translate to solve an algebraic equation system.

1. Alice must choose "well" the polynomials on F.
2. Take the set of polynomials F as a transcription of a NP-complete problem.
3. First proposal: Koblitz and Fellows studied the problems based on graph theory.

- *Barkee Cryptosystem*:
Public Key: An ideal $I =< f_1, \cdots, f_m >$, $f_i \in P$ and a subset of normal forms $N = \{g_1, \cdots, g_r\}$ on P with respect to the ideal I.
Private Key: The Gröbner basis G of I.
Encryption: Bob sends a message $m \in Kg_1 + \cdots + Kg_r$, he chooses an arbitrary polynomial $h \in I$ and he computes $c := m + h$.
Decryption: Alice compute the remainder of the division algorithm, $(c)^G$, and she gets the message m.

Gröbner basis attack

Suppose that now on a public key criptosystem there is a hacker, Eve, that intercept a ciphertext and she is going to try to decipher the message. As she knows the public key she can describe the cipher mapping $\epsilon : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^s$, using polynomials $f_1, ..., f_s \in \mathbb{Z}_2[x_1, ..., x_n]$, where the indeterminates $x_1, ..., x_n$ correspond to the plaintext bits. Suppose that Eve gets a ciphertext c_i, $\mathbf{1} \leq i \leq s$, if she is able to solve the equation system $f_i(x_1, ..., x_n) = c_i$, $\mathbf{1} \leq i \leq s$, she will have the plaintext.
Then the problem has been reduced to solve a polynomial equation system. Alice takes the ideal $I =< f_1, \cdots, f_s >$ and she computes a reduced Gröbner basis respect to the lexicographic term ordering. Now she brings I into normal x_n-position, so that she can be sure that the last coordinates of the points of $V(I)$ are pairwise distinct, so the setting of the Shape Lemma are verified then the reduced Gröbner basis G of I has the following shape: $G = \{x_1 - g_1(x_n), \cdots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)\}$. If she is able to factorize $g_n(x_n)$, it will be easy to calculate the zeros of $g_n(x_n)$ and substituting these into the others polynomials g_i, she will have the points of $V(I)$ and the solutions of the system.

Conclusions

The Gröbner basis theory gives us a tool really useful for cryptoanalysis, but it does not give us security on cryptosystem, because every system lies on Gröbner basis is susceptible to be attacked. Moreover the develop of quantum computation make classical cryptosystem unsafer, but there is not a sufficiently powerful quantum computer able to broke a cryptosystem yet. Then the classical computation has a role to play and it is interesting its study for cryptosystem lying on it.

- Baumslag, G., Fine, B. Kreuzer, M. and Rosenberger, G. *A course in Mathematical cryptography*. De Gruyter (2015).
- Van, L. *Polly Two-A Public Key Cryptosystem based on Polly Cracker*. Ruhr-Universität Bochum (2002), 1-11.