UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Tesis de Licenciatura

Algoritmos de factorización de polinomios multivariados y nuevas estimaciones sobre los ceros de un polinomio sobre un cuerpo finito

Melina L. Privitelli

Director: Dr. Antonio A. Cafure

Marzo 2009

A la memoria de Antonio Arcuri.

Agradecimientos

Quiero darle las gracias a cada una de las personas que me ayudaron a alcanzar esta meta:

A mi mamá Elena, a mi papá José, a mis tíos y primos por acompañarme siempre y apoyarme en los momentos más difíciles. A mi querido tío Antonio, que seguramente debe estar muy feliz por mi.

A Nino, mi amigo y director, por confiar en mí, por su ayuda incondicional, por alentarme en los peores momentos, porque gracias a su esfuerzo pude entender y aprender estos temas, por su paciencia, y sobre todo por darme la oportunidad de hacer mi tesina en un tema que me encanta.

A Guillermo Matera, por sus sugerencias para la presentación, y por haber escuchado más de una vez el algoritmo de factorización.

A los jurados, Pablo Solernó y Gabriela Jerónimo, por tomarse el trabajo de leer mi tesina con todo detalle y porque sus comentarios y correcciones fueron muy útiles para poder mejorar la versión final de este trabajo.

A Gabriel Minian, por la buena predisposición que siempre tuvo hacia mi persona, y por ayudarme con los trámites para la presentación de mi tesina.

A Marita, por esas largas charlas volviendo de Merlo, y porque sus palabras siempre fueron de mucha ayuda.

A mis amigos: Patri, María Marta, Mariana, Mercedes, Ezequiel, Ale, Gerardo, Guillermo, Nelson, Eugenia y Lucas, porque hicieron más sencillos todos estos años.

A Betty, mi suegra, por aguantarme los fines de semana estudiando en su casa.

A Nicolás, mi novio y una de las personas más lindas que conocí, siento que no me va a alcanzar la vida para darle las gracias. Sin lugar a dudas es el principal responsable de que yo haya llegado hasta acá. Gracias por quererme como soy y no intentar cambiarme, por apoyarme y acompañarme en todas mis decisiones, por haber hecho que todo tenga sentido y por haberme convertido en una persona feliz.

Índice general

Introducción **5**

1 Variedades algebraicas y polinomios absolutamente irreducibles **8**
1.1 Preliminares de Geometría Algebraica 8
1.1.1 Dimensión y Grado de una variedad 9
1.2 Polinomios absolutamente irreducibles 11
1.3 Levantamiento de Hensel 15

2 Algoritmos de factorización y una versión del Teorema de Bertini **18**
2.1 Algoritmo de factorización para polinomios bivariados 18
2.1.1 Recombinación 28
2.2 Generalización a polinomios multivariados 33
2.2.1 Reducción a dos variables 33
2.3 Teorema de Bertini 36

3 Estimación sobre la cantidad de ceros q-racionales de un polinomio absolutamente irreducible **42**
3.1 Número promedio de ceros en $\mathbb{F}_q^n$ 42
3.2 Estimación sobre los ceros q-racionales de f 47

4 Aplicaciones a la Teoría de Códigos **56**
4.1 Generalidades sobre Códigos 56
4.1.1 Problema de decodificación en Reed-Solomon 59
4.2 Reducción a una Hipersuperficie 61
4.2.1 Absoluta Irreducibilidad de $C_{f_0,\ldots,f_d}$ 61
4.3 Aplicación de las estimaciones al problema de códigos 66

Bibliografía **68**

Introducción

Diversos algoritmos de factorización utilizan el esquema de levantamiento de Hensel y recombinación. A grandes rasgos estos algoritmos están conformados por tres etapas. La primera de ellas consiste en especializar $n-1$ variables del polinomio f para obtener un polinomio univariado y posteriormente factorizarlo. Esta factorización permite, en la segunda etapa, obtener los factores analíticos de f con un cierto grado de precisión; es decir, los factores en el álgebra de series de potencias (levantamiento de Hensel). La tercera y última etapa consiste en recombinar dichos factores analíticos para obtener los factores de f en el cuerpo de base.

La idea de factorizar polinomios utilizando el levantamiento de Hensel surge por primera vez en un trabajo de H. Zassenhaus del año 1969 para polinomios con coeficientes enteros [Zas69]. En la década del 70 este método comienza a utilizarse para factorizar polinomios bivariados, a partir de los trabajos de R. Musser [Mus75] y P. Wang y L. Rothschild [WR75, Wan78]. En el peor de los casos, la tercera etapa exigía calcular todas las posibles combinaciones. El costo de este proceso era exponencial en el número de factores analíticos y, luego, en el grado total del polinomio. En los años 80 surgieron diversos algoritmos de factorización de tiempo polinomial a partir de los trabajos de A. Lenstra (1984, 1985 y 1987), A. L. Chistov (1984, 1987, 1991), D. Grigoriev (1984) y E. Kaltofen (1985, 1990, 1995), quien junto a J.von zur Gathen obtienen un algoritmo de tiempo polinomial utilizando el método de aproximación de Newton para polinomios multivariados con coeficientes racionales o en un cuerpo finito. Más allá de estos avances, los algoritmos basados en el levantamiento de Hensel y la recombinación permanecieron vigentes ya que sólo en el peor de los casos, la recombinación podía ser muy costosa.

En 1999, W. Ruppert [Rup86, Rup99] vincula la absoluta irreducibilidad de un polinomio f con la existencia de una 1-forma cerrada $W = \frac{h}{f}dx + \frac{g}{f}dy$, donde g y h son polinomios en $\mathbb{K}[X,Y]$ satisfaciendo ciertas condiciones de grado. A partir de esta caracterización S. Gao [Gao03] obtiene un algoritmo que calcula la factorización absoluta y racional de un polinomio. El núcleo de su trabajo reside en resolver de manera eficiente el sistema lineal de ecuaciones que se construye a partir de la condición

$$\frac{\partial}{\partial X}\left(\frac{g}{f}\right) = \frac{\partial}{\partial Y}\left(\frac{h}{f}\right).$$

En el año 2004, K. Belabas, M. Van Hoeij, J. Klüeners y A. Steel desarrollaron el método de la derivada logarítmica para la recombinación, que en polinomios bivariados requiere precisión mayor o igual a $d_X(d_Y-1)+1$, siendo d_X y d_Y los grados en las variables X e Y

respectivamente, y sin imponer condiciones sobre la característica del cuerpo [BHKS04]. También en el año 2004, A.Bostan, G.Lecerf, B.Salvy, É.Schost y B.Wiebelt, desarrollan un algoritmo basado en el levantamiento de Hensel que requiere precisión $\sigma = 3d - 2$ y característica cero o mayor o igual a $d(d-1)+1$ [AGS$^+$04]. En esta tesina estudiaremos el algoritmo desarrollado por G. Lecerf [Lec06, Lec07], el cual requiere encontrar los factores analíticos de f a precisión mayor o igual a $2d$ (o sea precisión lineal en el grado del polinomio) y permite obtener la recombinación resolviendo un sistema de ecuaciones lineales, imponiendo ciertas condiciones sobre la característica. Lecerf combina el levantamiento de Hensel con las ideas de Gao y su algoritmo se basa en encontrar expresiones para g y h de la ecuación de Ruppert, en términos de los factores analíticos de f.

A partir de los años 80, se obtuvieron diferentes versiones del Teorema de Bertini a partir de algoritmos de factorización para polinomios multivariados. Dado un polinomio $f \in \mathbb{K}[X_1, \ldots, X_n]$, se quiere caracterizar las $3n$-uplas en $\mathbb{K}^{3n}$ para las cuales se preserva el patrón de factorización al considerar el polinomio

$$f_{\gamma,\alpha,\beta}(\gamma_1 + \alpha_1 X + \beta_1 Y, \ldots, \gamma_n + \alpha_n X + \beta_n Y).$$

El teorema de Bertini nos proporciona una estimación sobre la cantidad de $3n$-uplas para las cuales esto no sucede. El algoritmo que estudiaremos en esta tesina nos permite derivar en la que actualmente es la mejor versión del Teorema de Bertini. Como consecuencia de esto, proporcionaremos una mejora en la estimación sobre la cantidad de ceros q-racionales de un polinomio absolutamente irreducible en $\mathbb{F}_q[X_1, \ldots, X_n]$.

El primer resultado explícito para la estimación de ceros q-racionales de un polinomio absolutamente irreducible fue obtenido por W.Schmidt [Sch76], quien demostró que si $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ es un polinomio absolutamente irreducible de grado $d > 0$ entonces el número N de ceros de f en $\mathbb{F}_q^n$ satisface:

$$|N - q^{n-1}| \leq q^{n-2}(\sqrt{2}d^{\frac{5}{2}}q^{\frac{1}{2}} + 2d\theta)$$

donde θ es igual a $2dk^{2^k}$ y $k = \binom{d+1}{2}$. A. Cafure y G. Matera [CM06], siguiendo las técnicas de Schmidt e inspirados en un trabajo de E. Kaltofen [Kal91], mejoran exponencialmente esta estimación obteniendo

$$|N(f) - q^{n-1}| < (d-1)(d-2)q^{n-\frac{3}{2}} + 5d^{\frac{13}{3}}q^{n-2},$$

donde este resultado es válido para una característica arbitraria. Utilizando la versión del Teorema de Bertini que se deriva del algoritmo de Lecerf, probaremos que la cantidad N de ceros en $\mathbb{F}_q^n$ de un polinomio absolutamente irreducible de grado d satisface

$$|N - q^{n-1}| < (d-1)(d-2)q^{n-\frac{3}{2}} + 6d^3q^{n-2}, \tag{1}$$

con la condición de que la característica sea mayor o igual a $d(d-1)+1$. También exhibiremos una estimación que mejora (1), aunque será válida bajo una cierta condición de regularidad. Schmidt probó [Sch74] que si $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ es un polinomio absoluta-

mente irreducible de grado $d > 0$ entonces, suponiendo que $q > c_0(\epsilon)n^3d^{5+\epsilon}$, se verifica

$$|N - q^{n-1}| < (d-1)(d-2)q^{n-\frac{3}{2}} + 6d^2q^{n-2}.$$

Por otra parte A. Cafure y G.Matera [CM06] demuestran que bajo la condición $q > 15d^{\frac{13}{3}}$ se tiene

$$|N - q^{n-1}| < (d-1)(d-2)q^{n-\frac{3}{2}} + (5d^2 + d + 1)q^{n-2}. \quad (2)$$

En esta tesina mostraremos que la estimación (2) es también válida para $q \geq 16d^4$ pero para característica mayor o igual a $d(d-1)+1$.

Las estimaciones sobre la cantidad de ceros q-racionales tienen diversas aplicaciones, entre ellas podemos nombrar: algoritmos de busqueda de puntos q-racionales, problemas de criptografía, problemas relacionados con la teoría de códigos. Nosotros finalizaremos este trabajo estudiando un problema concreto de teoría de códigos. Los códigos de Reed-Solomon fueron inventados por I.Reed y G.Solomon en el año 1960. Estos son muy utilizados en aplicaciones tecnológicas entre las que se encuentran, entre otras, el almacenamiento de datos y las comunicaciones inalámbricas y satelitales. En 2007, Q.Cheng y E.Murray [CM07] estudiaron el problema de determinar si una palabra recibida es o no un *deep hole*. Concretamente ellas traducen dicho problema al de determinar si una hipersuperficie absolutamente irreducible posee puntos en $\mathbb{F}_q^n$ con coordenadas no nulas y distintas entre si. En el trabajo mencionado demuestran que si $u \in \mathbb{F}_q^n$ es una palabra recibida generada por un polinomio de grado $k+d$, u no puede ser un *deep hole* si $d < q^{\frac{3}{13}-\epsilon}$ y $k < q^{\frac{1}{4}-\epsilon}$. Mostraremos que estas condiciones pueden ser optimizadas a partir de la mejora en las estimaciones para hipersuperficies.

La tesina está organizada de la siguiente manera.

En el capítulo 1 hacemos una revisión de los conceptos básicos de geometría algebraica para establecer nociones que utilizaremos a lo largo de esta tesina. También estudiaremos resultados relacionados con la absoluta irreducibilidad de polinomios y presentaremos el método de levantamiento de Hensel que utilizaremos posteriormente. En este capítulo seguimos a [LN83], [CLO98], [Kun85] y [Hei83].

En el capítulo 2 desarrollamos en una primera instancia el algoritmo de factorización de Lecerf para polinomios bivariados y posteriormente exhibimos su generalización a polinomios multivariados. Finalmente, basándonos en dichos algoritmos, obtenemos la mejor versión del Teorema de Bertini.

En el capítulo 3 presentamos, en primer lugar, los resultados clásicos sobre cotas para los ceros de polinomios sobre cuerpos finitos y número promedio de ceros en $\mathbb{F}_q^n$. Luego estimamos la cantidad de ceros en $\mathbb{F}_q^n$ de un polinomio absolutamente irreducible. Para ello, nos basamos en el trabajo de A.Cafure y G.Matera [CM06]. Finalmente estableciendo condiciones sobre la característica y sobre la cantidad de elementos del cuerpo finito, mostraremos que es posible mejorar aún más nuestra estimación.

En el capítulo 4 desarrollamos los conceptos básicos de la teoría de códigos. Para ello hemos consultado los textos [HP04], [Pre92] y [WP03]. Luego seguimos el trabajo de Q.Chen y E.Murray [CM07] obteniendo los resultados arriba mencionados.

Capítulo 1

Variedades algebraicas y polinomios absolutamente irreducibles

En primer lugar, haremos una revisión de los conceptos básicos de geometría algebraica con el objetivo de presentar las nociones que utilizaremos a lo largo de esta tesina. Por otra parte, estudiaremos un concepto central en este trabajo que es el de polinomio absolutamente irreducible y repasaremos algunos resultados clásicos para determinar la absoluta irreducibilidad. Finalizamos el capítulo desarrollando el método de levantamiento de Hensel, en el cual se basará el algoritmo de factorización que describiremos posteriormente.

1.1. Preliminares de Geometría Algebraica

Sea $\mathbb{K}$ un cuerpo y $\overline{\mathbb{K}}$ su clausura algebraica. Denotamos como $\mathbb{A}^n(\mathbb{K})$ el espacio afín definido sobre $\mathbb{K}$ de dimensión n. Cuando consideremos el espacio afín sobre $\overline{\mathbb{K}}^n$ dotado de la topología Zariski, simplemente escribiremos $\mathbb{A}^n$.

Definición 1.1. Un subconjunto $V \subset \mathbb{A}^n$ se denomina una $\mathbb{K}$-**variedad afín** si existen polinomios $f_1, \ldots, f_m \in \mathbb{K}[X_1, \ldots, X_n]$ tales que V es el conjunto de ceros comunes de $f_1, \ldots, f_m$ en $\mathbb{A}^n$. Es decir

$$V := V(f_1, \ldots, f_m) := \{x \in \mathbb{A}^n \mid f_1 = 0, \ldots, f_m = 0\}.$$

En particular una $\mathbb{K}$-**variedad afín** se dice una $\mathbb{K}$-**hipersuperficie** si es el conjunto de ceros de un único polinomio $f \in \mathbb{K}[X_1, \ldots, X_n]$.

Definición 1.2. Sea V una $\mathbb{K}$-variedad afín. El conjunto de los polinomios en $\mathbb{K}[X_1, \ldots, X_n]$ que se anulan sobre V

$$I(V) := \{f \in \mathbb{K}[X_1, \ldots, X_n] : f(x) = 0 \,\text{para todo}\, x \in V\},$$

se denomina el ideal de la variedad. Además, se verifica que $I(V)$ es un ideal radical.

Definición 1.3. Sea V una $\mathbb{K}$-variedad. Decimos que es **irreducible** si no se puede descomponer como unión de $\mathbb{K}$-variedades propias. Si V es irreducible como $\overline{\mathbb{K}}$-variedad entonces V se dice **absolutamente irreducible**.

Una forma de decidir si una variedad es irreducible o no es estudiar su ideal. Concretamente, V es irreducible si y solo si su ideal es primo. Como consecuencia, una $\mathbb{K}$-hipersuperficie es irreducible si y solo si es el conjunto de ceros de un polinomio irreducible $f \in \mathbb{K}[X_1, \ldots, X_n]$.

1.1.1. Dimensión y Grado de una variedad

Definición 1.4. Sea V una $\mathbb{K}$-variedad afín. Entonces el anillo

$$\mathbb{K}[V] := \mathbb{K}[X_1, \ldots, X_n] \,/\, I(V)$$

se denomina el **anillo de coordenadas de** V.

Una $\mathbb{K}$-variedad es irreducible si y solo si $\mathbb{K}[V]$ es un dominio íntegro. Su cuerpo de fracciones, notado $\mathbb{K}(V)$, se denomina el **cuerpo de funciones racionales de** V. Damos ahora la definición de dimensión de una variedad.

Definición 1.5. Sea V una $\mathbb{K}$-variedad irreducible. Definimos la **dimensión de** V como el grado de trascendencia de $\mathbb{K}(V)$ sobre $\mathbb{K}$:

$$\dim V = \operatorname{tr\,deg}(\mathbb{K}(V)/\mathbb{K}).$$

Es decir, el máximo número de elementos algebraicamente independientes sobre $\mathbb{K}$. Si V es una $\mathbb{K}$-variedad arbitraria y $V = V_1 \cup \cdots \cup V_r$ es su descomposición en componentes $\mathbb{K}$-irreducibles, entonces definimos su dimensión como

$$\dim V = \max_{1 \le i \le r} \{\dim\, V_i\}\,.$$

Ejemplo 1.6. Si $V = \mathbb{A}^n(\mathbb{K})$ entonces $\mathbb{K}(V) = \mathbb{K}(X_1, \ldots, X_n)$, cuyo grado de trascendencia sobre $\mathbb{K}$ igual a n y por lo tanto la dimensión de $\mathbb{A}^n(\mathbb{K})$ es n.

Ejemplo 1.7. Sea $V := V(2X+Y-Z)$ una $\mathbb{K}$-variedad lineal. El ideal de V $(2X+Y-Z)$, que resulta primo ya que el polinomio $f(X,Y,Z) = 2X + Y - Z$ es irreducible sobre $\mathbb{K}[X,Y,Z]$. Por lo tanto V es una variedad irreducible. El anillo de coordenadas $\mathbb{K}[V]$ resulta isomorfo al anillo de polinomios $\mathbb{K}[X,Y]$, luego V tiene dimensión 2. En general, en el caso de $\mathbb{K}$-variedades lineales el anillo de coordenadas es isomorfo a un anillo de polinomios sobre $\mathbb{K}$. En consecuencia, las variedades lineales son irreducibles.

Observación 1.8. Si H es una $\mathbb{K}$-hipersuperficie en $\mathbb{A}^n$ su dimensión es $n-1$. Una manera de demostrar este resultado es probar que todas sus componentes $\mathbb{K}$-irreducibles tienen dimensión $n-1$.

Observación 1.9. Si V es una $\mathbb{K}$-variedad en $\mathbb{A}^n$ de dimensión cero entonces V está formada por finitos puntos. Recíprocamente, si V está formada por finitos puntos, entonces su dimensión es cero.

A continuación damos la definición de grado de una variedad.

Definición 1.10. Sea V una $\mathbb{K}$-variedad equidimensional de dimensión r. Definimos el **grado** de V como el número máximo de puntos en la intersección de V con una variedad lineal L de codimensión r para la cual el número $|V \cap L|$ es finito. Si V es una $\mathbb{K}$-variedad arbitraria y $V = V_1 \cup \cdots \cup V_s$ es su descomposición en $\mathbb{K}$-componentes irreducibles, siguiendo [Hei83] definimos el grado de V como la suma de los grados de sus $\mathbb{K}$-componentes:

$$\deg V = \sum_{i=1}^{s} \deg V_i.$$

Ejemplo 1.11. Si V una variedad lineal entonces su grado es 1. El grado de una hipersuperficie irreducible coincide con el grado del polinomio f que la define. El grado de una variedad de dimensión cero es la cantidad de puntos de la misma.

Una de las principales propiedades de la definición de grado que hemos dado es su comportamiento con respecto a la intersección de variedades. A continuación enunciamos la denominada Desigualdad de Bézout ([Hei83]).

Teorema 1.12 (Desigualdad de Bézout)**.** *Sean V y W variedades de $\mathbb{A}^n$.Entonces*

$$\deg (V \cap W) \leq \deg V \cdot \deg W.$$

Finalizamos esta sección enunciando un resultado que será de suma importancia al momento de obtener las estimaciones.

Proposición 1.13. *[HS82] Sean $V_1, \ldots, V_s \subset \mathbb{A}^n$ variedades. Sea r la dimensión de V_1 y notemos $D = \max\{\deg V_2, \ldots, \deg V_s\}$. Entonces se verifica*

$$\deg (V_1 \cap \cdots \cap V_s) \leq \deg V_1 \cdot D^r.$$

Demostración. Observemos que, sin pérdida de generalidad, podemos suponer que V_1 es irreducible. En efecto, si no lo fuera entonces podemos escribir $V_1 = C_1 \cup \cdots \cup C_t$ donde cada C_k es una componente irreducible de V_1. Supongamos que para cada C_k se verifica la desigualdad dada por el teorema, es decir

$$\deg (C_k \cap V_2 \cap \cdots \cap V_s) \leq \deg C_k \cdot D^{\dim C_k}.$$

Entonces se verifica que

$$\begin{aligned}
\deg\left(V_1 \cap \cdots \cap V_s\right) &\leq \sum_{k=1}^{t} \deg\left(C_k \cap V_2 \cap \cdots \cap V_s\right) \\
&\leq \sum_{k=1}^{t} \deg\, C_k \cdot D^{\dim\, C_k} \\
&\leq \sum_{k=1}^{t} \deg\, C_k \cdot D^{r} \\
&\leq \deg V_1 \cdot D^r.
\end{aligned}$$

Entonces asumimos que V_1 es irreducible y hacemos inducción en la dimensión de V_1. Notemos que si $V_1 \subset V_2 \cap \cdots \cap V_s$, entonces $V_1 \cap \cdots \cap V_s = V_1$ con lo cual $\deg\left(V_1 \cap \cdots \cap V_s\right) = \deg V_1$ y luego vale el resultado. Supongamos entonces que V_1 no está contenido en V_2 lo que implica que $\dim\left(V_1 \cap V_2\right) < \dim V_1 = r$. Entonces aplicando hipótesis inductiva a $V_1 \cap V_2$ tenemos:

$$\deg\left(\left(V_1 \cap V_2\right) \cap V_3 \cap \cdots \cap V_s\right) \leq \deg\left(V_1 \cap V_2\right) \cdot D^{r-1},$$

por último, por la desigualdad de Bézout, obtenemos

$$\deg\, V_1 \cdot \deg\, V_2 \cdot D^{r-1} \leq \deg\, V_1 \cdot D^r.$$

□

1.2. Polinomios absolutamente irreducibles

Definición 1.14. Sea $\mathbb{K}$ un cuerpo arbitrario. Un polinomio $f \in \mathbb{K}[X_1, \ldots, X_n]$ se dice **absolutamente irreducible** si es irreducible como polinomio en $\overline{\mathbb{K}}[X_1, \ldots, X_n]$.

Ejemplo 1.15. El polinomio $f(X, Y) = X^2 - 2Y^2 \in \mathbb{F}_5[X, Y]$ es irreducible en $\mathbb{F}_5[X, Y]$, pero visto en $\mathbb{F}_5(\sqrt{2})[X, Y]$ no lo es ya que admite la factorización $g(X, Y) = (X - \sqrt{2}Y) \cdot (X + \sqrt{2}Y)$. Notemos que $\mathbb{F}_5(\sqrt{2})$ es el cuerpo finito de 25 elementos $\mathbb{F}_{25}$.

Presentamos a continuación un criterio de absoluta irreducibilidad para polinomios $f \in \mathbb{K}[X, Y]$ de la forma:

$$f(X, Y) = a_0 Y^n + a_1(X) Y^{n-1} + \cdots + a_n(X), \tag{1.1}$$

siendo $\mathbb{K}$ un cuerpo arbitrario, $a_i \in \mathbb{K}[X]$ para $i \in \{1, \ldots, n\}$ y $a_0 \in \mathbb{K}$ no nulo. Para polinomios con estas características definimos la función:

$$\varphi(f) = \max_{1 \leq i \leq n} \left\{ \frac{\deg a_i}{i} \right\}.$$

Lema 1.16. *Sea $f \in \mathbb{K}[X,Y]$ un polinomio como en (1.1). Si existen polinomios no constantes g,h $\in \mathbb{K}[X,Y]$ tales que $f(X,Y) = g(X,Y) \cdot h(X,Y)$ (i.e., f no es irreducible) entonces se verifica que*

$$\varphi(f) = \max\{\varphi(g), \varphi(h)\}.$$

Demostración. En primer lugar observemos que los polinomios g y h son de la forma (1.1). Escribimos entonces

$$\begin{aligned} g(X,Y) = &\quad b_0 Y^r + b_1(X)Y^{r-1} + \cdots + b_r(X) \\ h(X,Y) = &\quad c_0 Y^s + c_1(X)Y^{s-1} + \cdots + c_s(X) \end{aligned}$$

donde $b_j \in \mathbb{K}[X]$, $c_k \in \mathbb{K}[X]$ y c_0 y b_0 son constantes no nulas en $\mathbb{K}$. Es claro que $r+s = n$ y que $r, s < n$. Observemos luego que para todo $i \in \{1, \ldots, n\}$ se verifica la siguiente igualdad:

$$a_i(X) = \sum_{j+k=i} b_j(X) \cdot c_k(X). \tag{1.2}$$

Por definición de la función φ se tiene

$$\begin{aligned} \deg(c_k(X) \cdot b_j(X)) &\leq j\varphi(g) + k\varphi(h) \\ &\leq (j+k) \cdot \max\{\varphi(g), \varphi(h)\}, \end{aligned}$$

luego por (1.2) concluimos que

$$\deg a_i(X) \leq i \cdot \max\{\varphi(g), \varphi(h)\},$$

por lo tanto

$$\varphi(f) \leq \max\{\varphi(g), \varphi(h)\}.$$

Probaremos a continuación la otra desigualdad. Notamos $\varphi(f) = \varphi$; luego

$$f(X, Y^\varphi) = g(X, Y^\varphi) \cdot h(X, Y^\varphi). \tag{1.3}$$

Observemos que la igualdad anterior tiene sentido a pesar de que $\varphi \in \mathbb{Q}$ y podría entonces no ser un entero positivo. Afirmamos que el grado total de $f(X, Y^\varphi)$ es $n\varphi$. Esto se debe a que

$$f(X, Y^\varphi) = a_0 Y^{n\varphi} + a_1(X)Y^{(n-1)\varphi} + \cdots + a_n(X),$$

y al hecho de que para todo $1 \leq i \leq n$ se verifica

$$\begin{aligned} \deg(a_i(X)Y^{(n-i)\varphi}) &= \deg a_i(X) + (n-i)\varphi \\ &\leq i\varphi + (n-i)\varphi = n\varphi. \end{aligned}$$

Por otra parte, dado que $\deg g(X, Y^\varphi) \geq r\varphi$ y $\deg h(X, Y^\varphi) \geq s\varphi$ obtenemos

$$\deg(g(X, Y^\varphi) \cdot h(X, Y^\varphi)) \geq r\varphi + s\varphi = n\varphi,$$

luego como $\deg f(X, Y^\varphi) = n\varphi$, la igualdad (1.3) implica que

$$\deg g(X, Y^\varphi) = r\varphi \quad \text{y} \quad \deg h(X, Y^\varphi) = s\varphi.$$

De la expresión

$$g(X, Y) = a_0 Y^{r\varphi} + a_1(X)Y^{(r-1)\varphi} + \cdots + a_r(X),$$

y de la igualdad $\deg g(X, Y^\varphi) = r\varphi$, deducimos

$$\deg(b_j(X)Y^{(r-j)\varphi}) = \deg b_j(X) + (r-j)\varphi \leq r\varphi.$$

Por lo tanto probamos que para todo $j \in \{1, \ldots, r\}$ se verifica que $\deg b_j(X) \leq j\varphi$, y luego $\varphi(g) \leq \varphi$. Análogamente se demuestra que $\varphi(h) \leq \varphi$, y así se obtiene la desigualdad

$$\varphi(f) \geq \text{máx}\left\{\varphi(g), \varphi(h)\right\},$$

lo que concluye la demostración. □

Teorema 1.17. *Sea $f \in \mathbb{K}[X, Y]$ un polinomio de la forma dada en (1.1). Supongamos que el grado de a_n es m, que los enteros m y n son coprimos y además se verifica*

$$\frac{m}{n} > \frac{\deg a_i}{i},$$

para todo $i \in \{1, \ldots, n-1\}$. Entonces f es absolutamente irreducible.

Demostración. Supongamos que existen g,$h \in \overline{\mathbb{K}}[X, Y]$ tales que

$$f(X, Y) = g(X, Y) \cdot h(X, Y).$$

Con las notaciones dadas anteriormente, tenemos

$$\varphi(g) = \frac{\alpha}{\beta} \quad \text{y} \quad \varphi(h) = \frac{\gamma}{\delta},$$

siendo α, β, γ, δ números naturales y además $\beta \leq r < n$ y $\delta \leq s < n$. Por hipótesis sabemos que $\varphi(f) = \frac{m}{n}$. Por otra parte como m y n son coprimos y β y δ son menores a n, deducimos que

$$\frac{m}{n} \neq \text{máx}\left\{\frac{\alpha}{\beta}, \frac{\gamma}{\delta}\right\},$$

obteniendo de esta forma

$$\varphi(f) \neq \text{máx}\left\{\varphi(g), \varphi(h)\right\},$$

lo que contradice el lema anterior. Luego f es absolutamente irreducible. □

Ejemplo 1.18. Sea el polinomio $f(X, Y) = 2Y^3 - XY^2 + 4Y^2 + YX^2 + 3XY + Y + X^5 \in \mathbb{Q}[X, Y]$. Notemos que f se puede escribir como: $f(X, Y) = 2Y^3 + (-X + 4)Y^2 + (X^2 + 3X + 1)Y + X^5 \in \mathbb{Q}[X, Y]$. Luego $\deg a_3 = 5$ que es coprimo con $n = 3$. Por otro lado se tiene que $\frac{5}{3} > \frac{\deg a_i}{i}$ para $i = 1, 2$. Por lo tanto f es absolutamente irreducible.

Finalizamos esta seccion con el **Criterio de absoluta irreducibilidad de Stepanov**. Seguimos la demostración del libro [LN83].

Teorema 1.19. *Sea $\mathbb{K}$ un cuerpo arbitrario, $f \in \mathbb{K}[X]$ un polinomio no constante, y $m \in \mathbb{N}$. Supongamos que f se factoriza en $\overline{\mathbb{K}}$ como*

$$f(X) = a(X - \alpha_1)^{e_1} \cdots (X - \alpha_d)^{e_d},$$

con $\alpha_i \neq \alpha_j$ si $i \neq j$. Entonces el polinomio $Y^m - f(X)$ es absolutamente irreducible si y solo si $\gcd(m, e_1, \ldots, e_d) = 1$.

Demostración. Vamos a probar que $Y^m - f(X)$ no es absolutamente irreducible si y solo si $\gcd(m, e_1, \ldots, e_d) > 1$. Supongamos que $Y^m - f(X)$ es reducible sobre alguna extensión algebraica L de $\mathbb{K}$. Consideremos el polinomio $Y^m - 1$. Podemos asumir que este se factoriza como producto de polinomios de grado uno sobre L. Escribamos entonces

$$Y^m - 1 = (Y - \xi_1) \cdots (Y - \xi_m)$$

con $\xi_i \in L$. Como $Y^m - f(X)$ es reducible sobre L existen entonces polinomios F,$G \in L[X, Y]$ de grados positivos, tales que

$$Y^m - f(X) = r(X, Y) \cdot s(X, Y).$$

Consideramos a $Y^m - f(X)$ como un polinomio en Y con coeficientes en $L(X)$, luego este se factoriza como producto de polinomios de grado uno sobre la clausura algebraica de $L(X)$, escribimos entonces

$$Y^m - f(X) = (Y - \beta_1) \cdots (Y - \beta_m), \tag{1.4}$$

donde $\beta_1, \ldots, \beta_m \in \overline{L(X)}$. Sea $\theta \in \overline{L(X)}$ una solución de la ecuación $Y^m = f(X)$. Luego se verifica

$$\theta^m = f(X). \tag{1.5}$$

Notemos que (1.4) se puede factorizar de la siguiente manera

$$Y^m - f(X) = (Y - \xi_1\theta) \cdots (Y - \xi_m\theta).$$

Por unicidad de la factorización obtenemos

$$r(X, Y) = b(Y - \xi_{j_1}\theta) \cdots (Y - \xi_{j_n}\theta), \tag{1.6}$$

para $j_1, \ldots, j_n \in \{1, \ldots, m\}$, con $b \in L$ no nulo y $1 \leq n < m$. Comparando ambos lados de la igualdad (1.6) deducimos que

$$(-1)^n b \xi_{j_1} \cdots \xi_{j_n} \theta^n \in L[X],$$

y, por lo tanto, que $\theta^n \in L[X]$. Consideramos ℓ el menor entero positivo tal que $\theta^\ell \in L(X)$. Luego $\ell \leq n < m$, y para cada natural u tal que $\theta^u \in L(X)$ se tiene que u es múltiplo

de ℓ. En particular, resulta que ℓ divide a m. Notamos $t = \frac{m}{\ell}$, luego $t > 1$ y $\theta^\ell = \frac{g}{h}$ con g, $h \in L[X]$, coprimos y h no nulo. De acuerdo a esta notación y a la igualdad (1.5), se verifica la siguiente identidad:

$$f \cdot h^t = g^t \tag{1.7}$$

Si comparamos en ambos lados de la igualdad (1.7) las multiplicidades de las raíces α_i, $1 \leq i \leq d$, deducimos que t divide a cada e_i y luego t divide a $\gcd(m, e_1, \ldots, e_d)$, lo que implica que $\gcd(m, e_1, \ldots, e_d) > 1$.

Recíprocamente, supongamos que $e = \gcd(m, e_1, \ldots, e_d)$ y que $e > 1$. Sabemos que f se factoriza en $\overline{\mathbb{K}}$ como

$$f(X) = a(X - \alpha_1)^{e_1} \cdots (X - \alpha_d)^{e_d}.$$

Consideramos un elemento $\delta \in \overline{\mathbb{K}}$ tal que $\delta^e = a$ y sea el polinomio

$$g(X) = \delta(X - \alpha_1)^{\frac{e_1}{e}} \cdots (X - \alpha_d)^{\frac{e_d}{e}}.$$

Entonces tomando $s = \frac{m}{e}$, obtenemos

$$\begin{aligned} Y^m - f(X) &= (Y^s)^e - g(X)^e \\ &= (Y^s - g(X))(Y^{(e-1)s} + Y^{(e-2)s} g(X) + \cdots + g(X)^{e-1}), \end{aligned}$$

y por lo tanto $Y^m - f(X)$ no es absolutamente irreducible. □

Ejemplo 1.20. Sea el polinomio $f(X, Y) = Y^5 + X^2 + 1 \in \mathbb{F}_2[X, Y]$. Como los grados de X e Y son coprimos entonces aplicando el criterio de Stepanov, f es absolutamente irreducible.

Ejemplo 1.21. Sea $f(Z_1, \ldots, Z_n, Y) = Y^d + Z_1^{d-1} Y - Z_2^{d-1} - 1 \in \mathbb{C}[Z_1, \ldots, Z_n, Y]$, con $n \geq 2$. Utilizando el criterio de Stepanov probaremos que f es absolutamente irreducible. Consideremos el polinomio $g(Z_2, Y) = f(0, Z_2, 0, \ldots, 0, Y)$, es decir, $g(Z_2, Y) = Y^d - Z_2^{d-1} - 1$. Luego g es un polinomio de grado d. Dado que d y $d - 1$ son coprimos, por el criterio de Stepanov, g resulta absolutamente irreducible. Como f y g tienen el mismo grado esto implica que f es absolutamente irreducible.

1.3. Levantamiento de Hensel

En esta tesina estudiaremos un algoritmo de factorización de polinomios que se basa en un método llamado **levantamiento de Hensel**. En lineas generales, la idea es la siguiente: dado un polinomio f y una factorización de él módulo un ideal I, el levantamiento de Hensel permite obtener factorizaciones de f módulo I^{2^k}, para un k positivo arbitrario. Describiremos a continuación dicho método siguiendo el libro [vzGG99].

Lema 1.22 (Lema de Hensel)**.** *Sean R un anillo conmutativo con unidad, $I \subset R$ un ideal y f un elemento de R. Supongamos que existen $g, h \in R$ tales que*

1. $sg + th \equiv 1 \quad (I)$ *con* $s, t \in R$

2. $f \equiv gh \quad (I)$.

Entonces existen $g^*, h^* \in R$ *que verifican*

1. $f \equiv g^* h^* \quad (I^2)$

2. $g^* \equiv g \quad (I)$

3. $h^* \equiv h \quad (I)$

4. $s^* g^* + t^* h^* \equiv 1 \quad (I^2)$ *con* $s^*, t^* \in R$.

Además g^* *y* h^* *son únicos en el siguiente sentido: si existen* $g' \equiv g \quad (I)$ *y* $h' \equiv h \quad (I)$ *tales que* $f \equiv g' \cdot h' \quad (I^2)$ *entonces se verifica* $g' \equiv g^*(1+u) \quad (I^2)$ *y* $h' \equiv h^*(1-u)\,(I^2)$, *para algún* $u \in I$.

Demostración. Consideramos $m := f - gh$. Luego, como $f \equiv gh \quad (I)$ se tiene que $m \in I$. Definimos $g^* := g + tm$ y $h^* := h + sm$. Dado que $m \in I$, se verifica que $g^* \equiv g\,(I)$ y $h^* \equiv h \quad (I)$. Veamos entonces que $f \equiv g^* h^* \quad (I^2)$. En efecto,

$$\begin{aligned} f - g^* h^* &= f - (g + tm) \cdot (h + sm) \\ &= f - gh - m(sg + th) - stm^2 \\ &= m(1 - (sg + th)) - stm^2 \\ &\equiv 0 \quad (I^2), \end{aligned}$$

pues $m \in I$ y $sg + th \equiv 1 \quad (I)$. Probemos que $s^* g^* + t^* h^* \equiv 1 \quad (I^2)$ con $s^*, t^* \in R$. Para ello consideramos $q = sg^* + th^* - 1$, como $sg^* + th^* \equiv sg + th\,(I)$, se verifica que $q \in I$. Definimos luego $s^* = s - sq$ y $t^* = t - tq$. Verifiquemos que $s^* g^* + t^* h^* \equiv 1 \quad (I^2)$.

$$\begin{aligned} s^* g^* + t^* h^* - 1 &= sg^* - sqg^* + th^* - tqh^* - 1 \\ &= sg^* + th^* - 1 - q(sg^* + th^*) \\ &= q(1 - (sg^* + th^*)) \\ &= -q^2 \\ &\equiv 0 \quad (I^2). \end{aligned}$$

Finalmente veamos la unicidad. Sean $m_1 := g' - g^*$ y $m_2 := h' - h^*$. Se tiene que $m_1 \in I$ pues g' y g^* son congruentes módulo I. Análogamente tenemos $m_2 \in I$. Tomamos $u := m_1 s^* - m_2 t^*$, de donde $u \in I$. Por hipótesis $f \equiv g'h' \equiv g^* h^*\,(I^2)$. Por lo tanto podemos

escribir

$$\begin{aligned}(g^* + m_1) \cdot (h^* + m_2) &\equiv g^* h^* \quad (I^2) \\ m_1 h^* + m_2 g^* &\equiv 0 \quad (I^2) \\ m_2 g^* &\equiv -m_1 h^* \quad (I^2) \\ s^* m_2 g^* &\equiv -s^* m_1 h^* \quad (I^2) \\ m_2(1 - t^* h^*) &\equiv -s^* m_1 h^* \quad (I^2) \\ m_2 &\equiv h^*(-u) \quad (I^2) \\ h' &\equiv h^*(1-u) \quad (I^2).\end{aligned}$$

De manera similar se prueba $g' \equiv g^*(1+u) \quad (I^2)$. □

Ejemplo 1.23. Consideramos el polinomio $f(X,Y) = X^2 + X + Y^2 \in \mathbb{R}[X,Y]$ y el polinomio univariado $f(X,0) = X^2 + X = X(X+1)$. Podemos pensar que esta es una factorización de f módulo (Y). Es decir

$$f(X,Y) \equiv X(X+1) \quad (Y).$$

Encontremos una factorización módulo (Y^2). Sean $g_0 = X$, $s_0 = -1$, $h_0 = X+1$ y $t_0 = 1$. Entonces se verifica

$$s_0 g_0 + t_0 h_0 \equiv 1 \quad (Y).$$

Calculamos $m_0 = f - g_0 h_0 = Y^2 \equiv 0 \quad (Y^2)$. Luego,

$$g_1 = g_0 + t_0 m_0 = X$$

$$h_1 = h_0 + s_0 m_0 = X + 1,$$

con lo cual

$$f(X,Y) \equiv X(X+1) \quad (Y^2).$$

Continuando, $m_1 = f - g_1 h_1 \equiv Y^2 \, (Y^4)$, $g_2 = X + Y^2$, $h_2 = X + 1 - Y^2$, obteniendo así una factorización módulo (Y^4)

$$f(X,Y) \equiv (X + Y^2)(X + 1 - Y^2) \quad (Y^4).$$

Capítulo 2

Algoritmos de factorización y una versión del Teorema de Bertini

Mediante algoritmos de factorización para polinomios multivariados se pueden obtener diferentes versiones del Teorema de Bertini. En este capítulo estudiaremos el algoritmo desarrollado por G. Lecerf [Lec06] para polinomios bivariados y su generalización a n variables [Lec07]. Finalmente exhibiremos la actualmente mejor versión del teorema de Bertini, obtenida a partir de dicho algoritmo.

2.1. Algoritmo de factorización para polinomios bivariados

Sea $\mathbb{K}$ un cuerpo y sea $f \in \mathbb{K}[X,Y]$ un polinomio de grado d. Estudiaremos un algoritmo que nos permitirá encontrar los factores racionales irreducibles de f, es decir, $f_1, \ldots, f_r \in \mathbb{K}[X,Y]$. El algoritmo que describiremos en esta sección es el desarrollado por G. Lecerf en [Lec06]. Muchos algoritmos de factorización se pueden dividir a grandes rasgos en tres pasos. En primer lugar se especializa una de las variables y se factoriza el polinomio univariado obtenido. A partir de esta factorización y utilizando el levantamiento de Hensel encontramos $\mathsf{f}_1, \ldots, \mathsf{f}_s \in \mathbb{K}[[X]][Y]$, los factores analíticos de f con un cierto orden de precisión. Finalmente los factores racionales se obtienen recombinando los analíticos. La etapa de recombinación presentaba la dificultad de exigir una cantidad exponencial de combinaciones. G.Lecerf reduce este problema al de resolver un sistema de ecuaciones lineales. Su trabajo combina el levantamiento de Hensel con las ideas de W. Ruppert [Rup99] y S.Gao [Gao03]. En 1999 Ruppert exhibe un resultado en el cual vincula la absoluta irreducibilidad de un polinomio con la existencia de soluciones no nulas de una cierta ecuación diferencial. A continuación enunciamos dicho resultado.

Teorema 2.1. *[Rup99] Sea $\mathbb{K}$ un cuerpo de característica cero y sea $f \in \mathbb{K}[X,Y]$ un polinomio de grado m en la variable X y grado n en la variable Y. Entonces f es absolutamente irreducible si y solo si no existen polinomios no nulos $g, h \in \overline{\mathbb{K}}[X,Y]$ con $\deg_X h \leq m-1$, $\deg_Y h \leq n$, $\deg_X g \leq m$ y $\deg_Y g \leq n-2$ que verifiquen la siguiente ecuación diferencial*

$$\frac{\partial}{\partial X}\left(\frac{g}{f}\right) = \frac{\partial}{\partial Y}\left(\frac{h}{f}\right). \tag{2.1}$$

En un cuerpo de característica positiva se verifica que si f es un polinomio reducible, de grado m en la variable X y grado n en la variable Y, entonces existen polinomios no nulos $g, h \in \overline{\mathbb{K}}[X, Y]$ con $\deg_X h \leq m-1$, $\deg_Y h \leq n$, $\deg_X g \leq m$ y $\deg_Y g \leq n-2$ que son soluciones de la ecuación diferencial (2.1).

Notemos que la ecuación (2.1) puede reescribirse de la siguiente manera

$$g\frac{\partial f}{\partial X} - f\frac{\partial g}{\partial X} = h\frac{\partial f}{\partial Y} - f\frac{\partial h}{\partial Y}. \tag{2.2}$$

Esta ecuación diferencial da lugar a un sistema de ecuaciones lineales cuyas incógnitas son los coeficientes de g y h. Gao [Gao03] toma estas ideas y muestra que la dimensión del espacio de soluciones del sistema en $\mathbb{K}$ y $\overline{\mathbb{K}}$ coincide con la cantidad de factores irreducibles sobre $\mathbb{K}$ y $\overline{\mathbb{K}}$, respectivamente. Además hallando una base del mismo se tiene una factorización de f.

Observación 2.2. Damos algunas notaciones que utilizaremos a lo largo del capítulo. El espacio vectorial de los polinomios de grado a lo sumo m lo notamos como $\mathbb{K}[X, Y]_m$. El cuerpo de fracciones de $\mathbb{K}[X]$ es $\mathbb{K}(X)$. El álgebra de series de potencias sobre $\mathbb{K}$ la notamos como $\mathbb{K}[[X]]$ y $\mathbb{K}((X))$ es su respectivo cuerpo de fracciones.

Vamos a trabajar bajo la siguiente hipótesis:

$$\text{Hipótesis } (\mathbf{S}) \begin{cases} (i) \quad \deg_Y(f) = \deg(f) = d \\ \\ (ii) \quad \operatorname{Res}_Y(f(0,Y), \dfrac{\partial f}{\partial Y}(0,Y)) \neq 0 \end{cases}$$

Observación 2.3. Notemos que la condición (i) de la hipótesis $(\mathbf{S})$ implica que f es mónico en Y, por lo tanto sus factores racionales y analíticos son mónicos en Y. Es claro que $r, s \geq 1$ y que $s \geq r$ debido a que $\mathbb{K}[X, Y] \subset \mathbb{K}[[X, Y]]$.

Por otra parte la condición (ii) implica que $d \geq 1$ y que $f(0, Y)$ es separable sobre $\mathbb{K}$. Luego los factores analíticos $\mathsf{f}_1, \ldots, \mathsf{f}_s$ son distintos entre sí ya que estos se obtienen a partir de los factores de $f(0, Y)$.

Recombinando los factores analíticos de f se obtienen sus factores racionales. Es decir se verifica la siguiente igualdad

$$f_i = \prod_{j=1}^{s} \mathsf{f}_j^{\mu_{ij}}$$

para $\mu_i = (\mu_{i1}, \ldots, \mu_{is}) \in \{0, 1\}^s$ para $i \in \{1, \ldots, r\}$, además tenemos que $\mu_1 + \cdots + \mu_r = (1, \ldots, 1)$. En consecuencia, podemos suponer que los vectores $\mu_1, \ldots, \mu_r$ son ortogonales dos a dos con el producto escalar canónico y forman una base escalonada reducida. El método de recombinación de Lecerf consiste en resolver un sistema de ecuaciones lineales que nos proporciona los valores de los μ_i para $i \in \{1, \ldots .r\}$.

Lema 2.4. *Sea $f \in \mathbb{K}[X_1, \ldots, X_n]$ un polinomio libre de cuadrados, de grado d. Supongamos que la característica de $\mathbb{K}$ es cero o mayor o igual a $d(d-1)+1$. Entonces a través de un cambio lineal de coordenadas se puede recuperar la hipótesis ($\mathbf{S}$).*

Demostración. Veamos que podemos obtener la condición (i). Sea f_d la componente homogénea de mayor grado de f y supongamos que Y tiene grado positivo en f_d. Por lo tanto

$$f_d = \sum_{j_1+j_2=d} a_{j_1 j_2} X^{j_1} Y^{j_2}.$$

Hacemos el siguiente cambio de variables:

$$X = Y_1 + \beta Y_2 \quad , \quad Y = Y_2,$$

con $\beta \in \mathbb{K}$. Se obtiene que el coeficiente de Y_2^d en $f(Y_1 + \beta Y_2, Y_2)$ es

$$\sum_{j_1 \,:\, j_1+j_2=d} a_{j_1 j_2} \beta^{j_1}. \tag{2.3}$$

Por lo tanto si podemos elegir β tal (2.3) sea no nulo, resultará que f es mónico en Y, y el grado en dicha variable es d. En cuerpos de característica cero es siempre posible encontrar tal β, en cuerpos de característica positiva nos alcanza con que la cantidad de elementos del cuerpo sea mayor al grado del polinomio. Notemos que la condición (i) se puede obtener independientemente de que el polinomio sea libre de cuadrados.

Veamos como obtener la condición (ii). Recordemos que la caraterística del cuerpo es cero o mayor o igual a $d(d-1)+1$. Como f es libre de cuadrados entonces podemos asumir que $\gcd(f, \frac{\partial f}{\partial Y}) = 1$. En particular, por la condición de la característica, se tiene que $\frac{\partial f}{\partial Y} \neq 0$. Luego si $\mathcal{D}(X)$ es el discriminante con respecto a la variable Y entre f y $\frac{\partial f}{\partial Y}$, entonces $\mathcal{D}$ es un polinomio no nulo de grado a lo sumo $d(d-1)$, por lo tanto existe $\gamma \in \mathbb{K}$ tal que $\mathcal{D}(\gamma) \neq 0$. Haciendo el siguiente cambio lineal de variables

$$X = Y_1 + \gamma \quad , \quad Y = Y_2,$$

se tiene que f cumple la condición (ii). □

Observación 2.5. Definimos los siguientes polinomios:

$$\widehat{f_i} := \prod_{j \neq i} f_j \qquad \widehat{\mathsf{f}_k} := \prod_{j \neq k} \mathsf{f}_j$$

para $i \in \{1, \ldots, r\}$ y $k \in \{1, \ldots, s\}$.

Observación 2.6. Supongamos que conocemos los vectores $\mu_1, \ldots, \mu_r$. Para cada $i \in \{1, \ldots, r\}$, derivamos ambos lados de $f_i = \prod_{j=1}^{s} \mathsf{f}_j^{\mu_{ij}}$ respecto de la variable Y, obteniendo

$$\frac{\partial f_i}{\partial Y} = \sum_{j=1}^{s} \mu_{ij} \frac{\partial \mathsf{f}_j}{\partial Y} \prod_{k \neq j}^{s} \mathsf{f}_k^{\mu_{ik}}. \tag{2.4}$$

Observemos que $\widehat{f_i}$ se puede escribir como

$$\widehat{f_i} = \prod_{k=1}^{s} \mathsf{f}_k^{1-\mu_{ik}},$$

y entonces multiplicando ambos lados de (2.4) por $\widehat{f_i}$ se tiene

$$\widehat{f_i}\frac{\partial f_i}{\partial Y} = \sum_{j=1}^{s} \mu_{ij}\widehat{\mathsf{f}}_j \frac{\partial \mathsf{f}_j}{\partial Y}.$$

Análogamente obtenemos

$$\widehat{f_i}\frac{\partial f_i}{\partial X} = \sum_{j=1}^{s} \mu_{ij}\widehat{\mathsf{f}}_j \frac{\partial \mathsf{f}_j}{\partial X}.$$

Por otro lado como $\dfrac{\partial f_i}{\partial X}$ y $\dfrac{\partial f_i}{\partial Y}$ tienen grado a lo sumo $\deg f_i - 1$ y el grado de $\widehat{f_i}$ es $d - \deg f_i$, se verifica que $\widehat{f_i}\dfrac{\partial f_i}{\partial X}$ y $\widehat{f_i}\dfrac{\partial f_i}{\partial Y}$ tienen grados a lo sumo $d-1$. Si consideramos σ un entero positivo y definimos los polinomios

$$g(X,Y) = \widehat{f_i}\frac{\partial f_i}{\partial Y} \quad \text{y} \quad h(X,Y) = \widehat{f_i}\frac{\partial f_i}{\partial X},$$

se verifica entonces que

$$g - \sum_{j=1}^{s} \mu_{ij}\widehat{\mathsf{f}}_j \frac{\partial \mathsf{f}_j}{\partial Y} \in (X,Y)^{\sigma},$$

$$h - \sum_{j=1}^{s} \mu_{ij}\widehat{\mathsf{f}}_j \frac{\partial \mathsf{f}_j}{\partial X} \in (X,Y)^{\sigma} + (X^{\sigma-1}).$$

Posteriormente veremos que g y h definidos como en la observación anterior, son soluciones de la ecuación (2.1) para un cierto valor de σ. Luego estamos encontrando expresiones para dichas soluciones en términos de los factores analíticos de f. Esta es la idea principal del algoritmo de Lecerf. Motivados por lo dicho anteriormente, consideramos la siguiente familia de espacios vectoriales.

Definición 2.7. Para cada $\sigma \geq 1$ definimos la siguiente familia de espacios vectoriales:

$$L_\sigma := \{((\ell_1,\ldots,\ell_s), g, h) \in \mathbb{K}^s \times \mathbb{K}[X,Y]_{d-1} \times \mathbb{K}[X,Y]_{d-1} \ \mid$$

$$g - \sum_{j=1}^{s} \ell_j\widehat{\mathsf{f}}_j \frac{\partial \mathsf{f}_j}{\partial Y} \in (X,Y)^{\sigma},$$

$$h - \sum_{j=1}^{s} \ell_j\widehat{\mathsf{f}}_j \frac{\partial \mathsf{f}_j}{\partial X} \in (X,Y)^{\sigma} + (X^{\sigma-1})\},$$

con $(X,Y)^\sigma, (X,Y)^\sigma + (X^{\sigma-1}) \subset \mathbb{K}[[X]][Y]$.

Sea Π la proyección canónica de L_σ en $\mathbb{K}^s$. Vamos a probar que si tomamos $\sigma \geq 2d$ entonces

$$\Pi(L_\sigma) =< \mu_1, \ldots, \mu_r >$$

y como estos son linealmente independientes luego forman una base de $\Pi(L_\sigma)$. Por lo tanto la dimensión del subespacio $\Pi(L_\sigma)$ nos proporciona la cantidad de factores irreducibles de f en $\mathbb{K}[X,Y]$. En la Observación 2.6 hemos demostrado el siguiente Lema:

Lema 2.8. *Con las notaciones y definiciones anteriores y bajo la hipótesis (**S**) se verifica que para cada $\sigma \geq 1$*

$$< \mu_1, \ldots, \mu_r > \subset \Pi(L_\sigma).$$

Demostración. Mostramos que

$$\left(\mu_i, \widehat{f}_i \frac{\partial f_i}{\partial Y}, \widehat{f}_i \frac{\partial f_i}{\partial X}\right) \in L_\sigma,$$

luego $\mu_i \in \Pi(L_\sigma)$. □

Notación Llamamos hipótesis (**C**) a la siguiente condición sobre la característica de $\mathbb{K}$:

$$\text{Hipótesis (}\mathbf{C}\text{)}: \quad \operatorname{car}\mathbb{K} = 0 \quad \text{ó} \quad \operatorname{car}\mathbb{K} \geq d(d-1)+1.$$

A continuación, veremos un Lema que nos permitirá probar que los vectores $\mu_1, \ldots, \mu_r$ forman una base del subespacio $\Pi(L_\sigma)$. Concretamente este Lema muestra que ser solución de la ecuación (2.1) implica que la derivada del residuo de $\frac{g}{f}$ en ϕ con $f(X,\phi) = 0$ es nula.

Lema 2.9. *Supongamos que se verifica la hipótesis (**S**) y sean $g, h \in \overline{\mathbb{K}}[X,Y]_{d-1}$ que verifican la ecuación (2.2). Sea $\phi \in \overline{\mathbb{K}}[[X]]$ tal que $f(X,\phi) = 0$, entonces:*

1. $\dfrac{d}{dX}\left(\dfrac{g(X,\phi)}{\dfrac{\partial f}{\partial Y}(X,\phi)}\right) = 0.$

2. *Si se cumple la hipótesis (**C**) entonces* $\dfrac{g(X,\phi)}{\dfrac{\partial f}{\partial Y}(X,\phi)} \in \overline{\mathbb{K}}.$

Demostración. De acuerdo con la hipótesis (**S**) el polinomio $f(0,Y)$ es separable sobre $\mathbb{K}$, luego $f(0,Y) = \prod_{i=1}^{d}(Y - a_i) \in \overline{\mathbb{K}}[Y]$ con $a_i \neq a_j$ si $i \neq j$. Aplicando el método de aproximación de Newton asociamos a cada a_i la serie de potencias $\phi_i \in \overline{\mathbb{K}}[[X]]$ tal que

$$f(X,\phi_i) = 0, \quad \phi_i(0) = a_i \quad \text{y} \quad \phi_i \neq \phi_j.$$

Podemos escribir entonces $f = \prod_{i=1}^{d}(Y-\phi_i) \in \overline{\mathbb{K}}[[X]][Y]$ y definir la partición $(S_i)_{i\in\{1,\dots,s\}}$ de $\{1,\dots,d\}$ satisfaciendo $\mathsf{f}_i = \prod_{j\in S_i}(Y-\phi_j)$. Observemos que el grado en la variable Y de g y h es menor o igual a $d-1$, mientras que el grado en Y de f es exactamente d; podemos desarrollar $\frac{g}{f}$ y $\frac{h}{f}$ en fracciones simples obteniendo:

$$\frac{g}{f} = \sum_{j=1}^{d} \frac{g_j}{Y-\phi_j} \quad , \quad \frac{h}{f} = \sum_{j=1}^{d} \frac{h_j}{Y-\phi_j} \tag{2.5}$$

con

$$g_j = \frac{g(X,\phi_j)}{\frac{\partial f}{\partial Y}(X,\phi_j)} \quad , \quad h_j = \frac{h(X,\phi_j)}{\frac{\partial f}{\partial Y}(X,\phi_j)}.$$

De la hipótsis (**S**) se deduce que $\dfrac{\partial f}{\partial Y}(X,\phi_j)$ es un elemento inversible de $\overline{\mathbb{K}}[[X]]$ y, por lo tanto, $g_j, h_j \in \overline{\mathbb{K}}[[X]]$ para cada $j \in \{1,\dots,d\}$, de esta forma concluimos que las igualdades de (2.5) vale en $\overline{\mathbb{K}}((X))(Y)$.

Derivando $\dfrac{g}{f}$ con respecto de X y $\dfrac{h}{f}$ con respecto a Y obtenemos

$$\begin{aligned} \frac{\partial}{\partial X}\left(\frac{g}{f}\right) &= \sum_{j=1}^{d}\left(\frac{g_j}{(Y-\phi_j)^2}\frac{d\phi_j}{dX} + \frac{1}{Y-\phi_j}\frac{dg_j}{dX}\right) \\ \frac{\partial}{\partial Y}\left(\frac{h}{f}\right) &= -\sum_{j=1}^{d}\frac{h_j}{(Y-\phi_j)^2}. \end{aligned}$$

Luego de la identidad (2.2) y por la unicidad en la descomposición en fracciones simples, deducimos

$$\frac{dg_j}{dX} = 0 \quad \forall j \in \{1,\dots,d\}.$$

De esta manera queda demostrada la primera afirmación del Lema.

Si $\operatorname{car}\mathbb{K} = 0$ se verifica que $g_j = g_j(0) \in \overline{\mathbb{K}}$ debido a que $\frac{dg_j}{dX} = 0$. Supongamos que $\operatorname{car}\mathbb{K} = p$. En este caso $\frac{dg_j}{dX} = 0$ implica que $g_j = g_j(0) + \mathcal{O}(X^p)$. Sea factor irreducible de f, $\overline{f}_i \in \overline{\mathbb{K}}[X,Y]$, tal que $\overline{f}_i(X,\phi_j)$. Consideramos la siguiente resultante

$$\Gamma(X) := \operatorname{Res}_Y\left(\overline{f}_i(X,Y), g(X,Y) - g_j(0)\frac{\partial f}{\partial Y}\right).$$

Se tiene que $\Gamma(X)$ es un polinomio de grado a lo sumo $(d-1)\cdot\deg\overline{f}_i \le d(d-1)$. Por otro lado se verifica que

$$\Gamma(X) = \prod_{\phi_l \mid f_i(X,\phi_l)=0}\left(g(X,\phi_l) - g_j(0)\frac{\partial f}{\partial Y}(X,\phi_l))\right)$$

Como $g(X,\phi_j) - g_j(0)\frac{\partial f}{\partial Y}(X,\phi_j) = \mathcal{O}(X^p)$ y como la característica de $\mathbb{K}$ es mayor a $d(d-1)$

necesariamente $\Gamma(X)$ debe ser el polinomio nulo. Por lo tanto, como $\overline{f}_i$ es irreducible se verifica que $\overline{f}_i$ divide a $g(X,Y) - g_j(0)\frac{\partial f}{\partial Y}$ con lo cual $g(X,\phi_j) - g_j(0)\frac{\partial f}{\partial Y}(X,\phi_j) = 0$. Deducimos finalmente que $g_j = g_j(0)$. □

A continuación demostraremos el teorema principal de esta sección. A partir de dicho teorema podremos obtener la recombinación.

Teorema 2.10. *Bajo las hipótesis (**S**) y (**C**), y considerando $\sigma \geq 2d$ se verifica*

$$\Pi(L_\sigma) =< \mu_1, \ldots, \mu_r > .$$

Demostración. De acuerdo con el Lema 2.8 solo resta demostrar $\Pi(L_\sigma) \subset < \mu_1, \ldots, \mu_r >$. Sea $(\ell_1, \ldots, \ell_s) \in \Pi(L_\sigma)$ y $g, h \in \mathbb{K}[X,Y]_{d-1}$ tales que

$$g - \sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y} \in (X,Y)^\sigma \qquad h - \sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial X} \in (X,Y)^\sigma + (X^{\sigma-1}).$$

Derivamos la primera expresión con respecto a X, y la segunda con respecto a Y obteniendo

$$\begin{aligned} \frac{\partial g}{\partial X} - \sum_{i=1}^{s} \ell_i \left(\frac{\partial \widehat{\mathsf{f}}_i}{\partial X} \frac{\partial \mathsf{f}_i}{\partial Y} + \widehat{\mathsf{f}}_i \frac{\partial^2 \mathsf{f}_i}{\partial XY} \right) \in (X,Y)^{\sigma-1}, \\ \frac{\partial h}{\partial Y} - \sum_{i=1}^{s} \ell_i \left(\frac{\partial \widehat{\mathsf{f}}_i}{\partial Y} \frac{\partial \mathsf{f}_i}{\partial X} + \widehat{\mathsf{f}}_i \frac{\partial^2 \mathsf{f}_i}{\partial XY} \right) \in (X,Y)^{\sigma-1}. \end{aligned} \tag{2.6}$$

Si multiplicamos las expresiones de (2.6) por f, los resultados obtenidos pertenecen al ideal $(X,Y)^{\sigma-1}$. Por otro lado, notemos que

$$\frac{\partial f}{\partial X} \cdot \left(g - \sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y} \right) \in (X,Y)^\sigma,$$

$$\frac{\partial f}{\partial Y} \cdot \left(h - \sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial X} \right) \in (X,Y)^\sigma + (X^{\sigma-1}).$$

Luego, podemos deducir que

$$g \cdot \frac{\partial f}{\partial X} - f \cdot \frac{\partial g}{\partial X} - \sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}}_i \left(\frac{\partial \mathsf{f}_i}{\partial Y} \left(\frac{\partial f}{\partial X} - \mathsf{f}_i \cdot \frac{\partial \widehat{\mathsf{f}}_i}{\partial X} \right) - f \cdot \frac{\partial^2 \mathsf{f}_i}{\partial XY} \right) \in (X,Y)^{\sigma-1},$$

$$h \cdot \frac{\partial f}{\partial Y} - f \cdot \frac{\partial h}{\partial Y} - \sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}}_i \left(\frac{\partial \mathsf{f}_i}{\partial X} \left(\frac{\partial f}{\partial Y} - \mathsf{f}_i \cdot \frac{\partial \widehat{\mathsf{f}}_i}{\partial Y} \right) - f \cdot \frac{\partial^2 \mathsf{f}_i}{\partial XY} \right) \in (X,Y)^{\sigma-1}.$$

Entonces, usando

$$\frac{\partial f}{\partial X} - \mathsf{f}_i \cdot \frac{\partial \widehat{\mathsf{f}_i}}{\partial X} = \sum_{j=1}^{s} \widehat{\mathsf{f}_j} \cdot \frac{\partial \mathsf{f}_j}{\partial X} - \sum_{j=1, j\neq i}^{s} \widehat{\mathsf{f}_j} \cdot \frac{\partial \mathsf{f}_j}{\partial X} = \widehat{\mathsf{f}_i} \cdot \frac{\partial \mathsf{f}_i}{\partial X},$$

$$\frac{\partial f}{\partial Y} - \mathsf{f}_i \cdot \frac{\partial \widehat{\mathsf{f}_i}}{\partial Y} = \sum_{j=1}^{s} \widehat{\mathsf{f}_j} \cdot \frac{\partial \mathsf{f}_j}{\partial Y} - \sum_{j=1, j\neq i}^{s} \widehat{\mathsf{f}_j} \cdot \frac{\partial \mathsf{f}_j}{\partial Y} = \widehat{\mathsf{f}_i} \cdot \frac{\partial \mathsf{f}_i}{\partial Y},$$

obtenemos

$$g \cdot \frac{\partial f}{\partial X} - f \cdot \frac{\partial g}{\partial X} - \left(h \cdot \frac{\partial f}{\partial Y} - f \cdot \frac{\partial h}{\partial Y} \right) \in (X, Y)^{\sigma - 1}.$$

Como $g \cdot \dfrac{\partial f}{\partial X} - f \cdot \dfrac{\partial g}{\partial X}$ y $h \cdot \dfrac{\partial f}{\partial Y} - f \cdot \dfrac{\partial h}{\partial Y}$ tienen grados a lo sumo $2d - 2$ y $\sigma \geq 2d$ deducimos

$$g \cdot \frac{\partial f}{\partial X} - f \cdot \frac{\partial g}{\partial X} = h \cdot \frac{\partial f}{\partial Y} - f \cdot \frac{\partial h}{\partial Y}$$

en $\mathbb{K}[[X]][Y]$ y, luego, en $\mathbb{K}[X, Y]$.

Sea $i \in \{1, \ldots, r\}$ y para j tal que $\mu_{ij} = 1$, consideramos una raíz $\phi_j \in \overline{\mathbb{K}}[[X]]$ de $\mathsf{f}_j(X, -)$; es decir, $\mathsf{f}_j(X, \phi_j) = 0$. Para este j, el Lema 2.9 nos muestra que $\dfrac{g(X, \phi_j)}{\frac{\partial f}{\partial Y}(X, \phi_j)} \in \overline{\mathbb{K}}$.

Reemplazando $X = 0$ en $g(X, Y) - \displaystyle\sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}_i} \frac{\partial \mathsf{f}_i}{\partial Y}(X, Y)$ obtenemos

$$g(0, Y) - \sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}_i} \frac{\partial \mathsf{f}_i}{\partial Y}(0, Y) \in (Y)^{\sigma}.$$

Como $\sigma \geq 2d \geq d$ y los grados en la variable Y de g y de $\widehat{\mathsf{f}_i} \dfrac{\partial \mathsf{f}_i}{\partial Y}$ son menores o iguales a $d - 1$ concluimos que

$$g(0, Y) - \sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}_i} \frac{\partial \mathsf{f}_i}{\partial Y}(0, Y) = 0.$$

En particular, se verifica la igualdad

$$g(0, \phi_j(0)) - \sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}_i} \frac{\partial \mathsf{f}_i}{\partial Y}(0, \phi_j(0)) = 0. \tag{2.7}$$

Teniendo en cuenta que $\mathsf{f}_j(X, \phi_j) = 0$ obtenemos

$$\sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}_i} \frac{\partial \mathsf{f}_i}{\partial Y}(0, \phi_j(0)) = \ell_j \widehat{\mathsf{f}_j} \frac{\partial \mathsf{f}_j}{\partial Y}(0, \phi_j(0)). \tag{2.8}$$

Por otro lado observemos que

$$\frac{\partial f}{\partial Y}(0, \phi_j(0)) = \sum_{k=1}^{s} \frac{\partial \mathsf{f}_k}{\partial Y}(0, \phi_j(0)) \cdot \widehat{\mathsf{f}_k}(0, \phi_j(0)) = \frac{\partial \mathsf{f}_j}{\partial Y}(0, \phi_j(0)) \cdot \widehat{\mathsf{f}_j}(0, \phi_j(0)). \tag{2.9}$$

Combinando (2.7), (2.8) y (2.9) se deduce

$$\ell_j = \frac{g(0,\phi_j(0))}{\frac{\partial f}{\partial Y}(0,\phi_j(0))} = \frac{g(X,\phi_j)}{\frac{\partial f}{\partial Y}(X,\phi_j)}.$$

O sea ℓ_j es igual al residuo de $\frac{g}{f}$ en ϕ_j. Sea k tal que $\mu_{ik} = 1$, haciendo la misma cuenta anterior deducimos

$$\ell_k = \frac{g(X,\phi_k)}{\frac{\partial f}{\partial Y}(X,\phi_k)},$$

pero como f_i divide a $g - \ell_j \frac{\partial f}{\partial Y}$ entonces vale que $\ell_j = \ell_k$. Es claro que para cada $1 \leq k \leq s$ existe un único i tal que $\mu_{ik} = 1$, luego mostramos que dados m y k tal que $\mu_{ik} = \mu_{im} = 1$ se verifica que $\ell_m = \ell_k = \alpha_i$, finalmente entonces podemos escribir:

$$(\ell_1, \ldots, \ell_s) = \alpha_1\mu_1 + \cdots + \alpha_r\mu_r.$$

□

Observación 2.11. Observando la demostración del Teorema anterior podemos deducir que si $((\ell_1, \ldots, \ell_s), g, h) \in L_\sigma$ con $\sigma \geq 2d$ entonces g y h son soluciones de la ecuación (2.1). Concretamente mostramos que si $(\ell_1, \ldots, \ell_s) \in \Pi(L_\sigma)$ entonces se verifica que

$$g \cdot \frac{\partial f}{\partial X} - f \cdot \frac{\partial g}{\partial X} - \left(h \cdot \frac{\partial f}{\partial Y} - f \cdot \frac{\partial h}{\partial Y} \right) \in (X,Y)^{\sigma-1}. \tag{2.10}$$

Dado que $g \cdot \frac{\partial f}{\partial X} - f \cdot \frac{\partial g}{\partial X}$ y $h \cdot \frac{\partial f}{\partial Y} - f \cdot \frac{\partial h}{\partial Y}$ son polinomios de grado a lo sumo $2d-2$, la expresión (2.10) implica que g y h son soluciones de la ecuación (2.2).

Ahora mostraremos con un ejemplo que si tomamos $\sigma = 2d-2$ no se cumple que $\Pi(L_\sigma) =< \mu_1, \ldots, \mu_r >$. Con lo cual la cota $\sigma \geq 2d$ es óptima.

Ejemplo 2.12. Sean $\mathbb{K} = \mathbb{C}$ y el polinomio $f(X,Y) = Y^d - Y - X^{d-1}$ con $d \geq 2$. En principio, notemos que mediante el criterio de Eisenstein f resulta absolutamente irreducible. Observemos que el polinomio $f(0,Y) = Y^d - Y$ tiene d raíces diferentes en $\mathbb{C}$. A saber, si w es una raíz primitiva de la unidad de orden $d-1$, el conjunto de raíces de $f(0,Y)$ es: $\{1, w, \ldots, w^{d-2}, 0\}$. Las raíces $\phi_1, \ldots, \phi_d$ de f en $\mathbb{C}[[X]]$, obtenidas a partir de las de $f(0,Y)$ en $\mathbb{C}$, pueden expresarse como:

$$\phi_i = w^{i-1} + \tfrac{X^{d-1}}{d-1} + \mathcal{O}(X^{2d-2}), \quad \text{para} \;\; i \in \{1, \ldots, d-1\} \;\; \text{y} \;\; \phi_d = -X^{d-1} + \mathcal{O}(X^{2d-2}).$$

Luego como cada $Y - \phi_i \in \mathbb{C}[[X]][Y]$ y $f = (Y-\phi_1)\cdots(Y-\phi_d)$ entonces f posee d factores analíticos: $\mathsf{f}_i = Y - \phi_i$ para $i \in \{1, \ldots, d\}$ y de acuerdo a nuestra notación $d = s$.

Definimos los polinomios

$$g(X,Y) = (d-1)(Y + X^{d-1}) \quad \text{y} \quad h(X,Y) = (d-1)X^{d-2}Y,$$

sea $(\ell_1, \ldots, \ell_s) = (1, w, \ldots, w^{d-2}, 0)$. Vamos a probar que $((\ell_1, \ldots, \ell_s), g, h) \in L_{2d-2}$. Para

$i \in \{1, \ldots, d-1\}$ calculamos

$$\begin{aligned}
\frac{g(X,\phi_i)}{\frac{\partial f}{\partial Y}(X,\phi_i)} &= \frac{(d-1)(w^{i-1}+\frac{d}{d-1}X^{d-1})}{d(w^{i-1}+\frac{X^{d-1}}{d-1})^{d-1}-1}+\mathcal{O}(X^{2d-2}) \\
&= \frac{(d-1)(w^{i-1}+\frac{d}{d-1}X^{d-1})}{d((w^{i-1})^{d-1}+(w^{i-1})^{d-2}X^{d-1})-1}+\mathcal{O}(X^{2d-2}) \qquad (2.11) \\
&= \frac{(d-1)w^{i-1}+dX^{d-1}}{d-1+dw^{-(i-1)}X^{d-1}}+\mathcal{O}(X^{2d-2}) \\
&= w^{i-1}+\mathcal{O}(X^{2d-2}).
\end{aligned}$$

Notemos que $\dfrac{\partial f}{\partial Y} = \widehat{\mathsf{f}}_1 + \cdots + \widehat{\mathsf{f}}_s$ verificándose entonces $\frac{\partial f}{\partial Y}(X,\phi_i) = \widehat{\mathsf{f}}_i(X,\phi_i)$. Por (2.11) se tiene que $g(X,\phi_i) = w^{i-1}\cdot\widehat{\mathsf{f}}_i(X,\phi_i)+\mathcal{O}(X^{2d-2})$ para $i \in \{1,\ldots,d-1\}$, luego

$$g(X,Y) = \sum_{i=1}^{s} w^{i-1}\cdot\widehat{\mathsf{f}}_i(X,Y)+\mathcal{O}(X^{2d-2}),$$

de lo que deducimos

$$g-\sum_{i=1}^{s}\ell_i\widehat{\mathsf{f}}_i\frac{\partial \mathsf{f}_i}{\partial Y} = g-\sum_{i=1}^{s} w^{i-1}\cdot\widehat{\mathsf{f}}_i \in \mathcal{O}(X^{2d-2}).$$

Esto último prueba que

$$g-\sum_{i=1}^{s}\ell_i\widehat{\mathsf{f}}_i\frac{\partial \mathsf{f}_i}{\partial Y} \in (X,Y)^{2d-2}. \qquad (2.12)$$

Veamos ahora que $h-\displaystyle\sum_{i=1}^{s}\ell_i\widehat{\mathsf{f}}_i\frac{\partial \mathsf{f}_i}{\partial X} \in (X,Y)^{2d-2}+(X^{2d-3})$. Multiplicamos ambos lados de (2.12) por $X^{d-2} = \dfrac{\partial \mathsf{f}_i}{\partial X}+\mathcal{O}(X^{2d-3})$, y usamos que $\dfrac{\partial \mathsf{f}_i}{\partial Y}=1$, de esta forma obtenemos

$$X^{d-2}\cdot g-\sum_{i=1}^{s}\ell_i\widehat{\mathsf{f}}_i\frac{\partial \mathsf{f}_i}{\partial X} \in (X^{2d-3}),$$

ahora como $X^{d-2}\cdot g - h \in (X^{2d-3})$ deducimos

$$h-\sum_{i=1}^{s}\ell_i\widehat{\mathsf{f}}_i\frac{\partial \mathsf{f}_i}{\partial X} \in (X^{2d-3}). \qquad (2.13)$$

Combinando (2.12) y (2.13) hemos probamos que $((\ell_1,\ldots,\ell_s),g,h) \in L_{2d-2}$. Por lo tanto $(\ell_1,\ldots,\ell_s) \in \Pi(L_{2d-2})$.

Supongamos que $\Pi(L_{2d-2}) =< \mu_1,\ldots,\mu_r >$, entonces $(\ell_1,\ldots,\ell_s) = \alpha_1\mu_1+\cdots+\alpha_r\mu_r$. Existe $i \in \{1,\ldots,r\}$ tal que $\mu_{id}=1$, pero como $\ell_d = 0$ entonces $\alpha_i = 0$. Luego si existe $\mu_{ij}=1$ con $j \neq d$ se verifica que $\ell_j = 0$, pero esto no es posible por contrucción

de $(\ell_1, \ldots, \ell_s)$. Deducimos entonces que $\mu_{ij} = 0$ para todo $j \neq d$, lo que implica que $\mathsf{f}_d = f_i \in \mathbb{C}[X, Y]$ llegando así a un absurdo.

A continuación vamos a mostrar cómo calcular $\{\mu_1, \ldots, \mu_r\}$ a partir de conocer los factores analíticos $\mathsf{f}_1, \ldots, \mathsf{f}_s$ con un cierto grado de precisión σ. Por el teorema anterior, si tomamos precisión $\sigma \geq 2d$ debemos calcular entonces la base escalonada reducida de $\Pi(L_\sigma)$ y de esta forma hallamos los $\{\mu_1, \ldots, \mu_r\}$.

2.1.1. Recombinación

Supongamos que conocemos los factores analíticos $\mathsf{f}_1, \ldots, \mathsf{f}_s$ con precisión σ. Como hemos visto en la sección anterior, calculando la base escalonada reducida del subespacio $\Pi(L_\sigma)$, podemos obtener los factores racionales de f. Para ello consideramos el siguiente sistema lineal $\mathcal{D}_\sigma$ con s incógnitas $\ell_1, \ldots, \ell_s$:

$$\mathcal{D}_\sigma \begin{cases} \displaystyle\sum_{i=1}^{s} \ell_i \mathrm{coef}(\widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y}, X^j Y^k) = 0, \quad k \leq d-1, \quad d \leq j+k \leq \sigma - 1 \\ \\ \displaystyle\sum_{i=1}^{s} \ell_i \mathrm{coef}(\widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial X}, X^j Y^k) = 0, \quad k \leq d-1, \quad j \leq \sigma - 2, \quad d \leq j+k \leq \sigma - 1, \end{cases}$$

donde $\mathrm{coef}(g, X^j Y^k)$ denota el coeficiente del monomio $X^j Y^k$ de $g \in \mathbb{K}[[X]][[Y]]$. Como cada f_i es mónico en Y entonces $\frac{\partial \mathsf{f}_i}{\partial X}$ tiene grado en Y a lo sumo $\deg \mathsf{f}_i - 1$. De esto se deduce que $\widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y}$ y $\widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial X}$ tienen grados en Y a lo sumo $d-1$, lo cual justifica la restricción $k \leq d-1$. Por otra parte, notemos que el primer conjunto de ecuaciones recorre los monomios $X^j Y^k$ que no pertenecen a $(X, Y)^\sigma$ ni a $\mathbb{K}[X, Y]_{d-1}$, mientras que el segundo conjunto de ecuaciones recorre los monomios $X^j Y^k$ que no pertenecen a $(X, Y)^\sigma + (X^{\sigma-1})$ ni a $\mathbb{K}[X, Y]_{d-1}$. Veremos ahora un lema que proporciona la relación entre $\Pi(L_\sigma)$ y $\mathcal{D}_\sigma$.

Lema 2.13. *Bajo la hipótesis (**S**) y dado $\sigma \geq d$ se verifica que*

$$\Pi(L_\sigma) = \{(\ell_1, \ldots, \ell_s) \mid (\ell_1, \ldots, \ell_s) \text{ es solución de } D_\sigma\}.$$

Demostración. Sea $(\ell_1, \ldots, \ell_s)$ solución de D_σ. Para que $(\ell_1, \ldots, \ell_s) \in \Pi(L_\sigma)$ debemos ver que existen $g, h \in \mathbb{K}[X, Y]_{d-1}$ tales que

$$g - \sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y} \in (X, Y)^\sigma, \quad h - \sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial X} \in (X, Y)^\sigma + (X^{\sigma-1}).$$

Construimos g de la siguiente manera:

$$g(X, Y) = \sum_{i=1}^{s} \ell_i \mathrm{coef}(\widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y}, X^j Y^k) X^j Y^k \quad j, k \geq 0 \quad j + k \leq d - 1.$$

Luego, por construcción de g y por ser $(\ell_1, \ldots, \ell_s)$ solución de D_σ obtenemos

$$g - \sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y} \in (X, Y)^\sigma.$$

Análogamente definimos

$$h(X, Y) = \sum_{i=1}^{s} \ell_i \text{coef}(\widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial X}, X^j Y^k) X^j Y^k \quad j, k \geq 0 \quad j + k \leq d - 1.$$

Así $((\ell_1, \ldots, \ell_s), g, h) \in L_\sigma$.

Por otro lado, supongamos que $(\ell_1, \ldots, \ell_s) \in \Pi(L_\sigma)$. Dado que $g - \sum_{i=1}^{s} \ell_i \widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y} \in (X, Y)^\sigma$ entonces cada uno de sus monomios es divisible por $X^m Y^n$ con $n + m = \sigma$; en particular esto se debe cumplir para cada monomio $X^j Y^k$ con $d \leq j + k \leq \sigma - 1$. Concluimos entonces que

$$\sum_{i=1}^{s} \ell_i \text{coef}(\widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y}, X^j Y^k) = 0, \quad k \leq d - 1, \quad d \leq j + k \leq \sigma - 1,$$

de esta forma $(\ell_1, \ldots, \ell_s)$ verifica el primer conjunto de ecuaciones de $\mathcal{D}_\sigma$. De la misma manera se prueba que verifica el segundo conjunto de ecuaciones con lo cual $(\ell_1, \ldots, \ell_s)$ es solución de $\mathcal{D}_\sigma$. □

Si consideramos $\sigma \geq 2d$ y buscamos una base escalonada reducida del espacio de soluciones del sistema $\mathcal{D}_\sigma$, obtendremos los vectores $\mu_1, \ldots, \mu_r$ que nos permitirán recombinar los factores analíticos de f para encontrar los racionales. Finalmente enunciamos el algoritmo de factorización que calcula los factores racionales de f, combinando el Teorema 2.10 y el Lema 2.13.

Algoritmo de Factorización:

Input: Sea f de grado total d que satisface las hipótesis (**S**) y (**C**).
Output: $f_1, \ldots, f_r$ los factores irreducibles racionales de f.

1. Factorizar el polinomio univariado $f(0, Y)$ en $\mathbb{K}[Y]$
2. Hallar los factores irreducibles $\mathsf{f}_1(X, Y), \ldots, \mathsf{f}_s(X, Y)$ a precisión $\sigma = 2d$ utilizando el levantamiento de Hensel.
3. Recombinación:
   a) Para cada $i \in \{1, \ldots, s\}$ calcular $\widehat{\mathsf{f}}_i$ como el cociente de f por f_i, dividiendo con respecto a la variable Y y tomando precisión σ.
   b) Calcular $\left(\widehat{\mathsf{f}}_1 \frac{\partial \mathsf{f}_1}{\partial Y}, \ldots, \widehat{\mathsf{f}}_s \frac{\partial \mathsf{f}_s}{\partial Y}\right)$ con precisión σ en X.
   c) Calcular $\left(\widehat{\mathsf{f}}_1 \frac{\partial \mathsf{f}_1}{\partial X}, \ldots, \widehat{\mathsf{f}}_s \frac{\partial \mathsf{f}_s}{\partial X}\right)$ con precisión σ en X.
   d) Calcular la base escalonada reducida $\{\mu_1, \ldots, \mu_r\}$ de $\mathcal{D}_\sigma$.

e) Si $r = 1$ entonces obtenemos f. Si no para cada $i \in \{1, \ldots, r\}$ calcular f_i como $f_i = \prod_{j=1}^{s} \mathsf{f}_j^{\mu_{ij}}$ a precisión $X^{\deg f_i + 1}$.

A continuación ilustraremos con algunos ejemplos el algoritmo descripto.

Ejemplo 2.14. Sea $f(X, Y) = Y^2 - (X + 1) \in \mathbb{C}[X, Y]$. Por el criterio de Eisenstien sabemos que este polinomio es absolutamente irreducible. Aplicamos el algoritmo a este polinomio y mostramos que la dimensión del espacio de soluciones del sistema lineal es 1. Notemos que $\deg_Y f = \deg f = 2$, entonces $\sigma = 4$ y $f(0, Y) = Y^2 - 1 \in \mathbb{C}[Y]$. Aplicamos el levantamiento de Hensel a partir de la factorización de $f(0, Y)$ obteniendo:

$$\alpha_{1,0} = 1 \qquad \alpha_{2,0} = -1$$

$$\alpha_{1,1} = 1 + \tfrac{1}{2}X \qquad \alpha_{2,1} = -1 - \tfrac{1}{2}X$$

$$\alpha_{1,2} = 1 + \tfrac{1}{2}X - \tfrac{1}{8}X^2 + \tfrac{1}{16}X^3 \qquad \alpha_{2,2} = -1 - \tfrac{1}{2}X + \tfrac{1}{8}X^2 - \tfrac{1}{16}X^3.$$

Los factores analíticos a precisión σ son:

$$\mathsf{f}_1 = Y - 1 - \tfrac{1}{2}X + \tfrac{1}{8}X^2 - \tfrac{1}{16}X^3 \quad , \quad \mathsf{f}_2 = Y + 1 + \tfrac{1}{2}X - \tfrac{1}{8}X^2 + \tfrac{1}{16}X^3.$$

Luego

$$\widehat{\mathsf{f}}_1 \frac{\partial \mathsf{f}_1}{\partial Y} = Y + 1 + \frac{1}{2}X - \frac{1}{8}X^2 + \frac{1}{16}X^3 \qquad \widehat{\mathsf{f}}_2 \frac{\partial \mathsf{f}_2}{\partial Y} = Y - 1 - \frac{1}{2}X + \frac{1}{8}X^2 - \frac{1}{16}X^3$$

$$\widehat{\mathsf{f}}_1 \frac{\partial \mathsf{f}_1}{\partial X} = -\frac{1}{2} - \frac{1}{2}Y + \frac{1}{4}XY - \frac{3}{16}X^2Y \qquad \widehat{\mathsf{f}}_2 \frac{\partial \mathsf{f}_2}{\partial X} = -\frac{1}{2} + \frac{1}{2}Y - \frac{1}{4}XY + \frac{3}{16}X^2Y$$

El proceso de recombinación da lugar al siguiente sistema lineal:

$$\begin{cases} -\frac{1}{8}\ell_1 + \frac{1}{8}\ell_2 = 0 \\ \frac{1}{16}\ell_1 - \frac{1}{16}\ell_2 = 0 \\ \frac{1}{4}\ell_1 - \frac{1}{4}\ell_2 = 0 \\ -\frac{3}{16}\ell_1 + \frac{3}{16}\ell_2 = 0 \end{cases}$$

El espacio de soluciones de $\mathcal{D}_\sigma$ es

$$\{(\ell_1, \ell_2) \mid \ell_1 = \ell_2\} = < (1, 1) >,$$

luego f es irreducible y se puede obtener multiplicando a precisión 2 los factores analíticos dados anteriormente.

Ejemplo 2.15. Consideremos el polinomio $f(X, Y) = Y^4 - X^4 - 2Y^3 + 2YX^2 - Y^2 -$

$X^2 + 2Y \in \mathbb{Q}[X, Y]$. Comenzamos factorizando el polinomio $f(0, Y)$, obtenemos entonces

$$f(0, Y) = Y(Y - 1)(Y + 1)(Y - 2).$$

Hacemos levantamiento de Hensel para encontrar los factores analíticos a precisión $\sigma = 2d$

$$\mathsf{f}_1 = Y - 2 + \tfrac{1}{2}X^2 + \tfrac{1}{8}X^4 + \tfrac{1}{16}X^6$$

$$\mathsf{f}_2 = Y - 1 - \tfrac{1}{2}X^2 + \tfrac{1}{8}X^4 - \tfrac{1}{16}X^6$$

$$\mathsf{f}_3 = Y - \tfrac{1}{2}X^2 - \tfrac{1}{8}X^4 - \tfrac{1}{16}X^6$$

$$\mathsf{f}_4 = Y + 1 + \tfrac{1}{2}X^2 - \tfrac{1}{8}X^4 + \tfrac{1}{16}X^6.$$

Calculando, con ayuda del Maple, los $\left(\widehat{\mathsf{f}}_1 \frac{\partial \mathsf{f}_1}{\partial Y}, \ldots, \widehat{\mathsf{f}}_4 \frac{\partial \mathsf{f}_4}{\partial Y}\right)$ a precisión $\sigma = 8$, se tiene

$$\begin{aligned}
\widehat{\mathsf{f}}_1 \tfrac{\partial \mathsf{f}_1}{\partial Y} = \;& -YX^2 + Y^3 - Y + \tfrac{1}{2}X^2 + \tfrac{5}{8}X^4 + \tfrac{3}{16}X^6 \tfrac{1}{2}Y^2X^2 - \tfrac{1}{8}Y^2X^4 - \tfrac{1}{16}Y^2X^6 - \\
\widehat{\mathsf{f}}_2 \tfrac{\partial \mathsf{f}_2}{\partial Y} = \;& Y^3 - 2Y + X^2 + \tfrac{1}{2}X^4 - \tfrac{1}{8}X^6 - Y^2 + \tfrac{1}{2}X^2Y^2 - \tfrac{1}{8}X^2Y^4 + \tfrac{1}{16}X^6Y^2 - \\
& \tfrac{1}{8}X^6Y + \tfrac{1}{4}YX^4 \\
\widehat{\mathsf{f}}_3 \tfrac{\partial \mathsf{f}_3}{\partial Y} = \;& 2 - YX^2 + Y^3 - Y + \tfrac{3}{2}X^2 - \tfrac{5}{8}X^4 - \tfrac{3}{16}X^6 - 2Y^2 + \tfrac{1}{2}Y^2X^2 + \tfrac{1}{8}Y^2X^4 + \\
& \tfrac{1}{16}Y^2X^6 \\
\widehat{\mathsf{f}}_4 \tfrac{\partial \mathsf{f}_4}{\partial Y} = \;& 2X^2Y + Y^3 + 2Y - X^2 - \tfrac{1}{2}X^4 + \tfrac{1}{8}X^6 - 3Y^2 - \tfrac{1}{2}Y^2X^2 + \tfrac{1}{8}Y^2X^4 - \tfrac{1}{16}Y^2X^6 + \\
& \tfrac{1}{8}YX^6 - \tfrac{1}{4}YX^4.
\end{aligned}$$

Por otro lado, encontramos los $\left(\widehat{\mathsf{f}}_1 \frac{\partial \mathsf{f}_1}{\partial X}, \ldots, \widehat{\mathsf{f}}_4 \frac{\partial \mathsf{f}_4}{\partial X}\right)$ a precisión $\sigma - 1 = 7$

$$\begin{aligned}
\widehat{\mathsf{f}}_1 \tfrac{\partial \mathsf{f}_1}{\partial X} = \;& \tfrac{1}{2}X^3 + \tfrac{7}{8}X^5 - \tfrac{3}{2}YX^3 - \tfrac{7}{8}YX^5 + XY^3 + \tfrac{1}{2}X^3Y^3 + \tfrac{3}{8}X^5Y^3 - YX - \tfrac{1}{2}Y^2X^3 - \\
& \tfrac{3}{8}X^5Y^2 \\
\widehat{\mathsf{f}}_2 \tfrac{\partial \mathsf{f}_2}{\partial X} = \;& -X^3 - YX^3 + \tfrac{1}{2}YX^5 - XY^3 + \tfrac{1}{2}X^3Y^3 - \tfrac{3}{8}Y^3X^5 + 2XY - Y^2X^3 + Y^2X + \\
& \tfrac{3}{4}Y^2X^5 \\
\widehat{\mathsf{f}}_3 \tfrac{\partial \mathsf{f}_3}{\partial X} = \;& -2X - \tfrac{5}{2}X^3 - \tfrac{7}{8}X^5 + \tfrac{3}{2}YX^3 + \tfrac{7}{8}YX^5 - Y^3X - \tfrac{1}{2}Y^3X^3 - \tfrac{3}{8}Y^3X^5 + YX + \\
& \tfrac{1}{2}Y^2X^3 + \tfrac{3}{8}Y^2X^5 + 2Y^2X \\
\widehat{\mathsf{f}}_4 \tfrac{\partial \mathsf{f}_4}{\partial X} = \;& -X^3 - \tfrac{1}{2}YX^5 + YX^3 + Y^3X - \tfrac{1}{2}Y^3X^3 + \tfrac{3}{8}Y^3X^5 + 2YX - \tfrac{3}{4}Y^2X^5 - 3Y^2X + \\
& Y^2X^3.
\end{aligned}$$

Finalmente, resolvemos el sistema lineal cuya solución nos proporcionará la cantidad de factores de f en $\mathbb{Q}[X, Y]$ y nos permitirá recombinar los cuatro factores analíticos para obtener dichos factores racionales. El sitema original tiene 12 ecuaciones y 4 incógnitas.

Este resulta equivalente al sistema

$$\begin{cases} \ell_1 - \ell_2 - \ell_3 + \ell_4 = & 0 \\ \\ \ell_1 + \ell_2 - \ell_3 - \ell_4 = & 0 \end{cases}$$

Por lo tanto, una base escalonada reducida del espacio de soluciones es

$$\{(1,0,1,0),(0,1,0,1)\},$$

de donde hallamos que f tiene dos factores irreducibles en $\mathbb{Q}[X,Y]$. Del vector $(1,0,1,0)$ deducimos que uno de los factores racionales se obtiene multiplicando los factores analíticos f_1 y f_3; es decir

$$f_1 = \mathsf{f}_1 \cdot \mathsf{f}_2 = Y^2 - 2Y + X^2.$$

Y por otro lado, del vector $(0,1,0,1)$ sabemos que el segundo factor racional se obtiene multiplicando los analíticos f_2 y f_4:

$$f_2 = \mathsf{f}_2 \cdot \mathsf{f}_4 = Y^2 - X^2 - 1.$$

En particular, como el vector $(1,0,1,0) \in \Pi(L_\sigma)$ podemos encontrar las expresiones para g y h de forma tal que $((1,0,1,0),g,h) \in L_\sigma$. En efecto, dado que

$$g + \widehat{\mathsf{f}}_1 \frac{\partial \mathsf{f}_1}{\partial Y} + \widehat{\mathsf{f}}_3 \frac{\partial \mathsf{f}_3}{\partial Y} \in (X,Y)^\sigma,$$

$$h + \widehat{\mathsf{f}}_1 \frac{\partial \mathsf{f}_1}{\partial X} + \widehat{\mathsf{f}}_3 \frac{\partial \mathsf{f}_3}{\partial X} \in (X,Y)^\sigma + (X^{\sigma-1}),$$

obtenemos que

$$g(X,Y) = 2 - 2YX^2 + 2Y^3 - 2Y + 2X^2 - 2Y^2$$

$$h(X,Y) = -2X - 2X^3 + 2XY^2,$$

además g y h verifican la ecuación (2.2). Análogamente podemos encontrar g' y h' tales que $((0,1,0,1),g',h') \in L_\sigma$.En este caso se tiene

$$g' + \widehat{\mathsf{f}}_2 \frac{\partial \mathsf{f}_2}{\partial Y} + \widehat{\mathsf{f}}_4 \frac{\partial \mathsf{f}_4}{\partial Y} \in (X,Y)^\sigma,$$

$$h' + \widehat{\mathsf{f}}_2 \frac{\partial \mathsf{f}_2}{\partial X} + \widehat{\mathsf{f}}_4 \frac{\partial \mathsf{f}_4}{\partial X} \in (X,Y)^\sigma + (X^{\sigma-1}),$$

luego

$$g'(X,Y) = 2Y^3 - 4Y^2 + 2YX^2$$

$$h'(X,Y) = -2X^3 + 4XY - 2XY^2,$$

verificándose que g' y h' son soluciones de la ecuación (2.2). Como g, h, g' y h' satisfacen las condiciones de grado que enuncia el teorema de Ruppert, establecemos de otra forma

que f no es irreducible.

2.2. Generalización a polinomios multivariados

Estudiaremos a continuación la generalización para polinomios bivariados desarrollada por G.Lecerf en [Lec07]. Sea $\mathbb{K}$ un cuerpo verificando la hipótesis (**C**) y sea $f \in \mathbb{K}[Z_1, \ldots, Z_n, Y]$ de grado total d. Supongamos que f cumple la hipótesis (**S′**):

$$\text{Hipótesis } (\mathbf{S}') \begin{cases} (i) \quad \deg_Y(f) = \deg(f) = d \\ \\ (ii) \quad \operatorname{Res}_Y(f(0, \ldots, 0, Y), \dfrac{\partial f}{\partial Y}(0, \ldots, 0, Y)) \neq 0. \end{cases}$$

Nuestro objetivo es encontrar los factores irreducibles $f_1, \ldots, f_r$ en $\mathbb{K}[Z_1, \ldots, Z_n, Y]$. Sean $\mathsf{f}_1, \ldots, \mathsf{f}_s \in \mathbb{K}[[Z_1, \ldots, Z_n]][Y]$, los factores analíticos de f. Por la hipótesis (**S′**) tanto f como sus factores analíticos y racionales son mónicos en Y. Como en la sección anterior, a cada $i \in \{1, \ldots, r\}$ le asociamos el vector $\mu_i \in \{0, 1\}^s$ definido por

$$f_i = \prod_{j=1}^{s} \mathsf{f}_j^{\mu_{ij}}, \tag{2.14}$$

y el conjunto de vectores $\{\mu_1, \ldots, \mu_r\}$ que resultan linealmente independientes.

La idea será reducir este problema a dos variables para aplicar el algoritmo descripto en la sección anterior.

2.2.1. Reducción a dos variables

Consideramos un conjunto auxiliar de variables $a_1, \ldots, a_n$ y el polinomio

$$g(X, Y) := f(a_1 X, \ldots, a_n X, Y) \in \mathbb{K}_a[X, Y]$$

donde $\mathbb{K}_a := \mathbb{K}(a_1, \ldots, a_n)$.

Observación 2.16. Dado que f es mónico en Y y $\deg f = \deg_Y = d$ deducimos que g es mónico en Y visto en $\mathbb{K}[a_1, \ldots, a_n, X][Y]$ y además se verifica $\deg g = \deg_Y g = d$.

La hipótesis (**S′**) implica de forma directa que g verifica:

$$\text{Hipótesis } (\mathbf{S_a}) \begin{cases} (i) \quad \deg_Y(g) = \deg(g) = d \\ \\ (ii) \quad \operatorname{Res}_Y(g(0, Y), \dfrac{\partial g}{\partial Y}(0, Y)) \neq 0 \end{cases}$$

Se verifica que los factores irreducibles de g en $\mathbb{K}_a[X, Y]$ están en correspondencia biunívoca con los de f; o sea, los factores irreducibles de g se expresan como $g_i(X, Y) = f_i(a_1 X, \ldots, a_n X, Y)$ para $i \in \{1, \ldots, r\}$.

Consideramos los factores analíticos en $\mathbb{K}_a[X, Y]$ de g: $\mathsf{g}_1, \ldots, \mathsf{g}_s$, que se relacionan con los f_i de la siguiente manera: $\mathsf{g}_i(X, Y) = \mathsf{f}_i(a_1 X, \ldots, a_n X, Y)$ para $i \in \{1, \ldots, s\}$. Luego vale que $\mathsf{g}_i \in \mathbb{K}[a_1, \ldots, a_n][[X]][Y]$. Como consecuencia de (2.14) se satisface:

$$g_i = \prod_{j=1}^{s} \mathsf{g}_j^{\mu_{ij}}.$$

Observación 2.17. Definimos los siguientes polinomios:

$$\widehat{\mathsf{f}_i} = \prod_{j \neq i} \mathsf{f}_i \qquad \widehat{\mathsf{g}_i} = \prod_{j \neq i} \mathsf{g}_i$$

para $i \in \{1, \ldots, s\}$.

Estamos entonces en condiciones de aplicar el algoritmo dado en la sección anterior a g, obteniendo el siguiente sistema lineal sobre $\mathbb{K}_a$, con s incógnitas $\ell_1, \ldots, \ell_s$:

$$\mathcal{D}_{a,\sigma} \begin{cases} \displaystyle\sum_{i=1}^{s} \ell_i \mathrm{coef}(\widehat{\mathsf{g}_i}\frac{\partial \mathsf{g}_i}{\partial Y}, X^j Y^k) = 0, \quad k \leq d-1, \quad d \leq j+k \leq \sigma - 1 \\ \\ \displaystyle\sum_{i=1}^{s} \ell_i \mathrm{coef}(\widehat{\mathsf{g}_i}\frac{\partial \mathsf{g}_i}{\partial X}, X^j Y^k) = 0, \quad k \leq d-1, \quad j \leq \sigma - 2, \quad d \leq j+k \leq \sigma - 1. \end{cases} \tag{2.15}$$

Observación 2.18. Por el Teorema 2.10 y el Lema 2.13, si $\sigma \geq 2d$ y se verifican las hipótesis $(\mathbf{S}')$ y $(\mathbf{C})$, entonces encontrando una base escalonada reducida del espacio de soluciones del sistema $\mathcal{D}_{a,\sigma}$ podremos recombinar los factores analíticos de f para obtener así su factorización racional. Notemos que en este caso tenemos que resolver un sistema de ecuaciones lineales sobre $\mathbb{K}_a$. En lo que sigue vamos a mostrar que se puede eliminar la sustitución Z_i por $a_i X$ y obtener así una generalización más directa del algoritmo en dos variables. Con este objetivo vamos a probar primero un lema que permite resolver $\mathcal{D}_{a,\sigma}$ sobre $\mathbb{K}$ en vez de hacerlo sobre $\mathbb{K}_a$.

Lema 2.19. *Sean $\mathbb{E}$ un subcuerpo de $\mathbb{K}$, $\sigma \geq 2d$ y el subespacio de $\mathbb{E}^s$*

$$\mathcal{S}_{a,\sigma} = \{(\ell_1, \ldots, \ell_s) \in \mathbb{E}^s \mid (\ell_1, \ldots, \ell_s) \text{ es solución de } D_{a,\sigma}\}.$$

Se tiene que $\{\mu_1, \ldots, \mu_r\}$ es base escalonada reducida de $\mathcal{S}_{a,\sigma}$.

Demostración. Dado que para $i \in \{1, \ldots, r\}$ $\mu_i \in \{0,1\}^s$ entonces se verifica que $\mu_i \in \mathcal{S}_{a,\sigma}$ para cada $i \in \{1, \ldots, r\}$. Sea $(\ell_1, \ldots, \ell_s) \in \mathbb{E}^s$ solución de $D_{a,\sigma}$. Por la Observación 2.18 existen $\gamma_1, \ldots, \gamma_r \in \mathbb{K}_a$ tal que

$$(\ell_1, \ldots, \ell_s) = \gamma_1 \mu_1 + \cdots + \gamma_r \mu_r. \tag{2.16}$$

Luego por (2.16) y por ser $\mu_1, \ldots, \mu_r$ una base escalonada reducida tenemos que para cada γ_i existe ℓ_j tal que $\gamma_i = \ell_j$, luego $\gamma_1, \ldots, \gamma_r \in \mathbb{E}$. □

Observación 2.20. Damos ahora la generalización más directa del algoritmo descripto en la sección anterior, para ello consideramos el siguiente operador:

$$\Theta := Z_1 \frac{\partial}{\partial Z_1} + \cdots + Z_n \frac{\partial}{\partial Z_n},$$

y el sistema lineal:

$$\mathcal{D}_\sigma \begin{cases} \displaystyle\sum_{i=1}^{s} \ell_i \mathrm{coef}(\widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y}, Z_1^{j_1} \cdots Z_n^{j_n} Y^k) = 0, \quad k \leq d-1, \quad d \leq \overline{j} + k \leq \sigma - 1 \\ \\ \displaystyle\sum_{i=1}^{s} \ell_i \mathrm{coef}(\widehat{\mathsf{f}}_i \Theta \mathsf{f}_i, Z_1^{j_1} \cdots Z_n^{j_n} Y^k) = 0, \quad k \leq d-1, \quad \overline{j} \leq \sigma - 1, \quad d \leq \overline{j} + k \leq \sigma - 1, \end{cases}$$

con $\overline{j} = j_1 + \cdots + j_n$.

Proposición 2.21. *Con las hipótesis (**S'**) y (**C**) y $\sigma \geq 2d$, la base escalonada reducida de $\mathcal{D}_\sigma$ es $\{\mu_1, \ldots, \mu_r\}$.*

Demostración. Si vemos que las soluciones de $\mathcal{D}_{a,\sigma}$ coinciden con las de $\mathcal{D}_\sigma$ sobre $\mathbb{K}^s$, entonces por el Lema 2.19 resulta que $\{\mu_1, \ldots, \mu_r\}$ es base del espacio de soluciones de $\mathcal{D}_\sigma$. Como $\widehat{\mathsf{g}}_i \frac{\partial \mathsf{g}_i}{\partial Y} = \widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y}(a_1 X, \ldots, a_n X, Y)$, deducimos que $\mathrm{coef}(\widehat{\mathsf{g}}_i \frac{\partial \mathsf{g}_i}{\partial Y}, X^j Y^k)$ coincide con la componente homogénea de grado j del coeficiente de Y^k en $\widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y}(a_1, \ldots, a_n, Y)$ mirado en $\mathbb{K}[[a_1, \ldots, a_n]][Y]$. Sean j y k fijos, tomamos la siguiente ecuación de $\mathcal{D}_{a,\sigma}$:

$$\sum_{i=1}^{s} \ell_i \mathrm{coef}(\widehat{\mathsf{g}}_i \frac{\partial \mathsf{g}_i}{\partial Y}, X^j Y^k) = 0. \tag{2.17}$$

Notemos que por lo observado anteriormente, (2.17) se puede escribir como

$$\sum_{j_1 + \cdots + j_n = j} a_1^{j_1} \cdots a_n^{j_n} \sum_{i=1}^{s} \ell_i \mathrm{coef}(\widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y}, Z_1^{j_1} \cdots Z_n^{j_n} Y^k) = 0,$$

de esto deducimos que $(\ell_1, \ldots, \ell_s) \in \mathbb{K}^s$ es solución de la ecuación (2.17) si y solo si verifica las ecuaciones

$$\sum_{i=1}^{s} \ell_i \mathrm{coef}(\widehat{\mathsf{f}}_i \frac{\partial \mathsf{f}_i}{\partial Y}, Z_1^{j_1} \cdots Z_n^{j_n} Y^k) = 0,$$

con $j_1 + \ldots + j_n = j$, luego el primer conjunto de ecuaciones de $\mathcal{D}_{a,\sigma}$ y $\mathcal{D}_\sigma$ tienen el mismo conjunto de soluciones sobre $\mathbb{K}^s$. Por otro lado observemos

$$\begin{aligned} X \frac{\partial \mathsf{g}_i}{\partial X} &= X \frac{\partial}{\partial X} \left(\mathsf{f}_i(a_1 X, \ldots, a_n X, Y) \right) \\ &= \sum_{j=1}^{n} X \cdot a_j \frac{\partial \mathsf{f}_i}{\partial Z_j}(a_1 X, \ldots, a_n X, Y) \\ &= (\Theta \mathsf{f}_i)(a_1 X, \ldots, a_n X, Y), \end{aligned}$$

de lo que deducimos $\mathrm{coef}(\widehat{\mathsf{g}}_i \frac{\partial \mathsf{g}_i}{\partial X}, X^j Y^k) = \mathrm{coef}(\widehat{\mathsf{g}}_i X \frac{\partial \mathsf{g}_i}{\partial X}, X^{j+1} Y^k)$ que es igual a la componente homogénea de grado $j+1$ del coeficiente de Y^k en $(\widehat{\mathsf{f}}_i \Theta \mathsf{f}_i)(a_1, \ldots, a_n, Y)$ visto en $\mathbb{K}[[a_1, \ldots, a_n]][Y]$. Análogamente se prueba que el segundo conjunto de ecuaciones de $\mathcal{D}_{a,\sigma}$

y $\mathcal{D}_\sigma$ tienen el mismo conjunto de soluciones sobre $\mathbb{K}^s$. □

Enunciamos ahora el algoritmo de factorización.

Algoritmo de Factorización:

Input: f de grado total d que satisface las hipótesis $(\mathbf{S}')$ y $(\mathbf{C})$.
Output: $f_1, \ldots, f_r$ los factores irreducibles racionales de f .

1. A partir del polinomio univariado $f(0, \ldots, 0, Y)$ calcular los factores irreducibles $\mathsf{f}_1(0, \ldots, 0, Y), \ldots, \mathsf{f}_s(0, \ldots, 0, Y) \in \mathbb{K}[Y]$.
2. Utilizando el levantamiento de Hensel (ver [])obtener $\mathsf{f}_1, \ldots, \mathsf{f}_s$ a precisión $(Z_1, \ldots, Z_n)^\sigma$ con $\sigma = 2d$.
3. Recombinación:
   a) Para cada $i \in \{1, \ldots, s\}$ calcular $\widehat{\mathsf{f}}_i$ como el cociente de f por f_i en $\mathbb{K}[[Z_1, \ldots, Z_n]][Y]$ a precisión $(Z_1, \ldots, Z_n)^\sigma$.
   b) Calcular $\left(\widehat{\mathsf{f}}_1 \frac{\partial \mathsf{f}_1}{\partial Y}, \ldots, \widehat{\mathsf{f}}_s \frac{\partial \mathsf{f}_s}{\partial Y}\right)$ con precisión $(Z_1, \ldots, Z_n)^\sigma$.
   c) Calcular $\left(\widehat{\mathsf{f}}_1 \frac{\partial \mathsf{f}_1}{\partial X}, \ldots, \widehat{\mathsf{f}}_s \frac{\partial \mathsf{f}_s}{\partial X}\right)$ con precisión $(Z_1, \ldots, Z_n)^\sigma$.
   d) Calcular la base escalonada reducida de $\mathcal{D}_\sigma$.
   e) Si $r = 1$ entonces obtenemos f. Si no para cada $i \in \{1, \ldots, r\}$ calcular f_i como $f_i = \prod_{j=1}^{s} \mathsf{f}_j^{\mu_{ij}}$ a precisión $(Z_1, \ldots, Z_n)^{\deg f_i + 1}$.

2.3. Teorema de Bertini

En esta sección estudiaremos la versión del teorema de Bertini que se obtiene a partir del algoritmo desarrollado anteriormente. Para ello seguiremos el trabajo de G.Lecerf [Lec07].

Definición 2.22. Sean $f \in \mathbb{K}[Z_1, \ldots, Z_n, Y]$ de grado total d y $(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n$. Decimos que $(\alpha_1, \ldots, \alpha_n)$ es un **punto de Bertini para f** si para todo factor irreducible f_i de f el polinomio $f_i(\alpha_1 X, \ldots, \alpha_n X, Y)$ es irreducible. En otras palabras, si existe una correspondencia biunívoca entre los factores irreducibles de f y los de $h(X, Y) := f(\alpha_1 X, \ldots, \alpha_n X, Y) \in \mathbb{K}[X, Y]$. Denotamos por $\mathcal{B}_h(f)$ al complemento del conjunto de puntos de Bertini.

Observación 2.23. En general, el punto $(\alpha_1, \ldots, \alpha_n)$ es elegido con coordenadas en un subconjunto finito $\mathcal{S} \subset \mathbb{K}$.

Ejemplo 2.24. Sean $n \geq 2$, $\mathbb{K} = \mathbb{C}$ y $f(Z_1, \ldots, Z_n, Y) = Y^d + Z_1^{d-1} Y - Z_2^{d-1} - 1$. En el capítulo 1, Ejemplo 1.21 probamos que este polinomio es absolutamente irreducible.

Consideramos $\mathcal{S} = \{z \in \mathbb{C} \mid z \text{ es raíz de } Y^{d(d-1)} - 1\}$. Dado $(\alpha_1, \ldots, \alpha_n) \in \mathcal{S}^n$ queremos determinar si es o no un punto de Bertini para f. Consideramos entonces el

polinomio $h(X,Y) := f(\alpha_1 X, \ldots, \alpha_n X, Y)$. Para cada $(\alpha_1, \ldots, \alpha_n) \in \mathcal{S}^n$ el polinomio $g(Y) = Y - (\frac{\alpha_2}{\alpha_1})^{d-1}$ divide a $h(X,Y) = Y^d + \alpha_1^{d-1} X^{d-1} Y - \alpha_2^{d-1} X^{d-1} - 1$. En consecuencia, cada punto de $\mathcal{S}^n$ no es un punto de Bertini para f. La proporción de puntos que no son de Bertini para f en $\mathcal{S}^n$ es:

$$\frac{|\mathcal{B}_h(f) \cap \mathcal{S}^n|}{|\mathcal{S}|^n} = \frac{d(d-1)}{|\mathcal{S}|} = 1.$$

Observación 2.25. Continuando con el ejemplo 2.24, afirmamos que no existe un polinomio no nulo $\mathsf{A} \in \mathbb{K}[a_1, \ldots, a_n]$ de grado menor o igual a $d(d-1)-1$ que se anule en el conjunto $\mathcal{B}_h(f)$. En efecto, supongamos que existe un polinomio con dichas características. Por el Lema de Zippel-Schwartz sabemos que A tiene a lo sumo $\deg \mathsf{A} |\mathcal{S}|^{n-1}$ ceros en $\mathcal{S}^n$. Por lo tanto se verifica la siguiente desigualdad:

$$\frac{|\{(x_1, \ldots, x_n) \in \mathcal{S}^n \ \mid \ \mathsf{A}(x_1, \ldots, x_n) = 0\}|}{|\mathcal{S}|^n} \leq \frac{\deg \mathsf{A}}{|S|} \leq \frac{d(d-1)-1}{d(d-1)} < 1$$

Por otro lado, como A se anula en $\mathcal{B}_h(f)$ y $\mathcal{S}^n \subset \mathcal{B}_h(f)$ entonces obtenemos

$$\frac{|\{(x_1, \ldots, x_n) \in \mathcal{S}^n \ \mid \ \mathsf{A}(x_1, \ldots, x_n) = 0\}|}{|\mathcal{S}|^n} = 1,$$

llegando de esta forma a un absurdo.

Teorema 2.26. *Sea $f \in \mathbb{K}[Z_1, \ldots, Z_n, Y]$ de grado total d verificando las hipótesis ($\boldsymbol{S'}$) y ($\boldsymbol{C}$). Existe un polinomio no nulo $\mathsf{A} \in \mathbb{K}[a_1, \ldots, a_n]$ de grado menor o igual a $(2d-1)(d-1)$ que se anula en $\mathcal{B}_h(f)$.*

Demostración. Observemos que podemos suponer que f es irreducible. En efecto, si $f = f_1 \cdots f_m$, donde cada f_i es irreducible de grado positivo d_i $(1 \leq i \leq m)$, aplicamos el teorema a cada f_i y hallamos $\mathsf{A}_i \in \mathsf{A} \in \mathbb{K}[a_1, \ldots, a_n]$ de grado a lo sumo $(d_i - 1)(2d_i - 1)$ para $1 \leq i \leq m$. El polinomio buscado será $\mathsf{A} = \prod_{i=1}^m \mathsf{A}_i$. Como la aplicación $\delta : d \longrightarrow (d-1)(2d-1)$ verifica que $\delta(d_1) + \delta(d_2) \leq \delta(d_1 + d_2)$ entonces deducimos que $\deg(\mathsf{A}) \leq (d-1)(2d-1)$. Por lo tanto trabajaremos con p irreducible.

Sean $\sigma = 2d$, $(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n$ y $h(X,Y) := f(\alpha_1 X, \ldots, \alpha_n X, Y) \in \mathbb{K}[X,Y]$. Consideramos el siguiente sistema:

$$\mathcal{D}_{\alpha,\sigma} \begin{cases} \displaystyle\sum_{i=1}^{s} \ell_i \mathrm{coef}(\widehat{\mathsf{h}_i} \frac{\partial \mathsf{h}_i}{\partial Y}, X^j Y^k) = 0, \quad k \leq d-1, \quad d \leq j+k \leq \sigma - 1 \\ \\ \displaystyle\sum_{i=1}^{s} \ell_i \mathrm{coef}(\widehat{\mathsf{h}_i} \frac{\partial \mathsf{h}_i}{\partial X}, X^j Y^k) = 0, \quad k \leq d-1, \quad j \leq \sigma - 2, \quad d \leq j+k \leq \sigma - 1, \end{cases}$$

donde $\mathsf{h}_1(X,Y), \ldots, \mathsf{h}_s(X,Y)$ representan los factores mónicos irreducibles de $h(X,Y)$ en el anillo de series formales $\mathbb{K}[[X]][Y]$ y $\widehat{\mathsf{h}_i} = \prod_{j \neq i} \mathsf{h}_j$ para $i \in \{1, \ldots, s\}$. Por el Teorema 2.10 y el Lema 2.13, la dimensión del espacio de soluciones de $\mathcal{D}_{\alpha,\sigma}$ es igual a la cantidad de factores irreducibles de h. Sea $\mathcal{D}_{a,\sigma}$, el sistema definido como en (2.15). Luego, su rango

es $s-1$ ya que f es irreducible. De esto se deduce que existe un menor $\mathsf{A} \in \mathbb{K}[a_1, \ldots, a_n]$ de rango $s-1$ de la matriz $\mathcal{D}_{a,\sigma}$. Notemos que $\mathcal{D}_{\alpha,\sigma}$ coincide con la especialización de $\mathcal{D}_{a,\sigma}$ en $a_1 = \alpha_1, \ldots, a_n = \alpha_n$. Por lo tanto si elegimos $(\alpha_1, \ldots, \alpha_n)$ de forma tal que $\mathsf{A}(\alpha_1, \ldots, \alpha_n) \neq 0$ la matriz $\mathcal{D}_{\alpha,\sigma}$ tiene rango $s-1$ y por lo tanto h es irreducible. Concluimos que si $(\alpha_1, \ldots, \alpha_n) \in \mathcal{B}_h(f)$ entonces $(\alpha_1, \ldots, \alpha_n)$ es raíz de A. Probemos ahora que A satisface la condición sobre el grado. Por la demostración de la Proposición 2.21 para cada $j \in \{0, \ldots, \sigma-1\}$, $\operatorname{coef}(\widehat{\mathsf{g}}_i \frac{\partial \mathsf{g}_i}{\partial Y}, X^j Y^k)$ es un polinomio de grado a lo sumo j y para cada $j \in \{0, \ldots, \sigma-2\}$, $\operatorname{coef}(\widehat{\mathsf{g}}_i \frac{\partial \mathsf{g}_i}{\partial X}, X^j Y^k)$ es un polinomio de grado a lo sumo $j+1$; deducimos entonces que $\deg \mathsf{A} \leq (s-1)(2d-1) \leq (d-1)(2d-1)$. □

Observación 2.27. Del Teorema 2.26 y del Ejemplo 2.24 se deduce la siguiente cota:

$$\max_f \{\min_{\mathsf{A}} \{\deg(\mathsf{A}) \mid \mathsf{A}(\mathcal{B}_h(f)) = 0\}\} \geq d(d-1),$$

donde el máximo se toma sobre $f \in \mathbb{K}[Z_1, \ldots, Z_n, Y]$ que cumplen las hipótesis (**C**) y (**S′**) y el mínimo se toma sobre $\mathsf{A} \in \mathbb{K}[a_1, \ldots, a_n]$ no nulos.

Corolario 2.28. *Sea $f \in \mathbb{K}[Z_1, \ldots, Z_n, Y]$ verificando las hipótesis (**C**) y (**S′**). Para todo subconjunto no vacío y finito $\mathcal{S} \subset \mathbb{K}$ se tiene*

$$\frac{|\mathcal{B}_h(f) \cap \mathcal{S}^n|}{|\mathcal{S}|^n} \leq \frac{(d-1)(2d-1)}{|\mathcal{S}|}.$$

Demostración. Por el Teorema 2.26 existe un polinomio A de grado a lo sumo $(d-1)(2d-1)$ que se anula en $\mathcal{B}_h(f)$. Se verifica entonces

$$\frac{|\mathcal{B}_h(f) \cap \mathcal{S}^n|}{|\mathcal{S}|^n} \leq \frac{|\{(x_1, \ldots, x_n) \in \mathcal{S}^n \mid \mathsf{A}(x_1, \ldots, x_n) = 0\}|}{|\mathcal{S}|^n}.$$

Por otro lado por Zippel-Schwartz aplicado al polinomio A se deduce

$$\frac{|\{(x_1, \ldots, x_n) \in \mathcal{S}^n \mid \mathsf{A}(x_1, \ldots, x_n) = 0\}|}{|\mathcal{S}|^n} \leq \frac{(d-1)(2d-1)}{|\mathcal{S}|},$$

concluyendo que

$$\frac{|\mathcal{B}_h(f) \cap \mathcal{S}^n|}{|\mathcal{S}|^n} \leq \frac{(d-1)(2d-1)}{|\mathcal{S}|}.$$

□

Observación 2.29. Informalmente hablando, por el Corolario anterior deducimos que es necesario y suficiente tomar $\mathcal{S}$ con $|\mathcal{S}| \gg d^2$ para tener alta probabilidad de éxito en encontrar un punto de Bertini al elegir aleatoriamente en el conjunto $\mathcal{S}^n$.

Observación 2.30. Nuevamente por el Ejemplo 2.24 y el Corolario 2.28 deducimos que

$$\max \left(\frac{|\mathcal{B}_h(f) \cap \mathcal{S}^n|}{|\mathcal{S}|^{n-1}} \mid \mathcal{S} \subset \mathbb{K} \text{ y } f \text{ satisfaciendo las hipótesis (C) y (S')} \right) \geq d(d-1),$$

donde el máximo se toma sobre los subconjuntos finitos $\mathcal{S} \subset \mathbb{K}$.

Dado un polinomio $p \in \mathbb{K}[v_1, \ldots, v_n]$ de grado total $d \geq 1$ y elementos α, β , $\gamma \in \mathbb{K}^{3n}$, definimos el siguiente polinomio de $\mathbb{K}[X, Y]$:

$$p_{\alpha\beta\gamma} := p(\alpha_1 X + \beta_1 Y + \gamma_1, \ldots, \alpha_n X + \beta_n Y + \gamma_n).$$

Definición 2.31. Con las notaciones y definiciones dadas anteriormente, decimos que $(\alpha, \beta, \gamma) \in \mathbb{K}^{3n}$ es un punto de Bertini para p si existe una correspondencia biunívoca entre los factores irreducibles de p y los de $p_{\alpha\beta\gamma}$. Notamos como $\mathcal{B}(p)$ al complemento del conjunto de puntos de Bertini para p en $\mathbb{K}^{3n}$.

Observación 2.32. Dado un subconjunto finito $\mathcal{S} \subset \mathbb{K}$, notemos con $\mathcal{B}(p, \mathcal{S})$ a la proporción de puntos que no son de Bertini para p en $\mathcal{S}^{3n}$; es decir,

$$\mathcal{B}(p, \mathcal{S}) := \frac{|\mathcal{B}(p) \cap \mathcal{S}^{3n}|}{|\mathcal{S}|^{3n}}$$

Corolario 2.33. *Sea $p \in \mathbb{K}[v_1, \ldots, v_n]$ de grado total $d \geq 1$. Supongamos que se cumple la hipótesis (**C**). Sea $\mathcal{S} \subset \mathbb{K}$ un subconjunto no vacío y finito. Se verifica entonces*

$$\mathcal{B}(p, \mathcal{S}) \leq \frac{3d(d-1)+1}{|\mathcal{S}|}.$$

Demostración. Al igual que en el teorema 2.26, como la aplicación $\delta : d \longrightarrow 3d(d-1)+1$ verifica que $\delta(d_1) + \delta(d_2) \leq \delta(d_1 + d_2)$ podemos suponer que p es irreducible.

Sean $w_1, \ldots, w_n, z_1, \ldots, z_n$ nuevas variables y sean β y γ elementos de $\mathbb{K}^n$. Definimos los siguientes polinomios:

$$p_\beta := p(w_1 + \beta_1 Y, \ldots, w_n + \beta_n Y) \in \mathbb{K}[w_1, \ldots, w_n, Y]$$

$$p_{\beta\gamma} := p_\beta(z_1 + \gamma_1, \ldots, z_n + \gamma_n, Y) \in \mathbb{K}[z_1, \ldots, z_n, Y].$$

En primer lugar, vamos a mostrar que podemos elegir β y $\gamma \in \mathbb{K}^n$ de forma tal que $p_{\beta\gamma}$ verifique las condiciones del Teorema 2.26; para ello tenemos que mostrar que se satisface la hipótesis($\mathbf{S}'$) para $p_{\beta\gamma}$. Sea $p_d \in \mathbb{K}[v_1, \ldots, v_n]$ la componente homogénea de mayor grado de p. Observemos que si tomamos β de forma tal que $p_d(\beta_1, \ldots, \beta_n) \neq 0$ entonces se verifica que $\deg p_\beta = \deg_Y p_\beta = d$ y además es mónico en Y. Entonces para β bajo esta condición consideramos $\mathcal{D}_\beta \in \mathbb{K}[w_1, \ldots, w_n]$, el discriminante de p_β con respecto a Y. La hipótesis (**C**) implica que $\frac{\partial p_\beta}{\partial Y}$ no es el polinomio nulo, como p_β es libre de cuadrados obtenemos entonces que $\mathcal{D}_\beta$ es un polinomio no nulo de grado a lo sumo $d(d-1)$. Por lo tanto podemos elegir $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{K}^n$ tal que $\mathcal{D}_\beta(\gamma_1, \ldots, \gamma_n) \neq 0$. Afirmamos que con β y γ elegidos de esta forma $p_{\beta\gamma}$ cumple la hipótesis ($\mathbf{S}'$). En efecto, como $p_d(\beta_1, \ldots, \beta_n) \neq 0$ resulta que $p_{\beta\gamma}$ es mónico en Y y además $\deg p_{\beta\gamma} = \deg_Y p_{\beta\gamma} = d$. Por otro lado

$$\mathrm{Res}_Y \left(p_{\beta\gamma}(0, \ldots, 0, Y), \frac{\partial p_{\beta\gamma}}{\partial Y}(0, \ldots, 0, Y) \right) \neq 0,$$

dado que

$$p_{\beta\gamma}(0, \ldots, 0, Y) = p_\beta(\gamma_1, \ldots, \gamma_n, Y)$$

$$\frac{\partial p_{\beta\gamma}}{\partial Y}(0,\ldots,0,Y) = \frac{\partial p_\beta}{\partial Y}(\gamma_1,\ldots,\gamma_n,Y)$$

y $\mathcal{D}_\beta(\gamma_1,\ldots,\gamma_n) \neq 0$. Por el Teorema 2.26 existe $\mathsf{A}_{\beta\gamma} \in \mathbb{K}[a_1,\ldots,a_n]$ de grado a lo sumo $(d-1)(2d-1)$ con la siguiente propiedad: si $(\alpha_1,\ldots,\alpha_n) \in \mathbb{K}^n$ verifica que $\mathsf{A}_{\beta\gamma}(\alpha_1,\ldots,\alpha_n) \neq 0$ entonces el polinomio $h(X,Y) := p_{\beta\gamma}(\alpha_1 X,\ldots,\alpha_n X, Y)$ es irreducible. Observemos que en realidad $h(X,Y) = p(\alpha_1 X + \beta_1 Y + \gamma_1,\ldots,\alpha_n X + \beta_n Y + \gamma_n)$. Por lo tanto

$$\begin{aligned}\mathcal{B}(p) \subset \mathbb{K}^n \times \{\beta \in \mathbb{K}^n \;\mid\; p_d(\beta) = 0\} \times \mathbb{K}^n \\ \cup\; \mathbb{K}^n \times \left\{(\beta,\gamma) \in \mathbb{K}^{2n} \;\mid\; p_d(\beta) \neq 0,\;\; \mathcal{D}_\beta(\gamma) = 0\right\} \\ \cup\; \left\{(\alpha,\beta,\gamma) \in \mathbb{K}^{3n} \;\mid\; p_d(\beta) \neq 0,\;\; \mathcal{D}_\beta(\gamma) \neq 0,\;\; \mathsf{A}_{\beta\gamma}(\alpha) = 0\right\}.\end{aligned}$$

Notando

$$\begin{aligned}\mathcal{A} = \mathcal{S}^n \times \{\beta \in \mathcal{S}^n \;\mid\; p_d(\beta) = 0\} \times \mathcal{S}^n \\ \mathcal{B} = \mathcal{S}^n \times \left\{(\beta,\gamma) \in \mathcal{S}^{2n} \;\mid\; p_d(\beta) \neq 0,\;\; \mathcal{D}_\beta(\gamma) = 0\right\} \\ \mathcal{C} = \left\{(\alpha,\beta,\gamma) \in \mathcal{S}^{3n} \;\mid\; p_d(\beta) \neq 0,\;\; \mathcal{D}_\beta(\gamma) \neq 0,\;\; \mathsf{A}_{\beta\gamma}(\alpha) = 0\right\},\end{aligned}$$

se verifica

$$\mathcal{B}(p) \cap \mathcal{S}^{3n} \subset \mathcal{A} \cup \mathcal{B} \cup \mathcal{C}.$$

Luego,

$$|\mathcal{B}(p) \cap \mathcal{S}^{3n}| \leq |\mathcal{A}| + |\mathcal{B}| + |\mathcal{C}|$$

Aplicando Zippel-Schwartz a p_d, $\mathcal{D}_\beta$ y a $\mathsf{A}_{\beta\gamma}$ obtenemos:

$$|\mathcal{A}| \leq d|\mathcal{S}|^{3n-1}$$

$$|\mathcal{B}| \leq d(d-1)|\mathcal{S}|^{3n-1}$$

$$|\mathcal{C}| \leq (2d-1)(d-1)|\mathcal{S}|^{3n-1},$$

y por lo tanto concluimos

$$\mathcal{B}(p,\mathcal{S}) \leq \frac{3d(d-1)+1}{|\mathcal{S}|}.$$

□

Corolario 2.34. *Sea $f \in \mathbb{F}_q[X_1,\ldots,X_n]$ absolutamente irreducible de grado positivo d y supongamos que la característica de $\mathbb{F}_q$ es mayor o igual a $d(d-1)+1$. Notamos como $f_{\gamma\alpha\beta}$ al siguiente polinomio:*

$$f_{\gamma\alpha\beta}(X,Y) = f(\gamma_1 + \alpha_1 X + \beta_1 Y,\ldots,\gamma_n + \alpha_n X + \beta_n Y).$$

Se verifica entonces

$$|\left\{(\gamma,\alpha,\beta) \in \mathbb{F}_q^{3n} \,|\, f_{\gamma\alpha\beta} \;\; \textit{no es absolutamente irreducible}\right\}| \leq (3d(d-1)+1)q^{3n-1}.$$

Demostración. Aplicamos el Corolario 2.33 con $\mathbb{K} = \overline{\mathbb{F}_q}$ y $\mathcal{S} = \mathbb{F}_q$. Por hipótesis f es

irreducible en $\overline{\mathbb{F}}_q[X_1, \ldots, X_n]$. Notamos al conjunto de puntos que no son de Bertini para f en $\overline{\mathbb{F}}_q^{3n}$ como $\mathcal{B}(f)$. Por lo tanto se tiene que $(\gamma, \alpha, \beta) \in \mathcal{B}(f)$ si el polinomio $f_{\gamma\alpha\beta}$ no es irreducible en $\overline{\mathbb{F}}_q[X, Y]$. Por el Corolario 2.33 tenemos la estimación

$$|\mathcal{B}(f) \cap \mathbb{F}_q^{3n}| \leq (3d(d-1)+1)q^{3n-1}.$$

Ahora observemos que

$$\left\{(\gamma, \alpha, \beta) \in \mathbb{F}_q^{3n} \,|\, f_{\gamma\alpha\beta} \text{ no es absolutamente irreducible}\right\} \subset \mathcal{B}(f) \cap \mathbb{F}_q^{3n},$$

de lo que se deduce lo que queríamos probar. □

Capítulo 3

Estimación sobre la cantidad de ceros q-racionales de un polinomio absolutamente irreducible

En este capítulo probaremos una estimación sobre la cantidad de ceros q-racionales de un polinomio absolutamente irreducible. Seguiremos el trabajo de [CM06] con algunas modificaciones que provienen de utilizar la versión del Teorema de Bertini desarrollada en el capítulo anterior. Esto último nos permitirá obtener una mejora en las estimaciones. Previamente proporcionaremos algunas cotas superiores para la cantidad de puntos q-racionales de una variedad y resultados relacionados con el número promedio de ceros en $\mathbb{F}_q^n$.

3.1. Número promedio de ceros en $\mathbb{F}_q^n$

Una cantidad de resultados de álgebra se basan en el hecho de encontrar elementos de un cuerpo dado que no anulen a un cierto polinomio. Cuando trabajamos con cuerpos infinitos esto siempre es posible, pero en el caso de cuerpos finitos puede no ocurrir. Por ejemplo si consideramos en $\mathbb{F}_5[X]$ el polinomio $f(X) = X^5 - X$, resulta $f(x) = 0$ para todo x en $\mathbb{F}_5$. Esto se debe a que en cuerpo finitos un polinomio no nulo puede inducir la función nula. En esta sección revisaremos algunos resultados relacionados con la existencia de ceros q-racionales de un polinomio.

Proposición 3.1. *[CM06, Lema 2.1] Sea V una $\mathbb{F}_q$-variedad de dimensión $r \geq 0$ y grado δ. Entonces se satisface la siguiente desigualdad*

$$|V \cap \mathbb{F}_q^n| \leq \delta q^r.$$

Demostración. Consideramos las siguientes $\mathbb{F}_q$-variedades

$$\begin{aligned} V_1 &= \{x \in \overline{\mathbb{F}_q}^n \,:\, X_1^q - X_1 = 0\} \\ &\vdots \\ V_n &= \{x \in \overline{\mathbb{F}_q}^n \,:\, X_n^q - X_n = 0\}. \end{aligned}$$

El grado de V es δ y el grado de cada V_i es q, por otra parte se verifica la siguiente igualdad:

$$\left|V \cap \mathbb{F}_q^n\right| = |V \cap V_1 \cap \cdots \cap V_n|.$$

Dado que $V \cap V_1 \cap \cdots \cap V_n$ tiene finitos puntos, resulta ser una variedad de dimensión cero y por lo tanto su grado coincide con el cardinal de la misma. De esta forma se obtiene

$$\left|V \cap \mathbb{F}_q^n\right| = \deg(V \cap V_1 \cap \cdots \cap V_n).$$

Finalmente de la desigualdad de Bézout y de la Proposición 1.13 deducimos la estimación buscada:

$$\left|V \cap \mathbb{F}_q^n\right| \leq \deg V q^r = \delta \cdot q^r.$$

□

Observación 3.2. Notemos que en el caso en que $r = n - 1$, es decir cuando V es una hipersuperficie definida por un polinomio $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ de grado δ, el resultado anterior implica que la cantidad de ceros de f en $\mathbb{F}_q^n$ es a lo sumo δq^{n-1}.

Corolario 3.3. *Sea $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ un polinomio no nulo de grado d. Si $q > d$ entonces existe $x \in \mathbb{F}_q^n$ tal que $f(x) \neq 0$.*

Demostración. Por la Proposición 3.2 f tiene a los sumo $d \cdot q^{n-1}$ ceros en $\mathbb{F}_q^n$. Como $q > d$, la cantidad de elementos de $\mathbb{F}_q^n$ es mayor que la cantidad de ceros de f en $\mathbb{F}_q^n$. Por lo tanto debe existir $x \in \mathbb{F}_q^n$ tal que $f(x) \neq 0$. □

Observación 3.4. Notemos que la condición $q > d$ puede ser desmedida. Por ejemplo, consideremos el polinomio $f(X, Y, Z) = X^2 \cdot Y^3 \cdot Z^2 + 1$ en $f \in \mathbb{F}_5[X, Y, Z]$. En este caso $q = 5$ y $d = 6$ con lo cual no se verifica la condición $q > d$, sin embargo existen elementos de $\mathbb{F}_5^3$ que no lo anulan (por ejemplo $(1, 1, 1)$).

Proposición 3.5. *Sea V una $\mathbb{F}_q$-variedad de dimensión $r \geq 0$ y grado δ. Entonces se satisface la siguiente desigualdad*

$$|V \cap (\mathbb{F}_q^*)^n| \leq \delta(q-1)^r.$$

Demostración. La demostración es análoga a la de la Proposición 3.2, considerando las variedades

$$V_i = \{x \in \overline{\mathbb{F}_q}^n \,:\, X_i^{q-1} - 1 = 0\},$$

para $i \in \{1, \ldots, r\}$. □

Podemos obtener un resultado similar al de la Observación 3.2 pero considerando los ceros de f en $(\mathbb{F}_q^*)^n$, es decir con coordenadas no nulas.

Observación 3.6. Sea $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ un polinomio no nulo de grado d. Entonces se satisface la siguiente estimación

$$|\left\{x \in (\mathbb{F}_q^*)^n \,:\, f(x) = 0\right\}| \leq d \cdot (q-1)^{n-1}.$$

Proposición 3.7. *Sean $f, g \in \mathbb{F}_q[X_1, \ldots, X_n]$ polinomios no nulos y coprimos, de grados d_1 y d_2 respectivamente. Entonces se verifica la siguiente cota superior:*

$$|\left\{x \in \mathbb{F}_q^n : f(x) = g(x) = 0\right\}| \leq d_1 d_2 q^{n-2}.$$

Demostración. Definimos la variedad $V = \left\{x \in \overline{\mathbb{F}_q}^n \,:\, f(x) = g(x) = 0\right\}$. De la desigualdad de Bézout obtenemos que $\deg V \leq d_1 d_2$. Notamos $N = |V \cap \mathbb{F}_q^n|$. Podemos suponer que $N > 0$ y que d_1 y d_2 son positivos. Dado que f y g son coprimos la dimensión de V es menor o igual a $n-2$. Luego se verifica la siguiente igualdad

$$\left\{x \in \mathbb{F}_q^n : f(x) = g(x) = 0\right\} = V \cap V_1 \cap \cdots \cap V_n,$$

donde $V_1, \ldots, V_n$ denotan las variedades de la Observación 3.2. Cada V_i tiene grado igual a q y el grado de $V \cap V_1 \cap \cdots \cap V_n$ es igual a la cantidad de puntos de la misma pues es una variedad de dimensión cero. Finalmente de la Proposición 1.13 se deduce

$$N \leq \deg V q^{\dim V} \leq d_1 d_2 q^{n-2}.$$

□

A continuación damos una cota para la cantidad de ceros con alguna coordenada nula o con algún par de coordenadas iguales. Este resultado será utilizado en el capítulo siguiente para obtener la estimación del teorema principal.

Proposición 3.8. *Sea $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ un polinomio irreducible de grado d y sea $\overline{N}(f)$ la cantidad de ceros de f en $\mathbb{F}_q^n$ con alguna coordenada nula o algún par de coordenadas iguales. Se verifica la siguiente cota superior:*

$$\overline{N}(f) \leq \frac{n(n+1)}{2} d q^{n-2}$$

Demostración. Sea H_1 la $\mathbb{F}_q$-hipersuperficie que define el polinomio $\prod_{i=1}^n X_i \prod_{i \neq j} (X_i - X_j)$ y H_2 la $\mathbb{F}_q$-hipersuperficie que define f. Sus grados son $\frac{n(n+1)}{2}$ y d respectivamente. Luego, por la desigualdad de Bézout obtenemos

$$\deg(H_1 \cap H_2) \leq \frac{n(n+1)}{2} d.$$

Notemos que podemos asumir que f no es asociado con X_i para $i \in \{1, \ldots, n\}$, ni a $X_i - X_j$ para $i \neq j$, ya que si no el resultado se verifica trivialmente. Luego la dimensión de la

variedad $H_1 \cap H_2$ es $n-2$ pues f y el polinomio que define a H_1 son coprimos. Nos interesa dar una cota superior para $|(H_1 \cap H_2) \cap \mathbb{F}_q^n|$. Aplicando entonces [HS82] deducimos que

$$|(H_1 \cap H_2) \cap \mathbb{F}_q^n| \leq \frac{n(n+1)}{2} d q^{n-2},$$

lo que concluye la demostración. □

Proposición 3.9 (Número promedio de ceros de un polinomio)**.** *Sea d un entero positivo y sea Ω_d el conjunto de los polinomios en $\mathbb{F}_q[X_1, \ldots, X_n]$ de grado a lo sumo d. Consideramos $f \in \Omega_d$ y notamos como $N(f)$ el número de ceros de f en $\mathbb{F}_q^n$. Se verifica entonces la siguiente identidad:*

$$\frac{1}{|\Omega_d|} \sum_{f \in \Omega_d} N(f) = q^{n-1}.$$

Demostración. Fijemos $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ y contemos la cantidad de polinomios en Ω_d para los cuales a es raíz. Dado un polinomio $g \in \Omega_d$ este se puede escribir como

$$g(X) = \sum_{(i_1,\ldots,i_n) \in \omega_d} b_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}$$

donde ω_d es el conjunto de las n-uplas de enteros no negativos $(i_1, \ldots, i_n)$ cumpliendo $i_1 + \cdots + i_n \leq d$. Si a es raíz de g entonces a verifica la identidad

$$\sum_{(i_1,\ldots,i_n) \in \omega_d} b_{i_1,\ldots,i_n} a_1^{i_1} \cdots a_n^{i_n} = 0,$$

que resulta una ecuación con $|\omega_d|$ incógnitas $b_{i_1,\ldots,i_n}$. Se deduce entonces que existen $q^{|\omega_d|-1}$ polinomios distintos, para los cuales a es raíz. Luego, podemos escribir

$$\begin{aligned}
\sum_{f \in \Omega_d} N(f) &= \sum_{f \in \Omega_d} \sum_{\substack{x \in \mathbb{F}_q^n \\ f(x)=0}} 1 \\
&= \sum_{x \in \mathbb{F}_q^n} \sum_{\substack{f \in \Omega_d \\ f(x)=0}} 1 \\
&= \sum_{x \in \mathbb{F}_q^n} q^{|\omega_d|-1} \\
&= q^n q^{|\omega_d|-1},
\end{aligned}$$

como $|\Omega_d| = q^{|\omega_d|}$ obtenemos

$$\sum_{f \in \Omega_d} N(f) = q^{n-1} |\Omega_d|,$$

lo que concluye la demostración. □

Observación 3.10. De manera similar se puede probar que el número promedio de ceros

con coordenadas no nulas de un polinomio f de grado d es

$$\frac{1}{|\Omega_d|}\sum_{f\in\Omega_d} N^*(f) = \frac{(q-1)^n}{q},$$

donde $N^*(f)$ denota los ceros de f en $(\mathbb{F}_q^*)^n$.

Observación 3.11. Dado un polinomio $f \in \mathbb{F}_q[X_1,\ldots,X_n]$, puede ocurrir que la cantidad de ceros del mismo difiera bastante del número promedio. Por ejemplo si consideramos el polinomio $f(X,Y) = X^4 + Y^4 - 2 \in \mathbb{F}_5[X,Y]$ el número promedio de ceros es $q = 5$, mientras que la cantidad de ceros de f es 16.

Sabemos que la cantidad promedio de ceros de un polinomio de $\mathbb{F}_q[X_1,\ldots,X_n]$ de grado a lo sumo d es q^{n-1}. A continuación presentaremos un resultado que permite obtener una expresión de la desviación de este promedio.

Proposición 3.12. *Considerando las notaciones del Teorema 3.9 se tiene la siguiente igualdad:*

$$\frac{1}{|\Omega_d|}\sum_{f\,\in\,\Omega_d} (N(f) - q^{n-1})^2 = q^{n-1} - q^{n-2}.$$

Demostración. Fijamos $b = (b_1,\ldots,b_n) \in \mathbb{F}_q^n$ y $c = (c_1,\ldots,c_n) \in \mathbb{F}_q^n$. Se tiene

$$\begin{aligned}
\sum_{f\,\in\,\Omega_d} N(f)^2 &= \sum_{f\,\in\,\Omega_d} \Big(\sum_{\substack{c\,\in\,\mathbb{F}_q^n\\ f(c)=0}} 1\Big)^2 \\
&= \sum_{f\,\in\,\Omega_d} \sum_{\substack{b\,\in\,\mathbb{F}_q^n\\ f(b)=0}} \sum_{\substack{c\,\in\,\mathbb{F}_q^n\\ f(c)=0}} 1 \\
&= \sum_{b,c\,\in\,\mathbb{F}_q^n} \sum_{\substack{f\,\in\,\Omega_d\\ f(b)=f(c)=0}} 1.
\end{aligned}$$

Si $b = c$ vimos en la demostración del Teorema 3.9 que el valor de la suma interna es $q^{|\omega_d|-1}$. Por otra parte, si $b \neq c$ entonces de la condición $f(b) = f(c) = 0$ se obtiene un sistema de dos ecuaciones lineales de rango 2 cuyas incógnitas son los coeficientes de f. Por lo tanto, tenemos $q^{|\omega_d|-2}$ soluciones. De esto se deduce

$$\begin{aligned}
\sum_{f\,\in\,\Omega_d} N(f)^2 &= \sum_{c\,\in\,\mathbb{F}_q^n} |\Omega_d| q^{-1} + \sum_{\substack{b,c\,\in\,\mathbb{F}_q^n\\ b\neq c}} |\Omega_d| q^{-2} \\
&= q^n |\Omega_d| q^{-1} + q^n(q^n-1)|\Omega_d| q^{-2} \\
&= |\Omega_d|(q^{2n-2} + q^{n-1} - q^{n-2}).
\end{aligned}$$

De esta última igualdad y el Teorema 3.9 obtenemos

$$\begin{aligned}\sum_{f\in\Omega_d}(N(f)-q^{n-1})^2 &= \sum_{f\in\Omega_d}N(f)^2-2q^{n-1}\sum_{f\in\Omega_d}N(f)+q^{2n-2}\sum_{f\in\Omega_d}1\\ &= |\Omega_d|(q^{2n-2}+q^{n-1}-q^{n-2})-2q^{n-1}|\Omega_d|q^{n-1}+q^{2n-2}|\Omega_d|\\ &= |\Omega_d|(q^{n-1}-q^{n-2}),\end{aligned}$$

lo que concluye la demostración. □

Este teorema establece que el valor promedio de $(N(f)-q^{n-1})^2$ es del orden $\mathcal{O}(q^{n-1})$. Es de esperar entonces que a menudo se verifique $N(f)-q^{n-1}=\mathcal{O}(q^{\frac{n-1}{2}})$. En particular, esto se alcanza para el caso de curvas absolutamente irreducibles como muestra el teorema de Weil (Teorema 3.13).

Las estimaciones sobre la cantidad de ceros q-racionales de un polinomio absolutamente irreducible se apoyan en un resultado fundamental de A.Weil para curvas sobre cuerpos finitos. Weil obtuvo la siguiente estimación

Teorema 3.13. *[Wei48] Sea $f(X,Y)$ un polinomio de $\mathbb{F}_q[X,Y]$ absolutamente irreducible de grado $d>0$. Sea N el número de ceros de f en $\mathbb{F}_q^2$. Entonces se verifica que*

$$|N-q|\leq\omega(q,d), \tag{3.1}$$

donde $\omega(q,d)=(d-1)(d-2)q^{\frac{1}{2}}+d+1$.

En particular, para polinomios absolutamente irreducibles de $\mathbb{F}_q[X,Y]$, este resultado nos da una cota para el error que se comete al estimar la cantidad de ceros q-racionales con el número promedio de ceros. Existen polinomios para los cuales se verifica la igualdad en (3.1), ejemplos de ello se pueden ver en [Gar95].

3.2. Estimación sobre los ceros q-racionales de f

Definición 3.14. Sea V una $\mathbb{F}_q$-variedad y $x\in V\cap\mathbb{F}_q^n$. Llamaremos a x un **punto q-racional de V**.

Observación 3.15. Es fácil exhibir $\mathbb{F}_q$-variedades que no poseen puntos q-racionales. Por ejemplo, consideramos la $\mathbb{F}_5$-hipersuperficie definida por el polinomio $f(X,Y)=X^2-2(XY+1)^2$. Notemos que f admite la factorización $f(X,Y)=(X-\sqrt{2}(XY+1))\cdot(X+\sqrt{2}(XY+1))$ en $\mathbb{F}_5(\sqrt{2})[X,Y]$. Luego si $(x,y)\in\mathbb{F}_5^2$ es un cero de f, tenemos que $x=0$, lo que implica que $\sqrt{2}(x\cdot y+1)\neq 0$. Por lo tanto la hipersuperficie no tiene puntos en $\mathbb{F}_5$.

Sea L una $\mathbb{F}_q$-variedad lineal de dimensión 2. Entonces esta puede ser parametrizada de la siguiente manera:

$$\begin{cases} X_1=\gamma_1+\alpha_1X+\beta_1Y\\ \vdots\\ X_n=\gamma_n+\alpha_nX+\beta_nY\end{cases}$$

con $\alpha = (\alpha_1, \ldots, \alpha_1)$, $\beta = (\beta_1, \ldots, \beta_1)$ y $\gamma = (\gamma_1, \ldots, \gamma_1)$ elementos de $\mathbb{F}_q^n$ y α y β linealmente independientes.

Notaremos como M_2 al conjunto de las $\mathbb{F}_q$-variedades lineales de dimensión 2. Dados $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ y $L \in M_2$, definimos el polinomio $f_L \in \mathbb{F}_q[X, Y]$ como

$$f_L(X, Y) := f(\gamma_1 + \alpha_1 X + \beta_1 Y, \ldots, \gamma_n + \alpha_n X + \beta_n Y).$$

Observación 3.16. Notemos que para cada variedad L el polinomio f_L está bien definido salvo un cambio de coordenadas lineales sobre $\mathbb{F}_q$. Por lo tanto tiene sentido referirse al grado de f_L y a la absoluta irreducibilidad del mismo ([Sch76]).

Para deducir nuestra estimación recurriremos al teorema de A.Weil para polinomios bivariados absolutamente irreducibles sobre cuerpos finitos. Es por esto que debemos distinguir los casos en los que f_L sea absolutamente irreducible o no. Si f_L no es absolutamente irreducible podría ocurrir que f_L sea el polinomio nulo, un ejemplo sencillo de esto se obtiene considerando $f(X_1, X_2, X_3) = X_1 + X_2 - X_3$ en $\mathbb{F}_5[X_1, X_2, X_3]$ y la variedad L parametrizada por: $(X_1, X_2, X_3) = \gamma + \alpha \cdot X + \beta \cdot Y$ con $\alpha = (1, 0, 1)$, $\beta = (4, 2, 1)$, $\gamma = (3, 2, 0)$.

De acuerdo con la versión del Teorema de Bertini que utilizaremos, debemos considerar la condición sobre la característica: $p > d(d-1) + 1$. Luego si f_L no es el polinomio nulo, como $q > d$, f_L no induce la función nula. En otras palabras, no tiene q^2 ceros. Distinguiremos entonces los siguientes situaciones:

(i) $f_L(X, Y)$ es absolutamente irreducible.

(ii) $f_L(X, Y)$ no es absolutamente irreducible y no es el polinomio nulo.

(iii) $f_L(X, Y)$ es el polinomio nulo.

Luego estan bien definidos los siguientes números:

1. $A = |M_2|$
2. $B = |\{L \in M_2 \mid f_L \text{ no es absolutamente irreducible y no es el polinomio nulo}\}|$
3. $C = |\{L \in M_2 \mid f_L \text{ es el polinomio nulo}\}|$.

A continuación veremos una serie de lemas que nos permitirán probar el resultado principal del capítulo. En dichos lemas exhibiremos cotas superiores para las proporciones: $\frac{B}{A}$ y $\frac{C}{A}$. Comenzamos calculando el valor de A.

Lema 3.17. *Se verifica*

$$A = \frac{q^n(q^n - 1)(q^n - q)}{q^2(q^2 - q)(q^2 - 1)}.$$

Demostración. Dado que los vectores $\alpha = (\alpha_1, \ldots, \alpha_n)$ y $\beta = (\beta_1, \ldots, \beta_n)$ deben ser linealmente independientes, la cantidad de parametrizaciones para elementos de M_2 es

$$q^n(q^n - 1)(q^n - q).$$

Por otro lado diferentes parametrizaciones pueden definir una misma variedad L. Un $\mathbb{F}_q$-subespacio de dimensión 2 posee q^2 vectores, luego tenemos q^2-1 posibilidades de elegir un vector no nulo del mismo. Dado un vector fijo del subespacio, este tiene q múltiplos; por lo tanto un $\mathbb{F}_q$-subespacio de dimensión 2 admite $(q^2-1)(q^2-q)$ parametrizaciones distintas. Cocluimos entonces que dada una variedad en M_2 esta posee

$$q^2(q^2-1)(q^2-q)$$

parametrizaciones distintas, lo que implica que

$$A = \frac{q^n(q^n-1)(q^n-q)}{q^2(q^2-q)(q^2-1)}.$$

□

Lema 3.18. *Sea $f \in \mathbb{F}_q[X_1,\ldots,X_n]$ un polinomio absolutamente irreducible de grado $d>0$ y $p \geq d(d-1)+1$. Se satisface la siguiente estimación:*

$$\frac{B}{A} \leq \frac{6d^2-6d+2}{q}.$$

Demostración. El conjunto de los $(\gamma,\alpha,\beta) \in \mathbb{F}_q^{3n}$ que parametrizan una $\mathbb{F}_q$-variedad lineal de dimensión 2 sobre la cual f_L no es absolutamente irreducible está contenido en el siguiente conjunto:

$$\{(\gamma,\alpha,\beta) \in \mathbb{F}_q^{3n} \mid f(\gamma_1+\alpha_1X+\beta_1Y,\ldots,\gamma_n+\alpha_nX+\beta_nY) \text{ no es absolutamente irreducible}\}.$$

Luego por el Corolario 2.34 deducimos que

$$\left|\{(\gamma,\alpha,\beta) \in \mathbb{F}_q^{3n} \mid f_L \text{ no es absolutamente irreducible}\}\right| \leq (3d(d-1)+1)q^{3n-1}.$$

Notemos que cada $\mathbb{F}_q$-variedad lineal de dimensión 2 admite $q^2(q^2-q)(q^2-1)$ parametrizaciones distintas, por lo tanto se tiene la siguiente cota superior para B:

$$B \leq \frac{(3d(d-1)+1)q^{3n-1}}{q^2(q^2-q)(q^2-1)}.$$

Luego

$$\frac{B}{A} \leq \frac{(3d(d-1)+1)q^{3n-1}}{q^n(q^n-q)(q^n-1)}.$$

Finalmente utilizando la siguiente cota:

$$\frac{q^{3n}}{2} \leq q^n(q^n-q)(q^n-1)$$

concluimos

$$\frac{B}{A} \leq \frac{6d^2-6d+2}{q}.$$

□

A continuación damos una definición que será de utilidad en los próximos resultados.

Definición 3.19. Sean $\mathbb{K}$ un cuerpo arbitrario, f,$g \in \mathbb{K}[X_1, \ldots, X_n]$. Decimos que f es equivalente a g si existe una matriz $C \in \mathbb{K}^{n\times n}$ inversible y un vector $v \in \mathbb{K}^n$ tal que

$$f(X_1, \ldots, X_n) = g((X_1, \ldots, X_n) \cdot C + v).$$

Lema 3.20. *Sea $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ un polinomio irreducible de grado $d > 0$. Supongamos que f no es equivalente a un polinomio $g \in \mathbb{F}_q[X_1, \ldots, X_{n-2}]$. Se verifica entonces la siguiente acotación:*

$$\frac{C}{A} \leq \frac{d^2}{q^2}.$$

Demostración. Consideramos el subespacio $X_1 = \ldots = X_{n-2} = 0$ de M_2. Existen q^{n-2} variedades lineales de dimensión 2 paralelas a él. Sea $L: \quad X_1 = c_1, \ldots, X_{n-2} = c_{n-2}$ una de ellas, verificando además que f_L es el polinomio nulo. Escribimos a f de la siguiente manera:

$$f(X_1, \ldots, X_n) = \sum_{i,j\in I} f_{ij}(X_1, \ldots, X_{n-2}) X_{n-1}^i X_n^j,$$

con $I \subset \mathbb{N}_0^2$ un subconjunto finito. Afirmamos que los polinomios f_{ij} no pueden tener un factor en común. En efecto si existiera $g \in \mathbb{F}_q[X_1, \ldots, X_{n-2}]$ factor en común entonces g divide a f, luego como f es irreducible se verifica que $f = c \cdot g$ con $c \in \mathbb{F}_q^*$, pero esto es absurdo pues f no es equivalente a un polinomio en $n-2$ variables. Por otra parte como f se anula sobre L entonces se debe cumplir que $f_{ij}(c_1, \ldots, c_{n-2}) = 0 \ \forall i, j \in I$. Como los f_{ij} no tienen factores en común, por la Proposición 3.7 deducimos que

$$|\{c \in \mathbb{F}_q^{n-2} \ \mid \ f_{ij}(c) = 0 \ \ \forall i, j \in I\}| \leq d^2 q^{n-4},$$

por lo tanto existen a lo sumo $d^2 q^{n-4}$ $\mathbb{F}_q$-variedades lineales de dimensión 2 paralelas a $X_1 = \ldots = X_{n-2} = 0$, verificando que la restricción de f a las mismas resulta el polinomio nulo. Notamos con M_0 la cantidad de subespacios distintos de M_2. Repitiendo el razonamiento anterior para cada uno de ellos obtenemos

$$C \leq d^2 q^{n-4} M_0.$$

Finalmente obtenemos

$$\frac{C}{A} \leq \frac{d^2 q^{n-4} M_0}{q^{n-2} M_0} = \frac{d^2}{q^2}.$$

□

Observación 3.21. Notemos que para cada $x \in \mathbb{F}_q$ la cantidad de variedades de M_2 a las que pertenece dicho punto es

$$D = \frac{(q^n - q)(q^n - 1)}{(q^2 - q)(q^2 - 1)},$$

luego se verifica

$$\frac{A}{D} = q^{n-2}.$$

A continuación enunciamos el teorema principal del capítulo.

Teorema 3.22. *Consideremos $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ un polinomio absolutamente irreducible de grado $d > 0$. Supongamos que $p > d(d-1)+1$. Sea $N(f)$ el número de ceros de f en $\mathbb{F}_q^2$, se verifica entonces la siguiente estimación*

$$|N(f) - q^{n-1}| \leq (d-1)(d-2)q^{n-\frac{3}{2}} + 6d^3q^{n-2}.$$

Demostración. Es claro que vale para $n = 1$. Si $n = 2$ se deduce inmediatamente del Teorema de Weil. Suponemos entonces que $n \geq 3$. Por otra parte podemos asumir que f no es equivalente a un polinomio en $n-2$ variables, es decir que no existe un cambio de coordenadas $\mathbb{F}_q$-lineal de forma tal que $f \in \mathbb{F}_q[X_1, \ldots, X_{n-2}]$. Si esto fuera asi, como el número de ceros de f en $\mathbb{F}_q^n$ es igual a $q^2N'(f)$ siendo $N'(f)$ el número de ceros de f en $\mathbb{F}_q^{n-2}$, tendríamos

$$|N(f) - q^{n-1}| = |q^2N'(f) - q^{n-1}| = q^2|N'(f) - q^{n-3}|$$

y podríamos deducir el resultado por inducción en n.

Notamos como $N(f_L)$ al número de ceros de f_L en $\mathbb{F}_q^n$. Por lo tanto se verifica que

$$N(f) = \frac{1}{D}\sum_{L \in M_2} N(f_L),$$

luego como $q^{n-1} = \frac{A}{D} \cdot q$, obtenemos

$$|N(f) - q^{n-1}| = |\frac{1}{D}\sum_{L \in M_2} N(f_L) - \frac{A}{D}.q| \leq \frac{1}{D}\sum_{L \in M_2} |N(f_L) - q|.$$

Definimos los siguientes conjuntos:

$M^1 = \{L \in M_2 \mid f_L \text{ es absolutamente irreducible}\}$

$M^2 = \{L \in M_2 \mid f_L \text{ no es absolutamente irreducible y no es el polinomio nulo}\}$

$M^3 = \{L \in M_2 \mid f_L \text{ es el polinomio nulo}\}$,

entonces con estas notaciones escribimos

$$\frac{1}{D}\sum_{L \in M_2} |N(f_L) - q| = \frac{1}{D}\left(\sum_{L \in M^1} |N(f_L) - q| + \sum_{L \in M^2} |N(f_L) - q| + \sum_{L \in M^3} |N(f_L) - q|\right).$$

Del Teorema de Weil y de la Proposición 3.2 se deduce

$$|N(f_L) - q| \leq \begin{cases} w(q,d) & \text{si } f_L \text{ es absolutamente irreducible} \\ dq & \text{si } f_L \text{ no es absolutamente irreducible y no es el polinomio nulo} \\ q^2 & \text{si } f_L \text{ es el polinomio nulo} \end{cases}$$

y por lo tanto se verifica

$$\begin{aligned}\sum_{L\in M^1}|N(f_L)-q| &\leq w(q,d)A\\ \sum_{L\in M^2}|N(f_L)-q| &\leq dqB\\ \sum_{L\in M^3}|N(f_L)-q| &\leq q^2C.\end{aligned}$$

Entonces

$$\frac{1}{D}\sum_{L\in M_2}|N(f_L)-q|\leq\frac{A}{D}\left(w(q,d)+dq\frac{B}{A}+q^2\frac{C}{A}\right).$$

Por los Lemas 3.18, 3.20 y la Observación 3.21 se tiene:

$$\frac{B}{A}\leq\frac{6d^2-6d+2}{q},\qquad\frac{C}{A}\leq\frac{d^2}{q^2}\qquad\text{y}\qquad\frac{A}{D}=q^{n-2},$$

con lo cual

$$\begin{aligned}\frac{1}{D}\sum_{L\in M_2}|N(f_L)-q| &\leq q^{n-2}\left(w(q,d)+6d^3-5d^2+2d\right)\\ &\leq q^{n-2}\left((d-1)(d-2)q^{\frac{1}{2}}+6d^3-5d^2+2d+d+1\right)\\ &\leq q^{n-2}\left((d-1)(d-2)q^{\frac{1}{2}}+6d^3\right)\\ &= (d-1)(d-2)q^{n-\frac{3}{2}}+6d^3q^{n-2}.\end{aligned}$$

concluyendo así la demostración. □

Observación 3.23. En [CM06], A.Cafure y G.Matera exhiben la siguiente estimación:

$$|N(f)-q^{n-1}|<(d-1)(d-2)q^{n-\frac{3}{2}}+5d^{\frac{13}{3}}q^{n-2},$$

sin imponer condiciones sobre la característica. Hemos mostrado que dicha estimación mejora utilizando la versión del Teorema de Bertini obtenida por Lecerf [Lec07], pero pidiendo que la característica sea $p>d(d-1)+1$.

Vamos a exhibir a continuación una estimación que mejora la dada en el Teorema 3.22, aunque esta es válida bajo una cierta condición de regularidad. Invocamos las notaciones utilizadas a lo largo de todo el capítulo y comenzamos dando algunas definiciones.

Definición 3.24. Sea L una $\mathbb{F}_q$-variedad lineal de dimensión 2. Supongamos que f_L no es el polinomio nulo. Notamos como $\nu(L)$ al número de factores absolutamente irreducibles de f_L en $\mathbb{F}_q[X,Y]$. Luego se verifica que $0\leq\nu(L)\leq d$. Si f_L es el polinomio nulo entonces definimos $\nu(L):=q$.

Definición 3.25. Con las notaciones de la definición anterior, consideramos para cada $j \in \{0, 1, 2, \ldots, d-1\}$ el conjunto

$$\pi_j := \{L \in M_2 \,|\, |\nu(L) - 1| = j\},$$

es decir, si $j \in \{0, 2, \ldots, d-1\}$ entonces π_j es el conjunto de las $\mathbb{F}_q$-variedades lineales de dimensión 2 para las cuales f_L tiene $j+1$ factores absolutamente irreducibles en $\mathbb{F}_q[X, Y]$. Si $j = 1$ y $L \in \pi_1$ entonces f_L tiene 0 ó 2 factores absolutamente irreducibles en $\mathbb{F}_q[X, Y]$. Por último definimos π_{q-1} como el conjunto de las $\mathbb{F}_q$-variedades lineales de dimensión 2 tales que f_L es el polinomio nulo.

Enunciamos un resultado de [Sch74] que utilizaremos para deducir la nueva estimación.

Lema 3.26. *[Sch74, Lema 5] Sea $f \in \mathbb{F}_q[X, Y]$ un polinomio de grado $d > 0$ y sea ν el número de factores absolutamente irreducibles de f en $\mathbb{F}_q[X, Y]$. Entonces el número N de ceros de f en $\mathbb{F}_q^2$ satisface*

$$|N - \nu q| \leq w(q, d) + d^2,$$

donde $w(q, d) := (d-1)(d-2)q^{\frac{1}{2}} + d + 1$.

Teorema 3.27. *Sea $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ un polinomio de grado $d > 0$. Supongamos que la característica de $\mathbb{F}_q$ es mayor o igual a $d(d-1)+1$ y que $q \geq 16d^4$. Entonces se satisface la siguiente estimación*

$$|N(f) - q^{n-1}| \leq (d-1)(d-2)q^{n-\frac{3}{2}} + (d^2 + 5d + 1)q^{n-2}.$$

Demostración. Es claro que la estimación es válida para $d = 1$, supongamos entonces $d \geq 2$. Sea $L \in \pi_j$ con $j > 0$, por lo tanto f_L tiene $(j+1)$ factores absolutamente irreducibles en $\mathbb{F}_q[X, Y]$. Por el Lema anterior se verifica

$$|N(f_L) - (j+1)q| \leq w(q, d) + d^2,$$

siendo $N(f_L)$ la cantidad de ceros de f_L en $\mathbb{F}_q^2$. Por lo tanto se tiene la siguiente cota inferior

$$N(f_L) - q \geq jq - w(q, d) - d^2. \tag{3.2}$$

Utilizando (3.2) y la estimación obtenida en el Teorema 3.22, deducimos

$$\begin{aligned} |N(f_L) - N(f)q^{2-n}| &\geq |N(f_L) - q| - q^{2-n}|N(f) - q^{n-1}| \\ &\geq jq - w(q, d) - d^2 - w(q, d) - 6d^3 \\ &\geq \tfrac{1}{2}jq, \end{aligned}$$

donde esta última desigualdad se satisface si

$$\frac{1}{2}jq \geq 2q^{\frac{1}{2}}(d-1)(d-2) + 2(d+1) + d^2 + 6d^3. \tag{3.3}$$

Para que se verifique la desigualdad (3.3), necesitamos $q \geq 16d^4$. Luego estamos en las

hipótesis del Lema 6 de [Sch74] y por lo tanto se tiene

$$\frac{q^2}{4}\sum_{j=1}^{q-1} j^2|\pi_j| \leq dDq^{n-1},$$

lo que implica que

$$\sum_{j=1}^{q-1} j|\pi_j| \leq 4dDq^{n-3}. \tag{3.4}$$

Por el Lema 3.26, si $j \in \{0,\ldots,d-1\}$ y $L \in \pi_j$, se verifica

$$|N(f_L) - q| \leq w(q,d) + d^2 + jq. \tag{3.5}$$

Finalmente combinando (3.4) y (3.5) obtenemos

$$\begin{aligned}
|N(f) - q^{n-1}| &\leq \frac{1}{D}\sum_{L\in M_2} |N(f_L) - q| \\
&\leq \frac{1}{D}\left(\sum_{j=0}^{d-1}\sum_{L\in\pi_j} |N(f_L) - q| + \sum_{L\in\pi_{q-1}} |N(f_L) - q|\right) \\
&\leq \frac{1}{D}\left(\sum_{j=0}^{d-1}\sum_{L\in\pi_j} (w(q,d) + d^2 + jq) + |\pi_{q-1}|(q^2 - q)\right) \\
&\leq \frac{1}{D}\left(\sum_{j=0}^{d-1}(w(q,d) + d^2 + jq)|\pi_j| + |\pi_{q-1}|(q^2 - q)\right) \\
&\leq \frac{1}{D}\left(\left(\sum_{j=0}^{d-1}|\pi_j|\right)(w(q,d) + d^2) + q\sum_{j=1}^{q-1} j|\pi_j|\right) \\
&\leq \frac{1}{D}\left(A(w(q,d) + d^2) + 4q^{n-2}dD\right) \\
&\leq q^{n-2}(w(q,d) + d^2 + 4d) \\
&\leq q^{n-2}(w(q,d) + 5d^2) \\
&= (d-1)(d-2)q^{n-\frac{3}{2}} + q^{n-2}(d^2 + 5d + 1),
\end{aligned}$$

lo que concluye la demostración. □

Observación 3.28. Consideremos el cuerpo primo $\mathbb{F}_p$, en esta tesina logramos dar una mejor estimación para la cantidad de ceros q-racionales de un polinomio absolutamente

irreducible de grado d, en los casos en los que $d^2 < p < d^4$.

En lo siguiente enunciaremos un resultado de existencia de ceros en $\mathbb{F}_q^n$ de un polinomio absolutamente irreducible.

Teorema 3.29. *[CM06, Teorema 5.4] Si $q > 2d^4$ y $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ es un polinomio absolutamente irreducible de grado $d > 0$, entonces f tiene al menos un cero en $\mathbb{F}_q^n$.*

Demostración. Sea f un polinomio absolutamente irreducible de grado $d > 0$. Como $q > 2d^4$ por el Corolario 2.34 sabemos que existe $(\gamma, \alpha, \beta) \in \mathbb{F}_q^{3n}$ tal que el polinomio $f_L(X, Y) := f(\gamma_1 + \alpha_1 X + \beta_1 Y, \ldots, \gamma_n + \alpha_1 X + \beta_n Y)$ es absolutamente irreducible. Luego por la estimación de Weil sabemos que f_L tiene al menos $q - (d-1)(d-2)q^{n-\frac{1}{2}} - d - 1$ ceros en $\mathbb{F}_q^2$. Para que este número sea positivo necesitamos tomar $q > 2d^4$. Finalmente entonces bajo esta condición sobre q podemos garantizar que f tiene al menos un cero en $\mathbb{F}_q^n$. □

Observación 3.30. Mediante una mejor versión del Teorema de Bertini desarrollada en esta tesina pudimos mejorar la estimación de la cantidad de ceros q-racionales de un polinomio absolutamente irreducible, obtenida en [CM06], pero no se logra mejorar el resultado de existencia.

Capítulo 4

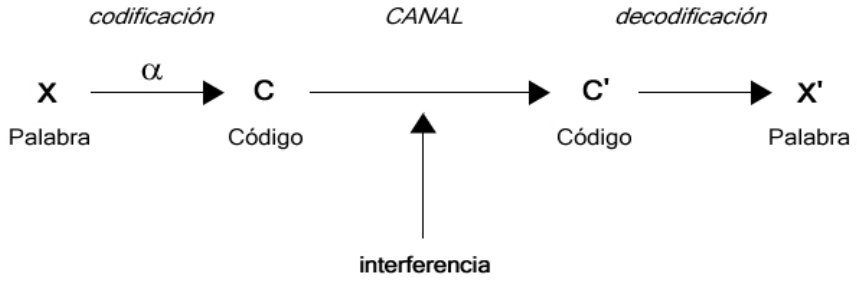
Aplicaciones a la Teoría de Códigos

En este capítulo presentaremos las definiciones y resultados básicos de la Teoría de Códigos de Reed-Solomon. La idea es hacerlo a modo ilustrativo para tener noción del contexto en el que vamos a trabajar. El problema de códigos que trataremos es el de determinar si una palabra recibida es o no un *deep hole*. Q. Cheng y E. Murray, siguiendo el trabajo de [CM06], traducen este problema al de determinar si una hipersuperficie absolutamente irreducible posee puntos q-racionales con coordenadas distintas y no nulas. Nuestro objetivo es, basándonos en el trabajo de Q. Cheng y E. Murray [CM07] y en las estimaciones del capítulo anterior, presentar una caracterización más precisa acerca de cuando una palabra recibida es un deep hole.

4.1. Generalidades sobre Códigos

Un **alfabeto** $\mathcal{A}$ es un conjunto finito de símbolos. Una palabra es una sucesión finita de elementos de $\mathcal{A}$. Un *códigos lineal* es un subespacio de $\mathbb{F}_q^n$. Debido a esto la codificación y decodificación resultan más prácticas y eficientes. La situación que se presenta en general es la siguiente. Supongamos que queremos transmitir una palabra a través de un canal de comunicación. En primer lugar se hace una traducción entre la palabra original: x (o palabra fuente) y el tipo de mensaje c que el canal está capacitado para enviar (palabra código). Este proceso se llama codificación. Una vez codificada, la palabra se envía a través del canal y el receptor recibe la palabra codificada y posiblemente errónea, ya que en todo el proceso de comunicación hay ruido e interferencias. La palabra recibida c' es decodificada obteniendo así x'. Puede verse todo el proceso resumido en el Esquema 1.

Puede ocurrir que $x \neq x'$, en estos casos se quiere poder detectar el error y en lo posible corregirlo. La teoría de códigos auto-correctores se ocupa de la codificación y decodificación junto con el problema de detectar y corregir errores. Un código se dice que no detecta errores si al haber un error en la transmisión la palabra recibida es otra palabra del código. Por ejemplo si consideramos $\mathcal{C} = \{00, 01, 10, 11\}$ y la palabra transmitida es 00, si cometemos un error en la transmisión recibimos $01, 10$ que son elementos del código.



Esquema 1. Proceso de transmisión de mensaje.

En lo que sigue formalizaremos estas ideas, y nos concentraremos en los códigos de Reed-Solomon. Trabajaremos con $\mathbb{F}_q$ un cuerpo finito de característica p.

Sea $n \leq q$, fijamos un subconjunto $\mathcal{D} = \{x_1, x_2, \ldots, x_n\}$ contenido en $\mathbb{F}_q$ al que denominaremos **conjunto de evaluación**. Consideramos un entero positivo k menor o igual a n, y la siguiente transformación lineal:

$$\alpha : \mathbb{F}_q^k \to \mathbb{F}_q^n \mid \quad \alpha(a_0, \ldots, a_{k-1}) = (f(x_1), \ldots, f(x_n)),$$

donde $f(X) = a_{k-1}X^{k-1} + \cdots + a_1X + a_0 \in \mathbb{F}_q[X]$. La función α es la función de **codificación**, $(a_0, \ldots, a_{k-1})$ es la palabra o mensaje a codificar y $(f(x_1), \ldots, f(x_n))$ es la palabra o mensaje codificado.

Observación 4.1. Es sencillo probar que α es monomorfismo. Luego dos palabras distintas tienen distintas codificaciones. Por lo tanto la imagen de α es un subespacio de dimensión k de $\mathbb{F}_q^n$.

Definición 4.2. Con las notaciones anteriores, se denomina un **código de Reed-Solomon** de longitud n y dimensión k al subespacio imagen de α, y lo notamos como $\mathcal{C}_q(\mathcal{D}, k)$. En otras palabras, un código de Reed-Solomon $\mathcal{C}_q(\mathcal{D}, k)$ de longitud n y dimensión k sobre $\mathbb{F}_q$ es:

$$\mathcal{C}_q(\mathcal{D}, k) = \{(f(x_1), f(x_2), \ldots, f(x_n)) \in \mathbb{F}_q^n \mid f(x) \in \mathbb{F}_q[X], \deg f \leq k-1\}.$$

Sus elementos se llaman **códigos** o **palabras código**.

Notemos entonces que los códigos de Reed-Solomon son lineales.

Definición 4.3. Sean $\mathcal{C}$ un código de Reed-Solomon, $c \in \mathcal{C}$ y un polinomio $f \in \mathbb{F}_q[X]$. Decimos entonces que c es generado por f si se verifica que $c = (f(x_1), \ldots, f(x_n))$.

Observación 4.4. La matriz de α en las bases canónicas de $\mathbb{F}_q^k$ y $\mathbb{F}_q^n$ es la siguiente matriz:

$$[\alpha]_E = \begin{pmatrix} 1 & x_1 & \cdots & x_1^{k-1} \\ 1 & x_2 & \cdots & x_2^{k-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & x_n & \cdots & x_n^{k-1} \end{pmatrix}.$$

Como α es monomorfismo el rango de esta matriz es k. Por otro lado observemos que para codificar una palabra $a = (a_1, \ldots, a_{k-1})$ debemos hacer el producto $[\alpha]_E \cdot a$.

Supongamos que hemos recibido una palabra B que no es un elemento del código. Para su decodificación trataremos de encontrar el elemento del código más cercano a B. Es por esto que necesitamos tener una noción de distancia en $\mathcal{C}$.

Definición 4.5. Dados x, $y \in \mathbb{F}_q^n$ se define la **distancia de Hamming** entre x e y como la cantidad de coordenadas en las que difieren. Es decir,

$$d(x,y) := |\{i : \quad x_i \neq y_i, \quad 1 \leq i \leq n\}|.$$

A continuación definiremos la **distancia mínima de un código**. Este concepto es importante a la hora de determinar la capacidad que tiene el código para corregir errores.

Definición 4.6. Sea $\mathcal{C}$ un código de Reed-Solomon, definimos la **distancia mínima de** $\mathcal{C}$ como:

$$d(\mathcal{C}) := \text{mín}\{d(w,t) \quad | \quad w \neq t, \quad w,t \in \mathcal{C}\}.$$

Definición 4.7. Sea $u \in \mathbb{F}_q^n$. Definimos la distancia de u al código como

$$d(u,\mathcal{C}) := \min_{c \in \mathcal{C}}\{d(u,c)\}.$$

Observemos que dado $u \in \mathbb{F}_q^n$, u es un elemento del código si y solo si $d(u,\mathcal{C}) = 0$.

Proposición 4.8. *Sea $\mathcal{C}_q(\mathcal{D},k)$ un Código de Reed-Solomon de longitud n y dimensión k. Se verifica que la distancia mínima es $n-k+1$.*

Demostración. Para simplificar la escritura notamos $\mathcal{C} = \mathcal{C}_q(\mathcal{D},k)$. Primero veamos que $d(\mathcal{C}) \geq n-k+1$. Supongamos que w y t son dos elementos del código que coinciden en k o más coordenadas. Consideremos los polinomios $w(X)$ y $t(X)$ que generan a w y a t, respectivamente. Por lo tanto obtenemos que el polinomio $r(X) = w(X) - t(X)$ tiene al menos k raíces, lo que es absurdo pues su grado es menor o igual a $k-1$.

Por otro lado consideramos $x_1, \ldots, x_{k-1}$ elementos distintos en $\mathcal{D}$ y definimos el siguiente polinomio en $\mathbb{F}_q[X]$:

$$w(X) = (X - x_1)\ldots(X - x_{k-1}).$$

Si w es la palabra que genera $w(X)$, se verifica que la distancia entre el código nulo y w es $n-k+1$. Concluimos entonces que $d(\mathcal{C}) = n-k+1$. □

Definición 4.9. Sea $\mathcal{C}$ un código de Reed-Solomon. Definimos el **radio de recubrimiento** de $\mathcal{C}$ como

$$\rho := \max_{y \in \mathbb{F}_q^n}\{\min_{c \in \mathcal{C}} d(y,c)\} = \max_{y \in \mathbb{F}_q^n} d(y,\mathcal{C}).$$

Proposición 4.10. *Sea $\mathcal{C}$ un Código de Reed-Solomon de longitud n y dimensión k. Entonces su radio de recubrimiento es $n-k$.*

Demostración. Sea $f \in \mathbb{F}_q[X]$ un polinomio de grado k y $x = (f(x_1), \ldots, f(x_n)) \in \mathbb{F}_q^n$. Afirmamos que la distancia de x al código es mayor o igual a $n-k$. Supongamos que no.

Existe entonces $c \in \mathcal{C}$ tal que $d(c,x) \leq n-k-1$. Siendo $c(X)$ el polinomio de grado a lo sumo $k-1$ que genera a c, tenemos que $f(X)-c(X)$ tiene grado k y al menos $k+1$ raíces, lo que resulta absurdo. Concluimos que $d(x,\mathcal{C}) \geq n-k$, luego $\rho \geq n-k$.

Veamos que para todo $y \in \mathbb{F}_q^n$ se verifica que $d(y,\mathcal{C}) \leq n-k$. Si y es un elemento del código es claro pues $d(y,\mathcal{C})=0$. Sea entonces $y \notin \mathcal{C}$. Como $\mathcal{C}$ es un subespacio de dimensión k de $\mathbb{F}_q^n$ podemos encontrar un sistema de $n-k$ ecuaciones linealmente independientes que lo definen sobre $\mathbb{F}_q$. Podemos elegir k coordenadas de y, y reemplazando en dicho sistema, encontrar un elemento del código que coincida con y en por lo menos k coordenadas. Entonces obtenemos $\rho \leq n-k$, lo que concluye la demostración. □

Definición 4.11. Sean $\mathcal{C}$ un código de Reed-Solomon y $u \in \mathbb{F}_q^n$ tal que u no es un elemento del código. Decimos que u es un *deep hole* si verifica

$$d(u,\mathcal{C}) = \rho.$$

El siguiente lema nos permite dar una caracterización de los *deep holes* de un código.

Lema 4.12. *Sean $x \in \mathbb{F}_q^n$ y $B(x,\rho) = \{y \in \mathbb{F}_q^n \mid d(y,x) < \rho\}$. Se verifica que x es un deep hole si y solo si $B(x,\rho) \cap \mathcal{C} = \emptyset$.*

Demostración. Si x es un *deep hole* entonces $d(x,\mathcal{C}) = \rho$, luego no puede existir ningún elemento del código en $B(x,\rho)$ y, por lo tanto, $B(x,\rho) \cap \mathcal{C} = \emptyset$.

Recíprocamente, si $B(x,\rho) \cap \mathcal{C} = \emptyset$, entonces $d(x,\mathcal{C}) \geq \rho$. Pero como ρ es el radio de recubrimiento tenemos que $d(x,\mathcal{C}) = \rho$. Es decir, x es un *deep hole*. □

Definición 4.13. Sea $\mathcal{C}_q(\mathcal{D},k)$ un código de Reed-Solomon de longitud n y dimensión k. Si el conjunto evaluación $\mathcal{D}$ es $\mathbb{F}_q^*$ entonces el código recibe el nombre de **código de Reed-Solomon Standard**.

En lo que sigue, trabajaremos con códigos de Reed-Solomon Standard.

4.1.1. Problema de decodificación en Reed-Solomon

Sea $\mathcal{C}$ un código de Reed-Solomon de longitud n y dimensión k y sea $\mathcal{D} = \{x_1, \ldots, x_n\}$ el conjunto evaluación. Supongamos que hemos recibido una palabra $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$. Para decodificar nos interesa encontrar un polinomio de grado menor o igual a $k-1$ que pase por la mayor cantidad posible de los puntos:

$$(x_1, u_1), \ldots, (x_n, u_n).$$

Con ese objetivo construimos el polinomio interpolador de Lagrange para los puntos $(x_1, u_1), \ldots, (x_n, u_n)$ en $\mathbb{F}_q[X]$

$$u(X) = \sum_{i=1}^{n} u_i \frac{\prod_{j \neq i}(X - x_j)}{\prod_{j \neq i}(x_i - x_j)}.$$

Observemos que $u(X)$ es el único polinomio de grado a lo sumo $n-1$ que verifica que $u(x_i) = u_i$ para $1 \leq i \leq n$. Si el grado de $u(X)$ es menor o igual a $k-1$ entonces u es una palabra del código y por lo tanto no es un *deep hole*. Veamos que ocurre en los casos en los que el grado de $u(X)$ es mayor o igual a k.

Proposición 4.14. *Sea $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ una palabra recibida y supongamos que el grado de $u(X)$ es k. Entonces u es un deep hole.*

Demostración. Supongamos que u no es un *deep hole* entonces, por el Lema 4.12 existe $c = (c_1, \ldots, c_n)$ generado por un polinomio $c(X)$ de grado menor o igual a $k-1$ tal que $c \in B(u, \rho)$. Luego $d(u, c) \leq \rho - 1 = n - k - 1$ o sea c y u coinciden en por lo menos $k+1$ coodenadas. Esto último implica que el polinomio $r(x) = u(X) - c(X)$ tiene al menos $k+1$ raíces, lo cual es absurdo porque tiene grado k. Luego u es un *deep hole*. □

Proposición 4.15. *Sea $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ una palabra recibida y supongamos que el grado de $u(X)$ es $k+1$. Entonces u no es un deep hole.*

Demostración. Supongamos que u es un deep hole, entonces $d(u, \mathcal{C}) = n - k$. Luego existe un elemento del código c tal que $d(y, c) = n - k$. Si notamos como $c(X)$ al polinomio que genera a c, obtenemos que $u(X) - c(X)$ es un polinomio de grado $k+1$ con k raíces distintas. Luego como el grado de $u(X) - c(X)$ es $k+1$ entonces $u(X) - c(X)$ posee $k+1$ raíces distintas, pero esto contradice que $d(y, c) = n - k$. Concluimos que los polinomios de grado $k+1$ no generan deep holes. □

Hacemos algunos ejemplos para terminar esta sección.

Ejemplo 4.16. Sea el código $\mathcal{C}_3(\mathbb{F}_3, 1)$ cuya matriz en las bases canónicas es:

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Luego, $\mathcal{C} =< (1,1,1) >$ y el radio de recubrimiento es $\rho = 2$. Por lo tanto, si $u = (a, b, c)$ con todas coodenadas distintas entonces u es un *deep hole*. En efecto, si c es un elemento del código, entonces la distancia de c a u es 2. Si tomamos $u = (a, a, b)$ con $a \neq b$ entonces u no es un *deep hole* ya que $d((a, a, b), \mathcal{C}) = 1$.

Ejemplo 4.17. Sea $\mathcal{C}_5(\mathbb{F}_5^*, 3)$. Consideremos un polinomio de la forma $f(X) = (X-1)(X-2)(X-3)X^d$ con $d \geq 1$ y u una palabra generada por él. El radio de recubrimiento es $\rho = 1$. Afirmamos que $d(u, \mathcal{C}) = 1$. En efecto, la distancia de u al código nulo es 1. Si la distancia de u al código fuese menor a 1 entonces $u \in \mathcal{C}$, lo que implicaría que un polinomio de grado menor o igual a 2 tenga 3 raíces distintas. Por lo tanto $d(u, \mathcal{C}) = 1 = \rho$. Es decir u es *un deep hole*.

4.2. Reducción a una Hipersuperficie

Motivados por la sección anterior vamos a estudiar bajo qué condiciones una palabra recibida, generada por un polinomio de grado mayor a k, es o no un *deep hole*. En particular consideramos el caso en que la palabra recibida u es generada por un polinomio de la forma:

$$f(X) = X^{k+d} + f_{d-1}X^{k+d-1} + \cdots + f_0X^k + t(X) \in \mathbb{F}_q[X],$$

donde $t(X)$ es un polinomio de grado menor o igual a $k-1$ y $k \geq d$. Consideramos las variables $x_1, \ldots, x_{k+1}$ y definimos el siguiente polinomio

$$\Pi = (X - x_1)(X - x_2)\cdots(X - x_{k+1}).$$

Pensamos a Π como un polinomio en la variable X con coeficientes en $\mathbb{F}_q[x_1, \ldots, x_{k+1}]$. Luego si hacemos la división $f(X) : \Pi(X)$ en $\mathbb{F}_q[x_1, \ldots, x_{k+1}][X]$, el resto resulta un polinomio cuyo grado en X es menor o igual a k. Sea $C_{f_0,\ldots,f_{d-1}} \in \mathbb{F}_q[x_1, \ldots, x_{k+1}]$ el coeficiente principal del resto. Nuestro objetivo será estudiar si es posible o no elegir $x_1, \ldots, x_{k+1}$, elementos distintos de $\mathbb{F}_q^*$ de forma tal que $C_{f_0,\ldots,f_{d-1}}$ sea nulo. Si esto ocurre, por el algoritmo de división tendremos:

$$f(X) - r(X) = \Pi(X) \cdot c(X), \tag{4.1}$$

con $\deg r(X)$ menor o igual a $k-1$. Luego, $r(X)$ genera un elemento del código al que denotaremos r. Como el lado derecho de (4.1) se anula en $k+1$ elementos distintos de $\mathbb{F}_q^*$, obtenemos que la distancia entre r y u es menor o igual a $n-k-1$ y por lo tanto u no es un *deep hole*.

Las estimaciones sobre la cantidad de ceros q-racionales de un polinomio absolutamente irreducible serán utilizadas para poder determinar bajo qué condiciones podemos encontrar $x_1, \ldots, x_{k+1}$ de forma tal que el coeficiente principal del resto $C_{f_0,\ldots,f_{d-1}}$ sea nulo. Es por esto que debemos probar que $C_{f_0,\ldots,f_{d-1}}$ es absolutamente irreducible.

4.2.1. Absoluta Irreducibilidad de $C_{f_0,\ldots,f_d}$

Observemos que $\Pi(X)$ se puede escribir en términos de los polinomios simétricos de la siguiente manera:

$$\Pi(X) = X^{k+1} + \Pi_1X^k + \Pi_2X^{k-1} + \cdots + \Pi_{k+1},$$

donde Π_i es el i-ésimo polinomio simétrico en las variables $x_1, \ldots, x_{k+1}$.

El resto de la división $f(X) : \Pi(X)$ es un polinomio en $\mathbb{F}_q[x_1, \ldots, x_{k+1}][X]$ de grado menor o igual a k, su coeficiente principal $C_{f_0,\ldots,f_{d-1}}$ es un polinomio en las variables $x_1, \ldots, x_{k+1}$ de grado total d.

Para probar que $C_{f_0,\ldots,f_{d-1}}$ es absolutamente irreducible vamos a mostrar que su componente homogénea de mayor grado $\chi_{f_0,\ldots,f_{d-1}}$ es absolutamente irreducible. Esto se justifica con el siguiente lema.

Lema 4.18. *Sea $\mathbb{K}$ un cuerpo y $f \in \mathbb{K}[X_1, \ldots, X_n]$. Supongamos que f tiene grado d y*

$f(X) = f_d(X) + \cdots + f_0(X)$, *donde* $f_i(X)$ *es la componente homogénea de grado* i. *Si* $f_d(X)$ *es absolutamente irreducible, entonces* $f(X)$ *también lo es.*

Demostración. Supongamos que f no es absolutamente irreducible. Entonces existen g y $h \in \overline{\mathbb{K}}[X_1, \ldots, X_n]$ no constantes, de grados d_1 y d_2 respectivamente, tales que $f = g \cdot h$. Sean g_{d_1} y h_{d_2} las componentes homogéneas de mayor grado de g y h respectivamente, luego $f_d = g_{d_1} \cdot h_{d_2}$, pero esto es absurdo ya que f_d es absolutamente irreducible. □

Observación 4.19. No vale el recíproco del lema anterior. Por ejemplo $f(X, Y) = X^3 + Y^2$ es absolutamente irreducible (esto se puede obtener, por ejemplo, utilizando el criterio de Stepanov) pero su componente homogénea de mayor grado no.

Debemos probar entonces que $\chi_{f_0,\ldots,f_{d-1}}$ es absolutamente irreducible. Para ello vamos a encontrar una expresión del polinomio $\chi_{f_0,\ldots,f_{d-1}}(x_1, x_2, 1, 0, 0, \ldots, 0)$ y además mostraremos que su grado es d. Luego como los polinomios $\chi_{f_0,\ldots,f_{d-1}}(x_1, x_2, 1, 0, 0, \ldots, 0)$ y $\chi_{f_0,\ldots,f_{d-1}}(x_1, x_2, x_3, \ldots, x_{k+1})$ tienen el mismo grado, la absoluta irreducibilidad del primero implica la absoluta irreducibilidad del último. Concretamente probaremos que $\chi_{f_0,\ldots,f_{d-1}}(x_1, x_2, 1, 0, 0, \ldots, 0)$ es absolutamente irreducible. A continuación encontraremos una expresión para el polinomio $\chi_{f_0,\ldots,f_{d-1}}(x_1, x_2, 1, 0, 0, \ldots, 0)$.

Observación 4.20. Notemos que se verifica que $\chi_{f_0,\ldots,f_{d-1}}$ coincide con el coeficiente principal del resto de la división $X^{k+d} : \Pi$. En particular esto nos permite independizarnos de los coeficientes $f_0, \ldots, f_{d-1}$, por lo que podemos notar al coeficiente principal del resto como C y su componente homogénea de grado d como χ_d.

Lema 4.21. *Se verifica que* $\chi_d(x_1, x_2, 1, 0, 0, \ldots, 0) = \sum_{i+j \leq d} x_1^i x_2^j$.

Demostración. Por la Observación 4.20 anterior necesitamos calcular el coeficiente principal del resto de la división: $X^{k+d} : (X - x_1)(X - x_2)(X - 1)x^{k-2}$. Esto es equivalente al calcular el coeficiente principal del resto de la división: $X^{d+2} : (X - x_1)(X - x_2)(X - 1)$. Dicho resto $m(X)$ es un polinomio de grado 2 en la variable x que verifica: $m(x_1) = x_1^{d+2}$, $m(x_2) = x_2^{d+2}$ y $m(1) = 1$. Obtenemos el siguiente sistema de ecuaciones:

$$\begin{cases} ax_1^2 + bx_1 + c = x_1^{d+2} \\ ax_2^2 + bx_2 + c = x_2^{d+2} \\ a + b + c = 1 \end{cases}$$

Sustituimos en las dos primeras ecuaciones $c = 1 - b - a$ y obtenemos

$$a(x_1^2 - 1) + b(x_1 - 1) = x_1^{d+2} - 1$$

$$a(x_2^2 - 1) + b(x_2 - 1) = x_2^{d+2} - 1,$$

despejando a se tiene

$$(x_1^{d+1} + \cdots + 1) - (x_2^{d+1} + \cdots + 1) = a(x_1 - x_2),$$

finalmente se obtiene

$$a = \frac{x_2^{d+1} - x_1^{d+1}}{x_2 - x_1} + \frac{x_2^d - x_1^d}{x_2 - x_1} + \cdots + \frac{x_2 - x_1}{x_2 - x_1}$$

Por lo tanto,

$$a = (x_2^d + x_2^{d-1}x_1 + \cdots + x_1^d) + (x_2^{d-1} + x_2^{d-2}x_1 + \cdots + x_1^{d-1}) + \cdots + x_2 + x_1 + 1.$$

□

Finalizamos esta sección probando que el polinomio $\chi_d(x_1, x_2, 1, 0, 0, \ldots, 0)$ es absolutamente irreducible. En realidad vamos a demostrar un resultado más fuerte que es que la curva $C \subset \mathbb{P}^2$ (el espacio proyectivo de dimensión 2), definida por la homogeneización del polinomio

$$f(X, Y) = \sum_{i+j \leq d} X^i Y^j$$

no tiene puntos singulares. En el espacio proyectivo las componentes irreducibles de una hipersuperficie tienen intersección no vacía, de hecho dicha intersección está contenida en la variedad de puntos singulares de la misma. Por lo tanto una manera de probar que el polinomio es absolutamente irreducible es viendo que la curva que este define no posee puntos singulares.

Lema 4.22. *Sea p un número primo mayor a 2 y d un entero positivo tal que $d + 2 < p$. El polinomio $f(X, Y) = \sum_{i+j \leq d} X^i Y^j$ es absolutamente irreducible.*

Demostración. Tenemos que ver entonces que el sistema

$$\begin{cases} f(X,Y) &= 0 \\ \frac{\partial f}{\partial X} &= 0 \\ \frac{\partial f}{\partial Y} &= 0 \end{cases}$$

no tiene solución. Observemos que $f(X, Y)$ se puede escribir como

$$f(X, Y) = X^d + (Y + 1)X^{d-1} + (Y^2 + Y + 1)X^{d-2} + \cdots + Y^d + Y^{d-1} + \cdots + 1,$$

o equivalentemente

$$f(X, Y) = Y^d + (X + 1)Y^{d-1} + (X^2 + X + 1)Y^{d-2} + \cdots + X^d + X^{d-1} + \cdots + 1.$$

Luego las derivadas son:

$$\frac{\partial f}{\partial X} = dX^{d-1} + (d-1)(Y+1)X^{d-2} + (d-2)(Y^2 + Y + 1)X^{d-3} + \cdots + Y^{d-1} + \cdots + 1,$$

$$\frac{\partial f}{\partial Y} = dY^{d-1} + (d-1)(X+1)Y^{d-2} + (d-2)(X^2+X+1)Y^{d-3} + \cdots + X^{d-1} + \cdots + 1.$$

Supongamos que existe una solución (x, y) del sistema. En primer lugar vamos a probar que necesariamente debe ser $x = y$. Con este objetivo, hallamos las siguientes expresiones:

$$(X-Y)f(X,Y) \quad \text{y} \quad f(X,Y) + (X-Y)\tfrac{\partial f}{\partial X}.$$

Es sencillo ver que

$$(X-Y)f(X,Y) = X^{d+1} + X^d + \cdots + X - Y^{d+1} - Y^d - \cdots - Y. \tag{4.2}$$

Si reemplazamos en (4.2) $X = x$ e $Y = y$, como (x, y) es solución del sistema se tiene la siguiente igualdad

$$x^{d+1} + x^d + \cdots + x = y^{d+1} + y^d + \cdots + y. \tag{4.3}$$

Trabajamos ahora con $f(X,Y) + (X-Y)\frac{\partial f}{\partial X}$. De las identidades

$$X\frac{\partial f}{\partial X} = dX^d + (d-1)(Y+1)X^{d-1} + \cdots + X(Y^{d-1} + \cdots + 1)$$

y

$$Y\frac{\partial f}{\partial X} = dX^{d-1}Y + (d-1)(Y^2+Y)X^{d-2} + \cdots + Y^d + \cdots + Y,$$

obtenemos

$$f(X,Y) + (X-Y)\frac{\partial f}{\partial X} = (d+1)X^d + dX^{d-1} + \cdots + 1.$$

Reemplazando en la expresión anterior $X = x$ e $Y = y$, se verifica entonces

$$0 = (d+1)x^d + dx^{d-1} + \cdots + 1. \tag{4.4}$$

Si multiplicamos (4.4) por x y a este resultado le restamos (4.4) obtenemos

$$(d+1)x^{d+1} = x^d + x^{d-1} + \cdots + 1. \tag{4.5}$$

Haciendo el mismo procedimiento con $\frac{\partial f}{\partial Y}$ concluimos que vale la siguiente igualdad

$$(d+1)y^{d+1} = y^d + y^{d-1} + \cdots + 1. \tag{4.6}$$

En particular de (4.5) y (4.6) se deduce que x e y son no nulos. Por otra parte por (4.3), (4.5) y (4.6) se verifica

$$(d+2)x^{d+1} = (d+2)y^{d+1},$$

y como p no divide a $(d+2)$ obtenemos

$$x^{d+1} = y^{d+1}. \tag{4.7}$$

Por otro lado si multiplicamos (4.5) por x, (4.6) por y, y utilizamos (4.4) concluimos que

$(d+1)x^{d+2} = (d+1)y^{d+2}$, nuevamente como p no divide a $(d+1)$ se tiene

$$x^{d+2} = y^{d+2}. \tag{4.8}$$

Luego por (4.7) y (4.8) se tiene que $x = y$. Reescribimos $f(x,y)$ y $\frac{\partial f}{\partial X}(x,y)$ teniendo en cuenta que $x = y$, esto da lugar a las siguientes identidades

$$(d+1)x^d + dx^{d-1} + \cdots + 1 = 0, \tag{4.9}$$

$$(d + (d-1) + \cdots + 1)x^{d-1} + ((d-1) + \cdots + 1)x^{d-2} + \cdots + 1 = 0. \tag{4.10}$$

Si restamos de (4.9) la identidad (4.10), se tiene

$$(d+1)x^d - ((d-1) + \cdots + 1)x^{d-1} - \cdots - x = 0$$

Sacando factor común x y utilizando el hecho que $x \neq 0$ obtenemos

$$(d+1)x^{d-1} - ((d-1) + \cdots + 1)x^{d-2} - \cdots - 1 = 0$$

Reemplazamos por (4.10) en esta última igualdad para finalmente obtener

$$\begin{gathered}(d+1)x^{d-1} + (d + (d-1) + \cdots + 1)x^{d-1} = 0 \\ ((d+1) + d + \cdots + 1)x^{d-1} = 0 \\ \frac{1}{2}(d+1)(d+2)x^{d-1} = 0 \end{gathered} \tag{4.11}$$

Como p no divide a $(d+1)$ ni a $(d+2)$ entonces la igualdad (4.11) implica que $x = 0$ y luego $y = 0$, pero $(0,0)$ no puede ser solución del sistema ya en particular no verifica la ecuación $f(X,Y) = 0$. Hemos visto entonces que la curva no posee puntos singulares afines. Para finalizar la demostración debemos probar que no tiene puntos singulares en el infinito. Para ello mostraremos que si el polinomio $F(X,Y,Z)$ es la homogeneización de $f(X,Y)$, entonces el sistema

$$\begin{cases} F(X,Y,Z) &= 0 \\ \frac{\partial F}{\partial X} &= 0 \\ \frac{\partial F}{\partial Y} &= 0 \\ \frac{\partial F}{\partial Z} &= 0 \end{cases} \tag{4.12}$$

tiene única solución igual a (0,0,0). Sea $(x : y : 0)$ un punto infinito que es solución del sistema (4.12). De las condiciones $F(X,Y,Z) = 0$ y $\frac{\partial F}{\partial Z} = 0$ se obtienen las siguientes ecuaciones:

$$X^d + YX^{d-1} + Y^2X^{d-2} + \cdots + Y^{d-1}X + Y^d = 0, \tag{4.13}$$

y

$$X^{d-1} + YX^{d-2} + Y^2X^{d-2} + \cdots + Y^{d-2}X + Y^{d-1} = 0. \tag{4.14}$$

De (4.13) y (4.14) deducimos que $X^d = 0$, con lo cual $X = 0$. Por otro lado si reemplazamos en $\frac{\partial F}{\partial X} = 0$, $X = 0$ y $Z = 0$ concluimos que $Y = 0$ y por lo tanto la única solución del sistema es $(0, 0, 0)$. □

Observación 4.23. Notemos que en el Lema anterior se impuso una condición sobre la característica del cuerpo. Mostraremos con un ejemplo que dicha restricción es esencial. Consideremos el caso $d = 3$ y $p = 5$. Luego estamos en la situación $p-2 = d$. El polinomio en cuestión es $f(X, Y) = X^3+(Y+1)X^2+(Y^2+Y+1)X+Y^3+Y^2+Y+1$. Este polinomio no es absolutamente irreducible en $\mathbb{F}_5[X, Y]$ pues admite la siguiente factorización:

$$f(X, Y) = (X + 2Y + 2) \cdot (X + 3Y + 1) \cdot (X + Y + 3).$$

4.3. Aplicación de las estimaciones al problema de códigos

Consideramos nuevamente $C \in \mathbb{F}_q[X_1, \ldots, X_{k+1}]$ el coeficiente principal del resto de la división $f : \Pi$. En la sección anterior mostramos que C es absolutamente irreducible si $d < p - 2$. Luego por el Teorema 3.22, si notamos como N a la cantidad de ceros q-racionales de C, deducimos la siguiente cota inferior:

$$N \geq q^k - (d-1)(d-2)q^{k-\frac{1}{2}} - 6d^3q^{k-1}.$$

Recordemos que esta cota es válida bajo la condición de que la característica sea mayor a $d(d-1)+1$. En lo que sigue trabajaremos bajo esta hipótesis. Para nuestro problema de códigos además de estar interesados en encontrar ceros q-racionales de C tales que sus coordenadas distintas entre sí y no nulas. Es decir buscamos soluciones en $\mathbb{F}_q^{k+1}$ de la ecuación $C(x_1, \ldots, x_{k+1}) = 0$ que no sean soluciones de

$$\prod_{i=1}^{k+1} X_i \prod_{i \neq j} (X_i - X_j) = 0.$$

Vamos a dar entonces una cota superior para el número de soluciones del sistema

$$\begin{cases} C(x_1, \ldots, x_{k+1}) & = & 0 \\ \\ \displaystyle\prod_{i=1}^{k+1} X_i \prod_{i \neq j} (X_i - X_j) & = & 0 \end{cases} \tag{4.15}$$

Proposición 4.24. *El sistema (4.15) tiene a lo sumo* $\frac{d}{2}(k^2 + 3k + 2)q^{k-1}$ *soluciones en* $\mathbb{F}_q^{k+1}$.

Demostración. Se obtiene de la Proposición 3.8. □

Por lo tanto la cantidad de puntos q-racionales con todas sus coordenadas distintas y no nulas que anulan a C, es mayor o igual a:

$$q^k - (d-2)(d-1)q^{k-\frac{1}{2}} - 6d^3q^{k-1} - \frac{d}{2}(k^2+3k+2)q^{k-1}.$$

Si consideramos $d < q^{\frac{1}{4}}$ y $k < q^{\frac{1}{4}}$, este número resulta positivo y luego podemos garantizar soluciones q-racionales de la ecuación $C(x_1, \ldots, x_{k+1}) = 0$ con coordenadas no nulas y distintas entre sí, lo que implica que la palabra generada por el polinomio $f(X)$ no sea un *deep hole*. En conclusión hemos probado el siguiente teorema.

Teorema 4.25. *Sea $\mathbb{F}_q$ un cuerpo de característica $p > d(d-1)+1$, $\mathcal{C} = \mathcal{C}(\mathbb{F}_q^*, k)$ un código de Reed-Solomon Standard de longitud n y dimensión k y $u \in \mathbb{F}_q^n$ una palabra recibida, generada por un polinomio de grado $k+d$. Si se verifica que $d < q^{\frac{1}{4}}$ y $k < q^{\frac{1}{4}}$ entonces u no es un* deep hole*.*

Observación 4.26. Sea $\mathbb{F}_q$ un cuerpo de característica $p > d(d-1)+1$, $\mathcal{C} = \mathcal{C}(\mathbb{F}_q^*, k)$ un código de Reed-Solomon Standard de longitud n y dimensión $k < q^{\frac{1}{4}}$. De manera sencilla probábamos que las palabras generadas por polinomios de grado k son *deep holes*, y las generadas por polinomios de grado $k+1$ no. A partir del teorema anterior obtenemos que todas las palabras generadas por polinomios de grado $k+d$ con $d < q^{\frac{1}{4}}$ tampoco pueden ser *deep holes*.

Observación 4.27. En [CM07] obtienen las condiciones $d < q^{\frac{3}{13}-\epsilon}$ y $k < q^{\frac{1}{4}-\epsilon}$. Dichas condiciones se han podido mejorar gracias a la utilización de una cota más fina para la cantidad de ceros q-racionales de un polinomio absolutamente irreducible, y a una mejor estimación sobre la cantidad de soluciones del sistema (4.15).

Bibliografía

[AGS+04] A.Bostan, G.Lecerf, B. Salvy, É.Schost, and B.Wiebelt. Complexity inssues in bivariate polynomial factorization. In J.R. Sendra, editor, *ISSAC 2004*, pages 42–49, New York, 2004. ACM Press.

[BHKS04] K. Belabas, M. Van Hoeij, J. Klüeners, and A. Steel. Factoring polynomials over finite fields. 2004.

[CLO98] D. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*, volume 185 of *Grad. Texts in Math.* Springer, New York, 1998.

[CM06] A. Cafure and G. Matera. Improved explicit estimates on the number of solutions of equations over a finite field. *Finite Fields Appl.*, 12(2):155–185, 2006.

[CM07] Qi Cheng and Elizabeth Murray. On deciding deep holes of reed-solomon codes. In *TAMC*, pages 296–305, 2007.

[Ful69] W. Fulton. *Algebraic curves*. W.A. Benjamin Inc., New York Amsterdam, 1969.

[Gao03] S. Gao. Factoring multivariate polynomials via partial differential equations. *Math. Comp.*, 72:801–822, 2003.

[Gar95] A. García. Pontos racionais em curvas sobre corpos finitos. IMPA, 1995.

[GCL92] K. Geddes, S. Czapor, and G. Labahn. *Algorithms for computer algebra*. Kluwer Acad. Publ., Dordrecht, 1992.

[Hei83] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comput. Sci.*, 24(3):239–277, 1983.

[HP04] J.F. Humphreys and M.Y. Prest. *Numbers, Groups and Codes*, volume 2. Cambridge, 2004.

[HS82] J. Heintz and C. P. Schnorr. Testing polynomials which are easy to compute. In *International Symposium on Logic and Algorithmic, Zurich 1980*, volume 30 of *Monogr. Enseig. Math.*, pages 237–254, 1982.

[Kal91] E. Kaltofen. Effective Noether irreducibility forms and applications. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing (New Orleans, Louisiana, May 6-8, 1991)*, pages 54–63, New York, 1991. ACM Press.

[Kun85] E. Kunz. *Introduction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, Boston, 1985.

[Lec06] G. Lecerf. Sharp precision in Hensel lifting for bivariate polynomial factorization. *Math. Comp.*, 75(254):921–933, 2006.

[Lec07] G. Lecerf. Improved dense multivariate polynomial factorization algorithms. *J. Symbolic Comput.*, 42:477–494, 2007.

[LN83] R. Lidl and H. Niederreiter. *Finite fields.* Addison–Wesley, Reading, Massachusetts, 1983.

[Mig92] M. Mignotte. *Mathematics for Computer Algebra.* Springer, Berlin Heidelberg New York, 1992.

[Mus75] D.R. Musser. Multivariate polynomial factorization. *J. ACM*, 22(2):291–308, 1975.

[Pre92] O. Pretzel. *Error-Correcting Codes and Finite Fields.* Clarendon Press, Oxford, 1992.

[Rup86] W. M. Ruppert. Reduzibilität ebener kurven. *J. Reine Angew. Math.*, (369):167–191, 1986.

[Rup99] W. M. Ruppert. Reducibility of polynomials $f(x, y)$ modulo p. *J. Number Theory*, 77(1):62–70, 1999.

[Sch74] W. Schmidt. A lower bound for the number of solutions of equations over finite fields. *J. Number Theory*, 6(6):448–480, 1974.

[Sch76] W. Schmidt. *Equations over Finite Fields. An Elementary Approach.* Number 536 in Lectures Notes in Math. Springer, New York, 1976.

[vzGG99] J. von zur Gathen and J. Gerhard. *Modern computer algebra.* Cambridge Univ. Press, Cambridge, 1999.

[Wan78] P.S. Wang. An improved multivariate polynomial factorization algorithm. *Math. Comp.*, 32:1215–1231, 1978.

[Wei48] A. Weil. *Sur les courbes algébriques et les varietés qui s'en déduisent.* Hermann, Paris, 1948.

[WP03] W.Huffman and V. Pless. *Fundamentals of Error-Correcting Codes.* Cambridge University Press, 2003.

[WR75] P.S. Wang and L.P. Rothschild. Factoring multivariate polynomials over the integers. *Math. Comp.*, 29:935–950, 1975.

[Zas69] H. Zassenhaus. On Hensel factorization I. *J. Number Theory*, 1:291–311, 1969.